UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
15/297,328	10/19/2016	SIVAKUMAR CHATURVEDI	DAMA-33216

CONFIRMATION NO. 6761

25883
HOWISON & ARNOTT, L.L.P
P.O. BOX 741715
DALLAS, TX 75374-1715

PUBLICATION NOTICE

OC000000089105825

Title:SYSTEM AND METHOD FOR PROVIDING ADDITIONAL FUNCTIONALITY TO EXISTING SOFTWARE IN AN INTEGRATED MANNER

Publication No.US-2017-0041382-A1
Publication Date:02/09/2017

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 (571) 272-3150 or (800) 972-6382, by facsimile at (571) 273-3250, 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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/297,328	02/21/2017	9578092	DAMA-33216	6761

25883 7590 02/01/2017

HOWISON & ARNOTT, L.L.P
P.O. BOX 741715
DALLAS, TX 75374-1715

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 0 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):

SIVAKUMAR CHATURVEDI, ALLEN, TX;
DAMAKA, INC., RICHARDSON, TX;
SATISH GUNDABATHULA, IRVING, TX;
RASHMI HIREMATH, ALLEN, TX;

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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.C.D/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	2194
	Examiner Name	Craig Dorais
	Attorney Docket Number	DAMA-33216

	216	20110307556	A1	2011-12-15	CHATURVEDI ET AL	
Change(s) applied to document, /C.C.B./ 1/11/2017	217	20130106989	A1	2013-05-02	~~TELIRIS, INC.~~ Gage et al.	
	218	20080244718	A1	2008-10-02	FROST ET AL	
	219	20120124191	A1	2012-05-17	LYON	
	220	20040193599	A1	2004-09-30	LIU ET AL.	
	221	20100058353	A1	2010-03-04	TURSKI	
	222	20130125145	A1	2013-05-16	BALMORI LABRA ET AL.	
	223	20150026700	A1	2015-01-22	CHATURVEDI ET AL.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
/C.C.D/	1	1848163	EP	A1	2007-10-24	SHARP KABUSHIKI KAISHA		

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.C.D/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	2194
	Examiner Name	Craig Dorais
	Attorney Docket Number	DAMA-33216

	172	20030135569		2003-07-17	KHAKOO ET AL.	
	173	20030158722	A1	2003-08-01	LORD, JOHN RAYMOND	
	174	20030177186	A1	2003-09-01	GOODMAN ET AL.	
	175	20030187650	A1	2003-10-01	MOORE ET AL.	
Change(s) applied to document, /C.C.B./ 1/11/2017	176	20040034776	A1	~~2003-10-01~~ 02/2004	FERNANDO ET AL.	
	177	20040039781	A1	2004-02-01	LAVALLEE ET AL.	
	178	20040044517	A1	2004-03-01	PALMQUIST, ROBERT	
	179	20040128554	A1	2004-07-01	MAHER, III, ET AL.	
	180	20040133689	A1	2004-07-08	VASISHT, SAMRAT	
	181	20040139228		2004-07-15	TAKEDA ET AL.	
	182	20040143678	A1	2004-07-01	CHARI ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.C.D/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	2194
	Examiner Name	Craig Dorais
	Attorney Docket Number	DAMA-33216

	53	7613171	B2	2009-11-00	ZEHAVI ET AL.	
	54	6842460	B1	2005-01-00	OLKKONEN ET AL.	
	55	6987756		2006-01-00	RAVINDRANATH ET AL.	
	56	7512652		2009-03-00	APPELMAN ET AL.	
	57	5761309	A	1998-06-01	OHASHI ET AL.	
	58	6141687	A	2000-10-01	BLAIR, DANA L.	
	59	6202084	B1	2001-03-13	KUMAR ET AL.	
	60	6219638	B1	2001-04-01	PADMANABHAN ET AL.	
	61	6360196	B1	2002-03-01	POZNASKI ET AL.	
Change(s) applied to document, /C.C.B./ 1/11/2017	62	6826613	B1	~~2002-03-01~~ 11/2004	WANG ET AL.	
	63	7013155	B1	2006-03-01	RUF ET AL.	

EFS Web 2.1.17

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)

25883 7590 01/03/2017
HOWISON & ARNOTT, L.L.P
P.O. BOX 741715
DALLAS, TX 75374-1715

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.
15/297,328	10/19/2016	SIVAKUMAR CHATURVEDI	DAMA-33216	6761

TITLE OF INVENTION: SYSTEM AND METHOD FOR PROVIDING ADDITIONAL FUNCTIONALITY TO EXISTING SOFTWARE IN AN INTEGRATED MANNER

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	04/03/2017

EXAMINER	ART UNIT	CLASS-SUBCLASS
DORAIS, CRAIG C	2194	719-313000

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 Howison & Arnott, L.L.P.
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: DAMAKA, INC.

(B) RESIDENCE: (CITY and STATE OR COUNTRY): RICHARDSON, TEXAS

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 credits any overpayment, to Deposit Account Number 200780 (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
- ☐ Applicant certifying micro entity status. See 37 CFR 1.29 — NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
- ☐ Applicant asserting small entity status. See 37 CFR 1.27 — NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
- ☐ Applicant changing to regular undiscounted fee status. — NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

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

Authorized Signature /Keith D. Harden, Reg. #74472/ Date January 6, 2017

Typed or printed name Keith D. Harden Registration No. 74472

PTOL-85 Part B (10-13) Approved for use through 10/31/2013. OMB 0651-0033 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Electronic Patent Application Fee Transmittal

Application Number:	15297328
Filing Date:	19-Oct-2016
Title of Invention:	SYSTEM AND METHOD FOR PROVIDING ADDITIONAL FUNCTIONALITY TO EXISTING SOFTWARE IN AN INTEGRATED MANNER
First Named Inventor/Applicant Name:	SIVAKUMAR CHATURVEDI
Filer:	Keith D. Harden
Attorney Docket Number:	DAMA-33216

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

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	480	480

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**480**

Electronic Acknowledgement Receipt

EFS ID:	28001159
Application Number:	15297328
International Application Number:	
Confirmation Number:	6761
Title of Invention:	SYSTEM AND METHOD FOR PROVIDING ADDITIONAL FUNCTIONALITY TO EXISTING SOFTWARE IN AN INTEGRATED MANNER
First Named Inventor/Applicant Name:	SIVAKUMAR CHATURVEDI
Customer Number:	25883
Filer:	Keith D. Harden
Filer Authorized By:	
Attorney Docket Number:	DAMA-33216
Receipt Date:	06-JAN-2017
Filing Date:	19-OCT-2016
Time Stamp:	21:10:43
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$480
RAM confirmation Number	010917INTEFSW00006620200780
Deposit Account	200780
Authorized User	Keith Harden

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

37 CFR 1.17 (Patent application and reexamination processing fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	DAM33216IssueFeeTransmittal.pdf	1600087 4efa3456f50a3fe6151e11c1e753b6467a227c93	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30510 1f375128cf7cbac7cbc634aa8d6f6e2cac6f9f2c	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1630597		

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.

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

25883 7590 01/03/2017

HOWISON & ARNOTT, L.L.P
P.O. BOX 741715
DALLAS, TX 75374-1715

EXAMINER	
DORAIS, CRAIG C	
ART UNIT	PAPER NUMBER
2194	

DATE MAILED: 01/03/2017

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/297,328	10/19/2016	SIVAKUMAR CHATURVEDI	DAMA-33216	6761

TITLE OF INVENTION: SYSTEM AND METHOD FOR PROVIDING ADDITIONAL FUNCTIONALITY TO EXISTING SOFTWARE IN AN INTEGRATED MANNER

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	04/03/2017

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

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

HOW TO REPLY TO THIS NOTICE:

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

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

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

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

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

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

IMPORTANT REMINDER: 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)

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)

25883 7590 01/03/2017
HOWISON & ARNOTT, L.L.P
P.O. BOX 741715
DALLAS, TX 75374-1715

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.
15/297,328	10/19/2016	SIVAKUMAR CHATURVEDI	DAMA-33216	6761

TITLE OF INVENTION: SYSTEM AND METHOD FOR PROVIDING ADDITIONAL FUNCTIONALITY TO EXISTING SOFTWARE IN AN INTEGRATED MANNER

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	04/03/2017

EXAMINER	ART UNIT	CLASS-SUBCLASS
DORAIS, CRAIG C	2194	719-313000

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 _____
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 credits any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

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

❑ Applicant certifying micro entity status. See 37 CFR 1.29

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

❑ Applicant asserting small entity status. See 37 CFR 1.27

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

❑ Applicant changing to regular undiscounted fee status.

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

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

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

PTOL-85 Part B (10-13) Approved for use through 10/31/2013. OMB 0651-0033 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/297,328	10/19/2016	SIVAKUMAR CHATURVEDI	DAMA-33216	6761

25883 7590 01/03/2017

HOWISON & ARNOTT, L.L.P
P.O. BOX 741715
DALLAS, TX 75374-1715

EXAMINER	
DORAIS, CRAIG C	
ART UNIT	PAPER NUMBER
2194	

DATE MAILED: 01/03/2017

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

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

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

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

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

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

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 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.

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.

Examiner-Initiated Interview Summary	Application No.	Applicant(s)	
	15/297,328	CHATURVEDI ET AL.	
	Examiner	Art Unit	
	CRAIG DORAIS	2194	

All participants (applicant, applicant's representative, PTO personnel):

(1) *CRAIG DORAIS*. (3)_____.

(2) *KEITH HARDEN*. (4)_____.

Date of Interview: *12/21/2016*.

Type: ☒ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☒ No.
If Yes, brief description: _____.

Issues Discussed ☐101 ☐112 ☐102 ☒103 ☐Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *none*.

Identification of prior art discussed: *none*.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Discussed the filing of a terminal disclaimer to place the application in a condition for allowance. Applicant's representative filed said terminal disclaimer on 12/21/2016.

Applicant recordation instructions: It is not necessary for applicant to provide a separate record of the substance of interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/CRAIG DORAIS/ Primary Examiner, Art Unit 2194	

Notice of Allowability	Application No. 15/297,328	Applicant(s) CHATURVEDI ET AL.	
	Examiner CRAIG DORAIS	Art Unit 2194	AIA (First Inventor to File) Status Yes

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

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

1. ☒ This communication is responsive to *Application filed on 10/19/2016*.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on_____.
2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are *1 - 30*. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some *c) ☐ None of the:
   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

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

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date See Continuation Sheet
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. ☒ Interview Summary (PTO-413), Paper No./Mail Date *20161222* .
5. ☐ Examiner's Amendment/Comment
6. ☒ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/CRAIG DORAIS/
Primary Examiner, Art Unit 2194

Continuation of Attachment(s) 2. Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date: 10/25/2016, 10/25/2016.

DETAILED ACTION

1. The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

2. This Office Action is in response to an filed on 10/19/2016.

3. Claims 1 – 30 are allowed.

Reasons for Allowance

4. The following is an examiner's statement of reasons for allowance: Independent claim 1 (and similarly, independent claims 7, 12 and 22), when considered as a whole, is allowable over the prior art of record. Specifically, the prior art of record fails to clearly teach or fairly suggest the combination of the following limitations, as recited in independent claim 1 (and similarly recited in independent claims 7, 12 and 22):

> establish the A/V service between the superblock application and the resource via the network interface, wherein establishing is not otherwise supported by the superblock application;
>
> provide video output for the A/V service to a video window within a display window associated with the superblock application, the video window displayable simultaneously with the display window of the superblock application; and provide audio for the A/V service.

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to CRAIG DORAIS whose telephone number is (571)270-3371. The examiner can normally be reached on Monday - Friday 8:30am - 5:00pm.

6. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Hyung Sough can be reached on (571)272-6799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

7. 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.

/CRAIG DORAIS/
Primary Examiner, Art Unit 2194

Examiner-Initiated Interview Summary	Application No.	Applicant(s)	
	15/297,328	CHATURVEDI ET AL.	
	Examiner	Art Unit	
	CRAIG DORAIS	2194	

All participants (applicant, applicant's representative, PTO personnel):

(1) *CRAIG DORAIS*. (3)_____.

(2) *KEITH HARDEN*. (4)_____.

Date of Interview: *12/21/2016*.

Type: ☒ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☒ No.
If Yes, brief description: _____.

Issues Discussed ☐101 ☐112 ☐102 ☒103 ☐Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *none*.

Identification of prior art discussed: *none*.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Discussed the filing of a terminal disclaimer to place the application in a condition for allowance. Applicant's representative filed said terminal disclaimer on 12/21/2016.

Applicant recordation instructions: It is not necessary for applicant to provide a separate record of the substance of interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/CRAIG DORAIS/ Primary Examiner, Art Unit 2194	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.C.D/

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
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 contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15297328
Filing Date	2016-10-19
First Named Inventor	CHATURVEDI, Sivakumar
Art Unit	2194
Examiner Name	Craig Dorais
Attorney Docket Number	DAMA-33216

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.C.D/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	2194
	Examiner Name	Craig Dorais
	Attorney Docket Number	DAMA-33216

/C.C.D/	1	International Search Report and Written Opinion of the International Searching Authority from PCT/US2006/040312, dated March 2, 2007.	
/C.C.D/	2	International Search Report and Written Opinion of the International Searching Authority from PCT/US2006/047841, dated September 12, 2008.	
/C.C.D/	3	International Search Report and Written Opinion of the International Searching Authority from PCT/US2007/002424, dated August 14, 2007.	
/C.C.D/	4	International Search Report and Written Opinion of the International Searching Authority from PCT/US2007/068820, dated June 11, 2008.	
/C.C.D/	5	International Search Report and Written Opinion of the International Searching Authority from PCT/US2007/068821, dated June 14, 2008.	
/C.C.D/	6	International Search Report and Written Opinion of the International Searching Authority from PCT/US2007068823, dated June 1, 2008.	
/C.C.D/	7	JEFF TYSON, "How Instant Messaging Works", www.verizon.com/learningcenter, March 9, 2005.	
/C.C.D/	8	RORY BLAND, et al,"P2P Routing" 03/2002.	
/C.C.D/	9	ROSENBERG, "STUN- Simple Traversal of UDP Through NAT", September 2002, XP015005058.	
/C.C.D/	10	SALMAN A. BASET, et al, "An Analysis Of The Skype Peer-To-Peer Internet Telephony Protocol", Department of Computer Science, Columbia University, New York, NY, USA, September 15, 2004.	
/C.C.D/	11	SINGH et al., "Peer-to Peer Internet Telephony Using SIP", Department of Computer Science, Columbia University, October 31, 2004, XP-002336408.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.C.D/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	2194
	Examiner Name	
	Attorney Docket Number	DAMA-33216

/C.C.D/	12	SINHA, S. and OGLIESKI, A., A TCP Tutorial, November 1998 (Date posted on Internet: 19 April 2001) [Retrieved from the Internet <URL:http//www.ssfnet.org/Exchange/tcp/tcpTutorialNotes.html>]	
/C.C.D/	13	Pejman Khadivi, Terence D. Todd and Dongmei Zhao, "Handoff trigger nodes for hybrid IEEE 802.11 WLAN/cellular networks," Proc. Of IEEE International Conference on Quality of Service in Heterogeneous Wired/Wireless Networks, pp. 164-170, 18 October 2004.	
/C.C.D/	14	International Search Report and Written Opinion of the International Searching Authority from PCT/US2008/078142, dated March 27, 2009.	
/C.C.D/	15	International Search Report and Written Opinion of the International Searching Authority from PCT/US2008/084950, dated April 27, 2009.	
/C.C.D/	16	Hao Wang, Skype VoIP service-architecture and comparison, In: INFOTECH Seminar Advanced Communication Services (ASC), 2005, pp. 4, 7, 8.	
/C.C.D/	17	Seta, N.; Miyajima, H.; Zhang, L;; Fujii, T., "All-SIP Mobility: Session Continuity on Handover in Heterogeneous Access Environment," Vehicular Technology Conference, 2007. VTC 2007-Spring. IEEE 65th, 22-25 April 2007, pages: 1121-1126.	
/C.C.D/	18	International Search Report and Written Opinion of the International Searching Authority from PCT/US2008/075141, dated March 5, 2009.	
/C.C.D/	19	Qian Zhang; Chuanxiong Guo; Zihua Guo; Wenwu Zhu, "Efficient mobility management for vertical handoff between WWAN and WLAN," Communications Magazine, IEEE, vol. 41. issue 11, November 2003, pages: 102-108.	
/C.C.D/	20	ISAACS, Ellen et al., "Hubbub: A sound-enhanced mobile instant messenger that supports awareness and opportunistic interactions," Proceedings of the SIGCHI Conference On Human Factors in Computing Systems; Vol. 4, Issue No. 1; Minneapolis, Minnesota; 20-25 April 2002; pgs. 179-186.	
/C.C.D/	21	PCT: International Preliminary Report on Patentability of PCT/US2008/084950; 01 June 2010; 5 pgs.	
/C.C.D/	22	International Search Report and Written Opinion of the International Searching Authority from PCT/US2014/039777, dated September 30, 2014.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.C.D/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	2194
	Examiner Name	Craig Dorais
	Attorney Docket Number	DAMA-33216

/C.C.D/	23	International Search Report and Written Opinion of the International Searching Authority from PCT/US2014/39782, dated October 17, 2014.	
/C.C.D/	24	International Search Report and Written Opinion of PCT/US2015/43633, 2015 October 26, 21 pgs.	
/C.C.D/	25	PCT: International Search Report and Written Opinion of PCT/US2015/43630 (related application), 2015 October 30, 20 pgs.	
/C.C.D/	26	PCT: International Preliminary Report on Patentability of PCT/US2014/039777; 28 January 2016; 8 pgs.	
/C.C.D/	27	PCT: International Preliminary Report on Patentability of PCT/US14/39782; 19 April 2016; 9 pgs.	

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/CRAIG C DORAIS/	Date Considered	12/20/2016

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

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	
	Examiner Name	
	Attorney Docket Number	DAMA-33216

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Keith D. Harden, Reg. #74472/	Date (YYYY-MM-DD)	2016-10-25
Name/Print	Keith D. Harden	Registration Number	74472

This collection of information is required by 37 CFR 1.97 and 1.98. 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 1 hour 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.**

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.C.D/

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
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 contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15297328
Filing Date	2016-10-19
First Named Inventor	CHATURVEDI, Sivakumar
Art Unit	2194
Examiner Name	Craig Dorais
Attorney Docket Number	DAMA-33216

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	7778187	B2	2010-08-00	CHATURVEDI ET AL.	
	2	6438376	B1	2002-08-20	ELLIOTT ET AL.	
	3	6898413	B2	2005-05-24	YIP ET AL.	
	4	7664495	B1	2010-02-16	BONNER ET AL.	
	5	7623516	B2	2009-11-24	CHATURVEDI ET AL.	
	6	7623476	B2	2009-11-24	RAVIKUMAR ET AL.	
	7	7590758	B2	2009-09-15	TAKEDA ET AL.	
	8	6128283	A	2000-10-03	SABAA ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.C.D/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	2194
	Examiner Name	Craig Dorais
	Attorney Docket Number	DAMA-33216

	9	6389016	B1	2002-05-00	SABAA ET AL.	
	10	7345999	B2	2008-03-00	SU ET AL.	
	11	7542472	B1	2009-06-00	GERENDAI ET AL.	
	12	8009586	B2	2011-08-00	CHATURVEDI ET AL.	
	13	7302496	B1	2007-11-27	METZGER	
	14	6161082		2000-12-12	GOLDBERG ET AL.	
	15	8065418		2011-11-00	ABUAN ET AL.	
	16	7656870	B2	2010-02-00	RAVIKUMAR ET AL.	
	17	7487248	B2	2009-02-00	MORAN ET AL.	
	18	7574523	B2	2009-08-00	TRAVERSAT ET AL.	
	19	7774495	B2	2010-08-00	PABLA ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.C.D/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	
	Examiner Name	Craig Dorais
	Attorney Docket Number	DAMA-33216

	20	7782866	B1	2010-08-00	WALSH ET AL.	
	21	6298129		2001-10-00	CULVER ET AL.	
	22	6754181		2004-06-00	ELLIOTT ET AL.	
	23	7006508		2006-02-00	BONDY ET AL.	
	24	7010109		2006-03-00	GRITZER ET AL.	
	25	7123710		2006-10-00	RAVISHANKAR	
	26	7570743		2009-08-04	BARCLAY ET AL.	
	27	7769881		2010-08-00	MATSUBARA ET AL.	
	28	7346044	B1	2008-03-00	CHOU ET AL.	
	29	7092385		2006-08-00	GALLANT ET AL.	
	30	5818447		1998-10-00	WOLF ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.C.D/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	2194
	Examiner Name	Craig Dorais
	Attorney Docket Number	DAMA-33216

	31	7917584		2011-03-00	ARTHURSSON, DANIEL	
	32	7564843	B2	2009-07-21	MANJUNATHA ET AL.	
	33	7185114	B1	2007-02-27	HARIHARASUBRAHMANIAN	
	34	6031818	A	2000-02-29	LO ET AL.	
	35	6311150	B1	2001-10-30	RAMASWAMY ET AL.	
	36	6999932	B1	2006-02-14	ZHOU, GUOJUN	
	37	7272377	B2	2007-09-18	COX ET AL.	
	38	7412374	B1	2008-08-12	SEILER ET AL.	
	39	6766373	B1	2004-07-20	BEADLE, BRUCE A.	
	40	7304985	B2	2007-12-04	SOJKA ET AL.	
	41	7353255	B2	2008-04-01	ACHARYA ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.C.D/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	2194
	Examiner Name	Craig Dorais
	Attorney Docket Number	DAMA-33216

	42	7477282	B2	2009-01-13	FIRESTONE ET AL.	
	43	5442637	A	1995-08-01	NGUYEN, MAI-HUONG	
	44	6343067	B1	2002-01-01	DROTTAR ET AL.	
	45	6473425	B1	2002-10-01	BELLATON ET AL.	
	46	6574668	B1	2003-06-01	GUBBI ET AL.	
	47	6850769	B2	2005-02-01	GROB ET AL.	
	48	7080158	B1	2006-07-01	SQUIRE, MATTHEW	
	49	5889762		1999-03-30	PAJUVIRTA ET AL	
	50	7184415	B2	2007-02-01	CHANEY ET AL.	
	51	5790637	A	1998-08-01	JOHNSON ET AL.	
	52	6836765	B1	2004-12-01	SUSSMAN, LESTER	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.C.D/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	2194
	Examiner Name	Craig Dorais
	Attorney Docket Number	DAMA-33216

	53	7613171	B2	2009-11-00	ZEHAVI ET AL.	
	54	6842460	B1	2005-01-00	OLKKONEN ET AL.	
	55	6987756		2006-01-00	RAVINDRANATH ET AL.	
	56	7512652		2009-03-00	APPELMAN ET AL.	
	57	5761309	A	1998-06-01	OHASHI ET AL.	
	58	6141687	A	2000-10-01	BLAIR, DANA L.	
	59	6202084	B1	2001-03-13	KUMAR ET AL.	
	60	6219638	B1	2001-04-01	PADMANABHAN ET AL.	
	61	6360196	B1	2002-03-01	POZNASKI ET AL.	
	62	6826613	B1	2002-03-01	WANG ET AL.	
	63	7013155	B1	2006-03-01	RUF ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.C.D/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	2194
	Examiner Name	Craig Dorais
	Attorney Docket Number	DAMA-33216

	64	7117526	B1	2006-10-01	SHORT, JOEL E.	
	65	7353252	B1	2008-04-01	YANG ET AL.	
	66	6940826	B1	2005-09-06	SIMARD ET AL.	
	67	6741691	B1	2004-05-25	RITTER ET AL.	
	68	6912278	B1	2005-06-28	HAMILTON, THOMAS	
	69	6963555	B1	2005-11-08	BRENNER ET AL.	
	70	6975718	B1	2005-12-13	PEARCE ET AL.	
	71	6999575	B1	2006-02-14	SHEINBEIN, DANIEL	
	72	7079529	B1	2006-07-18	KHUC, MINH DUY	
	73	7457279	B1	2008-11-25	SCOTT ET AL.	
	74	8407576	B1	2013-03-26	YIN ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.C.D/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	2194
	Examiner Name	Craig Dorais
	Attorney Docket Number	DAMA-33216

	75	6195694	B1	2001-02-27	CHEN ET AL.	
	76	8200796	B1	2012-06-12	MARGULIS	
	77	6606112	B1	2003-08-12	FALCO	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20030126213	A1	2003-07-03	BETZLER, BOAS	
	2	20030163525	A1	2003-08-28	HENDRIKS ET AL.	
	3	20040005877	A1	2004-01-00	VAANANEN, MIKKO KALERVO	
	4	20040249953	A1	2004-12-00	FERNANDEZ ET AL.	
	5	20080032695	A1	2008-02-07	ZHU ET AL.	
	6	20050136911	A1	2005-06-23	CSAPO ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.C.D/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	2194
	Examiner Name	Craig Dorais
	Attorney Docket Number	DAMA-33216

	7	20040203834	A1	2004-10-14	MAHANY, RONALD L.	
	8	20020173303	A1	2002-11-21	SHIBUTANI, AKIRA	
	9	20060002355	A1	2006-01-05	BAEK ET AL.	
	10	20060182100	A1	2006-08-17	LI, JIN ET AL.	
	11	20080080392	A1	2008-04-03	WALSH, RICHARD J. ET AL.	
	12	20090300673	A1	2009-12-03	BACHET, FRANCK ET AL.	
	13	20020037000	A1	2002-03-00	PARK ET AL.	
	14	20030043764	A1	2003-03-00	KIM ET AL.	
	15	20030202480	A1	2003-10-30	SWAMI, YOGESH PREM	
	16	20040052234	A1	2004-03-00	AMEIGEIRAS ET AL.	
	17	20040213184	A1	2004-10-00	HU ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.C.D/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	2194
	Examiner Name	Craig Dorais
	Attorney Docket Number	DAMA-33216

	18	20090003322	A1	2009-01-01	ISUMI, SHINYA	
	19	20090327516	A1	2009-12-31	AMISHIMA, MAKI ET AL.	
	20	20060187926	A1	2006-08-24	IMAI, NAOKI	
	21	20070019545	A1	2007-01-25	ALT, WADE R. ET AL.	
	22	20050208947	A1	2005-09-22	BAHL, PRADEEP	
	23	20070297430	A1	2007-12-27	NYKANEN, PETRI ET AL.	
	24	20030214955	A1	2003-11-20	KIM, JUN-HYEONG	
	25	20050270992	A1	2005-12-08	SANZGIRI, AJIT ET AL.	
	26	20090052399	A1	2009-02-26	SILVER ET AL.	
	27	20070206563	A1	2007-09-06	SILVER ET AL.	
	28	20030217318	A1	2003-11-00	CHOI, SUNG-KYU	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.C.D/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	2194
	Examiner Name	Craig Dorais
	Attorney Docket Number	DAMA-33216

	29	20020064167	A1	2002-05-00	KHAN ET AL.	
	30	20060203750	A1	2006-09-14	RAVIKUMAR ET AL.	
	31	20060120375	A1	2006-06-08	RAVIKUMAR ET AL.	
	32	20070165629	A1	2007-07-19	CHATURVEDI ET AL.	
	33	20080235511	A1	2008-09-25	O'BRIEN, WILLIAM G. ET AL.	
	34	20100049980	A1	2010-02-25	BARRIGA, LUIS ET AL.	
	35	20080250408	A1	2008-10-09	TSUI ET AL.	
	36	20090136016	A1	2009-05-28	GORNOI ET AL.	
	37	20080235362	A1	2008-09-25	KJESBU ET AL.	
	38	20040148434	A1	2004-07-29	MATSUBARA ET AL.	
	39	20090182815	A1	2009-07-16	CZECHOWSKI ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.C.D/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	2194
	Examiner Name	Craig Dorais
	Attorney Docket Number	DAMA-33216

	40	20080273541	A1	2008-11-06	PHARN	
	41	20030046585	A1	2003-03-06	MINNICK	
	42	20040024879	A1	2004-02-05	DINGMAN ET AL.	
	43	20090006076	A1	2009-01-01	JINDAL, DINESH K.	
	44	20100223047	A1	2010-09-02	CHRIST,	
	45	20100299150	A1	2010-11-25	FEIN ET AL.	
	46	20050198499	A1	2005-09-00	SALAPAKA ET AL.	
	47	20040139230	A1	2004-07-00	KIM, SEON KEON	
	48	20040240399	A1	2004-12-00	CORRAO ET AL.	
	49	20050201357	A1	2005-09-00	POYHONEN, PETTERI	
	50	20060121902	A1	2006-06-08	JAGADEESAN ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.C.D/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	2194
	Examiner Name	Craig Dorais
	Attorney Docket Number	DAMA-33216

	51	20060205436	A1	2006-09-00	LIU ET AL.	
	52	20050130650	A1	2005-06-16	CREAMER ET AL.	
	53	20090088150	A1	2009-04-02	CHATURVEDI ET AL.	
	54	20100011111	A1	2010-01-14	MOHAMMAD, VIZAEI	
	55	20080130639	A1	2008-06-00	COSTA-REQUENA ET AL.	
	56	20060072506	A1	2006-04-00	SAYEEDI ET AL.	
	57	20060062180	A1	2006-03-00	SAYEEDI ET AL.	
	58	20080019285	A1	2008-01-00	JOHN ET AL.	
	59	20070253435	A1	2007-11-00	KELLER ET AL.	
	60	20050120073	A1	2005-06-00	CHO, JOON-HO	
	61	20050033843	A1	2005-02-00	SHAHI ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.C.D/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	2194
	Examiner Name	Craig Dorais
	Attorney Docket Number	DAMA-33216

	62	20030088676	A1	2003-05-00	SMITH ET AL.	
	63	20070130253	A1	2007-06-00	NEWSON ET AL.	
	64	20100077023	A1	2010-03-00	ERIKSSON, ANDERS	
	65	20090055473	A1	2009-02-00	SYNNERGREN, PER	
	66	20080091813	A1	2008-04-00	BODLAENDER, MAARTEN	
	67	20070136459	A1	2007-06-00	ROCHE ET AL.	
	68	20050144288	A1	2005-06-00	LIAO, EN-YI	
	69	20040068567	A1	2004-04-00	MORAN ET AL.	
	70	20050220017	A1	2005-10-00	BRAND ET AL.	
	71	20030172145	A1	2003-09-00	NGUYEN	
	72	20110122864	A1	2011-05-26	CHERIFI ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.C.D/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	2194
	Examiner Name	Craig Dorais
	Attorney Docket Number	DAMA-33216

	73	20090257433	A1	2009-10-15	MUTIKAINEN ET AL.	
	74	20060195402	A1	2006-08-00	MALINA ET AL.	
	75	20100299313	A1	2010-11-00	ORSINI ET AL.	
	76	20060171534	A1	2006-08-03	BAUGHMAN, WILLIAM P.	
	77	20070260359	A1	2007-11-00	BENSON ET AL.	
	78	20080168440	A1	2008-07-00	REGNIER ET AL.	
	79	20020031212	A1	2002-03-00	O'NEIL ET AL.	
	80	20050132009	A1	2005-06-00	SOLIE, KEVIN	
	81	20090234967	A1	2009-09-00	YU ET AL.	
	82	20100011108	A1	2010-01-00	CLARK ET AL.	
	83	20080123685	A1	2008-05-00	VARMA ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.C.D/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	2194
	Examiner Name	Craig Dorais
	Attorney Docket Number	DAMA-33216

	84	20070082671	A1	2007-04-00	FENG ET AL.	
	85	20070025270	A1	2007-02-00	SYLVAIN, DANY	
	86	20060258289	A1	2006-11-00	DUA, ROBIN	
	87	20110099612	A1	2011-04-00	LEE ET AL.	
	88	20070274276	A1	2007-11-00	LAROIA ET AL.	
	89	20110040836	A1	2011-02-00	ALLEN ET AL.	
	90	20100312897	A1	2010-12-00	ALLEN ET AL.	
	91	20100312832	A1	2010-12-00	ALLEN ET AL.	
	92	20090156217	A1	2009-06-00	BAJPAI, RAJNEESH	
	93	20050138128	A1	2005-06-00	BANIEL ET AL.	
	94	20070116224	A1	2007-05-00	BURKE ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.C.D/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	2194
	Examiner Name	Craig Dorais
	Attorney Docket Number	DAMA-33216

	95	20050187781	A1	2005-08-00	CHRISTENSEN, TORE L.	
	96	20110314134	A1	2011-12-00	FOTI, GEORGE	
	97	20100107205	A1	2010-04-00	FOTI, GEORGE	
	98	20100279670	A1	2010-11-00	GHAI ET AL.	
	99	20120263144	A1	2012-10-00	NIX, JOHN A.	
	100	20110145687	A1	2011-06-00	GRIGSBY ET AL.	
	101	20070239892	A1	2007-10-00	OTT ET AL.	
	102	20020152325	A1	2002-10-00	ELGEBALY ET AL.	
	103	20020156844	A1	2002-10-00	MAEHIRO, KAZUTOYO	
	104	20030212772	A1	2003-11-00	HARRIS, ADAM PIERCE	
	105	20020124096	A1	2002-09-05	LOGUINOV ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.C.D/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	2194
	Examiner Name	Craig Dorais
	Attorney Docket Number	DAMA-33216

	106	20050201485	A1	2005-09-15	FAY	
	107	20060069775	A1	2006-03-30	ARTOBELLO ET AL.	
	108	20060165029	A1	2006-07-27	MELPIGNANO ET AL.	
	109	20050015502	A1	2005-01-20	KANG ET AL.	
	110	20030229715	A1	2003-12-11	BARATAKKE ET AL.	
	111	20010050923	A1	2001-12-13	PARK ET AL.	
	112	20040062267	A1	2004-04-01	MINAMI ET AL.	
	113	20020184310	A1	2002-12-01	TRAVERSAT ET AL.	
	114	20030076815	A1	2003-04-23	MILLER ET AL.	
	115	20040034793	A1	2004-02-19	YUAN, WEI	
	116	20040139225	A1	2004-07-15	TAKAHASHI, MASAYUKI	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.C.D/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	2194
	Examiner Name	Craig Dorais
	Attorney Docket Number	DAMA-33216

	117	20050033985	A1	2005-02-10	XU ET AL.	
	118	20050091407	A1	2005-04-28	VAZIRI ET AL.	
	119	20050195802	A1	2005-09-08	KLEIN ET AL.	
	120	20050286519	A1	2005-12-29	RAVIKUMAR ET AL.	
	121	20070016921	A1	2007-01-01	LEVI ET AL.	
	122	20030046056	A1	2003-03-06	GODOY ET AL.	
	123	20040158471	A1	2004-08-12	DAVIS ET AL.	
	124	20050086309	A1	2005-04-21	GALLI ET AL.	
	125	20040162871	A1	2004-08-19	PABLA ET AL.	
	126	20030115251	A1	2003-06-19	FREDRICKSON ET AL.	
	127	20020178087	A1	2002-11-28	HENDERSON ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.C.D/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	2194
	Examiner Name	Craig Dorais
	Attorney Docket Number	DAMA-33216

	128	20060183476	A1	2006-08-17	MORITA, J. ET AL.	
	129	20030220121	A1	2003-11-27	KONISHI, T. ET AL.	
	130	20080192756	A1	2008-08-14	DAMOLA ET AL.	
	131	20030072485	A1	2003-04-17	GUERIN ET AL.	
	132	20050008024	A1	2005-01-13	NEWPOL ET AL.	
	133	20020176404	A1	2002-11-28	GIRARD, GREGORY D.	
	134	20030137939	A1	2003-07-24	DUNNING ET AL.	
	135	20040100973	A1	2004-05-01	PRASAD, ANAND R.	
	136	20020080719	A1	2002-06-27	PARKVALL ET AL.	
	137	20040228279	A1	2004-11-18	MIDTUN ET AL.	
	138	20050050227	A1	2005-03-01	MICHELMAN, ERIC H.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.C.D/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	2194
	Examiner Name	Craig Dorais
	Attorney Docket Number	DAMA-33216

	139	20030217171	A1	2003-11-01	VON STUERMER ET AL.	
	140	20040267938	A1	2004-12-01	SHOROFF ET AL.	
	141	20020087887	A1	2002-07-01	BUSAM ET AL.	
	142	20020120757	A1	2002-08-01	SUTHERLAND ET AL.	
	143	20020166053	A1	2002-11-01	WILSON, RODGER P.	
	144	20030044020	A1	2003-03-01	ABOBA ET AL.	
	145	20030163697	A1	2003-08-01	PABLA ET AL.	
	146	20030177422	A1	2003-09-01	TARAROUKHINE ET AL.	
	147	20040260952	A1	2004-12-01	NEWMAN ET AL.	
	148	20050249196	A1	2005-11-01	ANSARI ET AL.	
	149	20060148516	A1	2006-07-01	REDDY ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.C.D/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	2194
	Examiner Name	Craig Dorais
	Attorney Docket Number	DAMA-33216

	150	20070110043	A1	2007-05-01	GIRARD, GREGORY D.	
	151	20080069105	A1	2008-03-01	COSTA ET AL.	
	152	20080320096	A1	2008-12-01	SZETO, CHRISTOPHER	
	153	20090192976	A1	2009-07-01	SPIVACK ET AL.	
	154	20050119005	A1	2005-06-00	SEGAL ET AL.	
	155	20060246903	A1	2006-11-00	KONG ET AL.	
	156	20030031210	A1	2003-02-00	HARRIS, JOHN M.	
	157	20030035441	A1	2003-02-00	CHENG ET AL.	
	158	20030174707	A1	2003-09-00	GROB ET AL.	
	159	20050138119	A1	2005-06-23	SARIDAKIS, TITOS	
	160	20020038282	A1	2002-03-01	MONTGOMERY, ROB R.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.C.D/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	2194
	Examiner Name	Craig Dorais
	Attorney Docket Number	DAMA-33216

	161	20020042769	A1	2002-04-01	GUJRAL ET AL.	
	162	20020062285	A1	2002-05-01	AMANN ET AL.	
	163	20020097150	A1	2002-07-01	SANDELMAN ET AL.	
	164	20020143548	A1	2002-10-01	KORALL ET AL.	
	165	20020150110		2002-10-17	INBAR ET AL.	
	166	20030009565		2003-01-09	ARAO	
	167	20030061025	A1	2003-03-01	ABIR, ELI	
	168	20030061481	A1	2003-03-27	LEVINE ET AL.	
	169	20030078858	A1	2003-04-01	ANGELOPOULOS ET AL.	
	170	20030105812	A1	2003-06-05	FLOWERS, JR., ET AL.	
	171	20030110047	A1	2003-06-01	SANTOSUOSSO, JOHN MATTHEW	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.C.D/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	2194
	Examiner Name	Craig Dorais
	Attorney Docket Number	DAMA-33216

	172	20030135569		2003-07-17	KHAKOO ET AL.	
	173	20030158722	A1	2003-08-01	LORD, JOHN RAYMOND	
	174	20030177186	A1	2003-09-01	GOODMAN ET AL.	
	175	20030187650	A1	2003-10-01	MOORE ET AL.	
	176	20040034776	A1	2003-10-01	FERNANDO ET AL.	
	177	20040039781	A1	2004-02-01	LAVALLEE ET AL.	
	178	20040044517	A1	2004-03-01	PALMQUIST, ROBERT	
	179	20040128554	A1	2004-07-01	MAHER, III, ET AL.	
	180	20040133689	A1	2004-07-08	VASISHT, SAMRAT	
	181	20040139228		2004-07-15	TAKEDA ET AL.	
	182	20040143678	A1	2004-07-01	CHARI ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.C.D/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	2194
	Examiner Name	Craig Dorais
	Attorney Docket Number	DAMA-33216

	183	20040153858	A1	2004-08-01	HWANG, SHAW HWA	
	184	20040267527	A1	2004-12-01	CREAMER ET AL.	
	185	20040268257	A1	2004-12-01	MUDUSURU, GIRI P.	
	186	20050004982	A1	2005-01-06	VERNON ET AL.	
	187	20050071481	A1	2005-03-01	DANIELI, DAMON V.	
	188	20050143105	A1	2005-06-01	OKAMOTO, YUKIFUMI	
	189	20050187957	A1	2005-08-01	KRAMER ET AL.	
	190	20050246193	A1	2005-11-03	ROEVER ET AL.	
	191	20050254440	A1	2005-11-17	SORRELL, JOHN D.	
	192	20060121986	A1	2006-06-01	PELKEY ET AL.	
	193	20060168643	A1	2006-07-01	HOWARD ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.C.D/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	2194
	Examiner Name	Craig Dorais
	Attorney Docket Number	DAMA-33216

	194	20060218624	A1	2006-09-28	RAVIKUMAR ET AL.	
	195	20060230166	A1	2006-10-01	PHILYAW, JEFFRY JOVAN	
	196	20070078785	A1	2007-04-01	BUSH ET AL.	
	197	20070111794	A1	2007-05-01	HOGAN ET AL.	
	198	20070190987	A1	2007-08-01	VAANANEN, MIKKO KALERVO	
	199	20080005328		2008-01-01	SHIVELY ET AL.	
	200	20050105524	A1	2005-05-19	STEVENS ET AL.	
	201	20040103212	A1	2004-05-27	TAKEUCHI ET AL.	
	202	20090240821	A1	2009-09-24	JUNCKER ET AL.	
	203	20110141220	A1	2011-06-16	MIURA	
	204	20100174783	A1	2010-07-08	ZAROM	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.C.D/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	2194
	Examiner Name	Craig Dorais
	Attorney Docket Number	DAMA-33216

	205	20070294626	A1	2007-12-20	FLETCHER ET AL.	
	206	20040249885	A1	2004-12-09	PETROPOULAKIS ET AL.	
	207	20110320821	A1	2011-12-29	ALKHATIB ET AL	
	208	20080320565	A1	2008-12-25	BUCH ET AL	
	209	20100191954	A1	2010-07-29	KIM ET AL	
	210	20130111064	A1	2013-05-02	MANI ET AL	
	211	20070280253	A1	2007-12-06	ROOHOLAMINI ET AL	
	212	20130067004	A1	2013-03-14	LOGUE ET AL	
	213	20080046984	A1	2008-02-21	BOHMER ET AL	
	214	20120078609	A1	2012-03-29	CHATURVEDI ET AL	
	215	20060233117	A1	2006-10-19	TOMSU ET AL	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.C.D/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	2194
	Examiner Name	Craig Dorais
	Attorney Docket Number	DAMA-33216

	216	20110307556	A1	2011-12-15	CHATURVEDI ET AL	
	217	20130106989	A1	2013-05-02	TELIRIS, INC.	
	218	20080244718	A1	2008-10-02	FROST ET AL	
	219	20120124191	A1	2012-05-17	LYON	
	220	20040193599	A1	2004-09-30	LIU ET AL.	
	221	20100058353	A1	2010-03-04	TURSKI	
	222	20130125145	A1	2013-05-16	BALMORI LABRA ET AL.	
	223	20150026700	A1	2015-01-22	CHATURVEDI ET AL.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
/C.C.D/	1	1848163	EP	A1	2007-10-24	SHARP KABUSHIKI KAISHA		

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.C.D/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	2194
	Examiner Name	Craig Dorais
	Attorney Docket Number	DAMA-33216

/C.C.D/	2	1988698	EP	A1	2008-11-05	RESEARCH IN MOTION LIMITED		
/C.C.D/	3	1988697	EP	A1	2008-11-05	RESEARCH IN MOTION LIMITED		
/C.C.D/	4	2006064047	WO	A1	2006-06-22	INTERNATIONAL BUSINESS MACHINES CORPORATION ET AL.		
/C.C.D/	5	1638275	EP	A2	2006-03-22	WECOMM LIMITED		
/C.C.D/	6	160339	EP	A1	2005-12-07	STMICROELECTRONICS S.R.I.		
/C.C.D/	7	1404082	EP	A2	2004-03-31	NORTEL NETWORKS LTD		
/C.C.D/	8	WO 2003/079635	WO		2003-09-25	IBM CORPORATION ET AL.		
/C.C.D/	9	WO 2004/063843	WO		2004-07-29	MATSUSHITA ELECTRIC IND CO LTD		
/C.C.D/	10	WO 2005/009019	WO		2005-01-27	SKYPER LTD. ET AL.		
/C.C.D/	11	2005-94600	JP		2005-04-07	NEC CORP.		
	12	2007-043598	JP		2007-02-15	2007-02-15		

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.C.D/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	2194
	Examiner Name	Craig Dorais
	Attorney Docket Number	DAMA-33216

/C.C.D/	13	10-2005-0030548	KR		2005-03-30	MICROSOFT CORP.		
/C.C.D/	14	WO 2006/075677	WO		2006-07-20	SHARP KABUSHIKI KAISHA		
/C.C.D/	15	WO 2008099420	WO	A2	2008-08-21	MADHOK		

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
/C.C.D/	1	PCT: International Search Report and Written Opinion for PCT/US2011/024870; 26 October 2011; 12 pages.	
/C.C.D/	2	J. ROSENBERG et al. " Session Traversal Utilities for NAT (STUN)", draft–ietf–behave–rfc3489bis–06, March 5, 2007.	
/C.C.D/	3	PCT: International Search Report and Written Opinion for PCT/US2011/028685; 9 November 2011; 10 pages.	
/C.C.D/	4	PCT: International Search Report and Written Opinion for PCT/US2011/029954; 24 November 2011; 8 pages.	
/C.C.D/	5	PCT: International Search Report and Written Opinion for PCT/US2011/024891; 25 November 2011; 9 pages.	
/C.C.D/	6	PCT: International Search Report and Written Opinion for PCT/US2011/031245; 26 December 2011; 13 pages.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.C.D/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	2194
	Examiner Name	Craig Dorais
	Attorney Docket Number	DAMA-33216

/C.C.D/	7	Wireless Application Protocol - Wireless Transport Layer Security Specification, Version 18-Feb-2000, Wireless Application Forum, Ltd. 2000; 99 pages.	
/C.C.D/	8	PCT: International Search Report and Written Opinion for PCT/US2011/040864; 17 February 2012; 8 pages.	
/C.C.D/	9	PCT: International Search Report and Written Opinion for PCT/US2011/041565; 5 January 2012; 7 pages.	
/C.C.D/	10	PCT: International Search Report and Written Opinion for PCT/US2011/031246; 27 December 2011; 8 pages.	
/C.C.D/	11	PCT: International Search Report and Written Opinion for PCT/US2011/049000; 27 March 2012; 10 pages.	
/C.C.D/	12	PCT: International Search Report and Written Opinion for PCT/US2011/051877; 13 April 2012; 7 pages.	
/C.C.D/	13	PCT: International Search Report and Written Opinion for PCT/US2011/055101; 22 May 2012; 9 pages.	
/C.C.D/	14	Balamurugan Karpagavinayagam et al. (Monitoring Architecture for Lawful Interception in VoIP Networks, ICIMP 2007, 24 Aug 2008).	
/C.C.D/	15	NiceLog User's Manual 385A0114-08 Rev. A2, March 2004.	
/C.C.D/	16	WISPA: Wireless Internet Service Providers Association; WISPA-CS-IPNA-2.0; May 1, 2009.	
/C.C.D/	17	PCT: International Preliminary Report on Patentability of PCT/US2011/024870; 30 August 2012; 7 pgs.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.C.D/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	2194
	Examiner Name	Craig Dorais
	Attorney Docket Number	DAMA-33216

/C.C.D/	18	RFC 5694 ("Peer-to-Peer (P2P) Architecture: Definition, Taxonomies, Examples, and Applicability", November 2009).	
/C.C.D/	19	Mahy et al., The Session Initiation Protocol (SIP) "Replaces" Header, September 2004, RFC 3891, pages 1-16.	
/C.C.D/	20	PCT: International Preliminary Report on Patentability of PCT/US2011/024891; 30 August 2012; 6 pgs.	
/C.C.D/	21	T. Dierks & E. Rescorla, The Transport Layer Security (TLS) Protocol (Ver. 1.2, 8/2008) retrieved at http://tools.ietf.org/html/rfc5246. Relevant pages provided.	
/C.C.D/	22	J. Rosenberg et al., SIP: Session Initiation Protocol (6/2008) retrieved at http://tools.ietf.org/html/rfc3261. Relevant pages provided.	
/C.C.D/	23	Philippe Bazot et al., Developing SIP and IP Multimedia Subsystem (IMS) Applications (2/5/2007) retrieved at redbooks IBM form number: SG24-7255-00. Relevant pages provided.	
/C.C.D/	24	PCT: International Preliminary Report on Patentability of PCT/US2011/028685; 4 October 2012; 6 pgs.	
/C.C.D/	25	PCT: International Preliminary Report on Patentability of PCT/US2011/031245; 26 October 2012; 9 pgs.	
/C.C.D/	26	PCT: International Preliminary Report on Patentability of PCT/US2011/029954; 11 October 2012; 5 pgs.	
/C.C.D/	27	PCT: International Preliminary Report on Patentability of PCT/US2011/031246; 08 November 2012; 5 pgs.	
/C.C.D/	28	Rosenberg, J; "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols"; 29 October 2007; I ETF; I ETF draft of RFC 5245, draft-ietf-mmusic-ice-19; pp 1-120.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.C.D/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	2194
	Examiner Name	Craig Dorais
	Attorney Docket Number	DAMA-33216

/C.C.D/	29	Blanchet et al; "IPv6 Tunnel Broker with the Tunnel Setup Protocol (TSP)"; 6 May 2008; IETF; IETF draft of RFC 5572, draftblanchet-v6ops-tunnelbroker-tsp-04; pp 1-33	
/C.C.D/	30	Cooper et al; "NAT Traversal for dSIP"; 25 February 2007; IETF; IETF draft draft-matthews-p2psip-dsip-nat-traversal-00; pp 1-23	
/C.C.D/	31	Cooper et al; "The Effect of NATs on P2PSIP Overlay Architecture"; IETF; IETF draft draft-matthews-p2psip-nats-and-overlays-01.txt; pp 1-20	
/C.C.D/	32	Srisuresh et al; "State of Peer-to-Peer(P2P) Communication Across Network Address Translators(NATs)"; 19 November 2007; I ETF; I ETF draft for RFC 5128, draft-ietf-behave-p2p-state-06.txt; pp 1-33	
/C.C.D/	33	PCT: International Search Report and Written Opinion for PCT/US2012/046026; 18 October 2012; 6 pages.	
/C.C.D/	34	DUNIGAN, Tom, "Almost TCP over UDP (atou)," last modified Jan. 12, 2004; retrieved on Jan. 18, 2011 from <http://www.csm.ornl.gov/~dunigan/net100/atou.html> 18 pgs.	
/C.C.D/	35	PCT: International Preliminary Report on Patentability of PCT/US2011/040864; 3 January 2013; 6 pgs.	
/C.C.D/	36	PCT: International Preliminary Report on Patentability of PCT/US2011/041565; 10 January 2013; 6 pgs.	
/C.C.D/	37	PCT: International Preliminary Report on Patentability of PCT/US2011/049000; 26 February 2013; 6 pgs.	
/C.C.D/	38	PCT: International Preliminary Report on Patentability of PCT/US2011/051877; 26 March 2013; 5 pgs.	
/C.C.D/	39	PCT: International Preliminary Report on Patentability of PCT/US2011/055101; 16 April 2013; 7 pgs.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.C.D/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	2194
	Examiner Name	Craig Dorais
	Attorney Docket Number	DAMA-33216

/C.C.D/	40	PCT: International Preliminary Report on Patentability of PCT/US2012/046026; 30 January 2014; 5 pgs.	
/C.C.D/	41	PCT: International Preliminary Report on Patentability of PCT/US2008/075141; 09 March 2010; 5 pgs.	
/C.C.D/	42	PCT: International Preliminary Report on Patentability of PCT/US2007/068820; 31December 2008; 8 pgs.	
/C.C.D/	43	PCT: International Preliminary Report on Patentability of PCT/US2007/068823; 27 November 2008; 8 pgs.	
/C.C.D/	44	PCT: International Preliminary Report on Patentability of PCT/US2006/047841; 06 November 2008; 7 pgs.	
/C.C.D/	45	PCT: International Preliminary Report on Patentability of PCT/US2007/002424; 07 August 2008; 6 pgs.	
/C.C.D/	46	PCT: International Preliminary Report on Patentability of PCT/US2006/040312; 02 May 2008; 5 pgs.	
/C.C.D/	47	PCT: International Preliminary Report on Patentability of PCT/IB2005/000821; 19 October 2006; 10 pgs.	
/C.C.D/	48	CHATHAPURAM, "Security in Peer-To-Peer Networks", August 8. 2001, XP002251813.	
/C.C.D/	49	International Search Report and Written Opinion of the International Searching Authority from PCT/IB2005/000821, dated August 5, 2005.	
/C.C.D/	50	International Search Report and Written Opinion of the International Searching Authority from PCT/US2006/032791, dated December 18, 2006.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	2194
	Examiner Name	Craig Dorais
	Attorney Docket Number	DAMA-33216

If you wish to add additional non-patent literature document citation information please click the Add button [Add]

EXAMINER SIGNATURE

Examiner Signature	/CRAIG C DORAIS/	Date Considered	12/21/2016

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

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	
	Examiner Name	
	Attorney Docket Number	DAMA-33216

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Keith D. Harden, Reg. #74472/	Date (YYYY-MM-DD)	2016-10-25
Name/Print	Keith D. Harden	Registration Number	74472

This collection of information is required by 37 CFR 1.97 and 1.98. 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 1 hour 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.**

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

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. 6761

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
15/297,328	10/19/2016 RULE	719	2194	DAMA-33216

APPLICANTS
DAMAKA, INC., RICHARDSON, TX;

INVENTORS
SIVAKUMAR CHATURVEDI, ALLEN, TX;
SATISH GUNDABATHULA, IRVING, TX;
RASHMI HIREMATH, ALLEN, TX;

**** CONTINUING DATA **************************
This application is a CON of 15/049,891 02/22/2016 PAT 9491233
which is a CON of 14/690,619 04/20/2015 PAT 9270744
which is a CON of 14/024,027 09/11/2013 PAT 9027032
which claims benefit of 61/846,958 07/16/2013

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

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED **** ** SMALL ENTITY **
10/28/2016

Foreign Priority claimed	35 USC 119(a-d) conditions met	Verified and Acknowledged	Met after Allowance	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
☐ Yes ☑ No	☐ Yes ☐ No	/CRAIG C DORAIS/ Examiner's Signature	☐ Initials	TX	12	30	4

ADDRESS
HOWISON & ARNOTT, L.L.P
P.O. BOX 741715
DALLAS, TX 75374-1715
UNITED STATES

TITLE
SYSTEM AND METHOD FOR PROVIDING ADDITIONAL FUNCTIONALITY TO EXISTING SOFTWARE IN AN INTEGRATED MANNER

FILING FEE RECEIVED		
1340	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

BIB (Rev. 05/07).

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15297328	CHATURVEDI ET AL.
	Examiner	**Art Unit**
	CRAIG DORAIS	2194

CPC						
Symbol					**Type**	**Version**
H04L		67	/	10	F	2013-01-01
H04L		65	/	60	I	2013-01-01
H04L		65	/	1069	I	2013-01-01
H04L		65	/	1089	I	2013-01-01
H04L		41	/	20	I	2013-01-01
H04L		41	/	28	I	2013-01-01
H04L		67	/	32	I	2013-01-01
G06F		15	/	167	I	2013-01-01
			/			
			/			
			/			
			/			
			/			
			/			
			/			

CPC Combination Sets							
Symbol					**Type**	**Set**	**Ranking**	**Version**
			/					
			/					

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	30	
/CRAIG DORAIS/ Primary Examiner.Art Unit 2194	12/22/2016	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	12	6A

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15297328	CHATURVEDI ET AL.
	Examiner	**Art Unit**
	CRAIG DORAIS	2194

US ORIGINAL CLASSIFICATION		INTERNATIONAL CLASSIFICATION	
CLASS	SUBCLASS	CLAIMED	NON-CLAIMED
719	313	G 06 F 3 / 00 (2006.01.01)	
CROSS REFERENCE(S)		G 06 F 9 / 44 (2006.01.01)	
		G 06 F 9 / 46 (2006.01.01)	
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)	G 06 F 13 / 00 (2006.01.01)	

NONE		**Total Claims Allowed:** 30
(Assistant Examiner)	(Date)	
/CRAIG DORAIS/ Primary Examiner.Art Unit 2194	12/22/2016	O.G. Print Claim(s): 12 / O.G. Print Figure: 6A
(Primary Examiner)	(Date)	

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15297328	CHATURVEDI ET AL.
	Examiner	**Art Unit**
	CRAIG DORAIS	2194

☐ 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	17	17												
2	2	18	18												
3	3	19	19												
4	4	20	20												
5	5	21	21												
6	6	22	22												
7	7	23	23												
8	8	24	24												
9	9	25	25												
10	10	26	26												
11	11	27	27												
12	12	28	28												
13	13	29	29												
14	14	30	30												
15	15														
16	16														

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	30	
/CRAIG DORAIS/ Primary Examiner.Art Unit 2194	12/22/2016	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	12	6A

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	37	("20010050923" | "20020143548" | "20020156844" | "20030202480" | "20040034776" | "20040103212" | "20050130650" | "20050132009" | "20050198499" | "20050201485" | "20060168643" | "20060258289" | "20070136459" | "20070165629" | "20070206563" | "20070297430" | "20080273541" | "20090052399" | "20090240821" | "20090327516" | "20110122864" | "20110314134" | "6128283" | "7079529" | "7092385" | "7487248" | "7623476" | "20030177422" | "20050033985" | "20050091407" | "6850769" | "7304985" | "20020037000" | "20020064167" | "20030110047" | "20030172145" | "20030214955" | "20040139230" | "20040153858" | "20040268257" | "20050136911" | "20050138128" | "20060072506" | "20060120375" | "20070082671" | "20070130253" | "20110145687" | "6219638" | "6754181" | "6999575" | "7185114" | "7590758" | "7623516" | "7774495" | "20030035441" | "20030076815" | "20030217171" | "20040260952" | "20050050227" | "5442637" | "5889762" | "6343067" | "7080158" | "20020031212" | "20020062285" | "20030046585" | "20040052234" | "20040139228" | "20040267527" | "20050187781" | "20060121902" | "20060171534" | "20060187926" | "20070253435" | "20080032695" | "20080168440" | "20090055473" | "20100049980" | "20100107205" | "20100312897" | "20110099612" | "20120263144" | "6141687" | "6898413" | "7010109" | "7345999" | "7457279" | "7542472" | "7570743" | "8065418" | "20020080719" | "20020176404" | "20030031210" | "20030115251" | "20070016921" | "6836765" | "20020042769" | "20020124096" | "20030009565" | "20030043764" | "20030105812" | "20040128554" | "20050004982" | "20050120073" | "20050220017" | "20060062180" | "20060182100" | "20060205436" | "20070019545" | "20080091813" | "20080130639" | "20090003322" | "20090156217" | "20090234967" | "20090257433" |	USPAT; USOCR	OR	OFF	2015/03/13 10:50

		"20100011108" | "20100011111" | "20100279670" | "20100299150" | "20100299313" | "7346044" | "7353252" | "7574523" | "7656870" | "20020087887" | "20020120757" | "20020184310" | "20030046056" | "20030163697" | "20040034793" | "20050195802" | "20070110043" | "20080320096" | "6987756" | "7184415" | "7272377" | "7412374" | "7477282" | "7512652" | "20020097150" | "20020152325" | "20030088676" | "20030126213" | "20030158722" | "20030163525").PN.				
S2	36	("20030187650" | "20040024879" | "20040068567" | "20040203834" | "20040240399" | "20050071481" | "20050143105" | "20050246193" | "20060002355" | "20060069775" | "20060203750" | "20070025270" | "20070190987" | "20070260359" | "20080123685" | "20080250408" | "20100077023" | "6963555" | "6975718" | "7006508" | "7013155" | "7564843" | "7782866" | "20040100973" | "20040158471" | "20040162871" | "20040228279" | "20040267938" | "20050008024" | "20050286519" | "20080192756" | "6766373" | "7613171" | "20020173303" | "20030078858" | "20030212772" | "20040005877" | "20040249953" | "20050033843" | "20050105524" | "20050270992" | "20070078785" | "20070111794" | "20070239892" | "20080019285" | "20080080392" | "20090136016" | "6298129" | "6360196" | "6826613" | "7117526" | "7302496" | "7664495" | "7778187" | "8009586" | "20020166053" | "20030044020" | "20030072485" | "20030174707" | "20050119005" | "20050249196" | "20090192976" | "6999932" | "7353255" | "20020150110" | "20040039781" | "20040044517" | "20040062267" | "20040148434" | "20040213184" | "20050015502" | "20050144288" | "20050201357" | "20060195402" | "20060218624" | "20060230166" | "20070116224" | "20070274276" | "20080005328" | "20090182815" | "20100312832" | "20110040836" | "5761309" | "6202084" | "6389016" | "6438376" | "6741691" | "6940826" | "7769881" | "20030137939" | "20040139225" | "20060183476" | "20060246903" | "20080069105" | "6031818" | "6311150" | "6574668" | "6842460" | "20020038282" | "20030061025" | "20030061481" | "20030135569" | "20030177186" | "20030217318" | "20030229715" | "20040133689" | "20040143678" | "20050187957" | "20050208947" | "20050254440" | "20060121986"	USPAT; USOCR	OR	OFF	2015/03/13 10:50

		"20060165029" | "20080235362" | "20080235511" | "20090006076" | "20090088150" | "20090300673" | "20100223047" | "5818447" | "6161082" | "6912278" | "7123710" | "7917584" | "20020178087" | "20030220121" | "20050086309" | "20050138119" | "20060148516" | "5790637" | "6473425").PN.				
S3	304	("20010050923" | "20020143548" | "20020156844" | "20030202480" | "20040034776" | "20040103212" | "20050130650" | "20050132009" | "20050198499" | "20050201485" | "20060168643" | "20060258289" | "20070136459" | "20070165629" | "20070206563" | "20070297430" | "20080273541" | "20090052399" | "20090240821" | "20090327516" | "20110122864" | "20110314134" | "6128283" | "7079529" | "7092385" | "7487248" | "7623476" | "20030177422" | "20050033985" | "20050091407" | "6850769" | "7304985" | "20020037000" | "20020064167" | "20030110047" | "20030172145" | "20030214955" | "20040139230" | "20040153858" | "20040268257" | "20050136911" | "20050138128" | "20060072506" | "20060120375" | "20070082671" | "20070130253" | "20110145687" | "6219638" | "6754181" | "6999575" | "7185114" | "7590758" | "7623516" | "7774495" | "20030035441" | "20030076815" | "20030217171" | "20040260952" | "20050050227" | "5442637" | "5889762" | "6343067" | "7080158" | "20020031212" | "20020062285" | "20030046585" | "20040052234" | "20040139228" | "20040267527" | "20050187781" | "20060121902" | "20060171534" | "20060187926" | "20070253435" | "20080032695" | "20080168440" | "20090055473" | "20100049980" | "20100107205" | "20100312897" | "20110099612" | "20120263144" | "6141687" | "6898413" | "7010109" | "7345999" | "7457279" | "7542472" | "7570743" | "8065418" | "20020080719" | "20020176404" | "20030031210" | "20030115251" | "20070016921" | "6836765" | "20020042769" | "20020124096" | "20030009565" | "20030043764" | "20030105812" | "20040128554" | "20050004982" | "20050120073" | "20050220017" | "20060062180" | "20060182100" | "20060205436" | "20070019545" | "20080091813" | "20080130639" | "20090003322" | "20090156217" | "20090234967" | "20090257433" | "20100011108" | "20100011111" | "20100279670" | "20100299150" |	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2015/03/13 11:25

		"20100299313" | "7346044" | "7353252" | "7574523" | "7656870" | "20020087887" | "20020120757" | "20020184310" | "20030046056" | "20030163697" | "20040034793" | "20050195802" | "20070110043" | "20080320096" | "6987756" | "7184415" | "7272377" | "7412374" | "7477282" | "7512652" | "20020097150" | "20020152325" | "20030088676" | "20030126213" | "20030158722" | "20030163525").PN.				
S4	36	("20030187650" | "20040024879" | "20040068567" | "20040203834" | "20040240399" | "20050071481" | "20050143105" | "20050246193" | "20060002355" | "20060069775" | "20060203750" | "20070025270" | "20070190987" | "20070260359" | "20080123685" | "20080250408" | "20100077023" | "6963555" | "6975718" | "7006508" | "7013155" | "7564843" | "7782866" | "20040100973" | "20040158471" | "20040162871" | "20040228279" | "20040267938" | "20050008024" | "20050286519" | "20080192756" | "6766373" | "7613171" | "20020173303" | "20030078858" | "20030212772" | "20040005877" | "20040249953" | "20050033843" | "20050105524" | "20050270992" | "20070078785" | "20070111794" | "20070239892" | "20080019285" | "20080080392" | "20090136016" | "6298129" | "6360196" | "6826613" | "7117526" | "7302496" | "7664495" | "7778187" | "8009586" | "20020166053" | "20030044020" | "20030072485" | "20030174707" | "20050119005" | "20050249196" | "20090192976" | "6999932" | "7353255" | "20020150110" | "20040039781" | "20040044517" | "20040062267" | "20040148434" | "20040213184" | "20050015502" | "20050144288" | "20050201357" | "20060195402" | "20060218624" | "20060230166" | "20070116224" | "20070274276" | "20080005328" | "20090182815" | "20100312832" | "20110040836" | "5761309" | "6202084" | "6389016" | "6438376" | "6741691" | "6940826" | "7769881" | "20030137939" | "20040139225" | "20060183476" | "20060246903" | "20080069105" | "6031818" | "6311150" | "6574668" | "6842460" | "20020038282" | "20030061025" | "20030061481" | "20030135569" | "20030177186" | "20030217318" | "20030229715" | "20040133689" | "20040143678" | "20050187957" | "20050208947" | "20050254440" | "20060121986" | "20060165029" | "20080235362" | "20080235511" | "20090006076" |	USPAT; USOCR	OR	OFF	2015/03/13 11:26

		"20090088150" | "20090300673" | "20100223047" | "5818447" | "6161082" | "6912278" | "7123710" | "7917584" | "20020178087" | "20030220121" | "20050086309" | "20050138119" | "20060148516" | "5790637" | "6473425").PN.				
S5	268	("20030187650" | "20040024879" | "20040068567" | "20040203834" | "20040240399" | "20050071481" | "20050143105" | "20050246193" | "20060002355" | "20060069775" | "20060203750" | "20070025270" | "20070190987" | "20070260359" | "20080123685" | "20080250408" | "20100077023" | "6963555" | "6975718" | "7006508" | "7013155" | "7564843" | "7782866" | "20040100973" | "20040158471" | "20040162871" | "20040228279" | "20040267938" | "20050008024" | "20050286519" | "20080192756" | "6766373" | "7613171" | "20020173303" | "20030078858" | "20030212772" | "20040005877" | "20040249953" | "20050033843" | "20050105524" | "20050270992" | "20070078785" | "20070111794" | "20070239892" | "20080019285" | "20080080392" | "20090136016" | "6298129" | "6360196" | "6826613" | "7117526" | "7302496" | "7664495" | "7778187" | "8009586" | "20020166053" | "20030044020" | "20030072485" | "20030174707" | "20050119005" | "20050249196" | "20090192976" | "6999932" | "7353255" | "20020150110" | "20040039781" | "20040044517" | "20040062267" | "20040148434" | "20040213184" | "20050015502" | "20050144288" | "20050201357" | "20060195402" | "20060218624" | "20060230166" | "20070116224" | "20070274276" | "20080005328" | "20090182815" | "20100312832" | "20110040836" | "5761309" | "6202084" | "6389016" | "6438376" | "6741691" | "6940826" | "7769881" | "20030137939" | "20040139225" | "20060183476" | "20060246903" | "20080069105" | "6031818" | "6311150" | "6574668" | "6842460" | "20020038282" | "20030061025" | "20030061481" | "20030135569" | "20030177186" | "20030217318" | "20030229715" | "20040133689" | "20040143678" | "20050187957" | "20050208947" | "20050254440" | "20060121986" | "20060165029" | "20080235362" | "20080235511" | "20090006076" | "20090088150" | "20090300673" | "20100223047" | "5818447" | "6161082" | "6912278" | "7123710" | "7917584" | "20020178087" | "20030220121" | "20050086309" | "20050138119" |	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2015/03/13 11:26

		"20060148516" | "5790637" | "6473425").PN.				
S6	98	CHATURVEDI-SIVAKUMAR-$.in. CHATURVEDI-SIVAKUMAR.in. GUNDABATHULA-SATISH.in. GUNDABATHULA-SATISH-$.in. HIREMATH-RASHMI.in. HIREMATH-RASHMI-$.in.	US-PGPUB; USPAT; EPO; JPO	OR	OFF	2015/03/13 12:02
S7	8533	(G06F9/54.cpc. G06F9/541.cpc. G06F9/542.cpc.) AND @ad<"20130911"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2015/03/13 15:56
S8	9338	(G06F9/54.cpc. G06F9/541.cpc. G06F9/542.cpc. G06F9/44526.cpc.) AND @ad<"20130911"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2015/03/13 15:59
S9	1053	plug-in AND (G06F9/54.cpc. G06F9/541.cpc. G06F9/542.cpc. G06F9/44526.cpc.) AND @ad<"20130911"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2015/03/13 16:14
S10	60	S8 AND ((plug-in plugin plug ADJ in addon add-on add ADJ on addin add-in add ADJ in extension) WITH (verify verifies verifying verified verification check checks checking checked determine determines determining determined) WITH (authority authorize authorizes authorizing authorized approve approves approving approved approval allow allows allowing allowed allowance ok okeys oking oked okes ok-ed ok-ing)) AND @ad<"20130911"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2015/03/13 16:21
S11	9338	(G06F9/54.cpc. G06F9/541.cpc. G06F9/542.cpc. G06F9/44526.cpc.) AND @ad<"20130911"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2015/03/13 16:50
S12	60	S11 AND ((plug-in plugin plug ADJ in addon add-on add ADJ on addin add-in add ADJ in extension) WITH (verify verifies verifying verified verification check checks checking checked determine determines determining determined) WITH (authority authorize authorizes authorizing authorized approve approves approving approved approval allow allows allowing allowed allowance ok okeys oking oked okes ok-ed ok-ing)) AND @ad<"20130911"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2015/03/13 16:50
S13	6	S11 AND ((plug-in plugin plug ADJ in addon add-on add ADJ on addin add-in add ADJ in extension) WITH (verify verifies verifying verified verification check checks checking checked determine determines determining determined) WITH (authority authorize authorizes authorizing authorized approve approves approving approved	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/03/13 16:50

		approval allow allows allowing allowed allowance ok okeys oking oked okes ok-ed ok-ing)) AND @ad<"20130911" NOT S12				
S14	34	S11 AND ((plug-in plugin plug ADJ in addon add-on add ADJ on addin add-in add ADJ in extension) WITH (verify verifies verifying verified verification check checks checking checked determine determines determining determined) WITH (authority authorize authorizes authorizing authorized approve approves approving approved approval allow allows allowing allowed allowance ok okeys oking oked okes ok-ed ok-ing able capable permission clearence)) AND @ad<"20130911" NOT S12	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/03/13 16:58
S15	9352	(G06F9/54.cpc. G06F9/541.cpc. G06F9/542.cpc. G06F9/44526.cpc.) AND @ad<"20130911"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2015/03/14 10:41
S16	60	S15 AND ((plug-in plugin plug ADJ in addon add-on add ADJ on addin add-in add ADJ in extension) WITH (verify verifies verifying verified verification check checks checking checked determine determines determining determined) WITH (authority authorize authorizes authorizing authorized approve approves approving approved approval allow allows allowing allowed allowance ok okeys oking oked okes ok-ed ok-ing)) AND @ad<"20130911"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2015/03/14 10:41
S17	5569	((plug-in plugin plug ADJ in addon add-on add ADJ on addin add-in add ADJ in extension) WITH (verify verifies verifying verified verification check checks checking checked determine determines determining determined) WITH (authority authorize authorizes authorizing authorized approve approves approving approved approval allow allows allowing allowed allowance ok okeys oking oked okes ok-ed ok-ing able capable permission clearence)) AND @ad<"20130911" NOT S16	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/03/14 10:41
S18	1248	((window screen pane image display) WITH (plug-in plugin plug ADJ in addon add-on add ADJ on addin add-in add ADJ in extension)) AND((plug-in plugin plug ADJ in addon add-on add ADJ on addin add-in add ADJ in extension) WITH (verify verifies verifying verified verification check checks checking checked determine determines determining determined) WITH (authority authorize authorizes authorizing authorized approve approves approving approved approval allow allows allowing allowed allowance ok	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/03/14 10:44

		okeys oking oked okes ok-ed ok-ing able capable permission clearence)) AND @ad<"20130911" NOT S16				
S19	6	S15 AND ((plug-in plugin plug ADJ in addon add-on add ADJ on addin add-in add ADJ in extension) WITH (verify verifies verifying verified verification check checks checking checked determine determines determining determined) WITH (authority authorize authorizes authorizing authorized approve approves approving approved approval allow allows allowing allowed allowance ok okeys oking oked okes ok-ed ok-ing)) AND @ad<"20130911" NOT S16	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/03/14 10:47
S20	34	S15 AND ((plug-in plugin plug ADJ in addon add-on add ADJ on addin add-in add ADJ in extension) WITH (verify verifies verifying verified verification check checks checking checked determine determines determining determined) WITH (authority authorize authorizes authorizing authorized approve approves approving approved approval allow allows allowing allowed allowance ok okeys oking oked okes ok-ed ok-ing able capable permission clearence)) AND @ad<"20130911" NOT S16	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/03/14 10:47
S22	125	((window screen pane image display) WITH (plug-in plugin plug ADJ in addon add-on add ADJ on addin add-in add ADJ in extension) WITH (both together simultaneously "same time" concurrent concurrently simultaneous)) AND((plug-in plugin plug ADJ in addon add-on add ADJ on addin add-in add ADJ in extension) WITH (verify verifies verifying verified verification check checks checking checked determine determines determining determined) WITH (authority authorize authorizes authorizing authorized approve approves approving approved approval allow allows allowing allowed allowance ok okeys oking oked okes ok-ed ok-ing able capable permission clearence)) AND @ad<"20130911" NOT S16	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/03/14 10:57
S24	1	((window screen pane image display) WITH (function ADJ block plug-in plugin plug ADJ in addon add-on add ADJ on addin add-in add ADJ in extension) WITH (both together simultaneously "same time" concurrent concurrently simultaneous)) AND((function ADJ block plug-in plugin plug ADJ in addon add-on add ADJ on addin add-in add ADJ in extension) WITH (verify verifies verifying verified verification check checks checking checked determine determines determining determined) WITH (authority authorize authorizes	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/03/14 11:21

		authorizing authorized approve approves approving approved approval allow allows allowing allowed allowance ok okeys oking oked okes ok-ed ok-ing able capable permission clearence)) AND @ad<"20130911" NOT (S16 S19 S20 S22)				
S25	2	((window screen pane image display) WITH (((function program application app sub) NEAR2 (block section segment)) plug-in plugin plug ADJ in addon add-on add ADJ on addin add-in add ADJ in extension) WITH (both together simultaneously "same time" concurrent concurrently simultaneous)) AND((function ADJ block plug-in plugin plug ADJ in addon add-on add ADJ on addin add-in add ADJ in extension) WITH (verify verifies verifying verified verification check checks checking checked determine determines determining determined) WITH (authority authorize authorizes authorizing authorized approve approves approving approved approval allow allows allowing allowed allowance ok okeys oking oked okes ok-ed ok-ing able capable permission clearence)) AND @ad<"20130911" NOT (S16 S19 S20 S22 S23)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/03/14 11:24
S26	876	G06F9/44526.cpc. AND @ad<"20130911"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2015/03/14 11:27
S27	37	("20010050923" | "20020143548" | "20020156844" | "20030202480" | "20040034776" | "20040103212" | "20050130650" | "20050132009" | "20050198499" | "20050201485" | "20060168643" | "20060258289" | "20070136459" | "20070165629" | "20070206563" | "20070297430" | "20080273541" | "20090052399" | "20090240821" | "20090327516" | "20110122864" | "20110314134" | "6128283" | "7079529" | "7092385" | "7487248" | "7623476" | "20030177422" | "20050033985" | "20050091407" | "6850769" | "7304985" | "20020037000" | "20020064167" | "20030110047" | "20030172145" | "20030214955" | "20040139230" | "20040153858" | "20040268257" | "20050136911" | "20050138128" | "20060072506" | "20060120375" | "20070082671" | "20070130253" | "20110145687" | "6219638" | "6754181" | "6999575" | "7185114" | "7590758" | "7623516" | "7774495" | "20030035441" | "20030076815" | "20030217171" | "20040260952" | "20050050227" | "5442637" | "5889762" | "6343067" |	USPAT; USOCR	OR	OFF	2015/03/14 11:29

		"7080158" | "20020031212" | "20020062285" | "20030046585" | "20040052234" | "20040139228" | "20040267527" | "20050187781" | "20060121902" | "20060171534" | "20060187926" | "20070253435" | "20080032695" | "20080168440" | "20090055473" | "20100049980" | "20100107205" | "20100312897" | "20110099612" | "20120263144" | "6141687" | "6898413" | "7010109" | "7345999" | "7457279" | "7542472" | "7570743" | "8065418" | "20020080719" | "20020176404" | "20030031210" | "20030115251" | "20070016921" | "6836765" | "20020042769" | "20020124096" | "20030009565" | "20030043764" | "20030105812" | "20040128554" | "20050004982" | "20050120073" | "20050220017" | "20060062180" | "20060182100" | "20060205436" | "20070019545" | "20080091813" | "20080130639" | "20090003322" | "20090156217" | "20090234967" | "20090257433" | "20100011108" | "20100011111" | "20100279670" | "20100299150" | "20100299313" | "7346044" | "7353252" | "7574523" | "7656870" | "20020087887" | "20020120757" | "20020184310" | "20030046056" | "20030163697" | "20040034793" | "20050195802" | "20070110043" | "20080320096" | "6987756" | "7184415" | "7272377" | "7412374" | "7477282" | "7512652" | "20020097150" | "20020152325" | "20030088676" | "20030126213" | "20030158722" | "20030163525").PN.				
S28	36	("20030187650" | "20040024879" | "20040068567" | "20040203834" | "20040240399" | "20050071481" | "20050143105" | "20050246193" | "20060002355" | "20060069775" | "20060203750" | "20070025270" | "20070190987" | "20070260359" | "20080123685" | "20080250408" | "20100077023" | "6963555" | "6975718" | "7006508" | "7013155" | "7564843" | "7782866" | "20040100973" | "20040158471" | "20040162871" | "20040228279" | "20040267938" | "20050008024" | "20050286519" | "20080192756" | "6766373" | "7613171" | "20020173303" | "20030078858" | "20030212772" | "20040005877" | "20040249953" | "20050033843" | "20050105524" | "20050270992" | "20070078785" | "20070111794" | "20070239892" | "20080019285" | "20080080392" | "20090136016" | "6298129" | "6360196" | "6826613" | "7117526" | "7302496" | "7664495" | "7778187" | "8009586" | "20020166053"	USPAT; USOCR	OR	OFF	2015/03/14 11:29

		| "20030044020" | "20030072485" | "20030174707" | "20050119005" | "20050249196" | "20090192976" | "6999932" | "7353255" | "20020150110" | "20040039781" | "20040044517" | "20040062267" | "20040148434" | "20040213184" | "20050015502" | "20050144288" | "20050201357" | "20060195402" | "20060218624" | "20060230166" | "20070116224" | "20070274276" | "20080005328" | "20090182815" | "20100312832" | "20110040836" | "5761309" | "6202084" | "6389016" | "6438376" | "6741691" | "6940826" | "7769881" | "20030137939" | "20040139225" | "20060183476" | "20060246903" | "20080069105" | "6031818" | "6311150" | "6574668" | "6842460" | "20020038282" | "20030061025" | "20030061481" | "20030135569" | "20030177186" | "20030217318" | "20030229715" | "20040133689" | "20040143678" | "20050187957" | "20050208947" | "20050254440" | "20060121986" | "20060165029" | "20080235362" | "20080235511" | "20090006076" | "20090088150" | "20090300673" | "20100223047" | "5818447" | "6161082" | "6912278" | "7123710" | "7917584" | "20020178087" | "20030220121" | "20050086309" | "20050138119" | "20060148516" | "5790637" | "6473425").PN.				
S29	304	("20010050923" | "20020143548" | "20020156844" | "20030202480" | "20040034776" | "20040103212" | "20050130650" | "20050132009" | "20050198499" | "20050201485" | "20060168643" | "20060258289" | "20070136459" | "20070165629" | "20070206563" | "20070297430" | "20080273541" | "20090052399" | "20090240821" | "20090327516" | "20110122864" | "20110314134" | "6128283" | "7079529" | "7092385" | "7487248" | "7623476" | "20030177422" | "20050033985" | "20050091407" | "6850769" | "7304985" | "20020037000" | "20020064167" | "20030110047" | "20030172145" | "20030214955" | "20040139230" | "20040153858" | "20040268257" | "20050136911" | "20050138128" | "20060072506" | "20060120375" | "20070082671" | "20070130253" | "20110145687" | "6219638" | "6754181" | "6999575" | "7185114" | "7590758" | "7623516" | "7774495" | "20030035441" | "20030076815" | "20030217171" | "20040260952" | "20050050227" | "5442637" | "5889762" | "6343067" | "7080158" | "20020031212" | "20020062285" | "20030046585" |	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2015/03/14 11:29

		"20040052234" | "20040139228" | "20040267527" | "20050187781" | "20060121902" | "20060171534" | "20060187926" | "20070253435" | "20080032695" | "20080168440" | "20090055473" | "20100049980" | "20100107205" | "20100312897" | "20110099612" | "20120263144" | "6141687" | "6898413" | "7010109" | "7345999" | "7457279" | "7542472" | "7570743" | "8065418" | "20020080719" | "20020176404" | "20030031210" | "20030115251" | "20070016921" | "6836765" | "20020042769" | "20020124096" | "20030009565" | "20030043764" | "20030105812" | "20040128554" | "20050004982" | "20050120073" | "20050220017" | "20060062180" | "20060182100" | "20060205436" | "20070019545" | "20080091813" | "20080130639" | "20090003322" | "20090156217" | "20090234967" | "20090257433" | "20100011108" | "20100011111" | "20100279670" | "20100299150" | "20100299313" | "7346044" | "7353252" | "7574523" | "7656870" | "20020087887" | "20020120757" | "20020184310" | "20030046056" | "20030163697" | "20040034793" | "20050195802" | "20070110043" | "20080320096" | "6987756" | "7184415" | "7272377" | "7412374" | "7477282" | "7512652" | "20020097150" | "20020152325" | "20030088676" | "20030126213" | "20030158722" | "20030163525").PN.				
S30	36	("20030187650" | "20040024879" | "20040068567" | "20040203834" | "20040240399" | "20050071481" | "20050143105" | "20050246193" | "20060002355" | "20060069775" | "20060203750" | "20070025270" | "20070190987" | "20070260359" | "20080123685" | "20080250408" | "20100077023" | "6963555" | "6975718" | "7006508" | "7013155" | "7564843" | "7782866" | "20040100973" | "20040158471" | "20040162871" | "20040228279" | "20040267938" | "20050008024" | "20050286519" | "20080192756" | "6766373" | "7613171" | "20020173303" | "20030078858" | "20030212772" | "20040005877" | "20040249953" | "20050033843" | "20050105524" | "20050270992" | "20070078785" | "20070111794" | "20070239892" | "20080019285" | "20080080392" | "20090136016" | "6298129" | "6360196" | "6826613" | "7117526" | "7302496" | "7664495" | "7778187" | "8009586" | "20020166053" | "20030044020" | "20030072485" | "20030174707" | "20050119005" |	USPAT; USOCR	OR	OFF	2015/03/14 11:29

		"20050249196" | "20090192976" | "6999932" | "7353255" | "20020150110" | "20040039781" | "20040044517" | "20040062267" | "20040148434" | "20040213184" | "20050015502" | "20050144288" | "20050201357" | "20060195402" | "20060218624" | "20060230166" | "20070116224" | "20070274276" | "20080005328" | "20090182815" | "20100312832" | "20110040836" | "5761309" | "6202084" | "6389016" | "6438376" | "6741691" | "6940826" | "7769881" | "20030137939" | "20040139225" | "20060183476" | "20060246903" | "20080069105" | "6031818" | "6311150" | "6574668" | "6842460" | "20020038282" | "20030061025" | "20030061481" | "20030135569" | "20030177186" | "20030217318" | "20030229715" | "20040133689" | "20040143678" | "20050187957" | "20050208947" | "20050254440" | "20060121986" | "20060165029" | "20080235362" | "20080235511" | "20090006076" | "20090088150" | "20090300673" | "20100223047" | "5818447" | "6161082" | "6912278" | "7123710" | "7917584" | "20020178087" | "20030220121" | "20050086309" | "20050138119" | "20060148516" | "5790637" | "6473425").PN.				
S31	268	("20030187650" | "20040024879" | "20040068567" | "20040203834" | "20040240399" | "20050071481" | "20050143105" | "20050246193" | "20060002355" | "20060069775" | "20060203750" | "20070025270" | "20070190987" | "20070260359" | "20080123685" | "20080250408" | "20100077023" | "6963555" | "6975718" | "7006508" | "7013155" | "7564843" | "7782866" | "20040100973" | "20040158471" | "20040162871" | "20040228279" | "20040267938" | "20050008024" | "20050286519" | "20080192756" | "6766373" | "7613171" | "20020173303" | "20030078858" | "20030212772" | "20040005877" | "20040249953" | "20050033843" | "20050105524" | "20050270992" | "20070078785" | "20070111794" | "20070239892" | "20080019285" | "20080080392" | "20090136016" | "6298129" | "6360196" | "6826613" | "7117526" | "7302496" | "7664495" | "7778187" | "8009586" | "20020166053" | "20030044020" | "20030072485" | "20030174707" | "20050119005" | "20050249196" | "20090192976" | "6999932" | "7353255" | "20020150110" | "20040039781" | "20040044517" | "20040062267" | "20040148434" | "20040213184" | "20050015502" |	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2015/03/14 11:29

		"20050144288" | "20050201357" | "20060195402" | "20060218624" | "20060230166" | "20070116224" | "20070274276" | "20080005328" | "20090182815" | "20100312832" | "20110040836" | "5761309" | "6202084" | "6389016" | "6438376" | "6741691" | "6940826" | "7769881" | "20030137939" | "20040139225" | "20060183476" | "20060246903" | "20080069105" | "6031818" | "6311150" | "6574668" | "6842460" | "20020038282" | "20030061025" | "20030061481" | "20030135569" | "20030177186" | "20030217318" | "20030229715" | "20040133689" | "20040143678" | "20050187957" | "20050208947" | "20050254440" | "20060121986" | "20060165029" | "20080235362" | "20080235511" | "20090006076" | "20090088150" | "20090300673" | "20100223047" | "5818447" | "6161082" | "6912278" | "7123710" | "7917584" | "20020178087" | "20030220121" | "20050086309" | "20050138119" | "20060148516" | "5790637" | "6473425").PN.				
S32	375	S26 AND (mobile cell cellular phone iphone) NOT (S16 S19 S20 S22 S24 S25 S27 S28 S29 S30 S31)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2015/03/14 11:29
S36	10617	(G06F9/54.cpc. G06F9/541.cpc. G06F9/542.cpc. G06F9/44526.cpc.) AND @ad<"20130911"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2015/12/30 09:19
S37	66	S36 AND ((plug-in plugin plug ADJ in addon add-on add ADJ on addin add-in add ADJ in extension) WITH (verify verifies verifying verified verification check checks checking checked determine determines determining determined) WITH (authority authorize authorizes authorizing authorized approve approves approving approved approval allow allows allowing allowed allowance ok okeys oking oked okes ok-ed ok-ing)) AND @ad<"20130911"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2015/12/30 09:19
S38	66	S37	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2015/12/30 09:19
S39	6	S36 AND ((plug-in plugin plug ADJ in addon add-on add ADJ on addin add-in add ADJ in extension) WITH (verify verifies verifying verified verification check checks checking checked determine determines determining determined) WITH (authority authorize authorizes authorizing authorized approve approves approving approved	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/12/30 09:24

		approval allow allows allowing allowed allowance ok okeys oking oked okes ok-ed ok-ing)) AND @ad<"20130911" NOT S37				
S40	6	S39	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2015/12/30 09:24
S41	37	S36 AND ((plug-in plugin plug ADJ in addon add-on add ADJ on addin add-in add ADJ in extension) WITH (verify verifies verifying verified verification check checks checking checked determine determines determining determined) WITH (authority authorize authorizes authorizing authorized approve approves approving approved approval allow allows allowing allowed allowance ok okeys oking oked okes ok-ed ok-ing able capable permission clearence)) AND @ad<"20130911" NOT S37	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/12/30 09:25
S42	37	S41	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2015/12/30 09:25
S43	132	((window screen pane image display) WITH (plug-in plugin plug ADJ in addon add-on add ADJ on addin add-in add ADJ in extension) WITH (both together simultaneously "same time" concurrent concurrently simultaneous)) AND((plug-in plugin plug ADJ in addon add-on add ADJ on addin add-in add ADJ in extension) WITH (verify verifies verifying verified verification check checks checking checked determine determines determining determined) WITH (authority authorize authorizes authorizing authorized approve approves approving approved approval allow allows allowing allowed allowance ok okeys oking oked okes ok-ed ok-ing able capable permission clearence)) AND @ad<"20130911" NOT S37	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/12/30 09:29
S44	132	S43	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2015/12/30 09:29
S45	1	((window screen pane image display) WITH (function ADJ block plug-in plugin plug ADJ in addon add-on add ADJ on addin add-in add ADJ in extension) WITH (both together simultaneously "same time" concurrent concurrently simultaneous)) AND((function ADJ block plug-in plugin plug ADJ in addon add-on add ADJ on addin add-in add ADJ in extension) WITH (verify verifies verifying verified verification check checks checking checked determine determines determining determined)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/12/30 09:30

		WITH (authority authorize authorizes authorizing authorized approve approves approving approved approval allow allows allowing allowed allowance ok okeys oking oked okes ok-ed ok-ing able capable permission clearence)) AND @ad<"20130911" NOT (S37 S39 S41 S43)				
S46	1	S45	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2015/12/30 09:30
S47	133	((window screen pane image display) WITH (function ADJ block plug-in plugin plug ADJ in addon add-on add ADJ on addin add-in add ADJ in extension) WITH (both together simultaneously "same time" concurrent concurrently simultaneous)) AND((function ADJ block plug-in plugin plug ADJ in addon add-on add ADJ on addin add-in add ADJ in extension) WITH (verify verifies verifying verified verification check checks checking checked determine determines determining determined) WITH (authority authorize authorizes authorizing authorized approve approves approving approved approval allow allows allowing allowed allowance ok okeys oking oked okes ok-ed ok-ing able capable permission clearence)) AND @ad<"20130911" NOT S37	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/12/30 09:31
S48	3	((window screen pane image display) WITH (((function program application app sub) NEAR2 (block section segment)) plug-in plugin plug ADJ in addon add-on add ADJ on addin add-in add ADJ in extension) WITH (both together simultaneously "same time" concurrent concurrently simultaneous)) AND((function ADJ block plug-in plugin plug ADJ in addon add-on add ADJ on addin add-in add ADJ in extension) WITH (verify verifies verifying verified verification check checks checking checked determine determines determining determined) WITH (authority authorize authorizes authorizing authorized approve approves approving approved approval allow allows allowing allowed allowance ok okeys oking oked okes ok-ed ok-ing able capable permission clearence)) AND @ad<"20130911" NOT (S37 S39 S41 S43 S47)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/12/30 09:31
S49	3	S48	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2015/12/30 09:31
S50	266	("20030187650" | "20040024879" | "20040068567" | "20040203834" | "20040240399" | "20050071481" |	US-PGPUB; USPAT; USOCR;	OR	OFF	2015/12/30 09:33

		"20050143105" | "20050246193" | "20060002355" | "20060069775" | "20060203750" | "20070025270" | "20070190987" | "20070260359" | "20080123685" | "20080250408" | "20100077023" | "6963555" | "6975718" | "7006508" | "7013155" | "7564843" | "7782866" | "20040100973" | "20040158471" | "20040162871" | "20040228279" | "20040267938" | "20050008024" | "20050286519" | "20080192756" | "6766373" | "7613171" | "20020173303" | "20030078858" | "20030212772" | "20040005877" | "20040249953" | "20050033843" | "20050105524" | "20050270992" | "20070078785" | "20070111794" | "20070239892" | "20080019285" | "20080080392" | "20090136016" | "6298129" | "6360196" | "6826613" | "7117526" | "7302496" | "7664495" | "7778187" | "8009586" | "20020166053" | "20030044020" | "20030072485" | "20030174707" | "20050119005" | "20050249196" | "20090192976" | "6999932" | "7353255" | "20020150110" | "20040039781" | "20040044517" | "20040062267" | "20040148434" | "20040213184" | "20050015502" | "20050144288" | "20050201357" | "20060195402" | "20060218624" | "20060230166" | "20070116224" | "20070274276" | "20080005328" | "20090182815" | "20100312832" | "20110040836" | "5761309" | "6202084" | "6389016" | "6438376" | "6741691" | "6940826" | "7769881" | "20030137939" | "20040139225" | "20060183476" | "20060246903" | "20080069105" | "6031818" | "6311150" | "6574668" | "6842460" | "20020038282" | "20030061025" | "20030061481" | "20030135569" | "20030177186" | "20030217318" | "20030229715" | "20040133689" | "20040143678" | "20050187957" | "20050208947" | "20050254440" | "20060121986" | "20060165029" | "20080235362" | "20080235511" | "20090006076" | "20090088150" | "20090300673" | "20100223047" | "5818447" | "6161082" | "6912278" | "7123710" | "7917584" | "20020178087" | "20030220121" | "20050086309" | "20050138119" | "20060148516" | "5790637" | "6473425").PN.	EPO; JPO; DERWENT; IBM_TDB			
S51	266	S50	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2015/12/30 09:33
S52	1021	G06F9/44526.cpc. AND @ad<"20130911"	US-PGPUB; USPAT; EPO; JPO; DERWENT;	OR	OFF	2015/12/30 09:58

			IBM_TDB			
S53	37	("20010050923" | "20020143548" | "20020156844" | "20030202480" | "20040034776" | "20040103212" | "20050130650" | "20050132009" | "20050198499" | "20050201485" | "20060168643" | "20060258289" | "20070136459" | "20070165629" | "20070206563" | "20070297430" | "20080273541" | "20090052399" | "20090240821" | "20090327516" | "20110122864" | "20110314134" | "6128283" | "7079529" | "7092385" | "7487248" | "7623476" | "20030177422" | "20050033985" | "20050091407" | "6850769" | "7304985" | "20020037000" | "20020064167" | "20030110047" | "20030172145" | "20030214955" | "20040139230" | "20040153858" | "20040268257" | "20050136911" | "20050138128" | "20060072506" | "20060120375" | "20070082671" | "20070130253" | "20110145687" | "6219638" | "6754181" | "6999575" | "7185114" | "7590758" | "7623516" | "7774495" | "20030035441" | "20030076815" | "20030217171" | "20040260952" | "20050050227" | "5442637" | "5889762" | "6343067" | "7080158" | "20020031212" | "20020062285" | "20030046585" | "20040052234" | "20040139228" | "20040267527" | "20050187781" | "20060121902" | "20060171534" | "20060187926" | "20070253435" | "20080032695" | "20080168440" | "20090055473" | "20100049980" | "20100107205" | "20100312897" | "20110099612" | "20120263144" | "6141687" | "6898413" | "7010109" | "7345999" | "7457279" | "7542472" | "7570743" | "8065418" | "20020080719" | "20020176404" | "20030031210" | "20030115251" | "20070016921" | "6836765" | "20020042769" | "20020124096" | "20030009565" | "20030043764" | "20030105812" | "20040128554" | "20050004982" | "20050120073" | "20050220017" | "20060062180" | "20060182100" | "20060205436" | "20070019545" | "20080091813" | "20080130639" | "20090003322" | "20090156217" | "20090234967" | "20090257433" | "20100011108" | "20100011111" | "20100279670" | "20100299150" | "20100299313" | "7346044" | "7353252" | "7574523" | "7656870" | "20020087887" | "20020120757" | "20020184310" | "20030046056" | "20030163697" | "20040034793" | "20050195802" | "20070110043" | "20080320096" | "6987756" | "7184415" | "7272377" | "7412374" | "7477282" |	USPAT; USOCR	OR	OFF	2015/12/30 09:58

		"7512652" | "20020097150" | "20020152325" | "20030088676" | "20030126213" | "20030158722" | "20030163525").PN.				
S54	36	("20030187650" | "20040024879" | "20040068567" | "20040203834" | "20040240399" | "20050071481" | "20050143105" | "20050246193" | "20060002355" | "20060069775" | "20060203750" | "20070025270" | "20070190987" | "20070260359" | "20080123685" | "20080250408" | "20100077023" | "6963555" | "6975718" | "7006508" | "7013155" | "7564843" | "7782866" | "20040100973" | "20040158471" | "20040162871" | "20040228279" | "20040267938" | "20050008024" | "20050286519" | "20080192756" | "6766373" | "7613171" | "20020173303" | "20030078858" | "20030212772" | "20040005877" | "20040249953" | "20050033843" | "20050105524" | "20050270992" | "20070078785" | "20070111794" | "20070239892" | "20080019285" | "20080080392" | "20090136016" | "6298129" | "6360196" | "6826613" | "7117526" | "7302496" | "7664495" | "7778187" | "8009586" | "20020166053" | "20030044020" | "20030072485" | "20030174707" | "20050119005" | "20050249196" | "20090192976" | "6999932" | "7353255" | "20020150110" | "20040039781" | "20040044517" | "20040062267" | "20040148434" | "20040213184" | "20050015502" | "20050144288" | "20050201357" | "20060195402" | "20060218624" | "20060230166" | "20070116224" | "20070274276" | "20080005328" | "20090182815" | "20100312832" | "20110040836" | "5761309" | "6202084" | "6389016" | "6438376" | "6741691" | "6940826" | "7769881" | "20030137939" | "20040139225" | "20060183476" | "20060246903" | "20080069105" | "6031818" | "6311150" | "6574668" | "6842460" | "20020038282" | "20030061025" | "20030061481" | "20030135569" | "20030177186" | "20030217318" | "20030229715" | "20040133689" | "20040143678" | "20050187957" | "20050208947" | "20050254440" | "20060121986" | "20060165029" | "20080235362" | "20080235511" | "20090006076" | "20090088150" | "20090300673" | "20100223047" | "5818447" | "6161082" | "6912278" | "7123710" | "7917584" | "20020178087" | "20030220121" | "20050086309" | "20050138119" | "20060148516" | "5790637" | "6473425").PN.	USPAT; USOCR	OR	OFF	2015/12/30 09:58
S55	300	("20010050923" | "20020143548" |	US-PGPUB;	OR	OFF	2015/12/30

		"20020156844" | "20030202480" | "20040034776" | "20040103212" | "20050130650" | "20050132009" | "20050198499" | "20050201485" | "20060168643" | "20060258289" | "20070136459" | "20070165629" | "20070206563" | "20070297430" | "20080273541" | "20090052399" | "20090240821" | "20090327516" | "20110122864" | "20110314134" | "6128283" | "7079529" | "7092385" | "7487248" | "7623476" | "20030177422" | "20050033985" | "20050091407" | "6850769" | "7304985" | "20020037000" | "20020064167" | "20030110047" | "20030172145" | "20030214955" | "20040139230" | "20040153858" | "20040268257" | "20050136911" | "20050138128" | "20060072506" | "20060120375" | "20070082671" | "20070130253" | "20110145687" | "6219638" | "6754181" | "6999575" | "7185114" | "7590758" | "7623516" | "7774495" | "20030035441" | "20030076815" | "20030217171" | "20040260952" | "20050050227" | "5442637" | "5889762" | "6343067" | "7080158" | "20020031212" | "20020062285" | "20030046585" | "20040052234" | "20040139228" | "20040267527" | "20050187781" | "20060121902" | "20060171534" | "20060187926" | "20070253435" | "20080032695" | "20080168440" | "20090055473" | "20100049980" | "20100107205" | "20100312897" | "20110099612" | "20120263144" | "6141687" | "6898413" | "7010109" | "7345999" | "7457279" | "7542472" | "7570743" | "8065418" | "20020080719" | "20020176404" | "20030031210" | "20030115251" | "20070016921" | "6836765" | "20020042769" | "20020124096" | "20030009565" | "20030043764" | "20030105812" | "20040128554" | "20050004982" | "20050120073" | "20050220017" | "20060062180" | "20060182100" | "20060205436" | "20070019545" | "20080091813" | "20080130639" | "20090003322" | "20090156217" | "20090234967" | "20090257433" | "20100011108" | "20100011111" | "20100279670" | "20100299150" | "20100299313" | "7346044" | "7353252" | "7574523" | "7656870" | "20020087887" | "20020120757" | "20020184310" | "20030046056" | "20030163697" | "20040034793" | "20050195802" | "20070110043" | "20080320096" | "6987756" | "7184415" | "7272377" | "7412374" | "7477282" | "7512652" | "20020097150" | "20020152325" | "20030088676" |	USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB			09:58

		"20030126213" | "20030158722" | "20030163525").PN.				
S56	36	("20030187650" | "20040024879" | "20040068567" | "20040203834" | "20040240399" | "20050071481" | "20050143105" | "20050246193" | "20060002355" | "20060069775" | "20060203750" | "20070025270" | "20070190987" | "20070260359" | "20080123685" | "20080250408" | "20100077023" | "6963555" | "6975718" | "7006508" | "7013155" | "7564843" | "7782866" | "20040100973" | "20040158471" | "20040162871" | "20040228279" | "20040267938" | "20050008024" | "20050286519" | "20080192756" | "6766373" | "7613171" | "20020173303" | "20030078858" | "20030212772" | "20040005877" | "20040249953" | "20050033843" | "20050105524" | "20050270992" | "20070078785" | "20070111794" | "20070239892" | "20080019285" | "20080080392" | "20090136016" | "6298129" | "6360196" | "6826613" | "7117526" | "7302496" | "7664495" | "7778187" | "8009586" | "20020166053" | "20030044020" | "20030072485" | "20030174707" | "20050119005" | "20050249196" | "20090192976" | "6999932" | "7353255" | "20020150110" | "20040039781" | "20040044517" | "20040062267" | "20040148434" | "20040213184" | "20050015502" | "20050144288" | "20050201357" | "20060195402" | "20060218624" | "20060230166" | "20070116224" | "20070274276" | "20080005328" | "20090182815" | "20100312832" | "20110040836" | "5761309" | "6202084" | "6389016" | "6438376" | "6741691" | "6940826" | "7769881" | "20030137939" | "20040139225" | "20060183476" | "20060246903" | "20080069105" | "6031818" | "6311150" | "6574668" | "6842460" | "20020038282" | "20030061025" | "20030061481" | "20030135569" | "20030177186" | "20030217318" | "20030229715" | "20040133689" | "20040143678" | "20050187957" | "20050208947" | "20050254440" | "20060121986" | "20060165029" | "20080235362" | "20080235511" | "20090006076" | "20090088150" | "20090300673" | "20100223047" | "5818447" | "6161082" | "6912278" | "7123710" | "7917584" | "20020178087" | "20030220121" | "20050086309" | "20050138119" | "20060148516" | "5790637" | "6473425").PN.	USPAT; USOCR	OR	OFF	2015/12/30 09:58
S57	438	S52 AND (mobile cell cellular phone iphone) NOT (S37 S39 S41 S43 S45 S48 S53 S54 S55 S56 S50)	US-PGPUB; USPAT; EPO; JPO;	OR	OFF	2015/12/30 09:58

			DERWENT; IBM_TDB			
S58	438	S57	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2015/12/30 09:58
S59	0	S36 AND without NEAR5 (switch switches switching switched swap swaps swapping swapped change changes changing changed move moves moving moved) WITH (superblock super-block super ADJ block function ADJ block function-block functionblock funblock program-block program ADJ block application ADJ block appblock app-block application-block)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2015/12/30 10:19
S60	273	without WITH (switch switches switching switched swap swaps swapping swapped change changes changing changed move moves moving moved) WITH (superblock super-block super ADJ block function ADJ block function-block functionblock funblock program-block program ADJ block application ADJ block appblock app-block application-block)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2015/12/30 10:20
S61	201	(instead place missing skipping) WITH (switch switches switching switched swap swaps swapping swapped change changes changing changed move moves moving moved) WITH (superblock super-block super ADJ block function ADJ block function-block functionblock funblock program-block program ADJ block application ADJ block appblock app-block application-block) AND @ad<"20130911"	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2015/12/30 10:40
S62	52840	(without instead place missing skipping) WITH (switch switches switching switched swap swaps swapping swapped change changes changing changed move moves moving moved) WITH (code ADJ block code-block code ADJ section code-section layer) AND @ad<"20130911" NOT (S60 S61)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2015/12/30 10:58
S63	39452	(without) WITH (switch switches switching switched swap swaps swapping swapped change changes changing changed move moves moving moved) WITH (code ADJ block code-block code ADJ section code-section layer) AND @ad<"20130911" NOT (S60 S61)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2015/12/30 10:58
S64	12	(without) NEAR2 (context NEAR1 (switch switches switching switched swap swaps swapping swapped change changes changing changed move moves moving moved)) WITH (code ADJ block code-block code ADJ section code-section layer) AND @ad<"20130911" NOT (S60 S61)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2015/12/30 10:59
S65	39	(without instead place missing skipping)	US-PGPUB;	OR	ON	2015/12/30

		WITH (context NEAR1 (switch switches switching switched swap swaps swapping swapped change changes changing changed move moves moving moved)) WITH (code ADJ block code-block code ADJ section code-section layer) AND @ad<"20130911" NOT (S60 S61)	US-PGPUB; USPAT; EPO; JPO; DERWENT			11:02
S66	27	(without instead place missing skipping) WITH (context NEAR1 (switch switches switching switched swap swaps swapping swapped change changes changing changed move moves moving moved)) WITH (code ADJ block code-block code ADJ section code-section layer) AND @ad<"20130911" NOT (S60 S61 S64)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2015/12/30 11:02
S67	5	(without instead place missing skipping) WITH (context NEAR3 (switch switches switching switched swap swaps swapping swapped change changes changing changed move moves moving moved)) WITH (code ADJ block code-block code ADJ section code-section layer) AND @ad<"20130911" NOT (S60 S61 S64 S66)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2015/12/30 11:08
S68	29	(without instead place missing skipping) WITH (context NEAR5 (switch switches switching switched swap swaps swapping swapped change changes changing changed move moves moving moved)) WITH (code ADJ block code-block code ADJ section code-section layer) AND @ad<"20130911" NOT (S60 S61 S64 S66 S67)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2015/12/30 11:16
S69	109	CHATURVEDI-SIVAKUMAR.in. GUNDABATHULA-SATISH.in. HIREMATH-RASHMI.in. CHATURVEDI-SIVAKUMAR-$.in. GUNDABATHULA-SATISH-$.in. HIREMATH-RASHMI-$.in.	US-PGPUB; USPAT	OR	ON	2015/12/30 13:08
S70	4	without ADJ switching NEAR3 context WITH superblock	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/01/03 11:20
S71	3	establishing WITH function WITH block WITH superblock	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/01/03 11:21
S72	11000	(G06F9/54.cpc. G06F9/541.cpc. G06F9/542.cpc. G06F9/44526.cpc.) AND @ad<"20130911"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/06/03 16:19
S73	67	S72 AND ((plug-in plugin plug ADJ in addon add-on add ADJ on addin add-in add ADJ in extension) WITH (verify verifies verifying verified verification check checks checking checked determine determines determining determined) WITH (authority authorize authorizes authorizing authorized	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/06/03 16:19

		approve approves approving approved approval allow allows allowing allowed allowance ok okeys oking oked okes ok-ed ok-ing)) AND @ad<"20130911"				
S74	67	S73	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/06/03 16:19
S75	67	S74	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/06/03 16:19
S76	6	S72 AND ((plug-in plugin plug ADJ in addon add-on add ADJ on addin add-in add ADJ in extension) WITH (verify verifies verifying verified verification check checks checking checked determine determines determining determined) WITH (authority authorize authorizes authorizing authorized approve approves approving approved approval allow allows allowing allowed allowance ok okeys oking oked okes ok-ed ok-ing)) AND @ad<"20130911" NOT S73	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/06/03 16:19
S77	6	S76	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/06/03 16:19
S78	6	S77	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/06/03 16:19
S79	37	S72 AND ((plug-in plugin plug ADJ in addon add-on add ADJ on addin add-in add ADJ in extension) WITH (verify verifies verifying verified verification check checks checking checked determine determines determining determined) WITH (authority authorize authorizes authorizing authorized approve approves approving approved approval allow allows allowing allowed allowance ok okeys oking oked okes ok-ed ok-ing able capable permission clearence)) AND @ad<"20130911" NOT S73	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/06/03 16:20
S80	37	S79	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/06/03 16:20
S81	37	S80	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/06/03 16:20
S82	133	((window screen pane image display) WITH (plug-in plugin plug ADJ in addon add-on add ADJ on addin add-in add ADJ	US-PGPUB; USPAT; EPO; JPO;	OR	ON	2016/06/03 16:20

		in extension) WITH (both together simultaneously "same time" concurrent concurrently simultaneous)) AND((plug-in plugin plug ADJ in addon add-on add ADJ on addin add-in add ADJ in extension) WITH (verify verifies verifying verified verification check checks checking checked determine determines determining determined) WITH (authority authorize authorizes authorizing authorized approve approves approving approved approval allow allows allowing allowed allowance ok okeys oking oked okes ok-ed ok-ing able capable permission clearence)) AND @ad<"20130911" NOT S73	DERWENT; IBM_TDB			
S83	133	S82	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/06/03 16:20
S84	133	S83	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/06/03 16:20
S85	1	((window screen pane image display) WITH (function ADJ block plug-in plugin plug ADJ in addon add-on add ADJ on addin add-in add ADJ in extension) WITH (both together simultaneously "same time" concurrent concurrently simultaneous)) AND((function ADJ block plug-in plugin plug ADJ in addon add-on add ADJ on addin add-in add ADJ in extension) WITH (verify verifies verifying verified verification check checks checking checked determine determines determining determined) WITH (authority authorize authorizes authorizing authorized approve approves approving approved approval allow allows allowing allowed allowance ok okeys oking oked okes ok-ed ok-ing able capable permission clearence)) AND @ad<"20130911" NOT (S73 S76 S79 S82)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/06/03 16:21
S86	1	S85	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/06/03 16:21
S87	1	S86	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/06/03 16:21
S88	134	((window screen pane image display) WITH (function ADJ block plug-in plugin plug ADJ in addon add-on add ADJ on addin add-in add ADJ in extension) WITH (both together simultaneously "same time" concurrent concurrently simultaneous)) AND((function ADJ	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/06/03 16:23

		block plug-in plugin plug ADJ in addon add-on add ADJ on addin add-in add ADJ in extension) WITH (verify verifies verifying verified verification check checks checking checked determine determines determining determined) WITH (authority authorize authorizes authorizing authorized approve approves approving approved approval allow allows allowing allowed allowance ok okeys oking oked okes ok-ed ok-ing able capable permission clearence)) AND @ad<"20130911" NOT S73				
S89	3	((window screen pane image display) WITH (((function program application app sub) NEAR2 (block section segment)) plug-in plugin plug ADJ in addon add-on add ADJ on addin add-in add ADJ in extension) WITH (both together simultaneously "same time" concurrent concurrently simultaneous)) AND((function ADJ block plug-in plugin plug ADJ in addon add-on add ADJ on addin add-in add ADJ in extension) WITH (verify verifies verifying verified verification check checks checking checked determine determines determining determined) WITH (authority authorize authorizes authorizing authorized approve approves approving approved approval allow allows allowing allowed allowance ok okeys oking oked okes ok-ed ok-ing able capable permission clearence)) AND @ad<"20130911" NOT (S73 S76 S79 S82 S88)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/06/03 16:23
S90	3	S89	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/06/03 16:23
S91	3	S90	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/06/03 16:23
S92	266	("20030187650" | "20040024879" | "20040068567" | "20040203834" | "20040240399" | "20050071481" | "20050143105" | "20050246193" | "20060002355" | "20060069775" | "20060203750" | "20070025270" | "20070190987" | "20070260359" | "20080123685" | "20080250408" | "20100077023" | "6963555" | "6975718" | "7006508" | "7013155" | "7564843" | "7782866" | "20040100973" | "20040158471" | "20040162871" | "20040228279" | "20040267938" | "20050008024" | "20050286519" | "20080192756" | "6766373" | "7613171" | "20020173303" | "20030078858" | "20030212772" | "20040005877" | "20040249953" | "20050033843" |	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/06/03 16:24

		"20050105524" | "20050270992" | "20070078785" | "20070111794" | "20070239892" | "20080019285" | "20080080392" | "20090136016" | "6298129" | "6360196" | "6826613" | "7117526" | "7302496" | "7664495" | "7778187" | "8009586" | "20020166053" | "20030044020" | "20030072485" | "20030174707" | "20050119005" | "20050249196" | "20090192976" | "6999932" | "7353255" | "20020150110" | "20040039781" | "20040044517" | "20040062267" | "20040148434" | "20040213184" | "20050015502" | "20050144288" | "20050201357" | "20060195402" | "20060218624" | "20060230166" | "20070116224" | "20070274276" | "20080005328" | "20090182815" | "20100312832" | "20110040836" | "5761309" | "6202084" | "6389016" | "6438376" | "6741691" | "6940826" | "7769881" | "20030137939" | "20040139225" | "20060183476" | "20060246903" | "20080069105" | "6031818" | "6311150" | "6574668" | "6842460" | "20020038282" | "20030061025" | "20030061481" | "20030135569" | "20030177186" | "20030217318" | "20030229715" | "20040133689" | "20040143678" | "20050187957" | "20050208947" | "20050254440" | "20060121986" | "20060165029" | "20080235362" | "20080235511" | "20090006076" | "20090088150" | "20090300673" | "20100223047" | "5818447" | "6161082" | "6912278" | "7123710" | "7917584" | "20020178087" | "20030220121" | "20050086309" | "20050138119" | "20060148516" | "5790637" | "6473425").PN.				
S93	266	S92	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/06/03 16:24
S94	266	S93	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/06/03 16:24
S95	1065	G06F9/44526.cpc. AND @ad<"20130911"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/06/03 16:25
S96	37	("20010050923" | "20020143548" | "20020156844" | "20030202480" | "20040034776" | "20040103212" | "20050130650" | "20050132009" | "20050198499" | "20050201485" | "20060168643" | "20060258289" | "20070136459" | "20070165629" | "20070206563" | "20070297430" |	USPAT; USOCR	OR	OFF	2016/06/03 16:25

		"20080273541" | "20090052399" | "20090240821" | "20090327516" | "20110122864" | "20110314134" | "6128283" | "7079529" | "7092385" | "7487248" | "7623476" | "20030177422" | "20050033985" | "20050091407" | "6850769" | "7304985" | "20020037000" | "20020064167" | "20030110047" | "20030172145" | "20030214955" | "20040139230" | "20040153858" | "20040268257" | "20050136911" | "20050138128" | "20060072506" | "20060120375" | "20070082671" | "20070130253" | "20110145687" | "6219638" | "6754181" | "6999575" | "7185114" | "7590758" | "7623516" | "7774495" | "20030035441" | "20030076815" | "20030217171" | "20040260952" | "20050050227" | "5442637" | "5889762" | "6343067" | "7080158" | "20020031212" | "20020062285" | "20030046585" | "20040052234" | "20040139228" | "20040267527" | "20050187781" | "20060121902" | "20060171534" | "20060187926" | "20070253435" | "20080032695" | "20080168440" | "20090055473" | "20100049980" | "20100107205" | "20100312897" | "20110099612" | "20120263144" | "6141687" | "6898413" | "7010109" | "7345999" | "7457279" | "7542472" | "7570743" | "8065418" | "20020080719" | "20020176404" | "20030031210" | "20030115251" | "20070016921" | "6836765" | "20020042769" | "20020124096" | "20030009565" | "20030043764" | "20030105812" | "20040128554" | "20050004982" | "20050120073" | "20050220017" | "20060062180" | "20060182100" | "20060205436" | "20070019545" | "20080091813" | "20080130639" | "20090003322" | "20090156217" | "20090234967" | "20090257433" | "20100011108" | "20100011111" | "20100279670" | "20100299150" | "20100299313" | "7346044" | "7353252" | "7574523" | "7656870" | "20020087887" | "20020120757" | "20020184310" | "20030046056" | "20030163697" | "20040034793" | "20050195802" | "20070110043" | "20080320096" | "6987756" | "7184415" | "7272377" | "7412374" | "7477282" | "7512652" | "20020097150" | "20020152325" | "20030088676" | "20030126213" | "20030158722" | "20030163525").PN.				
S97	36	("20030187650" | "20040024879" | "20040068567" | "20040203834" | "20040240399" | "20050071481" | "20050143105" | "20050246193" | "20060002355" | "20060069775" |	USPAT; USOCR	OR	OFF	2016/06/03 16:25

		"20060203750" | "20070025270" | "20070190987" | "20070260359" | "20080123685" | "20080250408" | "20100077023" | "6963555" | "6975718" | "7006508" | "7013155" | "7564843" | "7782866" | "20040100973" | "20040158471" | "20040162871" | "20040228279" | "20040267938" | "20050008024" | "20050286519" | "20080192756" | "6766373" | "7613171" | "20020173303" | "20030078858" | "20030212772" | "20040005877" | "20040249953" | "20050033843" | "20050105524" | "20050270992" | "20070078785" | "20070111794" | "20070239892" | "20080019285" | "20080080392" | "20090136016" | "6298129" | "6360196" | "6826613" | "7117526" | "7302496" | "7664495" | "7778187" | "8009586" | "20020166053" | "20030044020" | "20030072485" | "20030174707" | "20050119005" | "20050249196" | "20090192976" | "6999932" | "7353255" | "20020150110" | "20040039781" | "20040044517" | "20040062267" | "20040148434" | "20040213184" | "20050015502" | "20050144288" | "20050201357" | "20060195402" | "20060218624" | "20060230166" | "20070116224" | "20070274276" | "20080005328" | "20090182815" | "20100312832" | "20110040836" | "5761309" | "6202084" | "6389016" | "6438376" | "6741691" | "6940826" | "7769881" | "20030137939" | "20040139225" | "20060183476" | "20060246903" | "20080069105" | "6031818" | "6311150" | "6574668" | "6842460" | "20020038282" | "20030061025" | "20030061481" | "20030135569" | "20030177186" | "20030217318" | "20030229715" | "20040133689" | "20040143678" | "20050187957" | "20050208947" | "20050254440" | "20060121986" | "20060165029" | "20080235362" | "20080235511" | "20090006076" | "20090088150" | "20090300673" | "20100223047" | "5818447" | "6161082" | "6912278" | "7123710" | "7917584" | "20020178087" | "20030220121" | "20050086309" | "20050138119" | "20060148516" | "5790637" | "6473425").PN.				
S98	301	("20010050923" | "20020143548" | "20020156844" | "20030202480" | "20040034776" | "20040103212" | "20050130650" | "20050132009" | "20050198499" | "20050201485" | "20060168643" | "20060258289" | "20070136459" | "20070165629" | "20070206563" | "20070297430" | "20080273541" | "20090052399" | "20090240821" | "20090327516" |	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/06/03 16:25

		"20110122864" | "20110314134" | "6128283" | "7079529" | "7092385" | "7487248" | "7623476" | "20030177422" | "20050033985" | "20050091407" | "6850769" | "7304985" | "20020037000" | "20020064167" | "20030110047" | "20030172145" | "20030214955" | "20040139230" | "20040153858" | "20040268257" | "20050136911" | "20050138128" | "20060072506" | "20060120375" | "20070082671" | "20070130253" | "20110145687" | "6219638" | "6754181" | "6999575" | "7185114" | "7590758" | "7623516" | "7774495" | "20030035441" | "20030076815" | "20030217171" | "20040260952" | "20050050227" | "5442637" | "5889762" | "6343067" | "7080158" | "20020031212" | "20020062285" | "20030046585" | "20040052234" | "20040139228" | "20040267527" | "20050187781" | "20060121902" | "20060171534" | "20060187926" | "20070253435" | "20080032695" | "20080168440" | "20090055473" | "20100049980" | "20100107205" | "20100312897" | "20110099612" | "20120263144" | "6141687" | "6898413" | "7010109" | "7345999" | "7457279" | "7542472" | "7570743" | "8065418" | "20020080719" | "20020176404" | "20030031210" | "20030115251" | "20070016921" | "6836765" | "20020042769" | "20020124096" | "20030009565" | "20030043764" | "20030105812" | "20040128554" | "20050004982" | "20050120073" | "20050220017" | "20060062180" | "20060182100" | "20060205436" | "20070019545" | "20080091813" | "20080130639" | "20090003322" | "20090156217" | "20090234967" | "20090257433" | "20100011108" | "20100011111" | "20100279670" | "20100299150" | "20100299313" | "7346044" | "7353252" | "7574523" | "7656870" | "20020087887" | "20020120757" | "20020184310" | "20030046056" | "20030163697" | "20040034793" | "20050195802" | "20070110043" | "20080320096" | "6987756" | "7184415" | "7272377" | "7412374" | "7477282" | "7512652" | "20020097150" | "20020152325" | "20030088676" | "20030126213" | "20030158722" | "20030163525").PN.				
S99	36	("20030187650" | "20040024879" | "20040068567" | "20040203834" | "20040240399" | "20050071481" | "20050143105" | "20050246193" | "20060002355" | "20060069775" | "20060203750" | "20070025270" | "20070190987" | "20070260359" |	USPAT; USOCR	OR	OFF	2016/06/03 16:25

		"20080123685" | "20080250408" | "20100077023" | "6963555" | "6975718" | "7006508" | "7013155" | "7564843" | "7782866" | "20040100973" | "20040158471" | "20040162871" | "20040228279" | "20040267938" | "20050008024" | "20050286519" | "20080192756" | "6766373" | "7613171" | "20020173303" | "20030078858" | "20030212772" | "20040005877" | "20040249953" | "20050033843" | "20050105524" | "20050270992" | "20070078785" | "20070111794" | "20070239892" | "20080019285" | "20080080392" | "20090136016" | "6298129" | "6360196" | "6826613" | "7117526" | "7302496" | "7664495" | "7778187" | "8009586" | "20020166053" | "20030044020" | "20030072485" | "20030174707" | "20050119005" | "20050249196" | "20090192976" | "6999932" | "7353255" | "20020150110" | "20040039781" | "20040044517" | "20040062267" | "20040148434" | "20040213184" | "20050015502" | "20050144288" | "20050201357" | "20060195402" | "20060218624" | "20060230166" | "20070116224" | "20070274276" | "20080005328" | "20090182815" | "20100312832" | "20110040836" | "5761309" | "6202084" | "6389016" | "6438376" | "6741691" | "6940826" | "7769881" | "20030137939" | "20040139225" | "20060183476" | "20060246903" | "20080069105" | "6031818" | "6311150" | "6574668" | "6842460" | "20020038282" | "20030061025" | "20030061481" | "20030135569" | "20030177186" | "20030217318" | "20030229715" | "20040133689" | "20040143678" | "20050187957" | "20050208947" | "20050254440" | "20060121986" | "20060165029" | "20080235362" | "20080235511" | "20090006076" | "20090088150" | "20090300673" | "20100223047" | "5818447" | "6161082" | "6912278" | "7123710" | "7917584" | "20020178087" | "20030220121" | "20050086309" | "20050138119" | "20060148516" | "5790637" | "6473425").PN.				
S100	462	S95 AND (mobile cell cellular phone iphone) NOT (S73 S76 S79 S82 S85 S89 S96 S97 S98 S99 S92)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/06/03 16:25
S101	462	S100	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/06/03 16:25
S102	462	S101	US-PGPUB; USPAT;	OR	ON	2016/06/03 16:25

			EPO; JPO; DERWENT; IBM_TDB			
S103	0	S72 AND without NEAR5 (switch switches switching switched swap swaps swapping swapped change changes changing changed move moves moving moved) WITH (superblock super-block super ADJ block function ADJ block function-block functionblock funblock program-block program ADJ block application ADJ block appblock app-block application-block)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/06/03 16:27
S104	0	S103	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/06/03 16:27
S105	285	without WITH (switch switches switching switched swap swaps swapping swapped change changes changing changed move moves moving moved) WITH (superblock super-block super ADJ block function ADJ block function-block functionblock funblock program-block program ADJ block application ADJ block appblock app-block application-block)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/06/03 16:28
S106	285	S105	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/06/03 16:28
S107	203	(instead place missing skipping) WITH (switch switches switching switched swap swaps swapping swapped change changes changing changed move moves moving moved) WITH (superblock super-block super ADJ block function ADJ block function-block functionblock funblock program-block program ADJ block application ADJ block appblock app-block application-block) AND @ad<"20130911"	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/06/03 16:29
S108	203	S107	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/06/03 16:29
S109	12	(without) NEAR2 (context NEAR1 (switch switches switching switched swap swaps swapping swapped change changes changing changed move moves moving moved)) WITH (code ADJ block code-block code ADJ section code-section layer) AND @ad<"20130911" NOT (S105 S107)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/06/03 16:31
S110	12	S109	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/06/03 16:31

S111	40	(without instead place missing skipping) WITH (context NEAR1 (switch switches switching switched swap swaps swapping swapped change changes changing changed move moves moving moved)) WITH (code ADJ block code-block code ADJ section code-section layer) AND @ad<"20130911" NOT (S105 S107)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/06/03 16:31
S112	40	S111	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/06/03 16:31
S113	28	(without instead place missing skipping) WITH (context NEAR1 (switch switches switching switched swap swaps swapping swapped change changes changing changed move moves moving moved)) WITH (code ADJ block code-block code ADJ section code-section layer) AND @ad<"20130911" NOT (S105 S107 S109)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/06/03 16:34
S114	28	S113	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/06/03 16:34
S115	5	(without instead place missing skipping) WITH (context NEAR3 (switch switches switching switched swap swaps swapping swapped change changes changing changed move moves moving moved)) WITH (code ADJ block code-block code ADJ section code-section layer) AND @ad<"20130911" NOT (S105 S107 S109 S113)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/06/03 16:34
S116	5	S115	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/06/03 16:34
S117	29	(without instead place missing skipping) WITH (context NEAR5 (switch switches switching switched swap swaps swapping swapped change changes changing changed move moves moving moved)) WITH (code ADJ block code-block code ADJ section code-section layer) AND @ad<"20130911" NOT (S105 S107 S109 S113 S115)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/06/03 16:35
S118	29	S117	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/06/03 16:35
S119	119	CHATURVEDI-SIVAKUMAR.in. GUNDABATHULA-SATISH.in. HIREMATH-RASHMI.in. CHATURVEDI-SIVAKUMAR-$.in. GUNDABATHULA-SATISH-$.in. HIREMATH-RASHMI-$.in.	US-PGPUB; USPAT	OR	ON	2016/06/03 16:38

S120	119	S119	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/06/03 16:38
S121	5	without ADJ switching NEAR3 context WITH superblock	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/06/03 16:39
S122	5	S121	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/06/03 16:39
S123	4	establishing WITH function WITH block WITH superblock	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/06/03 16:39
S124	4	S123	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/06/03 16:39
S128	11491	(G06F9/54.cpc. G06F9/541.cpc. G06F9/542.cpc. G06F9/44526.cpc.) AND @ad<"20130911"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/20 10:19
S129	67	S128 AND ((plug-in plugin plug ADJ in addon add-on add ADJ on addin add-in add ADJ in extension) WITH (verify verifies verifying verified verification check checks checking checked determine determines determining determined) WITH (authority authorize authorizes authorizing authorized approve approves approving approved approval allow allows allowing allowed allowance ok okeys oking oked okes ok-ed ok-ing)) AND @ad<"20130911"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/20 10:19
S130	67	S129	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/12/20 10:19
S131	67	S130	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/12/20 10:19
S132	67	S131	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/12/20 10:19
S133	7	S128 AND ((plug-in plugin plug ADJ in addon add-on add ADJ on addin add-in add ADJ in extension) WITH (verify verifies verifying verified verification check checks checking checked determine determines determining determined) WITH (authority authorize	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/12/20 10:20

		authorizes authorizing authorized approve approves approving approved approval allow allows allowing allowed allowance ok okeys oking oked okes ok-ed ok-ing)) AND @ad<"20130911" NOT S129				
S134	7	S133	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/12/20 10:20
S135	7	S134	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/12/20 10:20
S136	7	S135	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/12/20 10:20
S137	39	S128 AND ((plug-in plugin plug ADJ in addon add-on add ADJ on addin add-in add ADJ in extension) WITH (verify verifies verifying verified verification check checks checking checked determine determines determining determined) WITH (authority authorize authorizes authorizing authorized approve approves approving approved approval allow allows allowing allowed allowance ok okeys oking oked okes ok-ed ok-ing able capable permission clearence)) AND @ad<"20130911" NOT S129	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/12/20 10:26
S138	39	S137	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/12/20 10:26
S139	39	S138	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/12/20 10:26
S140	39	S139	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/12/20 10:26
S141	135	((window screen pane image display) WITH (plug-in plugin plug ADJ in addon add-on add ADJ on addin add-in add ADJ in extension) WITH (both together simultaneously "same time" concurrent concurrently simultaneous)) AND((plug-in plugin plug ADJ in addon add-on add ADJ on addin add-in add ADJ in extension) WITH (verify verifies verifying verified verification check checks checking checked determine determines determining determined) WITH (authority authorize authorizes authorizing authorized approve approves approving approved approval allow	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/12/20 10:27

		allows allowing allowed allowance ok okeys oking oked okes ok-ed ok-ing able capable permission clearence)) AND @ad<"20130911" NOT S129				
S142	135	S141	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/12/20 10:27
S143	135	S142	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/12/20 10:27
S144	135	S143	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/12/20 10:27
S145	1	((window screen pane image display) WITH (function ADJ block plug-in plugin plug ADJ in addon add-on add ADJ on addin add-in add ADJ in extension) WITH (both together simultaneously "same time" concurrent concurrently simultaneous)) AND((function ADJ block plug-in plugin plug ADJ in addon add-on add ADJ on addin add-in add ADJ in extension) WITH (verify verifies verifying verified verification check checks checking checked determine determines determining determined) WITH (authority authorize authorizes authorizing authorized approve approves approving approved approval allow allows allowing allowed allowance ok okeys oking oked okes ok-ed ok-ing able capable permission clearence)) AND @ad<"20130911" NOT (S129 S133 S137 S141)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/12/20 10:28
S146	1	S145	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/12/20 10:28
S147	1	S146	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/12/20 10:28
S148	1	S147	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/12/20 10:28
S149	136	((window screen pane image display) WITH (function ADJ block plug-in plugin plug ADJ in addon add-on add ADJ on addin add-in add ADJ in extension) WITH (both together simultaneously "same time" concurrent concurrently simultaneous)) AND((function ADJ block plug-in plugin plug ADJ in addon add-on add ADJ on addin add-in add ADJ in extension) WITH (verify verifies	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/12/20 10:29

		verifying verified verification check checks checking checked determine determines determining determined) WITH (authority authorize authorizes authorizing authorized approve approves approving approved approval allow allows allowing allowed allowance ok okeys oking oked okes ok-ed ok-ing able capable permission clearence)) AND @ad<"20130911" NOT S129				
S150	3	((window screen pane image display) WITH (((function program application app sub) NEAR2 (block section segment)) plug-in plugin plug ADJ in addon add-on add ADJ on addin add-in add ADJ in extension) WITH (both together simultaneously "same time" concurrent concurrently simultaneous)) AND((function ADJ block plug-in plugin plug ADJ in addon add-on add ADJ on addin add-in add ADJ in extension) WITH (verify verifies verifying verified verification check checks checking checked determine determines determining determined) WITH (authority authorize authorizes authorizing authorized approve approves approving approved approval allow allows allowing allowed allowance ok okeys oking oked okes ok-ed ok-ing able capable permission clearence)) AND @ad<"20130911" NOT (S129 S133 S137 S141 S149)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/12/20 10:29
S151	3	S150	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/12/20 10:29
S152	3	S151	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/12/20 10:29
S153	3	S152	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/12/20 10:29
S154	268	("20030187650" | "20040024879" | "20040068567" | "20040203834" | "20040240399" | "20050071481" | "20050143105" | "20050246193" | "20060002355" | "20060069775" | "20060203750" | "20070025270" | "20070190987" | "20070260359" | "20080123685" | "20080250408" | "20100077023" | "6963555" | "6975718" | "7006508" | "7013155" | "7564843" | "7782866" | "20040100973" | "20040158471" | "20040162871" | "20040228279" | "20040267938" | "20050008024" | "20050286519" | "20080192756" | "6766373" | "7613171" | "20020173303" | "20030078858" |	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/20 10:31

		"20030212772" | "20040005877" | "20040249953" | "20050033843" | "20050105524" | "20050270992" | "20070078785" | "20070111794" | "20070239892" | "20080019285" | "20080080392" | "20090136016" | "6298129" | "6360196" | "6826613" | "7117526" | "7302496" | "7664495" | "7778187" | "8009586" | "20020166053" | "20030044020" | "20030072485" | "20030174707" | "20050119005" | "20050249196" | "20090192976" | "6999932" | "7353255" | "20020150110" | "20040039781" | "20040044517" | "20040062267" | "20040148434" | "20040213184" | "20050015502" | "20050144288" | "20050201357" | "20060195402" | "20060218624" | "20060230166" | "20070116224" | "20070274276" | "20080005328" | "20090182815" | "20100312832" | "20110040836" | "5761309" | "6202084" | "6389016" | "6438376" | "6741691" | "6940826" | "7769881" | "20030137939" | "20040139225" | "20060183476" | "20060246903" | "20080069105" | "6031818" | "6311150" | "6574668" | "6842460" | "20020038282" | "20030061025" | "20030061481" | "20030135569" | "20030177186" | "20030217318" | "20030229715" | "20040133689" | "20040143678" | "20050187957" | "20050208947" | "20050254440" | "20060121986" | "20060165029" | "20080235362" | "20080235511" | "20090006076" | "20090088150" | "20090300673" | "20100223047" | "5818447" | "6161082" | "6912278" | "7123710" | "7917584" | "20020178087" | "20030220121" | "20050086309" | "20050138119" | "20060148516" | "5790637" | "6473425").PN.				
S155	268	S154	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/12/20 10:31
S156	268	S155	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/12/20 10:31
S157	268	S156	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/12/20 10:31
S158	1107	G06F9/44526.cpc. AND @ad<"20130911"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/20 10:32
S159	37	("20010050923" | "20020143548" |	USPAT;	OR	OFF	2016/12/20

		"20020156844" | "20030202480" | "20040034776" | "20040103212" | "20050130650" | "20050132009" | "20050198499" | "20050201485" | "20060168643" | "20060258289" | "20070136459" | "20070165629" | "20070206563" | "20070297430" | "20080273541" | "20090052399" | "20090240821" | "20090327516" | "20110122864" | "20110314134" | "6128283" | "7079529" | "7092385" | "7487248" | "7623476" | "20030177422" | "20050033985" | "20050091407" | "6850769" | "7304985" | "20020037000" | "20020064167" | "20030110047" | "20030172145" | "20030214955" | "20040139230" | "20040153858" | "20040268257" | "20050136911" | "20050138128" | "20060072506" | "20060120375" | "20070082671" | "20070130253" | "20110145687" | "6219638" | "6754181" | "6999575" | "7185114" | "7590758" | "7623516" | "7774495" | "20030035441" | "20030076815" | "20030217171" | "20040260952" | "20050050227" | "5442637" | "5889762" | "6343067" | "7080158" | "20020031212" | "20020062285" | "20030046585" | "20040052234" | "20040139228" | "20040267527" | "20050187781" | "20060121902" | "20060171534" | "20060187926" | "20070253435" | "20080032695" | "20080168440" | "20090055473" | "20100049980" | "20100107205" | "20100312897" | "20110099612" | "20120263144" | "6141687" | "6898413" | "7010109" | "7345999" | "7457279" | "7542472" | "7570743" | "8065418" | "20020080719" | "20020176404" | "20030031210" | "20030115251" | "20070016921" | "6836765" | "20020042769" | "20020124096" | "20030009565" | "20030043764" | "20030105812" | "20040128554" | "20050004982" | "20050120073" | "20050220017" | "20060062180" | "20060182100" | "20060205436" | "20070019545" | "20080091813" | "20080130639" | "20090003322" | "20090156217" | "20090234967" | "20090257433" | "20100011108" | "20100011111" | "20100279670" | "20100299150" | "20100299313" | "7346044" | "7353252" | "7574523" | "7656870" | "20020087887" | "20020120757" | "20020184310" | "20030046056" | "20030163697" | "20040034793" | "20050195802" | "20070110043" | "20080320096" | "6987756" | "7184415" | "7272377" | "7412374" | "7477282" | "7512652" | "20020097150" | "20020152325" | "20030088676" |	USOCR			10:32	

		"20030126213" | "20030158722" | "20030163525").PN.				
S160	36	("20030187650" | "20040024879" | "20040068567" | "20040203834" | "20040240399" | "20050071481" | "20050143105" | "20050246193" | "20060002355" | "20060069775" | "20060203750" | "20070025270" | "20070190987" | "20070260359" | "20080123685" | "20080250408" | "20100077023" | "6963555" | "6975718" | "7006508" | "7013155" | "7564843" | "7782866" | "20040100973" | "20040158471" | "20040162871" | "20040228279" | "20040267938" | "20050008024" | "20050286519" | "20080192756" | "6766373" | "7613171" | "20020173303" | "20030078858" | "20030212772" | "20040005877" | "20040249953" | "20050033843" | "20050105524" | "20050270992" | "20070078785" | "20070111794" | "20070239892" | "20080019285" | "20080080392" | "20090136016" | "6298129" | "6360196" | "6826613" | "7117526" | "7302496" | "7664495" | "7778187" | "8009586" | "20020166053" | "20030044020" | "20030072485" | "20030174707" | "20050119005" | "20050249196" | "20090192976" | "6999932" | "7353255" | "20020150110" | "20040039781" | "20040044517" | "20040062267" | "20040148434" | "20040213184" | "20050015502" | "20050144288" | "20050201357" | "20060195402" | "20060218624" | "20060230166" | "20070116224" | "20070274276" | "20080005328" | "20090182815" | "20100312832" | "20110040836" | "5761309" | "6202084" | "6389016" | "6438376" | "6741691" | "6940826" | "7769881" | "20030137939" | "20040139225" | "20060183476" | "20060246903" | "20080069105" | "6031818" | "6311150" | "6574668" | "6842460" | "20020038282" | "20030061025" | "20030061481" | "20030135569" | "20030177186" | "20030217318" | "20030229715" | "20040133689" | "20040143678" | "20050187957" | "20050208947" | "20050254440" | "20060121986" | "20060165029" | "20080235362" | "20080235511" | "20090006076" | "20090088150" | "20090300673" | "20100223047" | "5818447" | "6161082" | "6912278" | "7123710" | "7917584" | "20020178087" | "20030220121" | "20050086309" | "20050138119" | "20060148516" | "5790637" | "6473425").PN.	USPAT; USOCR	OR	OFF	2016/12/20 10:32
S161	301	("20010050923" | "20020143548" | "20020156844" | "20030202480" | "20040034776" | "20040103212" |	US-PGPUB; USPAT; USOCR;	OR	OFF	2016/12/20 10:32

		"20050130650" | "20050132009" | "20050198499" | "20050201485" | "20060168643" | "20060258289" | "20070136459" | "20070165629" | "20070206563" | "20070297430" | "20080273541" | "20090052399" | "20090240821" | "20090327516" | "20110122864" | "20110314134" | "6128283" | "7079529" | "7092385" | "7487248" | "7623476" | "20030177422" | "20050033985" | "20050091407" | "6850769" | "7304985" | "20020037000" | "20020064167" | "20030110047" | "20030172145" | "20030214955" | "20040139230" | "20040153858" | "20040268257" | "20050136911" | "20050138128" | "20060072506" | "20060120375" | "20070082671" | "20070130253" | "20110145687" | "6219638" | "6754181" | "6999575" | "7185114" | "7590758" | "7623516" | "7774495" | "20030035441" | "20030076815" | "20030217171" | "20040260952" | "20050050227" | "5442637" | "5889762" | "6343067" | "7080158" | "20020031212" | "20020062285" | "20030046585" | "20040052234" | "20040139228" | "20040267527" | "20050187781" | "20060121902" | "20060171534" | "20060187926" | "20070253435" | "20080032695" | "20080168440" | "20090055473" | "20100049980" | "20100107205" | "20100312897" | "20110099612" | "20120263144" | "6141687" | "6898413" | "7010109" | "7345999" | "7457279" | "7542472" | "7570743" | "8065418" | "20020080719" | "20020176404" | "20030031210" | "20030115251" | "20070016921" | "6836765" | "20020042769" | "20020124096" | "20030009565" | "20030043764" | "20030105812" | "20040128554" | "20050004982" | "20050120073" | "20050220017" | "20060062180" | "20060182100" | "20060205436" | "20070019545" | "20080091813" | "20080130639" | "20090003322" | "20090156217" | "20090234967" | "20090257433" | "20100011108" | "20100011111" | "20100279670" | "20100299150" | "20100299313" | "7346044" | "7353252" | "7574523" | "7656870" | "20020087887" | "20020120757" | "20020184310" | "20030046056" | "20030163697" | "20040034793" | "20050195802" | "20070110043" | "20080320096" | "6987756" | "7184415" | "7272377" | "7412374" | "7477282" | "7512652" | "20020097150" | "20020152325" | "20030088676" | "20030126213" | "20030158722" | "20030163525").PN.	EPO; JPO; DERWENT; IBM_TDB				

S162	36	("20030187650" | "20040024879" | "20040068567" | "20040203834" | "20040240399" | "20050071481" | "20050143105" | "20050246193" | "20060002355" | "20060069775" | "20060203750" | "20070025270" | "20070190987" | "20070260359" | "20080123685" | "20080250408" | "20100077023" | "6963555" | "6975718" | "7006508" | "7013155" | "7564843" | "7782866" | "20040100973" | "20040158471" | "20040162871" | "20040228279" | "20040267938" | "20050008024" | "20050286519" | "20080192756" | "6766373" | "7613171" | "20020173303" | "20030078858" | "20030212772" | "20040005877" | "20040249953" | "20050033843" | "20050105524" | "20050270992" | "20070078785" | "20070111794" | "20070239892" | "20080019285" | "20080080392" | "20090136016" | "6298129" | "6360196" | "6826613" | "7117526" | "7302496" | "7664495" | "7778187" | "8009586" | "20020166053" | "20030044020" | "20030072485" | "20030174707" | "20050119005" | "20050249196" | "20090192976" | "6999932" | "7353255" | "20020150110" | "20040039781" | "20040044517" | "20040062267" | "20040148434" | "20040213184" | "20050015502" | "20050144288" | "20050201357" | "20060195402" | "20060218624" | "20060230166" | "20070116224" | "20070274276" | "20080005328" | "20090182815" | "20100312832" | "20110040836" | "5761309" | "6202084" | "6389016" | "6438376" | "6741691" | "6940826" | "7769881" | "20030137939" | "20040139225" | "20060183476" | "20060246903" | "20080069105" | "6031818" | "6311150" | "6574668" | "6842460" | "20020038282" | "20030061025" | "20030061481" | "20030135569" | "20030177186" | "20030217318" | "20030229715" | "20040133689" | "20040143678" | "20050187957" | "20050208947" | "20050254440" | "20060121986" | "20060165029" | "20080235362" | "20080235511" | "20090006076" | "20090088150" | "20090300673" | "20100223047" | "5818447" | "6161082" | "6912278" | "7123710" | "7917584" | "20020178087" | "20030220121" | "20050086309" | "20050138119" | "20060148516" | "5790637" | "6473425").PN.	USPAT; USOCR	OR	OFF	2016/12/20 10:32
S163	482	S158 AND (mobile cell cellular phone iphone) NOT (S129 S133 S137 S141 S145 S150 S159 S160 S161 S162 S154)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2016/12/20 10:32

S164	482	S163	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/12/20 10:32
S165	482	S164	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/12/20 10:32
S166	482	S165	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/12/20 10:32
S167	0	S128 AND without NEAR5 (switch switches switching switched swap swaps swapping swapped change changes changing changed move moves moving moved) WITH (superblock super-block super ADJ block function ADJ block function-block functionblock funblock program-block program ADJ block application ADJ block appblock app-block application-block)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/12/20 10:49
S168	0	S167	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/12/20 10:49
S169	0	S168	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/12/20 10:49
S170	292	without WITH (switch switches switching switched swap swaps swapping swapped change changes changing changed move moves moving moved) WITH (superblock super-block super ADJ block function ADJ block function-block functionblock funblock program-block program ADJ block application ADJ block appblock app-block application-block)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/12/20 10:49
S171	292	S170	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/12/20 10:49
S172	292	S171	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/12/20 10:49
S173	204	(instead place missing skipping) WITH (switch switches switching switched swap swaps swapping swapped change changes changing changed move moves moving moved) WITH (superblock super-block super ADJ block function ADJ block function-block functionblock funblock program-block program ADJ block application ADJ block appblock app-block application-block) AND @ad<"20130911"	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/12/20 10:50

S174	204	S173	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/12/20 10:50
S175	204	S174	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/12/20 10:50
S176	12	(without) NEAR2 (context NEAR1 (switch switches switching switched swap swaps swapping swapped change changes changing changed move moves moving moved)) WITH (code ADJ block code-block code ADJ section code-section layer) AND @ad<"20130911" NOT (S170 S173)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/12/20 10:51
S177	12	S176	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/12/20 10:51
S178	12	S177	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/12/20 10:51
S179	41	(without instead place missing skipping) WITH (context NEAR1 (switch switches switching switched swap swaps swapping swapped change changes changing changed move moves moving moved)) WITH (code ADJ block code-block code ADJ section code-section layer) AND @ad<"20130911" NOT (S170 S173)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/12/20 10:51
S180	41	S179	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/12/20 10:51
S181	41	S180	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/12/20 10:51
S182	29	(without instead place missing skipping) WITH (context NEAR1 (switch switches switching switched swap swaps swapping swapped change changes changing changed move moves moving moved)) WITH (code ADJ block code-block code ADJ section code-section layer) AND @ad<"20130911" NOT (S170 S173 S176)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/12/20 10:52
S183	29	S182	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/12/20 10:52
S184	29	S183	US-PGPUB; USPAT;	OR	ON	2016/12/20 10:52

			EPO; JPO; DERWENT			
S185	5	(without instead place missing skipping) WITH (context NEAR3 (switch switches switching switched swap swaps swapping swapped change changes changing changed move moves moving moved)) WITH (code ADJ block code-block code ADJ section code-section layer) AND @ad<"20130911" NOT (S170 S173 S176 S182)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/12/20 10:52
S186	5	S185	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/12/20 10:52
S187	5	S186	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/12/20 10:52
S188	7	without ADJ switching NEAR3 context WITH superblock	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/12/20 10:53
S189	7	S188	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/12/20 10:53
S190	7	S189	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/12/20 10:53
S191	7	establishing WITH function WITH block WITH superblock	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/12/20 10:53
S192	7	S191	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2016/12/20 10:53
S193	7	S192	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/12/20 10:53
S194	59	(establish establishes establishing established establishment ascertain ascertains ascertaining ascertained determine determines determining determined determination discover discovers discovering discovered discovery learn learns learning learned (find finds finding) ADJ out found certain confirm confirms confirming confirmed confirmation) WITH (lack lacks lacking lacked without) WITH (superblock super-block super ADJ block (parent child primary secondary top bottom) ADJ block) AND @ad<"20130911"	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/12/20 11:15

S195	56	(establish establishes establishing established establishment ascertain ascertains ascertaining ascertained determine determines determining determined determination discover discovers discovering discovered discovery learn learns learning learned (find finds finding) ADJ out found certain confirm confirms confirming confirmed confirmation) WITH (lack lacks lacking lacked without) WITH ((parent child primary secondary top bottom) ADJ (application program app)) AND @ad<"20130911"	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/12/20 11:25
S196	175	(network net grid web cloud LAN WAN) SAME ((lack lacks lacking lacked without) WITH ((master slave parent child primary secondary top bottom) ADJ (application program app))) AND @ad<"20130911" NOT (S194 S195)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/12/20 11:37
S197	2993	(network net grid web cloud LAN WAN) SAME ((lack lacks lacking lacked without) WITH ((support supports supporting supported supporter maintain maintains maintaining maintained maintanence) NEAR5 (application program app))) AND @ad<"20130911" NOT (S194 S195 S196)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/12/20 12:13
S198	1923	(network net grid web cloud LAN WAN) WITH ((lack lacks lacking lacked without) WITH ((support supports supporting supported supporter maintain maintains maintaining maintained maintanence) NEAR5 (application program app))) AND @ad<"20130911" NOT (S194 S195 S196)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/12/20 12:14
S199	1003	(network net grid web cloud LAN WAN) WITH ((lack lacks lacking lacked without) NEAR5 ((support supports supporting supported supporter maintain maintains maintaining maintained maintanence) NEAR5 (application program app))) AND @ad<"20130911" NOT (S194 S195 S196)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/12/20 12:14
S200	267	(network net grid web cloud LAN WAN) NEAR5 ((lack lacks lacking lacked without) NEAR3 ((support supports supporting supported supporter maintain maintains maintaining maintained maintanence) NEAR3 (application program app))) AND @ad<"20130911" NOT (S194 S195 S196)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/12/20 12:14
S201	60	("20010050923" | "20020031212" | "20020037000" | "20020038282" | "20020042769" | "20020062285" | "20020064167" | "20020080719" | "20020087887" | "20020097150" | "20020120757" | "20020124096" | "20020143548" | "20020150110" | "20020152325" | "20020156844" | "20020166053" | "20020173303" | "20020176404" | "20020178087" |	US-PGPUB; USPAT; USOCR	OR	OFF	2016/12/21 12:27

		"20020184310" | "20030009565" | "20030031210" | "20030035441" | "20030043764" | "20030044020" | "20030046056" | "20030046585" | "20030061025" | "20030061481" | "20030072485" | "20030076815" | "20030078858" | "20030088676" | "20030105812" | "20030110047" | "20030115251" | "20030126213" | "20030135569" | "20030137939" | "20030158722" | "20030163525" | "20030163697" | "20030172145" | "20030174707" | "20030177186" | "20030177422" | "20030187650" | "20030202480" | "20030212772" | "20030214955" | "20030217171" | "20030217318" | "20030220121" | "20030229715" | "20040005877" | "20040024879" | "20040034776" | "20040034793" | "20040039781").PN.				
S202	110	("20040044517" | "20040052234" | "20040062267" | "20040068567" | "20040100973" | "20040103212" | "20040128554" | "20040133689" | "20040139225" | "20040139228" | "20040139230" | "20040143678" | "20040148434" | "20040153858" | "20040158471" | "20040162871" | "20040193599" | "20040203834" | "20040213184" | "20040228279" | "20040240399" | "20040249885" | "20040249953" | "20040260952" | "20040267527" | "20040267938" | "20040268257" | "20050004982" | "20050008024" | "20050015502" | "20050033843" | "20050033985" | "20050050227" | "20050071481" | "20050086309" | "20050091407" | "20050105524" | "20050119005" | "20050120073" | "20050130650" | "20050132009" | "20050136911" | "20050138119" | "20050138128" | "20050143105" | "20050144288" | "20050187781" | "20050187957" | "20050195802" | "20050198499" | "20050201357" | "20050201485" | "20050208947" | "20050220017" | "20050246193" | "20050249196" | "20050254440" | "20050270992" | "20050286519" | "20060002355" | "20060062180" | "20060069775" | "20060072506" | "20060120375" | "20060121902" | "20060121986" | "20060148516" | "20060165029" | "20060168643" | "20060171534" | "20060182100" | "20060183476" | "20060187926" | "20060195402" | "20060203750" | "20060205436" | "20060218624" | "20060230166" | "20060233117" | "20060246903" | "20060258289" | "20070016921" | "20070019545" | "20070025270" | "20070078785" | "20070082671" | "20070110043" | "20070111794" |	US-PGPUB; USPAT; USOCR	OR	OFF	2016/12/21 12:27

		"20070116224" | "20070130253" | "20070136459" | "20070165629" | "20070190987" | "20070206563" | "20070239892" | "20070253435" | "20070260359" | "20070274276" | "20070280253" | "20070294626" | "20070297430" | "20080005328" | "20080019285" | "20080032695" | "20080046984" | "20080069105" | "20080080392" | "20080091813" | "20080123685" | "20080130639").PN.				
S203	130	("20080168440" | "20080192756" | "20080235362" | "20080235511" | "20080244718" | "20080250408" | "20080273541" | "20080320096" | "20080320565" | "20090003322" | "20090006076" | "20090052399" | "20090055473" | "20090088150" | "20090136016" | "20090156217" | "20090182815" | "20090192976" | "20090234967" | "20090240821" | "20090257433" | "20090300673" | "20090327516" | "20100011108" | "20100011111" | "20100049980" | "20100058353" | "20100077023" | "20100107205" | "20100174783" | "20100191954" | "20100223047" | "20100279670" | "20100299150" | "20100299313" | "20100312832" | "20100312897" | "20110040836" | "20110099612" | "20110122864" | "20110141220" | "20110145687" | "20110307556" | "20110314134" | "20110320821" | "20120078609" | "20120124191" | "20120263144" | "20130067004" | "20130106989" | "20130111064" | "20130125145" | "20150026700" | "5442637" | "5761309" | "5790637" | "5818447" | "5889762" | "6031818" | "6128283" | "6141687" | "6161082" | "6195694" | "6202084" | "6219638" | "6298129" | "6311150" | "6343067" | "6360196" | "6389016" | "6438376" | "6473425" | "6574668" | "6606112" | "6741691" | "6754181" | "6766373" | "6826613" | "6836765" | "6842460" | "6850769" | "6898413" | "6912278" | "6940826" | "6963555" | "6975718" | "6987756" | "6999575" | "6999932" | "7006508" | "7010109" | "7013155" | "7079529" | "7080158" | "7092385" | "7117526" | "7123710" | "7184415" | "7185114" | "7272377" | "7302496" | "7304985" | "7345999" | "7346044" | "7353252" | "7353255" | "7412374" | "7457279" | "7477282" | "7487248" | "7512652" | "7542472" | "7564843" | "7570743" | "7574523" | "7590758" | "7613171" | "7623476" | "7623516" | "7656870" | "7664495" | "7769881" | "7774495" | "7778187" | "7782866" | "7917584" | "8009586" | "8065418" | "8200796" | "8407576").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2016/12/21 12:27

S204	37	("20010050923" | "20020143548" | "20020156844" | "20030202480" | "20040034776" | "20040103212" | "20050130650" | "20050132009" | "20050198499" | "20050201485" | "20060168643" | "20060258289" | "20070136459" | "20070165629" | "20070206563" | "20070297430" | "20080273541" | "20090052399" | "20090240821" | "20090327516" | "20110122864" | "20110314134" | "6128283" | "7079529" | "7092385" | "7487248" | "7623476" | "20030177422" | "20050033985" | "20050091407" | "6850769" | "7304985" | "20020037000" | "20020064167" | "20030110047" | "20030172145" | "20030214955" | "20040139230" | "20040153858" | "20040268257" | "20050136911" | "20050138128" | "20060072506" | "20060120375" | "20070082671" | "20070130253" | "20110145687" | "6219638" | "6754181" | "6999575" | "7185114" | "7590758" | "7623516" | "7774495" | "20030035441" | "20030076815" | "20030217171" | "20040260952" | "20050050227" | "5442637" | "5889762" | "6343067" | "7080158" | "20020031212" | "20020062285" | "20030046585" | "20040052234" | "20040139228" | "20040267527" | "20050187781" | "20060121902" | "20060171534" | "20060187926" | "20070253435" | "20080032695" | "20080168440" | "20090055473" | "20100049980" | "20100107205" | "20100312897" | "20110099612" | "20120263144" | "6141687" | "6898413" | "7010109" | "7345999" | "7457279" | "7542472" | "7570743" | "8065418" | "20020080719" | "20020176404" | "20030031210" | "20030115251" | "20070016921" | "6836765" | "20020042769" | "20020124096" | "20030009565" | "20030043764" | "20030105812" | "20040128554" | "20050004982" | "20050120073" | "20050220017" | "20060062180" | "20060182100" | "20060205436" | "20070019545" | "20080091813" | "20080130639" | "20090003322" | "20090156217" | "20090234967" | "20090257433" | "20100011108" | "20100011111" | "20100279670" | "20100299150" | "20100299313" | "7346044" | "7353252" | "7574523" | "7656870" | "20020087887" | "20020120757" | "20020184310" | "20030046056" | "20030163697" | "20040034793" | "20050195802" | "20070110043" | "20080320096" | "6987756" | "7184415" | "7272377" | "7412374" | "7477282" | "7512652" | "20020097150" |	USPAT; USOCR	OR	OFF	2016/12/21 12:28

		"20020152325" | "20030088676" | "20030126213" | "20030158722" | "20030163525").PN.				
S205	36	("20030187650" | "20040024879" | "20040068567" | "20040203834" | "20040240399" | "20050071481" | "20050143105" | "20050246193" | "20060002355" | "20060069775" | "20060203750" | "20070025270" | "20070190987" | "20070260359" | "20080123685" | "20080250408" | "20100077023" | "6963555" | "6975718" | "7006508" | "7013155" | "7564843" | "7782866" | "20040100973" | "20040158471" | "20040162871" | "20040228279" | "20040267938" | "20050008024" | "20050286519" | "20080192756" | "6766373" | "7613171" | "20020173303" | "20030078858" | "20030212772" | "20040005877" | "20040249953" | "20050033843" | "20050105524" | "20050270992" | "20070078785" | "20070111794" | "20070239892" | "20080019285" | "20080080392" | "20090136016" | "6298129" | "6360196" | "6826613" | "7117526" | "7302496" | "7664495" | "7778187" | "8009586" | "20020166053" | "20030044020" | "20030072485" | "20030174707" | "20050119005" | "20050249196" | "20090192976" | "6999932" | "7353255" | "20020150110" | "20040039781" | "20040044517" | "20040062267" | "20040148434" | "20040213184" | "20050015502" | "20050144288" | "20050201357" | "20060195402" | "20060218624" | "20060230166" | "20070116224" | "20070274276" | "20080005328" | "20090182815" | "20100312832" | "20110040836" | "5761309" | "6202084" | "6389016" | "6438376" | "6741691" | "6940826" | "7769881" | "20030137939" | "20040139225" | "20060183476" | "20060246903" | "20080069105" | "6031818" | "6311150" | "6574668" | "6842460" | "20020038282" | "20030061025" | "20030061481" | "20030135569" | "20030177186" | "20030217318" | "20030229715" | "20040133689" | "20040143678" | "20050187957" | "20050208947" | "20050254440" | "20060121986" | "20060165029" | "20080235362" | "20080235511" | "20090006076" | "20090088150" | "20090300673" | "20100223047" | "5818447" | "6161082" | "6912278" | "7123710" | "7917584" | "20020178087" | "20030220121" | "20050086309" | "20050138119" | "20060148516" | "5790637" | "6473425").PN.	USPAT; USOCR	OR	OFF	2016/12/21 12:28
S206	301	("20010050923" | "20020143548" | "20020156844" | "20030202480" |	US-PGPUB; USPAT;	OR	OFF	2016/12/21 12:28

		"20040034776" | "20040103212" | "20050130650" | "20050132009" | "20050198499" | "20050201485" | "20060168643" | "20060258289" | "20070136459" | "20070165629" | "20070206563" | "20070297430" | "20080273541" | "20090052399" | "20090240821" | "20090327516" | "20110122864" | "20110314134" | "6128283" | "7079529" | "7092385" | "7487248" | "7623476" | "20030177422" | "20050033985" | "20050091407" | "6850769" | "7304985" | "20020037000" | "20020064167" | "20030110047" | "20030172145" | "20030214955" | "20040139230" | "20040153858" | "20040268257" | "20050136911" | "20050138128" | "20060072506" | "20060120375" | "20070082671" | "20070130253" | "20110145687" | "6219638" | "6754181" | "6999575" | "7185114" | "7590758" | "7623516" | "7774495" | "20030035441" | "20030076815" | "20030217171" | "20040260952" | "20050050227" | "5442637" | "5889762" | "6343067" | "7080158" | "20020031212" | "20020062285" | "20030046585" | "20040052234" | "20040139228" | "20040267527" | "20050187781" | "20060121902" | "20060171534" | "20060187926" | "20070253435" | "20080032695" | "20080168440" | "20090055473" | "20100049980" | "20100107205" | "20100312897" | "20110099612" | "20120263144" | "6141687" | "6898413" | "7010109" | "7345999" | "7457279" | "7542472" | "7570743" | "8065418" | "20020080719" | "20020176404" | "20030031210" | "20030115251" | "20070016921" | "6836765" | "20020042769" | "20020124096" | "20030009565" | "20030043764" | "20030105812" | "20040128554" | "20050004982" | "20050120073" | "20050220017" | "20060062180" | "20060182100" | "20060205436" | "20070019545" | "20080091813" | "20080130639" | "20090003322" | "20090156217" | "20090234967" | "20090257433" | "20100011108" | "20100011111" | "20100279670" | "20100299150" | "20100299313" | "7346044" | "7353252" | "7574523" | "7656870" | "20020087887" | "20020120757" | "20020184310" | "20030046056" | "20030163697" | "20040034793" | "20050195802" | "20070110043" | "20080320096" | "6987756" | "7184415" | "7272377" | "7412374" | "7477282" | "7512652" | "20020097150" | "20020152325" | "20030088676" | "20030126213" | "20030158722" |	USOCR; EPO; JPO; DERWENT; IBM_TDB				

		"20030163525").PN.				
S207	36	("20030187650" | "20040024879" | "20040068567" | "20040203834" | "20040240399" | "20050071481" | "20050143105" | "20050246193" | "20060002355" | "20060069775" | "20060203750" | "20070025270" | "20070190987" | "20070260359" | "20080123685" | "20080250408" | "20100077023" | "6963555" | "6975718" | "7006508" | "7013155" | "7564843" | "7782866" | "20040100973" | "20040158471" | "20040162871" | "20040228279" | "20040267938" | "20050008024" | "20050286519" | "20080192756" | "6766373" | "7613171" | "20020173303" | "20030078858" | "20030212772" | "20040005877" | "20040249953" | "20050033843" | "20050105524" | "20050270992" | "20070078785" | "20070111794" | "20070239892" | "20080019285" | "20080080392" | "20090136016" | "6298129" | "6360196" | "6826613" | "7117526" | "7302496" | "7664495" | "7778187" | "8009586" | "20020166053" | "20030044020" | "20030072485" | "20030174707" | "20050119005" | "20050249196" | "20090192976" | "6999932" | "7353255" | "20020150110" | "20040039781" | "20040044517" | "20040062267" | "20040148434" | "20040213184" | "20050015502" | "20050144288" | "20050201357" | "20060195402" | "20060218624" | "20060230166" | "20070116224" | "20070274276" | "20080005328" | "20090182815" | "20100312832" | "20110040836" | "5761309" | "6202084" | "6389016" | "6438376" | "6741691" | "6940826" | "7769881" | "20030137939" | "20040139225" | "20060183476" | "20060246903" | "20080069105" | "6031818" | "6311150" | "6574668" | "6842460" | "20020038282" | "20030061025" | "20030061481" | "20030135569" | "20030177186" | "20030217318" | "20030229715" | "20040133689" | "20040143678" | "20050187957" | "20050208947" | "20050254440" | "20060121986" | "20060165029" | "20080235362" | "20080235511" | "20090006076" | "20090088150" | "20090300673" | "20100223047" | "5818447" | "6161082" | "6912278" | "7123710" | "7917584" | "20020178087" | "20030220121" | "20050086309" | "20050138119" | "20060148516" | "5790637" | "6473425").PN.	USPAT; USOCR	OR	OFF	2016/12/21 12:28
S208	268	("20030187650" | "20040024879" | "20040068567" | "20040203834" | "20040240399" | "20050071481" | "20050143105" | "20050246193" |	US-PGPUB; USPAT; USOCR; EPO; JPO;	OR	OFF	2016/12/21 12:28

		"20060002355" | "20060069775" | "20060203750" | "20070025270" | "20070190987" | "20070260359" | "20080123685" | "20080250408" | "20100077023" | "6963555" | "6975718" | "7006508" | "7013155" | "7564843" | "7782866" | "20040100973" | "20040158471" | "20040162871" | "20040228279" | "20040267938" | "20050008024" | "20050286519" | "20080192756" | "6766373" | "7613171" | "20020173303" | "20030078858" | "20030212772" | "20040005877" | "20040249953" | "20050033843" | "20050105524" | "20050270992" | "20070078785" | "20070111794" | "20070239892" | "20080019285" | "20080080392" | "20090136016" | "6298129" | "6360196" | "6826613" | "7117526" | "7302496" | "7664495" | "7778187" | "8009586" | "20020166053" | "20030044020" | "20030072485" | "20030174707" | "20050119005" | "20050249196" | "20090192976" | "6999932" | "7353255" | "20020150110" | "20040039781" | "20040044517" | "20040062267" | "20040148434" | "20040213184" | "20050015502" | "20050144288" | "20050201357" | "20060195402" | "20060218624" | "20060230166" | "20070116224" | "20070274276" | "20080005328" | "20090182815" | "20100312832" | "20110040836" | "5761309" | "6202084" | "6389016" | "6438376" | "6741691" | "6940826" | "7769881" | "20030137939" | "20040139225" | "20060183476" | "20060246903" | "20080069105" | "6031818" | "6311150" | "6574668" | "6842460" | "20020038282" | "20030061025" | "20030061481" | "20030135569" | "20030177186" | "20030217318" | "20030229715" | "20040133689" | "20040143678" | "20050187957" | "20050208947" | "20050254440" | "20060121986" | "20060165029" | "20080235362" | "20080235511" | "20090006076" | "20090088150" | "20090300673" | "20100223047" | "5818447" | "6161082" | "6912278" | "7123710" | "7917584" | "20020178087" | "20030220121" | "20050086309" | "20050138119" | "20060148516" | "5790637" | "6473425").PN.	DERWENT; IBM_TDB			
S209	25	(S201 S202 S203) NOT (S204 S205 S206 S207 S208)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2016/12/21 12:28

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp

L1	23	audio/video NEAR3 functionality WITH block	US-PGPUB; USPAT	OR	ON	2016/12/22 09:43
L2	4	superblock NEAR5 audio/video	US-PGPUB; USPAT	OR	ON	2016/12/22 09:44
L3	1	A/V ADJ service WITH superblock	US-PGPUB; USPAT	OR	ON	2016/12/22 09:45
L4	0	provide ADJ audio WITH service	US-PGPUB; USPAT	OR	ON	2016/12/22 09:46
S34	12	719/313,319,329.ccls.		OR	OFF	2015/03/16 11:01
S35	23	719/313,319,329.ccls. G06F9/54 G06F9/541 G06F9/542 NOT S34		OR	OFF	2015/03/16 11:15
S125	4	function ADJ block WITH mobile WITH superblock	US-PGPUB; USPAT	OR	ON	2016/06/13 09:27
S126	2	function ADJ block WITH notifying WITH superblock	US-PGPUB; USPAT	OR	ON	2016/06/13 09:29
S127	2	switching ADJ context WITH establishing WITH superblock	US-PGPUB; USPAT	OR	ON	2016/06/13 09:30

12/22/2016 9:46:54 AM
C:\Users\cdorais\Documents\EAST\Workspaces\15297328AdditionalFuncntltyForSftwr-InIntgrtdManner.wsp

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15297328	CHATURVEDI ET AL.
	Examiner	Art Unit
	CRAIG DORAIS	2194

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES		
Search Notes	Date	Examiner
Refreshed East search. CPC and keyword searches. See attached. Google family searches (not relied upon).	12/21/2016	Craig Dorais

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner
	Keyword search as per MPEP 1302.08	12/21/2016	Craig Dorais

Doc Code: DIST.E.FILE **Document Description: Electronic Terminal Disclaimer - Filed**	PTO/SB/26 U.S. Patent and Trademark Office Department of Commerce

Electronic Petition Request	**TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT**
Application Number	15297328
Filing Date	19-Oct-2016
First Named Inventor	SIVAKUMAR CHATURVEDI
Attorney Docket Number	DAMA-33216
Title of Invention	SYSTEM AND METHOD FOR PROVIDING ADDITIONAL FUNCTIONALITY TO EXISTING SOFTWARE IN AN INTEGRATED MANNER

☒ Filing of terminal disclaimer does not obviate requirement for response under 37 CFR 1.111 to outstanding Office Action

☒ This electronic Terminal Disclaimer is not being used for a Joint Research Agreement.

Owner	Percent Interest
DAMAKA, INC.	100%

The owner(s) with percent interest listed above in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of prior patent number(s)

9491233

9270744

9027032

as the term of said prior patent is presently shortened by any terminal disclaimer. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the prior patent are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term of the prior patent, "as the term of said prior patent is presently shortened by any terminal disclaimer," in the event that said prior patent later:
- expires for failure to pay a maintenance fee;
- is held unenforceable;
- is found invalid by a court of competent jurisdiction;
- is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
- has all claims canceled by a reexamination certificate;
- is reissued; or
- is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

◉ Terminal disclaimer fee under 37 CFR 1.20(d) is included with Electronic Terminal Disclaimer request. ○ I certify, in accordance with 37 CFR 1.4(d)(4), that the terminal disclaimer fee under 37 CFR 1.20(d) required for this terminal disclaimer has already been paid in the above-identified application.	
Applicant claims the following fee status: ◉ Small Entity ○ Micro Entity ○ Regular Undiscounted 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.	
THIS PORTION MUST BE COMPLETED BY THE SIGNATORY OR SIGNATORIES I certify, in accordance with 37 CFR 1.4(d)(4) that I am: ◉ An attorney or agent registered to practice before the Patent and Trademark Office who is of record in this application Registration Number 74472 ○ A sole inventor ○ A joint inventor; I certify that I am authorized to sign this submission on behalf of all of the inventors as evidenced by the power of attorney in the application ○ A joint inventor; all of whom are signing this request	
Signature	/Keith D. Harden, Reg. #74472/
Name	Keith D. Harden

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).
Form PTO/SB/96 may be used for making this certification. See MPEP § 324.

Electronic Patent Application Fee Transmittal

Application Number:	15297328
Filing Date:	19-Oct-2016
Title of Invention:	SYSTEM AND METHOD FOR PROVIDING ADDITIONAL FUNCTIONALITY TO EXISTING SOFTWARE IN AN INTEGRATED MANNER
First Named Inventor/Applicant Name:	SIVAKUMAR CHATURVEDI
Filer:	Keith D. Harden
Attorney Docket Number:	DAMA-33216

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
STATUTORY OR TERMINAL DISCLAIMER	2814	1	160	160
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**160**

Doc Code: DISQ.E.FILE
Document Description: Electronic Terminal Disclaimer – Approved

Application No.: 15297328

Filing Date: 19-Oct-2016

Applicant/Patent under Reexamination: CHATURVEDI

Electronic Terminal Disclaimer filed on December 21, 2016

☒ APPROVED

This patent is subject to a terminal disclaimer

☐ DISAPPROVED

Approved/Disapproved by: Electronic Terminal Disclaimer automatically approved by EFS-Web

U.S. Patent and Trademark Office

Electronic Acknowledgement Receipt	
EFS ID:	27868059
Application Number:	15297328
International Application Number:	
Confirmation Number:	6761
Title of Invention:	SYSTEM AND METHOD FOR PROVIDING ADDITIONAL FUNCTIONALITY TO EXISTING SOFTWARE IN AN INTEGRATED MANNER
First Named Inventor/Applicant Name:	SIVAKUMAR CHATURVEDI
Customer Number:	25883
Filer:	Keith D. Harden
Filer Authorized By:	
Attorney Docket Number:	DAMA-33216
Receipt Date:	21-DEC-2016
Filing Date:	19-OCT-2016
Time Stamp:	16:23:30
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$160
RAM confirmation Number	122216INTEFSW00016784200780
Deposit Account	200780
Authorized User	Keith Harden
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.17 (Patent application and reexamination processing fees) 37 CFR 1.21 (Miscellaneous fees and charges)	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Electronic Terminal Disclaimer-Filed	eTerminal-Disclaimer.pdf	34168 656c680f150e5b6b82cbc5e6186e0d9cb3e83378	no	2
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30422 6367e5e8bfb28ada12c38772f20af5de8ce87029	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	64590		

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.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

HOWISON & ARNOTT, L.L.P
P.O. BOX 741715
DALLAS TX 75374-1715

MAILED
NOV 03 2016
OFFICE OF PETITIONS

Doc Code: TRACK1.GRANT

Decision Granting Request for Prioritized Examination (Track I or After RCE)	Application No.: 15/297,328

1. THE REQUEST FILED October 19, 2016 IS **GRANTED**.

The above-identified application has met the requirements for prioritized examination

A. ☒ for an original nonprovisional application (Track I).
B. ☐ for an application undergoing continued examination (RCE).

2. **The above-identified application will undergo prioritized examination.** The application will be accorded special status throughout its entire course of prosecution until one of the following occurs:

A. filing a **petition for extension of time** to extend the time period for filing a reply;
B. filing an **amendment to amend the application to contain more than four independent claims, more than thirty total claims**, or a multiple dependent claim;
C. filing a **request for continued examination**;
D. filing a notice of appeal;
E. filing a request for suspension of action;
F. mailing of a notice of allowance;
G. mailing of a final Office action;
H. completion of examination as defined in 37 CFR 41.102; or
I. abandonment of the application.

Telephone inquiries with regard to this decision should be directed to Brian W. Brown at 571-272-5338.

/Brian W. Brown/
[*Signature*]

Petitions Examiner, Office of Petitions
(Title)

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 15/297,328

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	70		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	300		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	360		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	30 minus 20 =	* 10	x 40 =	400	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	4 minus 3 =	* 1	x 210 =	210			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	1340		TOTAL	

APPLICATION AS AMENDED - PART II

AMENDMENT A

	(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))	*	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	

AMENDMENT B

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)		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 found in the appropriate box in column 1.

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
15/297,328	10/19/2016	2844	1340	DAMA-33216	30	4

CONFIRMATION NO. 6761

25883
HOWISON & ARNOTT, L.L.P
P.O. BOX 741715
DALLAS, TX 75374-1715

FILING RECEIPT



Date Mailed: 11/01/2016

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**

Inventor(s)

SIVAKUMAR CHATURVEDI, ALLEN, TX;
SATISH GUNDABATHULA, IRVING, TX;
RASHMI HIREMATH, ALLEN, TX;

Applicant(s)

DAMAKA, INC., RICHARDSON, TX;

Power of Attorney: The patent practitioners associated with Customer Number 25883

Domestic Priority data as claimed by applicant

This application is a CON of 15/049,891 02/22/2016 PAT 9491233
which is a CON of 14/690,619 04/20/2015 PAT 9270744
which is a CON of 14/024,027 09/11/2013 PAT 9027032
which claims benefit of 61/846,958 07/16/2013

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 10/28/2016
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 15/297,328**
Projected Publication Date: 02/09/2017
Non-Publication Request: No
Early Publication Request: No
**** SMALL ENTITY ****
Title

SYSTEM AND METHOD FOR PROVIDING ADDITIONAL FUNCTIONALITY TO EXISTING SOFTWARE IN AN INTEGRATED MANNER

Preliminary Class

326

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

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 (1-866-999-4258).

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 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).

SelectUSA

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 U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

PTO/SB/08a (01-10)
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 contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15297328
Filing Date	2016-10-19
First Named Inventor	CHATURVEDI, Sivakumar
Art Unit	
Examiner Name	
Attorney Docket Number	DAMA-33216

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	7778187	B2	2010-08-00	CHATURVEDI ET AL.	
	2	6438376	B1	2002-08-20	ELLIOTT ET AL.	
	3	6898413	B2	2005-05-24	YIP ET AL.	
	4	7664495	B1	2010-02-16	BONNER ET AL.	
	5	7623516	B2	2009-11-24	CHATURVEDI ET AL.	
	6	7623476	B2	2009-11-24	RAVIKUMAR ET AL.	
	7	7590758	B2	2009-09-15	TAKEDA ET AL.	
	8	6128283	A	2000-10-03	SABAA ET AL.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	
	Examiner Name	
	Attorney Docket Number	DAMA-33216

	9	6389016	B1	2002-05-00	SABAA ET AL.	
	10	7345999	B2	2008-03-00	SU ET AL.	
	11	7542472	B1	2009-06-00	GERENDAI ET AL.	
	12	8009586	B2	2011-08-00	CHATURVEDI ET AL.	
	13	7302496	B1	2007-11-27	METZGER	
	14	6161082		2000-12-12	GOLDBERG ET AL.	
	15	8065418		2011-11-00	ABUAN ET AL.	
	16	7656870	B2	2010-02-00	RAVIKUMAR ET AL.	
	17	7487248	B2	2009-02-00	MORAN ET AL.	
	18	7574523	B2	2009-08-00	TRAVERSAT ET AL.	
	19	7774495	B2	2010-08-00	PABLA ET AL.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	
	Examiner Name	
	Attorney Docket Number	DAMA-33216

	20	7782866	B1	2010-08-00	WALSH ET AL.	
	21	6298129		2001-10-00	CULVER ET AL.	
	22	6754181		2004-06-00	ELLIOTT ET AL.	
	23	7006508		2006-02-00	BONDY ET AL.	
	24	7010109		2006-03-00	GRITZER ET AL.	
	25	7123710		2006-10-00	RAVISHANKAR	
	26	7570743		2009-08-04	BARCLAY ET AL.	
	27	7769881		2010-08-00	MATSUBARA ET AL.	
	28	7346044	B1	2008-03-00	CHOU ET AL.	
	29	7092385		2006-08-00	GALLANT ET AL.	
	30	5818447		1998-10-00	WOLF ET AL.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	
	Examiner Name	
	Attorney Docket Number	DAMA-33216

	31	7917584		2011-03-00	ARTHURSSON, DANIEL	
	32	7564843	B2	2009-07-21	MANJUNATHA ET AL.	
	33	7185114	B1	2007-02-27	HARIHARASUBRAHMANIAN	
	34	6031818	A	2000-02-29	LO ET AL.	
	35	6311150	B1	2001-10-30	RAMASWAMY ET AL.	
	36	6999932	B1	2006-02-14	ZHOU, GUOJUN	
	37	7272377	B2	2007-09-18	COX ET AL.	
	38	7412374	B1	2008-08-12	SEILER ET AL.	
	39	6766373	B1	2004-07-20	BEADLE, BRUCE A.	
	40	7304985	B2	2007-12-04	SOJKA ET AL.	
	41	7353255	B2	2008-04-01	ACHARYA ET AL.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	
	Examiner Name	
	Attorney Docket Number	DAMA-33216

	42	7477282	B2	2009-01-13	FIRESTONE ET AL.	
	43	5442637	A	1995-08-01	NGUYEN, MAI-HUONG	
	44	6343067	B1	2002-01-01	DROTTAR ET AL.	
	45	6473425	B1	2002-10-01	BELLATON ET AL.	
	46	6574668	B1	2003-06-01	GUBBI ET AL.	
	47	6850769	B2	2005-02-01	GROB ET AL.	
	48	7080158	B1	2006-07-01	SQUIRE, MATTHEW	
	49	5889762		1999-03-30	PAJUVIRTA ET AL	
	50	7184415	B2	2007-02-01	CHANEY ET AL.	
	51	5790637	A	1998-08-01	JOHNSON ET AL.	
	52	6836765	B1	2004-12-01	SUSSMAN, LESTER	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	
	Examiner Name	
	Attorney Docket Number	DAMA-33216

	53	7613171	B2	2009-11-00	ZEHAVI ET AL.	
	54	6842460	B1	2005-01-00	OLKKONEN ET AL.	
	55	6987756		2006-01-00	RAVINDRANATH ET AL.	
	56	7512652		2009-03-00	APPELMAN ET AL.	
	57	5761309	A	1998-06-01	OHASHI ET AL.	
	58	6141687	A	2000-10-01	BLAIR, DANA L.	
	59	6202084	B1	2001-03-13	KUMAR ET AL.	
	60	6219638	B1	2001-04-01	PADMANABHAN ET AL.	
	61	6360196	B1	2002-03-01	POZNASKI ET AL.	
	62	6826613	B1	2002-03-01	WANG ET AL.	
	63	7013155	B1	2006-03-01	RUF ET AL.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	
	Examiner Name	
	Attorney Docket Number	DAMA-33216

	64	7117526	B1	2006-10-01	SHORT, JOEL E.	
	65	7353252	B1	2008-04-01	YANG ET AL.	
	66	6940826	B1	2005-09-06	SIMARD ET AL.	
	67	6741691	B1	2004-05-25	RITTER ET AL.	
	68	6912278	B1	2005-06-28	HAMILTON, THOMAS	
	69	6963555	B1	2005-11-08	BRENNER ET AL.	
	70	6975718	B1	2005-12-13	PEARCE ET AL.	
	71	6999575	B1	2006-02-14	SHEINBEIN, DANIEL	
	72	7079529	B1	2006-07-18	KHUC, MINH DUY	
	73	7457279	B1	2008-11-25	SCOTT ET AL.	
	74	8407576	B1	2013-03-26	YIN ET AL.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	
	Examiner Name	
	Attorney Docket Number	DAMA-33216

	75	6195694	B1	2001-02-27	CHEN ET AL.	
	76	8200796	B1	2012-06-12	MARGULIS	
	77	6606112	B1	2003-08-12	FALCO	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20030126213	A1	2003-07-03	BETZLER, BOAS	
	2	20030163525	A1	2003-08-28	HENDRIKS ET AL.	
	3	20040005877	A1	2004-01-00	VAANANEN, MIKKO KALERVO	
	4	20040249953	A1	2004-12-00	FERNANDEZ ET AL.	
	5	20080032695	A1	2008-02-07	ZHU ET AL.	
	6	20050136911	A1	2005-06-23	CSAPO ET AL.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	
	Examiner Name	
	Attorney Docket Number	DAMA-33216

	7	20040203834	A1	2004-10-14	MAHANY, RONALD L.	
	8	20020173303	A1	2002-11-21	SHIBUTANI, AKIRA	
	9	20060002355	A1	2006-01-05	BAEK ET AL.	
	10	20060182100	A1	2006-08-17	LI, JIN ET AL.	
	11	20080080392	A1	2008-04-03	WALSH, RICHARD J. ET AL.	
	12	20090300673	A1	2009-12-03	BACHET, FRANCK ET AL.	
	13	20020037000	A1	2002-03-00	PARK ET AL.	
	14	20030043764	A1	2003-03-00	KIM ET AL.	
	15	20030202480	A1	2003-10-30	SWAMI, YOGESH PREM	
	16	20040052234	A1	2004-03-00	AMEIGEIRAS ET AL.	
	17	20040213184	A1	2004-10-00	HU ET AL.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	
	Examiner Name	
	Attorney Docket Number	DAMA-33216

	18	20090003322	A1	2009-01-01	ISUMI, SHINYA	
	19	20090327516	A1	2009-12-31	AMISHIMA, MAKI ET AL.	
	20	20060187926	A1	2006-08-24	IMAI, NAOKI	
	21	20070019545	A1	2007-01-25	ALT, WADE R. ET AL.	
	22	20050208947	A1	2005-09-22	BAHL, PRADEEP	
	23	20070297430	A1	2007-12-27	NYKANEN, PETRI ET AL.	
	24	20030214955	A1	2003-11-20	KIM, JUN-HYEONG	
	25	20050270992	A1	2005-12-08	SANZGIRI, AJIT ET AL.	
	26	20090052399	A1	2009-02-26	SILVER ET AL.	
	27	20070206563	A1	2007-09-06	SILVER ET AL.	
	28	20030217318	A1	2003-11-00	CHOI, SUNG-KYU	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	
	Examiner Name	
	Attorney Docket Number	DAMA-33216

	29	20020064167	A1	2002-05-00	KHAN ET AL.	
	30	20060203750	A1	2006-09-14	RAVIKUMAR ET AL.	
	31	20060120375	A1	2006-06-08	RAVIKUMAR ET AL.	
	32	20070165629	A1	2007-07-19	CHATURVEDI ET AL.	
	33	20080235511	A1	2008-09-25	O'BRIEN, WILLIAM G. ET AL.	
	34	20100049980	A1	2010-02-25	BARRIGA, LUIS ET AL.	
	35	20080250408	A1	2008-10-09	TSUI ET AL.	
	36	20090136016	A1	2009-05-28	GORNOI ET AL.	
	37	20080235362	A1	2008-09-25	KJESBU ET AL.	
	38	20040148434	A1	2004-07-29	MATSUBARA ET AL.	
	39	20090182815	A1	2009-07-16	CZECHOWSKI ET AL.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	
	Examiner Name	
	Attorney Docket Number	DAMA-33216

	40	20080273541	A1	2008-11-06	PHARN	
	41	20030046585	A1	2003-03-06	MINNICK	
	42	20040024879	A1	2004-02-05	DINGMAN ET AL.	
	43	20090006076	A1	2009-01-01	JINDAL, DINESH K.	
	44	20100223047	A1	2010-09-02	CHRIST,	
	45	20100299150	A1	2010-11-25	FEIN ET AL.	
	46	20050198499	A1	2005-09-00	SALAPAKA ET AL.	
	47	20040139230	A1	2004-07-00	KIM, SEON KEON	
	48	20040240399	A1	2004-12-00	CORRAO ET AL.	
	49	20050201357	A1	2005-09-00	POYHONEN, PETTERI	
	50	20060121902	A1	2006-06-08	JAGADEESAN ET AL.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	
	Examiner Name	
	Attorney Docket Number	DAMA-33216

	51	20060205436	A1	2006-09-00	LIU ET AL.	
	52	20050130650	A1	2005-06-16	CREAMER ET AL.	
	53	20090088150	A1	2009-04-02	CHATURVEDI ET AL.	
	54	20100011111	A1	2010-01-14	MOHAMMAD, VIZAEI	
	55	20080130639	A1	2008-06-00	COSTA-REQUENA ET AL.	
	56	20060072506	A1	2006-04-00	SAYEEDI ET AL.	
	57	20060062180	A1	2006-03-00	SAYEEDI ET AL.	
	58	20080019285	A1	2008-01-00	JOHN ET AL.	
	59	20070253435	A1	2007-11-00	KELLER ET AL.	
	60	20050120073	A1	2005-06-00	CHO, JOON-HO	
	61	20050033843	A1	2005-02-00	SHAHI ET AL.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	
	Examiner Name	
	Attorney Docket Number	DAMA-33216

	62	20030088676	A1	2003-05-00	SMITH ET AL.	
	63	20070130253	A1	2007-06-00	NEWSON ET AL.	
	64	20100077023	A1	2010-03-00	ERIKSSON, ANDERS	
	65	20090055473	A1	2009-02-00	SYNNERGREN, PER	
	66	20080091813	A1	2008-04-00	BODLAENDER, MAARTEN	
	67	20070136459	A1	2007-06-00	ROCHE ET AL.	
	68	20050144288	A1	2005-06-00	LIAO, EN-YI	
	69	20040068567	A1	2004-04-00	MORAN ET AL.	
	70	20050220017	A1	2005-10-00	BRAND ET AL.	
	71	20030172145	A1	2003-09-00	NGUYEN	
	72	20110122864	A1	2011-05-26	CHERIFI ET AL.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	
	Examiner Name	
	Attorney Docket Number	DAMA-33216

	73	20090257433	A1	2009-10-15	MUTIKAINEN ET AL.	
	74	20060195402	A1	2006-08-00	MALINA ET AL.	
	75	20100299313	A1	2010-11-00	ORSINI ET AL.	
	76	20060171534	A1	2006-08-03	BAUGHMAN, WILLIAM P.	
	77	20070260359	A1	2007-11-00	BENSON ET AL.	
	78	20080168440	A1	2008-07-00	REGNIER ET AL.	
	79	20020031212	A1	2002-03-00	O'NEIL ET AL.	
	80	20050132009	A1	2005-06-00	SOLIE, KEVIN	
	81	20090234967	A1	2009-09-00	YU ET AL.	
	82	20100011108	A1	2010-01-00	CLARK ET AL.	
	83	20080123685	A1	2008-05-00	VARMA ET AL.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	
	Examiner Name	
	Attorney Docket Number	DAMA-33216

	84	20070082671	A1	2007-04-00	FENG ET AL.	
	85	20070025270	A1	2007-02-00	SYLVAIN, DANY	
	86	20060258289	A1	2006-11-00	DUA, ROBIN	
	87	20110099612	A1	2011-04-00	LEE ET AL.	
	88	20070274276	A1	2007-11-00	LAROIA ET AL.	
	89	20110040836	A1	2011-02-00	ALLEN ET AL.	
	90	20100312897	A1	2010-12-00	ALLEN ET AL.	
	91	20100312832	A1	2010-12-00	ALLEN ET AL.	
	92	20090156217	A1	2009-06-00	BAJPAI, RAJNEESH	
	93	20050138128	A1	2005-06-00	BANIEL ET AL.	
	94	20070116224	A1	2007-05-00	BURKE ET AL.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	
	Examiner Name	
	Attorney Docket Number	DAMA-33216

	95	20050187781	A1	2005-08-00	CHRISTENSEN, TORE L.	
	96	20110314134	A1	2011-12-00	FOTI, GEORGE	
	97	20100107205	A1	2010-04-00	FOTI, GEORGE	
	98	20100279670	A1	2010-11-00	GHAI ET AL.	
	99	20120263144	A1	2012-10-00	NIX, JOHN A.	
	100	20110145687	A1	2011-06-00	GRIGSBY ET AL.	
	101	20070239892	A1	2007-10-00	OTT ET AL.	
	102	20020152325	A1	2002-10-00	ELGEBALY ET AL.	
	103	20020156844	A1	2002-10-00	MAEHIRO, KAZUTOYO	
	104	20030212772	A1	2003-11-00	HARRIS, ADAM PIERCE	
	105	20020124096	A1	2002-09-05	LOGUINOV ET AL.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	
	Examiner Name	
	Attorney Docket Number	DAMA-33216

	106	20050201485	A1	2005-09-15	FAY	
	107	20060069775	A1	2006-03-30	ARTOBELLO ET AL.	
	108	20060165029	A1	2006-07-27	MELPIGNANO ET AL.	
	109	20050015502	A1	2005-01-20	KANG ET AL.	
	110	20030229715	A1	2003-12-11	BARATAKKE ET AL.	
	111	20010050923	A1	2001-12-13	PARK ET AL.	
	112	20040062267	A1	2004-04-01	MINAMI ET AL.	
	113	20020184310	A1	2002-12-01	TRAVERSAT ET AL.	
	114	20030076815	A1	2003-04-23	MILLER ET AL.	
	115	20040034793	A1	2004-02-19	YUAN, WEI	
	116	20040139225	A1	2004-07-15	TAKAHASHI, MASAYUKI	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	
	Examiner Name	
	Attorney Docket Number	DAMA-33216

	117	20050033985	A1	2005-02-10	XU ET AL.	
	118	20050091407	A1	2005-04-28	VAZIRI ET AL.	
	119	20050195802	A1	2005-09-08	KLEIN ET AL.	
	120	20050286519	A1	2005-12-29	RAVIKUMAR ET AL.	
	121	20070016921	A1	2007-01-01	LEVI ET AL.	
	122	20030046056	A1	2003-03-06	GODOY ET AL.	
	123	20040158471	A1	2004-08-12	DAVIS ET AL.	
	124	20050086309	A1	2005-04-21	GALLI ET AL.	
	125	20040162871	A1	2004-08-19	PABLA ET AL.	
	126	20030115251	A1	2003-06-19	FREDRICKSON ET AL.	
	127	20020178087	A1	2002-11-28	HENDERSON ET AL.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	
	Examiner Name	
	Attorney Docket Number	DAMA-33216

	128	20060183476	A1	2006-08-17	MORITA, J. ET AL.	
	129	20030220121	A1	2003-11-27	KONISHI, T. ET AL.	
	130	20080192756	A1	2008-08-14	DAMOLA ET AL.	
	131	20030072485	A1	2003-04-17	GUERIN ET AL.	
	132	20050008024	A1	2005-01-13	NEWPOL ET AL.	
	133	20020176404	A1	2002-11-28	GIRARD, GREGORY D.	
	134	20030137939	A1	2003-07-24	DUNNING ET AL.	
	135	20040100973	A1	2004-05-01	PRASAD, ANAND R.	
	136	20020080719	A1	2002-06-27	PARKVALL ET AL.	
	137	20040228279	A1	2004-11-18	MIDTUN ET AL.	
	138	20050050227	A1	2005-03-01	MICHELMAN, ERIC H.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	
	Examiner Name	
	Attorney Docket Number	DAMA-33216

	139	20030217171	A1	2003-11-01	VON STUERMER ET AL.	
	140	20040267938	A1	2004-12-01	SHOROFF ET AL.	
	141	20020087887	A1	2002-07-01	BUSAM ET AL.	
	142	20020120757	A1	2002-08-01	SUTHERLAND ET AL.	
	143	20020166053	A1	2002-11-01	WILSON, RODGER P.	
	144	20030044020	A1	2003-03-01	ABOBA ET AL.	
	145	20030163697	A1	2003-08-01	PABLA ET AL.	
	146	20030177422	A1	2003-09-01	TARAROUKHINE ET AL.	
	147	20040260952	A1	2004-12-01	NEWMAN ET AL.	
	148	20050249196	A1	2005-11-01	ANSARI ET AL.	
	149	20060148516	A1	2006-07-01	REDDY ET AL.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	
	Examiner Name	
	Attorney Docket Number	DAMA-33216

	150	20070110043	A1	2007-05-01	GIRARD, GREGORY D.	
	151	20080069105	A1	2008-03-01	COSTA ET AL.	
	152	20080320096	A1	2008-12-01	SZETO, CHRISTOPHER	
	153	20090192976	A1	2009-07-01	SPIVACK ET AL.	
	154	20050119005	A1	2005-06-00	SEGAL ET AL.	
	155	20060246903	A1	2006-11-00	KONG ET AL.	
	156	20030031210	A1	2003-02-00	HARRIS, JOHN M.	
	157	20030035441	A1	2003-02-00	CHENG ET AL.	
	158	20030174707	A1	2003-09-00	GROB ET AL.	
	159	20050138119	A1	2005-06-23	SARIDAKIS, TITOS	
	160	20020038282	A1	2002-03-01	MONTGOMERY, ROB R.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	
	Examiner Name	
	Attorney Docket Number	DAMA-33216

	161	20020042769	A1	2002-04-01	GUJRAL ET AL.	
	162	20020062285	A1	2002-05-01	AMANN ET AL.	
	163	20020097150	A1	2002-07-01	SANDELMAN ET AL.	
	164	20020143548	A1	2002-10-01	KORALL ET AL.	
	165	20020150110		2002-10-17	INBAR ET AL.	
	166	20030009565		2003-01-09	ARAO	
	167	20030061025	A1	2003-03-01	ABIR, ELI	
	168	20030061481	A1	2003-03-27	LEVINE ET AL.	
	169	20030078858	A1	2003-04-01	ANGELOPOULOS ET AL.	
	170	20030105812	A1	2003-06-05	FLOWERS, JR., ET AL.	
	171	20030110047	A1	2003-06-01	SANTOSUOSSO, JOHN MATTHEW	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	
	Examiner Name	
	Attorney Docket Number	DAMA-33216

	172	20030135569		2003-07-17	KHAKOO ET AL.	
	173	20030158722	A1	2003-08-01	LORD, JOHN RAYMOND	
	174	20030177186	A1	2003-09-01	GOODMAN ET AL.	
	175	20030187650	A1	2003-10-01	MOORE ET AL.	
	176	20040034776	A1	2003-10-01	FERNANDO ET AL.	
	177	20040039781	A1	2004-02-01	LAVALLEE ET AL.	
	178	20040044517	A1	2004-03-01	PALMQUIST, ROBERT	
	179	20040128554	A1	2004-07-01	MAHER, III, ET AL.	
	180	20040133689	A1	2004-07-08	VASISHT, SAMRAT	
	181	20040139228		2004-07-15	TAKEDA ET AL.	
	182	20040143678	A1	2004-07-01	CHARI ET AL.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	
	Examiner Name	
	Attorney Docket Number	DAMA-33216

	183	20040153858	A1	2004-08-01	HWANG, SHAW HWA	
	184	20040267527	A1	2004-12-01	CREAMER ET AL.	
	185	20040268257	A1	2004-12-01	MUDUSURU, GIRI P.	
	186	20050004982	A1	2005-01-06	VERNON ET AL.	
	187	20050071481	A1	2005-03-01	DANIELI, DAMON V.	
	188	20050143105	A1	2005-06-01	OKAMOTO, YUKIFUMI	
	189	20050187957	A1	2005-08-01	KRAMER ET AL.	
	190	20050246193	A1	2005-11-03	ROEVER ET AL.	
	191	20050254440	A1	2005-11-17	SORRELL, JOHN D.	
	192	20060121986	A1	2006-06-01	PELKEY ET AL.	
	193	20060168643	A1	2006-07-01	HOWARD ET AL.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	
	Examiner Name	
	Attorney Docket Number	DAMA-33216

	194	20060218624	A1	2006-09-28	RAVIKUMAR ET AL.	
	195	20060230166	A1	2006-10-01	PHILYAW, JEFFRY JOVAN	
	196	20070078785	A1	2007-04-01	BUSH ET AL.	
	197	20070111794	A1	2007-05-01	HOGAN ET AL.	
	198	20070190987	A1	2007-08-01	VAANANEN, MIKKO KALERVO	
	199	20080005328		2008-01-01	SHIVELY ET AL.	
	200	20050105524	A1	2005-05-19	STEVENS ET AL.	
	201	20040103212	A1	2004-05-27	TAKEUCHI ET AL.	
	202	20090240821	A1	2009-09-24	JUNCKER ET AL.	
	203	20110141220	A1	2011-06-16	MIURA	
	204	20100174783	A1	2010-07-08	ZAROM	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	
	Examiner Name	
	Attorney Docket Number	DAMA-33216

	205	20070294626	A1	2007-12-20	FLETCHER ET AL.	
	206	20040249885	A1	2004-12-09	PETROPOULAKIS ET AL.	
	207	20110320821	A1	2011-12-29	ALKHATIB ET AL	
	208	20080320565	A1	2008-12-25	BUCH ET AL	
	209	20100191954	A1	2010-07-29	KIM ET AL	
	210	20130111064	A1	2013-05-02	MANI ET AL	
	211	20070280253	A1	2007-12-06	ROOHOLAMINI ET AL	
	212	20130067004	A1	2013-03-14	LOGUE ET AL	
	213	20080046984	A1	2008-02-21	BOHMER ET AL	
	214	20120078609	A1	2012-03-29	CHATURVEDI ET AL	
	215	20060233117	A1	2006-10-19	TOMSU ET AL	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	
	Examiner Name	
	Attorney Docket Number	DAMA-33216

	216	20110307556	A1	2011-12-15	CHATURVEDI ET AL	
	217	20130106989	A1	2013-05-02	TELIRIS, INC.	
	218	20080244718	A1	2008-10-02	FROST ET AL	
	219	20120124191	A1	2012-05-17	LYON	
	220	20040193599	A1	2004-09-30	LIU ET AL.	
	221	20100058353	A1	2010-03-04	TURSKI	
	222	20130125145	A1	2013-05-16	BALMORI LABRA ET AL.	
	223	20150026700	A1	2015-01-22	CHATURVEDI ET AL.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	1848163	EP	A1	2007-10-24	SHARP KABUSHIKI KAISHA		

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	
	Examiner Name	
	Attorney Docket Number	DAMA-33216

	2	1988698	EP	A1	2008-11-05	RESEARCH IN MOTION LIMITED		
	3	1988697	EP	A1	2008-11-05	RESEARCH IN MOTION LIMITED		
	4	2006064047	WO	A1	2006-06-22	INTERNATIONAL BUSINESS MACHINES CORPORATION ET AL.		
	5	1638275	EP	A2	2006-03-22	WECOMM LIMITED		
	6	160339	EP	A1	2005-12-07	STMICROELECTRONICS S.R.I.		
	7	1404082	EP	A2	2004-03-31	NORTEL NETWORKS LTD		
	8	WO 2003/079635	WO		2003-09-25	IBM CORPORATION ET AL.		
	9	WO 2004/063843	WO		2004-07-29	MATSUSHITA ELECTRIC IND CO LTD		
	10	WO 2005/009019	WO		2005-01-27	SKYPER LTD. ET AL.		
	11	2005-94600	JP		2005-04-07	NEC CORP.		
	12	2007-043598	JP		2007-02-15	2007-02-15		

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	
	Examiner Name	
	Attorney Docket Number	DAMA-33216

	13	10-2005-0030548	KR		2005-03-30	MICROSOFT CORP.		
	14	WO 2006/075677	WO		2006-07-20	SHARP KABUSHIKI KAISHA		
	15	WO 2008099420	WO	A2	2008-08-21	MADHOK		

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5
	1	PCT: International Search Report and Written Opinion for PCT/US2011/024870; 26 October 2011; 12 pages.	
	2	J. ROSENBERG et al. " Session Traversal Utilities for NAT (STUN)", draft–ietf–behave–rfc3489bis–06, March 5, 2007.	
	3	PCT: International Search Report and Written Opinion for PCT/US2011/028685; 9 November 2011; 10 pages.	
	4	PCT: International Search Report and Written Opinion for PCT/US2011/029954; 24 November 2011; 8 pages.	
	5	PCT: International Search Report and Written Opinion for PCT/US2011/024891; 25 November 2011; 9 pages.	
	6	PCT: International Search Report and Written Opinion for PCT/US2011/031245; 26 December 2011; 13 pages.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	
	Examiner Name	
	Attorney Docket Number	DAMA-33216

	7	Wireless Application Protocol - Wireless Transport Layer Security Specification, Version 18-Feb-2000, Wireless Application Forum, Ltd. 2000; 99 pages.	
	8	PCT: International Search Report and Written Opinion for PCT/US2011/040864; 17 February 2012; 8 pages.	
	9	PCT: International Search Report and Written Opinion for PCT/US2011/041565; 5 January 2012; 7 pages.	
	10	PCT: International Search Report and Written Opinion for PCT/US2011/031246; 27 December 2011; 8 pages.	
	11	PCT: International Search Report and Written Opinion for PCT/US2011/049000; 27 March 2012; 10 pages.	
	12	PCT: International Search Report and Written Opinion for PCT/US2011/051877; 13 April 2012; 7 pages.	
	13	PCT: International Search Report and Written Opinion for PCT/US2011/055101; 22 May 2012; 9 pages.	
	14	Balamurugan Karpagavinayagam et al. (Monitoring Architecture for Lawful Interception in VoIP Networks, ICIMP 2007, 24 Aug 2008).	
	15	NiceLog User's Manual 385A0114-08 Rev. A2, March 2004.	
	16	WISPA: Wireless Internet Service Providers Association; WISPA-CS-IPNA-2.0; May 1, 2009.	
	17	PCT: International Preliminary Report on Patentability of PCT/US2011/024870; 30 August 2012; 7 pgs.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	
	Examiner Name	
	Attorney Docket Number	DAMA-33216

	18	RFC 5694 ("Peer-to-Peer (P2P) Architecture: Definition, Taxonomies, Examples, and Applicability", November 2009).	
	19	Mahy et al., The Session Initiation Protocol (SIP) "Replaces" Header, September 2004, RFC 3891, pages 1-16.	
	20	PCT: International Preliminary Report on Patentability of PCT/US2011/024891; 30 August 2012; 6 pgs.	
	21	T. Dierks & E. Rescorla, The Transport Layer Security (TLS) Protocol (Ver. 1.2, 8/2008) retrieved at http://tools.ietf.org/html/rfc5246. Relevant pages provided.	
	22	J. Rosenberg et al., SIP: Session Initiation Protocol (6/2008) retrieved at http://tools.ietf.org/html/rfc3261. Relevant pages provided.	
	23	Philippe Bazot et al., Developing SIP and IP Multimedia Subsystem (IMS) Applications (2/5/2007) retrieved at redbooks IBM form number: SG24-7255-00. Relevant pages provided.	
	24	PCT: International Preliminary Report on Patentability of PCT/US2011/028685; 4 October 2012; 6 pgs.	
	25	PCT: International Preliminary Report on Patentability of PCT/US2011/031245; 26 October 2012; 9 pgs.	
	26	PCT: International Preliminary Report on Patentability of PCT/US2011/029954; 11 October 2012; 5 pgs.	
	27	PCT: International Preliminary Report on Patentability of PCT/US2011/031246; 08 November 2012; 5 pgs.	
	28	Rosenberg, J; "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols"; 29 October 2007; I ETF; I ETF draft of RFC 5245, draft-ietf-mmusic-ice-19; pp 1-120.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	
	Examiner Name	
	Attorney Docket Number	DAMA-33216

	29	Blanchet et al; "IPv6 Tunnel Broker with the Tunnel Setup Protocol (TSP)"; 6 May 2008; IETF; IETF draft of RFC 5572, draftblanchet-v6ops-tunnelbroker-tsp-04; pp 1-33	
	30	Cooper et al; "NAT Traversal for dSIP"; 25 February 2007; IETF; IETF draft draft-matthews-p2psip-dsip-nat-traversal-00; pp 1-23	
	31	Cooper et al; "The Effect of NATs on P2PSIP Overlay Architecture"; IETF; IETF draft draft-matthews-p2psip-nats-and-overlays-01.txt; pp 1-20	
	32	Srisuresh et al; "State of Peer-to-Peer(P2P) Communication Across Network Address Translators(NATs)"; 19 November 2007; I ETF; I ETF draft for RFC 5128, draft-ietf-behave-p2p-state-06.txt; pp 1-33	
	33	PCT: International Search Report and Written Opinion for PCT/US2012/046026; 18 October 2012; 6 pages.	
	34	DUNIGAN, Tom, "Almost TCP over UDP (atou)," last modified Jan. 12, 2004; retrieved on Jan. 18, 2011 from <http://www.csm.ornl.gov/~dunigan/net100/atou.html> 18 pgs.	
	35	PCT: International Preliminary Report on Patentability of PCT/US2011/040864; 3 January 2013; 6 pgs.	
	36	PCT: International Preliminary Report on Patentability of PCT/US2011/041565; 10 January 2013; 6 pgs.	
	37	PCT: International Preliminary Report on Patentability of PCT/US2011/049000; 26 February 2013; 6 pgs.	
	38	PCT: International Preliminary Report on Patentability of PCT/US2011/051877; 26 March 2013; 5 pgs.	
	39	PCT: International Preliminary Report on Patentability of PCT/US2011/055101; 16 April 2013; 7 pgs.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	
	Examiner Name	
	Attorney Docket Number	DAMA-33216

	40	PCT: International Preliminary Report on Patentability of PCT/US2012/046026; 30 January 2014; 5 pgs.	
	41	PCT: International Preliminary Report on Patentability of PCT/US2008/075141; 09 March 2010; 5 pgs.	
	42	PCT: International Preliminary Report on Patentability of PCT/US2007/068820; 31December 2008; 8 pgs.	
	43	PCT: International Preliminary Report on Patentability of PCT/US2007/068823; 27 November 2008; 8 pgs.	
	44	PCT: International Preliminary Report on Patentability of PCT/US2006/047841; 06 November 2008; 7 pgs.	
	45	PCT: International Preliminary Report on Patentability of PCT/US2007/002424; 07 August 2008; 6 pgs.	
	46	PCT: International Preliminary Report on Patentability of PCT/US2006/040312; 02 May 2008; 5 pgs.	
	47	PCT: International Preliminary Report on Patentability of PCT/IB2005/000821; 19 October 2006; 10 pgs.	
	48	CHATHAPURAM, "Security in Peer-To-Peer Networks", August 8. 2001, XP002251813.	
	49	International Search Report and Written Opinion of the International Searching Authority from PCT/IB2005/000821, dated August 5, 2005.	
	50	International Search Report and Written Opinion of the International Searching Authority from PCT/US2006/032791, dated December 18, 2006.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	
	Examiner Name	
	Attorney Docket Number	DAMA-33216

If you wish to add additional non-patent literature document citation information please click the Add button	Add		
EXAMINER SIGNATURE			
Examiner Signature		Date Considered	

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

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	
	Examiner Name	
	Attorney Docket Number	DAMA-33216

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Keith D. Harden, Reg. #74472/	Date (YYYY-MM-DD)	2016-10-25
Name/Print	Keith D. Harden	Registration Number	74472

This collection of information is required by 37 CFR 1.97 and 1.98. 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 1 hour 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.**

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
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 contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	
	Examiner Name	
	Attorney Docket Number	DAMA-33216

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	
	Examiner Name	
	Attorney Docket Number	DAMA-33216

	1	International Search Report and Written Opinion of the International Searching Authority from PCT/US2006/040312, dated March 2, 2007.	
	2	International Search Report and Written Opinion of the International Searching Authority from PCT/US2006/047841, dated September 12, 2008.	
	3	International Search Report and Written Opinion of the International Searching Authority from PCT/US2007/002424, dated August 14, 2007.	
	4	International Search Report and Written Opinion of the International Searching Authority from PCT/US2007/068820, dated June 11, 2008.	
	5	International Search Report and Written Opinion of the International Searching Authority from PCT/US2007/068821, dated June 14, 2008.	
	6	International Search Report and Written Opinion of the International Searching Authority from PCT/US2007068823, dated June 1, 2008.	
	7	JEFF TYSON, "How Instant Messaging Works", www.verizon.com/learningcenter, March 9, 2005.	
	8	RORY BLAND, et al,"P2P Routing" 03/2002.	
	9	ROSENBERG, "STUN- Simple Traversal of UDP Through NAT", September 2002, XP015005058.	
	10	SALMAN A. BASET, et al, "An Analysis Of The Skype Peer-To-Peer Internet Telephony Protocol", Department of Computer Science, Columbia University, New York, NY, USA, September 15, 2004.	
	11	SINGH et al., "Peer-to Peer Internet Telephony Using SIP", Department of Computer Science, Columbia University, October 31, 2004, XP-002336408.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	
	Examiner Name	
	Attorney Docket Number	DAMA-33216

	12	SINHA, S. and OGLIESKI, A., A TCP Tutorial, November 1998 (Date posted on Internet: 19 April 2001) [Retrieved from the Internet <URL:http//www.ssfnet.org/Exchange/tcp/tcpTutorialNotes.html>]	
	13	Pejman Khadivi, Terence D. Todd and Dongmei Zhao, "Handoff trigger nodes for hybrid IEEE 802.11 WLAN/cellular networks," Proc. Of IEEE International Conference on Quality of Service in Heterogeneous Wired/Wireless Networks, pp. 164-170, 18 October 2004.	
	14	International Search Report and Written Opinion of the International Searching Authority from PCT/US2008/078142, dated March 27, 2009.	
	15	International Search Report and Written Opinion of the International Searching Authority from PCT/US2008/084950, dated April 27, 2009.	
	16	Hao Wang, Skype VoIP service-architecture and comparison, In: INFOTECH Seminar Advanced Communication Services (ASC), 2005, pp. 4, 7, 8.	
	17	Seta, N.; Miyajima, H.; Zhang, L;; Fujii, T., "All-SIP Mobility: Session Continuity on Handover in Heterogeneous Access Environment," Vehicular Technology Conference, 2007. VTC 2007-Spring. IEEE 65th, 22-25 April 2007, pages: 1121-1126.	
	18	International Search Report and Written Opinion of the International Searching Authority from PCT/US2008/075141, dated March 5, 2009.	
	19	Qian Zhang; Chuanxiong Guo; Zihua Guo; Wenwu Zhu, "Efficient mobility management for vertical handoff between WWAN and WLAN," Communications Magazine, IEEE, vol. 41. issue 11, November 2003, pages: 102-108.	
	20	ISAACS, Ellen et al., "Hubbub: A sound-enhanced mobile instant messenger that supports awareness and opportunistic interactions," Proceedings of the SIGCHI Conference On Human Factors in Computing Systems; Vol. 4, Issue No. 1; Minneapolis, Minnesota; 20-25 April 2002; pgs. 179-186.	
	21	PCT: International Preliminary Report on Patentability of PCT/US2008/084950; 01 June 2010; 5 pgs.	
	22	International Search Report and Written Opinion of the International Searching Authority from PCT/US2014/039777, dated September 30, 2014.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	
	Examiner Name	
	Attorney Docket Number	DAMA-33216

	23	International Search Report and Written Opinion of the International Searching Authority from PCT/US2014/39782, dated October 17, 2014.	
	24	International Search Report and Written Opinion of PCT/US2015/43633, 2015 October 26, 21 pgs.	
	25	PCT: International Search Report and Written Opinion of PCT/US2015/43630 (related application), 2015 October 30, 20 pgs.	
	26	PCT: International Preliminary Report on Patentability of PCT/US2014/039777; 28 January 2016; 8 pgs.	
	27	PCT: International Preliminary Report on Patentability of PCT/US14/39782; 19 April 2016; 9 pgs.	

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15297328
	Filing Date	2016-10-19
	First Named Inventor	CHATURVEDI, Sivakumar
	Art Unit	
	Examiner Name	
	Attorney Docket Number	DAMA-33216

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Keith D. Harden, Reg. #74472/	Date (YYYY-MM-DD)	2016-10-25
Name/Print	Keith D. Harden	Registration Number	74472

This collection of information is required by 37 CFR 1.97 and 1.98. 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 1 hour 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.**

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 404 082 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
31.03.2004 Bulletin 2004/14

(51) Int Cl.[7]: **H04L 29/06**

(21) Application number: **03016018.8**

(22) Date of filing: **15.07.2003**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LU MC NL PT RO SE SI SK TR
Designated Extension States:
AL LT LV MK

(30) Priority: **24.09.2002 US 253097**

(71) Applicant: **Nortel Networks Limited**
St. Laurent, Quebec H4S 2A9 (CA)

(72) Inventor: **Roshko, Michael E.**
Brentford, Middlesex TW8 9QJ (GB)

(74) Representative: **Anderson, Angela et al**
Nortel Networks
IP Law Group,
Harlow Laboratories,
London Road
Harlow, Essex CM17 9NA (GB)

(54) Methods for discovering network address and port translators

(57) Network Address and Port Translators (NATs) have the potential to interrupt the end-to-end nature of Internet applications, thereby threatening end-to-end security and other end-to-end functions. Thus it is important to be able to discover the existence of NATs and their type. Accordingly there is provided a method of discovering the existence and type of NAT that involves instigating a test call between media endpoints on a Media Gateway (MG) and a Media Gateway Controller (MGC). The MGC is able to deduce the existence of a NAT by examining the media packets sent to its endpoint. If a NAT is determined to be present the MGC instructs the endpoint on the MG to send media packets to another endpoint on the MGC. By comparing the IP addresses and ports of the media packets received at the endpoints of the MGC, the MGC is able to deduce whether the type of NAT is Cone or Symmetric.

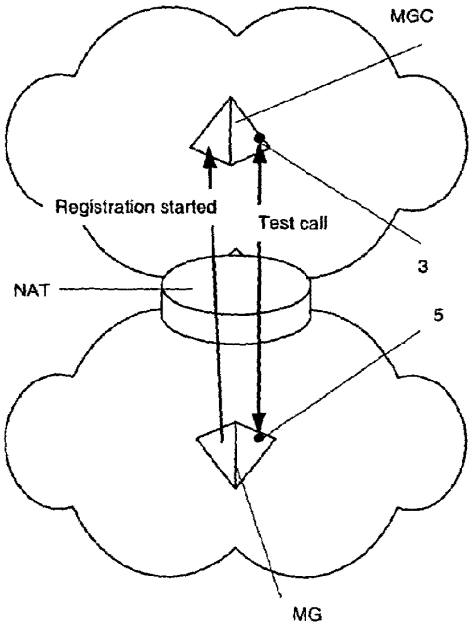


Fig. 1

EP 1 404 082 A2

Printed by Jouve, 75001 PARIS (FR)

Description

Field of the Invention

[0001] The present invention relates to a method of discovering Network Address and Port Translators, and, more particularly, to method of discovering Network Address and Port Translators sitting between Telephony Service Provider Networks and Networks containing Media Gateways.

Background of the invention

[0002] Network Address Translators (NATs) are used to interconnect a private network consisting of unregistered Internet Protocol (IP) addresses with a global IP network using a limited number of registered IP addresses. NATs are also used to avoid address renumbering in a private network when topology outside the private network changes for variety of reasons, such as customers changing providers, company backbones being reorganized, or providers merging or splitting. In addition, there are many other applications of NAT operation.

[0003] Basic Network Address Translation or Basic NAT is a method by which IP addresses are mapped from one group to another, transparent to end users. Network Address Port Translation, or NAPT is a method by which many network addresses and their Transmission Control Protocol/User Datagram Protocol (TCP/UDP) ports are translated into a single network address and TCP/UDP ports. Together, both these operations are referred to as traditional NAT.

[0004] NAT operation is asymmetrical with respect to the two Networks with which the NAT interfaces. In general, packets originating in the private network ("inside") are allowed to be sent to any address in the other network ("outside"). When the first packet of such a packet flow traverses the NAT, a NAT bind will be created, and the source IP address and port of the packet will be changed to reflect the NAT bind. Thus, when the packet arrives at its destination, it will appear to have come from a different source (i.e. from the NAT device). All subsequent packets of the flow will be modified in the same way. In contrast, packets originating from the outside network can not be routed to a host in the inside network, unless a NAT bind has previously been created in the NAT device. In such a case, the packets will have to be addressed to the IP address and port of the NAT bind on the NAT device. Upon receipt of the packets, the NAT device will translate the destination address and port into the proper inside address and port, and forward the packets on to their inside destination. Because of this asymmetry, hosts in the "inside" network are said to be "behind the NAT".

[0005] NATs are further classified based on the rules used to create NAT binds. NATs which create a unique bind for unique source and destination IP addresses and ports are known as Symmetric. NATs which create a unique bind for a unique source addess and port only (i. e. for any destination) are known as Cone.

[0006] Unless mentioned otherwise, the term NAT, as used in this specification, will pertain to traditional NAT, namely basic NAT as well as NAPT, and to the devices performing these functions: Network Address Translators, and Network Address and Port Translators.

[0007] A number of NAT deployments are currently in use and, naturally, a large number of internet applications work transparently with NATs. However, there are applications that fail if their packets traverse a NAT, such as applications that set-up voice over Internet Protocol (VoIP) calls. VoIP works by the two media endpoints involved in the call exchanging their Session Description Protocol (SDP). The SDP describes the IP address and port where the endpoint expects to receive media for the call, among other things. This exchange of SDP is made possible by the use of a protocol such as SIP, MGCP, H.248 (MEGACO), H.323, NCS or ASPEN, and often involves the help of a Media Gateway Contoller (MGC), typically a softswitch, to broker the exchange. NATs break this model, since the IP address and port embedded in SDP will not reflect the IP address and port modifications made by the NAT. In cases where NATs break the end-to-end functionality of applications, Application Level Gateways (ALGs) are required within the NAT to make application-specific changes to the packet contents so that it reflects the NAT bind, in order to ensure that the application can work through the NAT.

[0008] NATs have the potential to interrupt the end-to-end nature of Internet applications, thereby threatening end-to-end security and other end-to-end functions. In addition, NATs have topology restrictions and other constraints on the protocols and applications that run across the NATs. Thus it is important to be able to discover the existence of NATs and their type.

[0009] Known techniques for VoIP applications in which an MGC in a public TSP network is controlling a Media Gateway (MG) in a private network, involve determining a NAT's existence and type either through 'ad hoc' methods (for example, telephoning the owner of the MG and asking if they are using a NAT and then provisioning this information (by hand) into the MGC prior to bringing the MG into service), or by using a protocol such as Simple Traversal of UDP through NATs (STUN) to discover the presence and type of NATs between the MG and the TSP network. STUN is an Internet Engineering Task Force (IETF) Protocol, defined in the IETF draft "http://www.ietf.org/internet-drafts/draft-ietf-midcom-stun-02.txt", that allows applications to discover the presence and types of NATs in a network, as well as discovering the actual NAPT bind used for a particular media flow. It requires a STUN server in the outside network, and a STUN client in the inside network. By using the STUN protocol between the STUN client and server, the STUN client in the inside network is able to determine NAT existence, type and the actual NAT bind used

Ex.1002 / Page 179 of 1173
Cisco Systems, Inc.

for a media flow.

[0010] The disadvantage of the first technique is that it requires manual human intervention, and is unfeasible as a real solution. The disadvantage of the second technique is that STUN requires the introduction of new network components (STUN clients and servers) in both the TSP and MG networks. In addition, the STUN client must be integrated into the MGs themselves, which means that existing, deployed MGs must be upgraded to contain STUN clients before this technique can be used. Another disadvantage of the second technique is that NAT information is determined by the STUN client behind the NAT (i.e. by an agent in the inside), rather than by the MGC outside of the NAT, although the MGC may need to have knowledge of this information.

[0011] Thus there is a need for devising a method of discovering the existence of NATs and their type without requiring any new network elements, without requiring any new protocols or protocol extensions, without requiring any work on the MGs or NATS, without imposing any requirements on the networks outside the TSP network, that will work with existing deployments, using existing protocols.

[0012] The present invention aims to address the needs or at least mitigate the problems identified above.

[0013] This may be met by combinations of features of the main claims, the sub-claims disclose further advantageous embodiments of the invention.

Summary of the Invention

[0014] Accordingly, there is provided a method of determining the presence of a Network Address and Port Translator between a Telephony Service Provider Network and a network comprising a Media Gateway, said Telephony Service Provider Network comprising a Media Gateway Controller, said method comprising: instigating a test call between a first endpoint on the Media Gateway Controller acting as a calling party, and an endpoint on the Media Gateway acting as a called party; receiving a reply comprising the local Session Description Protocol of the endpoint of the Media Gateway at the Media Gateway Controller; receiving an empty/noise media packet from the Media Gateway at the first endpoint of the Media Gateway Controller; and comparing the source IP address and port of the empty/noise media packet received at the first endpoint of the Media Gateway Controller with the IP address and port contained in the received local Session Description Protocol of the endpoint of the Media Gateway, wherein if the IP addresses are different or the ports are different then a Network Address and Port Translator is determined to be present, otherwise, if the IP addresses are the same and the ports are the same then a Network Address and Port Translator is determined not to be present.

[0015] In a preferred embodiment, if a Network Address and Port Translator is found to present, said method further comprises determining the type of Network Address and Port Translator that is present. Preferably, determining the type of Network Address and Port Translator comprises: changing the remote Session Description Protocol for the call to one with a different IP address, but still on the same Media Gateway Controller, corresponding to a second virtual media endpoint; sending a message to modify the Session Description Protocol to the Media Gateway from the Media Gateway Controller; prompting the Media Gateway to send empty/noise media packets to the changed IP address and port corresponding to the second virtual media endpoint on the Media Gateway Controller; receiving the empty/noise media packets at the second virtual media endpoint on the Media Gateway Controller; comparing the source IP address and port of the empty/noise media packets received at the second virtual media endpoint of the Media Gateway Controller with the source IP address and port of the media packets received at the first virtual media endpoint of the Media Gateway Controller, wherein if the same source IP address and port is used for the media packets sent to the first and the second virtual media endpoints on the Media Gateway Controller, the Network Address and Port Translator is determined to be a Cone Network Address and Port Translator, but if a different source IP address or port is used for the media packets sent to the first and the second virtual media endpoints on the Media Gateway Controller, the Network Address and Port Translator is determined to be a Symmetric Network Address and Port Translator.

[0016] According to a second aspect of the invention there is provided a computer program for use in a computer for determining the presence of a Network Address and Port Translator between a Telephony Service Provider Network and a network comprising a Media Gateway, according to the first aspect.

[0017] According to a third aspect there is provided a computer program stored on a data carrier for use in a computer for determining the presence of a Network Address and Port Translator between a Telephony Service Provider Network and a network comprising a Media Gateway, according to the first aspect.

[0018] According to a fourth aspect there is provided a Media Gateway Controller comprising a first virtual media endpoint, and capable of determining the presence of a Network Address and Port Translator between a Telephony Service Provider Network in which said Media Gateway Controller is located, and a network comprising a Media Gateway, said Media Gateway Controller operable to: instigate a test call between its first virtual media endpoint acting as a calling party, and an endpoint on the Media Gateway acting as a called party; receive a reply comprising the local Session Description Protocol of the endpoint of the Media Gateway; receive empty/noise media packets from the Media Gateway at its first virtual media endpoint; and compare the source IP address and port of the empty/noise media packets received at its first virtual media endpoint with the IP ad-

Ex.1002 / Page 180 of 1173
Cisco Systems, Inc.

dress and port contained in the received local Session Description Protocol of the endpoint of the Media Gateway, wherein if the IP addresses are different or the ports are different then a Network Address and Port Translator is determined to be present, otherwise, if the IP addresses are the same and the ports are the same then a Network Address and Port Translator is determined not to be present.

[0019] In a preferred embodiment if a Network Address and Port Translator is found to be present, said Media Gateway Controller is operable to determine the type of Network Address and Port Translator that is present. Preferably, further comprising a second virtual media endpoint, wherein if a Network Address and Port Translator is found to be present, said Media Gateway Controller is operable to: change the remote Session Description Protocol for the call to one with a different IP address and port, but still on said Media Gateway Controller, corresponding to said second virtual media endpoint; send a message to modify the Session Description Protocol to the Media Gateway; receive empty/noise media data packets at the changed IP address and port, corresponding to its second virtual media endpoint, from the Media Gateway; and compare the source IP address and port of the empty/noise media packets received at its second virtual media endpoint with the IP address and port of the media packets received at its first virtual media endpoint, wherein if the same source IP address and port is used for the media packets sent to said first and said second virtual media endpoints, the Network Address and Port Translator is determined to be a Cone Network Address and Port Translator, but if a different source IP address or port is used for the media packets sent to said first and said second virtual media endpoints, the Network Address and Port Translator is determined to be a Symmetric Network Address and Port Translator.

[0020] According to a fifth aspect there is provided a packet-switched network comprising a Media Gateway Controller according to the forth aspect of the invention.

[0021] Other aspects and features of the present invention will become apparent to those ordinarily skilled in the art upon review of the following description of specific embodiments of the invention in conjunction with the accompanying figures.

Brief Description of the Drawings

[0022]

Figure 1 is a schematic diagram showing messaging for instigating a test call between a media endpoint of a Media Gateway and a virtual media endpoint on a Media Gateway Controller, during registration, in accordance with an embodiment of the present invention;

Figure 2 is a schematic diagram showing the IP address changes that take place during the messaging shown in Figure 1, when a Cone NAT has been detected in accordance with a preferred embodiment of the present invention;

Figure 3 is a message sequence chart following a specific format known in the art, and shows the flow of messaging that occurs between the Media Gateway Controller and the Media Gateway when a Cone NAT is detected in accordance with the preferred embodiment;

Figure 4 is a schematic diagram showing the IP address changes that take place during the messaging for a test call between the endpoints of a Media Gateway Controller and a Media Gateway when a Symmetric NAT has been detected in accordance with a further embodiment of the present invention;

Figure 5 is a message sequence chart following a specific format known in the art, and shows the flow of messaging that occurs between the Media Gateway Controller and the Media Gateway when a Symmetric NAT is detected in accordance with the embodiment of the invention shown in Figure 4;

Figure 6 is a message sequence chart following a specific format known in the art, and shows the flow of messaging that occurs in accordance with another embodiment of the present invention where a MGC virtual media endpoint and a Media Proxy are used to deduce the presence of Symmetric NAT; and

Figure 7 is a schematic diagram showing an example of a NAT aggregate.

Detailed description of the Preferred Embodiments

[0023] The following description is of a preferred embodiment by way of example only and without limitation to the combination of features necessary for carrying the invention into effect.

[0024] The present invention proposes a technique that involves instigating a "test call" during Media Gateway registration, as illustrated in Figure 1, to determine the existence and type of a NAT. In this test call a virtual media endpoint 3 on the Media Gateway Controller (MGC) acts as the calling party and a real media endpoint 5 on the Media Gateway (MG) acts as the called party. A media endpoint is a source or a sink of media flow, normally Real-time Transport Protocol (RTP) packets. The media endpoints on the MGC are "virtual" since a MGC would not normally have media endpoints and, therefore, they are not "real" endpoints, as such, as in the case of a MG. The MGC is able to deduce the existence of a Network Address Translator (NAT), by examining the media packets (usually RTP packets) sent

Ex.1002 / Page 181 of 1173
Cisco Systems, Inc.

to the virtual media endpoint 3. If a NAT is determined to be present, the MGC instructs the endpoint 5 to now send media packets to virtual media endpoint 4 on the MGC that has a different IP address than endpoint 3. By comparing the media packets received by endpoint 4 with the packets received previously by endpoint 3, the MGC is able to deduce whether the type of NAT is Cone or Symmetric.

[0025] An example of how a Cone NAT between a Telephony Service Provider (TSP) network and a network containing a MG can be detected is described with reference to Figure 2. This technique requires that the MGC has two virtual media endpoints with different IP addresses on which it may receive media packets. The MG is located behind a Cone NAT, and the MGC is located in the TSP network. When the MG is first being brought into service, it attempts to register with its MGC by sending a registration message to the MGC (for example, a ReStart In Progress (RSIP) message in Multimedia Gateway Control Protocol (MGCP)). Receipt of the registration message triggers the MGC to instigate a Test Call between its virtual media endpoints and a media endpoint on the MG to deduce that the MG is behind a Cone NAT. The first part of the test call establishes if there is a NAT between the MG and the TSP network, by comparing the address and port pair from the local Session Description Protocol (SDP) with that of the media packet (usually RTP) received on the first MGC virtual media endpoint. If a NAT is found, then the second part of the test call deduces the type of NAT by instructing the MG to send media to the second MGC virtual media endpoint, and comparing the source address and port pair from the packets received on the first MGC virtual media endpoint, with those received on the second MGC virtual media endpoint.

[0026] There are two message paths established between the MG and the MGC: one for the control messages exchange between the MG and the MGC (for example, MGCP messages such as CRCX, MDCX, DLCX); and one for the media path (for example RTP flow between the media endpoints). If the MG is behind a NAT, then when the MG registers with its MGC, the registration message (i.e. control message, for example RSIP), will go through the NAT, and as it does, a bind will be created. The MGC notes the source of the registration message and uses that address port for all future communication with that MG. Hence there are no problems with control messages traversing the NAT.

[0027] Figure 3 shows the flow of messages taking place between the MG and the MGC using pseudo-MGCP device control protocol. Firstly, the MG sends ReStart In Progress (RSIP) messages to register its media endpoints. The MGC chooses one of these for its test call and sends an Audit Endpoints message (AUEP) to it to make sure the media endpoint 5 is available, and to query its capabilities. The MG responds indicating that the media endpoint 5 is okay and what its capabilities are. At this time, the media endpoints have not been fully initialised in the MGC and the MG has not been supervised to scan for off-hook conditions etc. Therefore there is no need to worry about the media endpoints being used for real calls yet (as there will be no dial tone, and the MG will not report off-hook, digits, etc. to the MGC). The advantage of using this technique during registration is that it does not impact on the real-time usage of the device, i.e. the MG endpoints.

[0028] Next, the MGC sends a Create Connection (CRCX) message to the media endpoint on the MG to initiate a test call on the endpoint. The remote Session Description Protocol (SDP) sent in the CRCX message contains the IP address and port of a virtual media endpoint 3 on the MGC. The CRCX message also contains a prompt to place the media endpoint 5 of the MG into a mode requiring it to send media packets (i.e. sendonly or sendrecv mode.) The MG replies with the local SDP of the media endpoint 5, which the MGC takes note of. The MG then sends empty/silence/noise packets to the IP address and port that it was given in the remote SDP (i.e. to the virtual media endpoint 3 on the MGC). Note that the MG sends empty/silence/noise packets as it has no available voice data to send since the test call is being instigated during registration. The type of packet sent is dependent upon the configuration of the MG. As the packet goes through the NAT, a bind is created and its source address and port are changed. When the packet arrives at the virtual media endpoint 3 on the MGC, the MGC compares the source address and port of the packet with the IP address and port contained in the local SDP it had received previously from the media endpoint 5 on the MG. Since the source address and port of the packet differ from the address and port from the local SDP, the MGC concludes there is a NAT between the TSP network and the network containing the MG.

[0029] The MGC then sends a Modify connection (MDCX) message to the MG, changing the remote SDP for this call so that it contains the IP address and port of a second virtual media endpoint 4 on the MGC. The second virtual media endpoint 4 has a different IP address than that of the virtual media endpoint 3, but is still on the same MGC. The MG sends the empty/silence/noise packets to the new address and port. Since the NAT in this example is a Cone NAT, the same bind is used for these packets, and thus the source address and port is modified in the same way as before. When the packets arrive at the second virtual media endpoint 4 on the MGC, the MGC compares the source address and port of these packets with those that it had received on the virtual media endpoint 3. Since they are the same, the MGC concludes that the NAT is a Cone NAT. The MGC stores this information in its database for later use, and sends a DLCX message to take down the test call. MG registration then continues as usual.

[0030] Alternatively, this technique could be used during the setting up of a cali, rather than during registration. Advantageously, this allows real-time discovery of

Ex.1002 / Page 182 of 1173
Cisco Systems, Inc.

NATs, however, it will slow down the call set-up time. A further advantage of using this technique during the setting up of a call, is that by performing the test call on the MG endpoint actually involved in the call, it is possible to determine the actual NAT bind that will be used for the media flow of the call, if the NAT is a Cone NAT.

[0031] The information that the MGC has stored in its database allows it to know which MGs are behind NATs. It can then make use of a NAT traversal strategy (such as the use of a Media Proxy) for calls involving these MGs. MGCs are conventionally used for controlling the devices that source and sink media flows (usually RTP), but the described technique uses the MGC itself as a sink of a media flow.

[0032] With reference to Figures 4 and 5, the differences in logic for determining the existence of a Symmetric NAT are given below. As shown in Figure 4, instead of a Cone NAT there is now a Symmetric NAT between the TSP network and the MG's network.

[0033] The first part of the test call (that determines NAT existence) for Symmetric NATs is identical to the first part of the test call in the Cone NAT example. Likewise, the set-up for the second part of the test call is the same as the example of the Cone NAT, and the media endpoint 5 on the MG is instructed to send media to the second virtual media endpoint 4 on the MGC. As in the Cone NAT example, the MG sends the empty/silence/noise packets to the new address and port (the second virtual media endpoint 4), but since the NAT is Symmetric, a new bind is created for these packets. Thus the source address and port of these packets are modified differently than the packets that were sent to the media endpoint 3 on the MGC in the first part of the test call. When the packets arrive at the second virtual media endpoint 4 on the MGC, the MGC compares their source address and port with the source address and port of those packets that had arrived on the virtual media endpoint 3 in the first part of the test call. Since they are different, the MGC concludes that the NAT is a Symmetric NAT. Then as described previously for the example of the Cone NAT, the MGC stores this information in its database and sends a DLCX message to take down the test call, and MG registration continues as usual.

[0034] Advantageously, the described technique allows the existence and type of NAT to be determined without the necessity of changing anything outside the TSP network.

[0035] Although Multimedia Gateway Control Protocol (MGCP) is used in the examples described above, any Device Control Protocol (DCP), such as H.248 (MEGACO), NCS or ASPEN, could be used instead. In addition, Session Initiation Protocol (SIP), H.323, or other similar SDP exchange protocols that are not DCPs and that do not always fit into the MG/MGC architecture, could be used instead.

[0036] In the examples described above, a number of assumptions have been made. Firstly, it has been assumed that the MG will send empty/silence/noise media packets if it has been put into send mode but does not have any real media to send. The specifications of most DCPs require this behaviour, but if a MG cannot send such packets, then the method can be modified so that the endpoint is instructed to send a signal, for example a ring tone, instead of silence or noise. Secondly, it has been assumed that if the same NAT bind is used for a different destination, then the NAT must be some type of Cone NAT (whether it be full, restricted, or port restricted). This assumption is true by definition if one follows the definition of Cone and Symmetric NAT found in the Internet Engineering Task Force (IETF) STUN specification, "http://www.ietf.org/internet-drafts/draft-ietf-midcom-stun-02.txt". Further examples of how the present technique can used to determine the existence and type of NAT are described below.

[0037] In one variation of the present technique, one or both of the virtual media endpoints may be housed on a device external to the MGC, but under the MGC's control. Such a device would have to be capable of sinking a media flow, and have an interface in the TSP. This would allow the media flows for one or both parts of the test call to be sinked on the device external to the MGC, but reported to the MGC. Examples of such devices could be a MG located in the TSP dedicated for use in such test calls, or a Media Proxy. Such a variation using a Media Proxy is described below.

[0038] With reference to Figure 6, an example of how a virtual media endpoint on an MGC and a Media Proxy can be used to deduce the existence and type of a NAT (in this example, a Symmetric NAT) is shown in the message sequence chart. Note that the protocol shown for messaging between the MG and the MGC is psuedo-MGCP, whereas the protocol shown for messaging between the MGC and the Media Proxy is pseudo-H.248. Although, the skilled person will appreciate that any other suitable DCP or Media Proxy control protocol could be used instead. The procedure for deducing the existence of the NAT is the same as already discussed above for the example of the Cone NAT between the TSP Network and the network containing the MG, as illustrated in Figure 3. The steps common to both procedures are indicated in Figure 6 with an asterix next to them.

[0039] After the MGC has compared the source address and port of the empty/silence/noise packet with the address and port from the local SDP it had received previously, and concluded that there is a NAT because they are different, the MGC sends a message to the Media Proxy requesting the reservation of a public IP address and port for media flow. The Media Proxy sends a reply to the MGC containing the reserved IP address and port. The MGC sends another message to the Media Proxy telling it to inform the MGC of the source IP address and port of the first media packet it receives on its reserved IP address and port. The Media Proxy responds by indicating it will. Next the MGC sends a Modify Connection request (MDCX) to the media endpoint

Ex.1002 / Page 183 of 1173
Cisco Systems, Inc.

on the MG instructing it to send its media to the reserved IP address and port on the Media Proxy. The MG acknowledges the instruction, and then begins to send the empty/silence/noise RTP packets to the reserved IP address and port on the Media Proxy. As the RTP packets traverse the NAT, their source IP address and port are modified differently than the source IP address and port of those packets that were destined for the virtual media endpoint on the MGC, i.e. a new bind is created for these packets, because the NAT being traversed is a Symmetric NAT. When the first RTP packet arrives at the Media Proxy, the Media Proxy notifies the MGC of the packet's source IP address and port.. Then, as in the two previously described examples, the MGC compares the source address and port of this packet with that of the packets that had been sent to its virtual media endpoint. Since they are different, the MGC concludes that the NAT is a Symmetric NAT, and the MGC stores this information in its database and sends a DLCX message to take down the test call, and a message to the Media Proxy to free the IP address and port that it had reserved. MG registration then continues as usual.

[0040] The technique described in this document can be used even when there is more than one NAT between the MGC and MG, but only if arranged in series, i.e. non-parallel, as illustrated in Figure 7. The technique enables the detection of a NAT aggregate 7, and the type of the strongest NAT in the NAT aggregate 7. For example, if there are four NATs in series and one of them is a Symmetric NAT, then because a change in the source IP address and port is detected by the MGC due to the presence of the symmetric NAT, the MGC determines that there is at least one symmetric NAT in the NAT aggregate 7. It is not, however, possible for the MGC to determine whether there are any Cone NATs present in the NAT aggregate 7 in addition to the Symmetric one (s) detected, as the Cone NATs do not change the source IP address and port of packets based on destination. Only if all four NATs in the aggregate are Cone NATs, can the MGC determine that the NAT aggregate is composed of Cone NATs, because there is no change detected in the IP address and port using the technique described above.

[0041] Advantageously, the methods described herein may be implemented in software, hardware, or a mixture of both.

[0042] It will be appreciated that the techniques described herein may be used with trivial modifications as would be contemplated by the skilled person to deduce the existence and type of NATs in network systems having MGs and MGCs and/or Media Proxies, and that such modifications would fall within the scope of the invention as claimed.

[0043] Although the embodiments of the invention described with reference to the drawings comprise computer apparatus and processes performed in computer apparatus, the invention also extends to computer programs, particularly computer programs on or in a carrier, adapted for putting the invention into practice. The program may be in the form of source code, object code, a code intermediate source and object code such as in partially compiled form, or in any other form suitable for use in the implementation of the processes according to the invention. The carrier may be any entity or device capable of carrying the program.

[0044] For example, the carrier may comprise a storage medium, such as ROM, for example a CD ROM or a semiconductor ROM, or a magnetic recording medium, for example a floppy disc or hard disk. Further, the carrier may be a transmissible carrier such as an electrical or optical signal which may be conveyed via electrical or optical cable or by radio or other means.

[0045] When the program is embodied in a signal which may be conveyed directly by a cable or other device or means, the carrier may be constituted by such cable or other device or means.

[0046] Alternatively, the carrier may be an integrated circuit in which the program is embedded, the integrated circuit being adapted for performing, or for use in the performance of, the relevant processes.

[0047] Although the invention has been shown and described with respect to a best mode embodiment thereof, it should be understood by those skilled in the art that the foregoing and various other changes, omissions and additions in the form and detail thereof may be made therein without departing from the scope of the invention as claimed.

[0048] In summary, Network Address and Port Translators (NATs) have the potential to interrupt the end-to-end nature of Internet applications, thereby threatening end-to-end security and other end-to-end functions. Thus it is important to be able to discover the existence of NATs and their type. Accordingly there is provided a method of discovering the existence and type of NAT that involves instigating a test call between media endpoints on a Media Gateway (MG) and a Media Gateway Controller (MGC). The MGC is able to deduce the existence of a NAT by examining the media packets sent to its endpoint. If a NAT is determined to be present the MGC instructs the endpoint on the MG to send media packets to another endpoint on the MGC. By comparing the IP addresses and ports of the media packets received at the endpoints of the MGC, the MGC is able to deduce whether the type of NAT is Cone or Symmetric.

Claims

1. A method of determining the presence of a Network Address and Port Translator between a Telephony Service Provider Network and a network comprising a Media Gateway (MG), said Telephony Service Provider Network comprising a Media Gateway Controller (MGC), said method comprising:

   instigating a test call between a first endpoint

Ex.1002 / Page 184 of 1173
Cisco Systems, Inc.

(3) on the Media Gateway Controller acting as a calling party, and an endpoint (5) on the Media Gateway acting as a called party;
receiving a reply comprising the local Session Description Protocol of the endpoint of the Media Gateway at the Media Gateway Controller;
receiving an empty/noise media packet from the Media Gateway at the first endpoint of the Media Gateway Controller; and
comparing the source IP address and port of the empty/noise media packet received at the first endpoint of the Media Gateway Controller with the IP address and port contained in the received local Session Description Protocol of the endpoint of the Media Gateway,

wherein if the IP addresses are different or the ports are different then a Network Address and Port Translator is determined to be present, otherwise, if the IP addresses are the same and the ports are the same then a Network Address and Port Translator is determined not to be present.

2. A method according to claim 1, wherein instigating the test call comprises sending a message to create a connection to the endpoint on the Media Gateway from the Media Gateway Controller, wherein a remote Session Description Protocol is sent in the message to create the connection and corresponds to a first virtual media endpoint on the Media Gateway Controller.

3. A method according to claim 2, wherein the empty/noise media packets from the Media Gateway are received at the first virtual media endpoint on the Media Gateway Controller.

4. A method according to claim 2, wherein if a Network Address and Port Translator is found to present, said method further comprises:

determining the type of Network Address and Port Translator that is present.

5. A method according to claim 4, wherein determining the type of Network Address and Port Translator comprises:

changing the remote Session Description Protocol for the call to one with a different IP address, but still on the same Media Gateway Controller, corresponding to a second virtual media endpoint;
sending a message to modify the Session Description Protocol to the Media Gateway from the Media Gateway Controller;
prompting the Media Gateway to send empty/noise media packets to the changed IP address and port corresponding to the second virtual media endpoint on the Media Gateway Controller;
receiving the empty/noise media packets at the second virtual media endpoint on the Media Gateway Controller;
comparing the source IP address and port of the empty/noise media packets received at the second virtual media endpoint of the Media Gateway Controller with the source IP address and port of the media packets received at the first virtual media endpoint of the Media Gateway Controller,

wherein if the same source IP address and port is used for the media packets sent to the first and the second virtual media endpoints on the Media Gateway Controller, the Network Address and Port Translator is determined to be a Cone Network Address and Port Translator, but if a different source IP address or port is used for the media packets sent to the first and the second virtual media endpoints on the Media Gateway Controller, the Network Address and Port Translator is determined to be a Symmetric Network Address and Port Translator.

6. A method according to claim 5, wherein the message to create a connection instructs the endpoint on the Media Gateway to be in a mode for sending media packets.

7. A method according to any of the preceding claims, wherein the test call is instigated during registration of the Media Gateway with the Media Gateway Controller.

8. A method according to any of the preceding claims, wherein the test call between the Media Gateway and the Media Gateway Controller is instigated during set-up of an actual call.

9. A method according to any of the preceding claims, wherein the test call is instigated between the virtual media endpoint on the Media Gateway Controller and a real media endpoint on the Media Gateway.

10. A method according to any of the preceding claims, wherein the Media Gateway Controller stores information relating to the type of Network Address and Port Translator determined.

11. A method according to any of the preceding claims, wherein said Telephony Service Provider and said network comprising the Media Gateway are packet-switched networks.

12. A method according to any of the preceding claims

Ex.1002 / Page 185 of 1173
Cisco Systems, Inc.

for use with voice over IP applications

13. A method according to claim 5, wherein receipt of a registration message from the Media Gateway triggers the instigating of the test call.

14. A computer program for use in a computer for determining the presence of a Network Address and Port Translator between a Telephony Service Provider Network and a network comprising a Media Gateway, according to the method of any of the preceding claims.

15. A computer program stored on a data carrier for use in a computer for determining the presence of a Network Address and Port Translator between a Telephony Service Provider Network and a network comprising a Media Gateway, according to the method of any of claims 1 to 13.

16. A Media Gateway Controller comprising a first virtual media endpoint, and capable of determining the presence of a Network Address and Port Translator between a Telephony Service Provider Network in which said Media Gateway Controller is located, and a network comprising a Media Gateway, said Media Gateway Controller operable to:

instigate a test call between its first virtual media endpoint acting as a calling party, and an endpoint on the Media Gateway acting as a called party;
receive a reply comprising the local Session Description Protocol of the endpoint of the Media Gateway;
receive empty/noise media packets from the Media Gateway at its first virtual media endpoint; and
compare the source IP address and port of the empty/noise media packets received at its first virtual media endpoint with the IP address and port contained in the received local Session Description Protocol of the endpoint of the Media Gateway,

wherein if the IP addresses are different or the ports are different then a Network Address and Port Translator is determined to be present, otherwise, if the IP addresses are the same and the ports are the same then a Network Address and Port Translator is determined not to be present.

17. A Media Gateway Controller according to claim 16, wherein if a Network Address and Port Translator is found to be present, said Media Gateway Controller is operable to:

determine the type of Network Address and Port Translator that is present.

18. A Media Gateway Controller according to claim 15, further comprising a second virtual media endpoint, wherein if a Network Address and Port Translator is found to be present, said Media Gateway Controller is operable to:

change the remote Session Description Protocol for the call to one with a different IP address and port, but still on said Media Gateway Controller, corresponding to said second virtual media endpoint;
send a message to modify the Session Description Protocol to the Media Gateway;
receive empty/noise media data packets at the changed IP address and port, corresponding to its second virtual media endpoint, from the Media Gateway; and
compare the source IP address and port of the empty/noise media packets received at its second virtual media endpoint with the IP address and port of the media packets received at its first virtual media endpoint,

wherein if the same source IP address and port is used for the media packets sent to said first and said second virtual media endpoints, the Network Address and Port Translator is determined to be a Cone Network Address and Port Translator, but if a different source IP address or port is used for the media packets sent to said first and said second virtual media endpoints, the Network Address and Port Translator is determined to be a Symmetric Network Address and Port Translator.

19. A Media Gateway Controller according to claim 25, comprising a data store capable of holding information relating to the type of Network Address and Port Translator determined.

20. A packet-switched network comprising a Media Gateway Controller according to any of claims 16 to 19.

Ex.1002 / Page 186 of 1173
Cisco Systems, Inc.

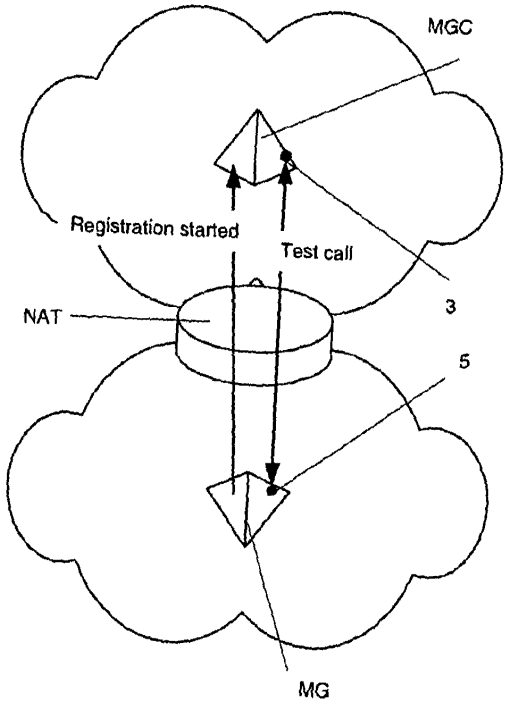

MGC
Registration started
Test call
3
NAT
5
MG

Fig. 1

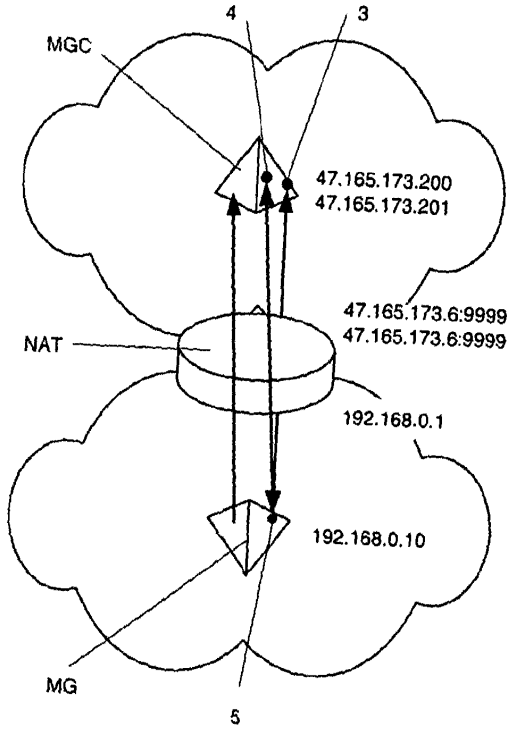

4
3
MGC
47.165.173.200
47.165.173.201
47.165.173.6:9999
47.165.173.6:9999
NAT
192.168.0.1
192.168.0.10
MG
5

Fig. 2

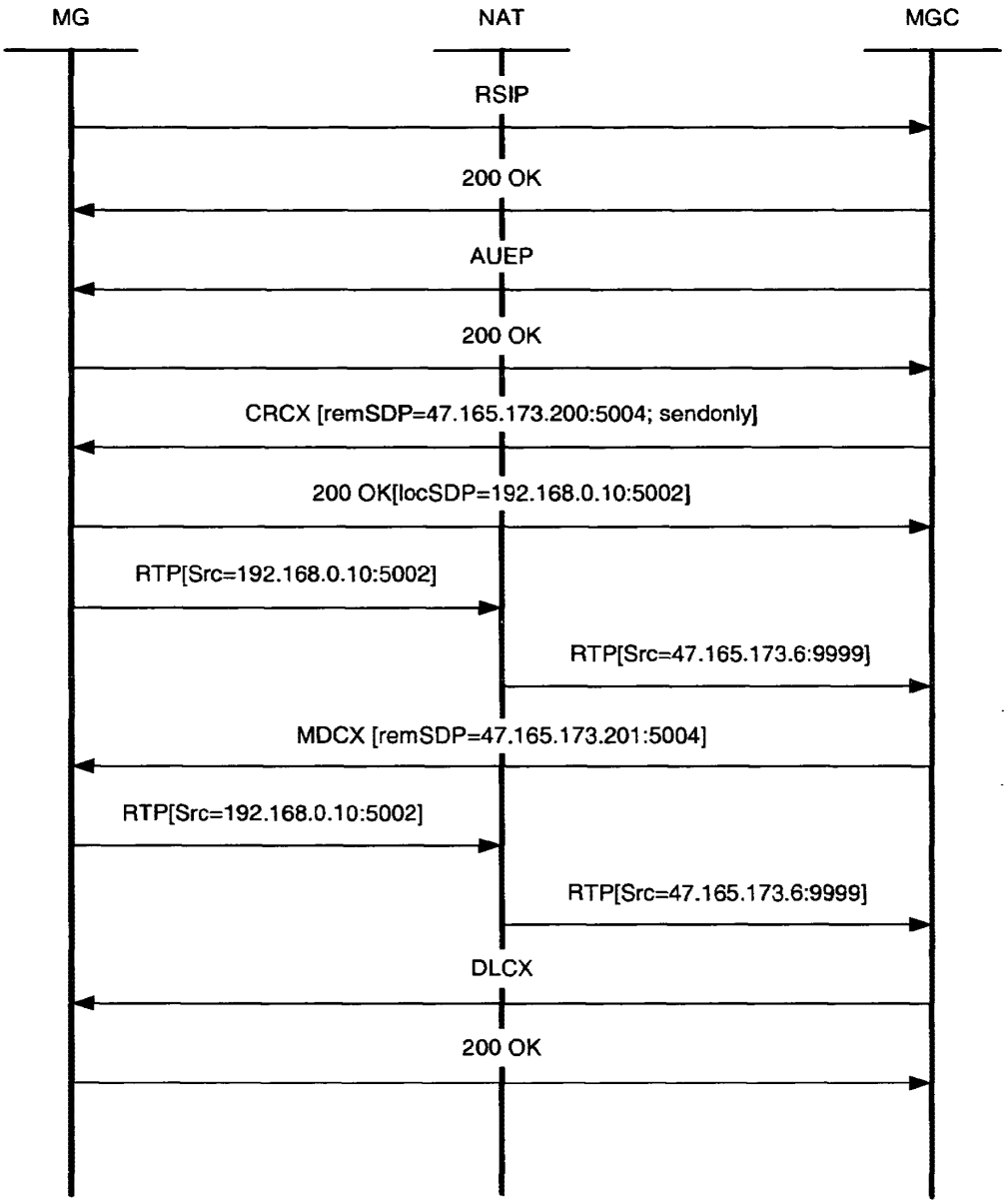


Fig. 3

Ex.1002 / Page 188 of 1173
Cisco Systems, Inc.

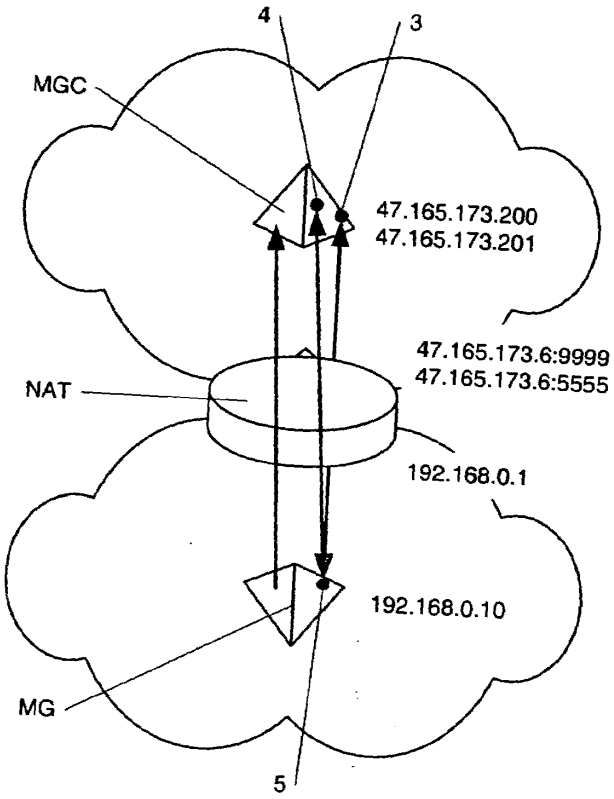

4
3
MGC
47.165.173.200
47.165.173.201
47.165.173.6:9999
47.165.173.6:5555
NAT
192.168.0.1
192.168.0.10
MG
5

Fig. 4

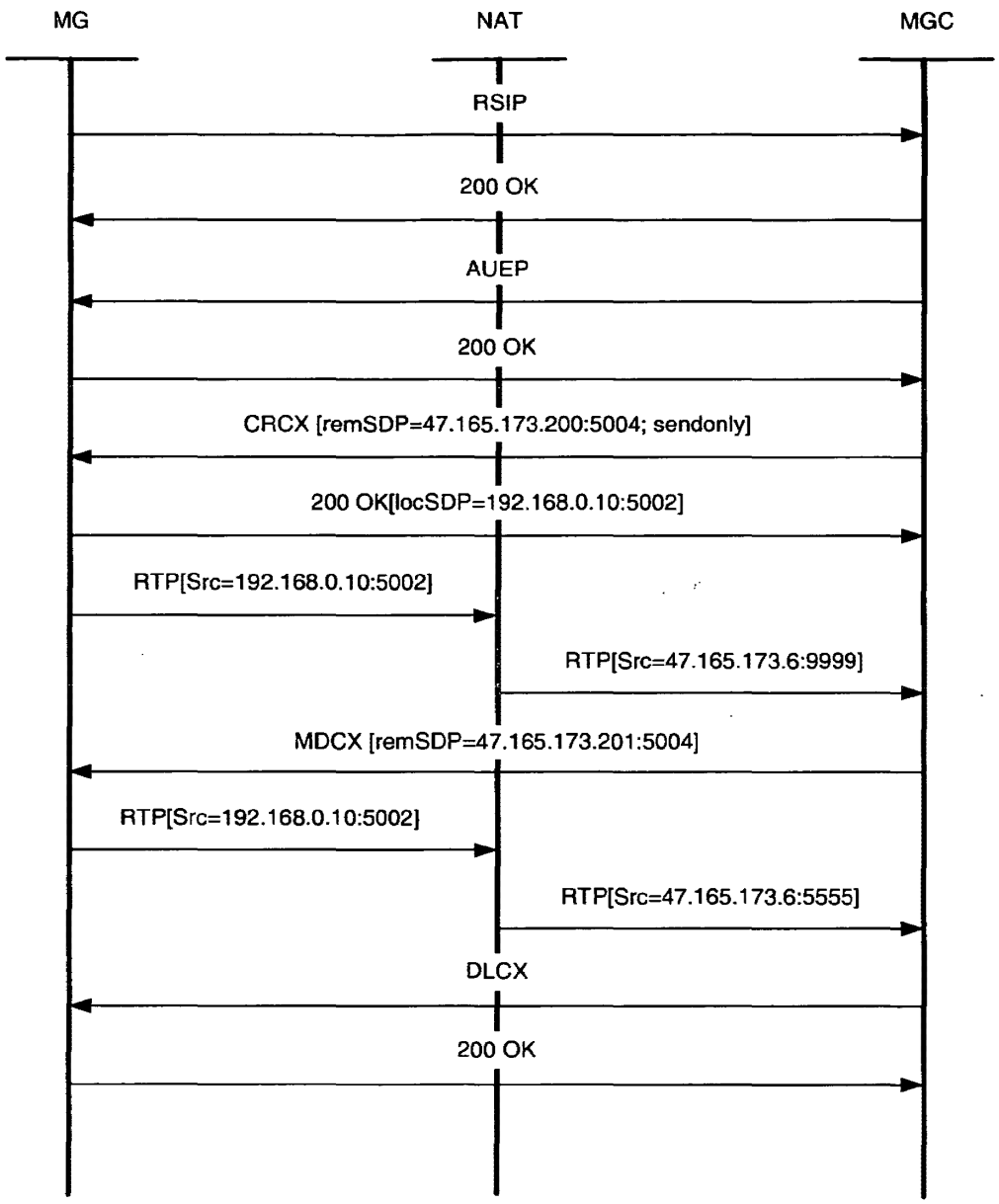


Fig. 5

Ex.1002 / Page 190 of 1173
Cisco Systems, Inc.

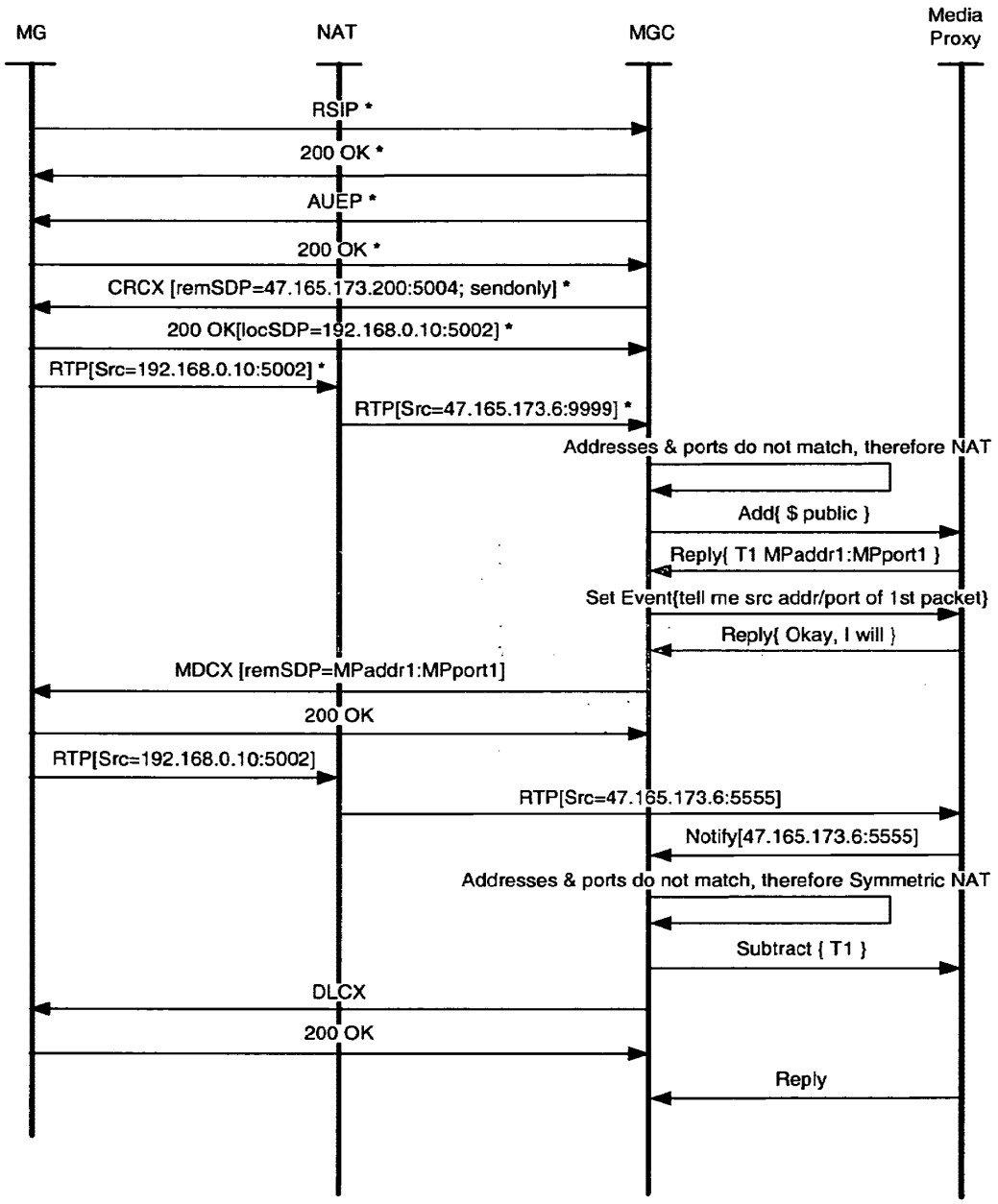

MG
NAT
MGC
Media Proxy
RSIP *
200 OK *
AUEP *
200 OK *
CRCX [remSDP=47.165.173.200:5004; sendonly] *
200 OK[locSDP=192.168.0.10:5002] *
RTP[Src=192.168.0.10:5002] *
RTP[Src=47.165.173.6:9999] *
Addresses & ports do not match, therefore NAT
Add{ $ public }
Reply{ T1 MPaddr1:MPport1 }
Set Event{tell me src addr/port of 1st packet}
Reply{ Okay, I will }
MDCX [remSDP=MPaddr1:MPport1]
200 OK
RTP[Src=192.168.0.10:5002]
RTP[Src=47.165.173.6:5555]
Notify[47.165.173.6:5555]
Addresses & ports do not match, therefore Symmetric NAT
Subtract { T1 }
DLCX
200 OK
Reply

Fig. 6

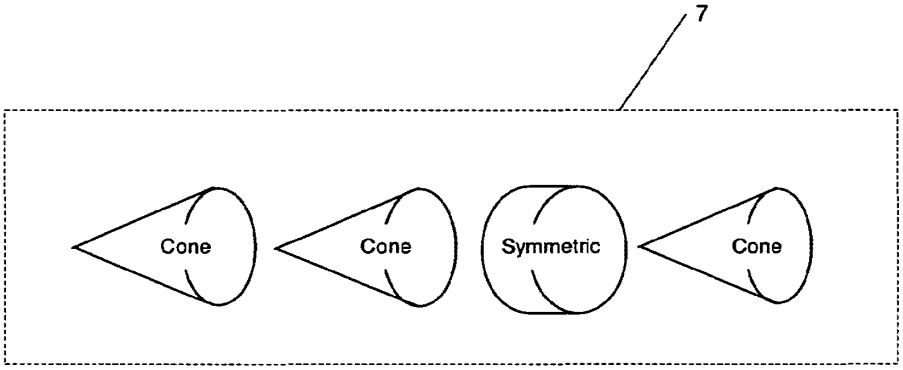


Fig. 7

Ex.1002 / Page 192 of 1173
Cisco Systems, Inc.

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
25 September 2003 (25.09.2003)

PCT

(10) International Publication Number
WO 03/079635 A1

(51) International Patent Classification[7]: H04L 29/06, 29/08

(21) International Application Number: PCT/GB03/00776

(22) International Filing Date: 24 February 2003 (24.02.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/098,976 15 March 2002 (15.03.2002) US

(71) Applicant: **INTERNATIONAL BUSINESS MACHINES CORPORATION** [US/US]; New Orchard Road, Armonk, NY 10504 (US).

(71) Applicant *(for MG only)*: **IBM UNITED KINGDOM LIMITED** [GB/GB]; PO Box 41, North Harbour, Portsmouth, Hampshire PO6 3AU (GB).

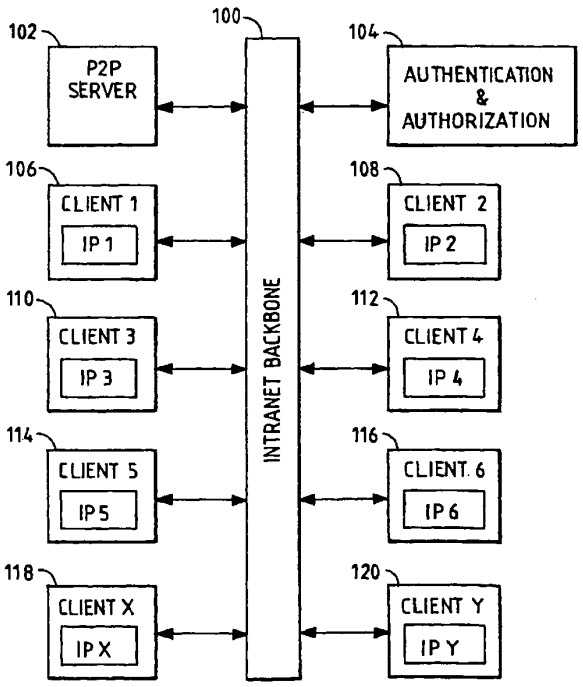
(72) Inventors: **GOODMAN, Brian**; 296 Painter Hill Road, Roxbury, CT 06783 (US). **ROONEY, John, Warren**; 1 Titicus Mountain Road, New Fairfield, CT 06812 (US). **SUBRAMANIAN, Ramesh**; 119 Old Town Farm Road, Woodbury, CT 06798 (US). **SWEENEY, William**; 208 East Rocks Road, Norwalk, CT 06851 (US).

(74) Agent: **BURT, Roger, James**; IBM United Kingdom Limited, Intellectual Property Law, Hursley Park, Winchester, Hampshire SO21 2JN (GB).

(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, 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.

[Continued on next page]

(54) Title: SECURED AND ACCESS CONTROLLED PEER-TO-PEER RESOURCE SHARING METHOD AND APPARATUS



(57) Abstract: A peer-to-peer network propagates searches from client to client. Resources within each client are selectively searched in response to authentication and authorization processes. Authentication information may be included in a search request or may be performed by an authentication process external to the client. Authorization is performed by a process external to the client. Only after authentication or authorization may resources of any particular client be accessed. The system allows for secure propagated searches and resource access in a peer-to-peer network environment. The network may further include a server for maintaining a list of clients connected to the peer-to-peer network in order to more efficiently facilitate peer-to-peer communications.

WO 03/079635 A1

(84) Designated States *(regional)*: ARIPO patent (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, 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.

SECURED AND ACCESS CONTROLLED PEER-TO-PEER RESOURCE SHARING METHOD AND APPARATUS

Field of the Invention

This invention is related to the field of peer-to-peer networks.

Background of the Invention

Until recently, corporate data and content within global or other large organizations were distributed by replicating and distributing such data and content using centralized content repositories. That is, the data was globally distributed, but made available within a location of geographical area by using a central server that was responsible for serving the content to clients located within the specified area.

The advent of peer-to-peer (P2P) computing has changed this approach. The accent has shifted from storing content in, and serving from, centralized servers to storing and serving at least some of the content from the client-side. In this P2P model, the content provider manages the content in a local client, and shares the content with anyone who accesses the content. In this model, content creation, storage and security dwells on the client side.

There are several advantages to this P2P approach. By shifting the responsibility for content to the client side, server-side management of diverse resources can be vastly reduced. Server managers need not be responsible for the integrity of the content. Problems arising from centralized distribution of content could be averted.

There are at least three architectural approaches to peer-to-peer resource sharing systems. P2P with centralized control, pure P2P with no centralized control and a hybrid approach that incorporates some of the aspects of the other two.

One example of P2P with a centralized controller is a system referred to as Napster. The Napster system uses a central server to maintain a list of connected clients. Every client connects to the central server, which scans the clients' disks for shared resources and maintains directories and indexes of the shared resources. A client searching for a resource performs the search on the maintained directories and indexes of the central server. Once a client knows where to find the resources that

is it seeking (i.e. which client has the files it is searching for), it makes a direct connection to the appropriate client and transfers the resources.

Napster is not web-based, and does not run in a browser. It is a stand-alone application that runs on each individual client, and uses TCP/IP for its data-communication and data transfers. Since Napster depends on a central server that acts as a collector and regulator of information, the clients are not guaranteed anonymity. The Napster system is also vulnerable if the central server fails.

A good example of pure P2P with no centralized control is a system referred to as Gnutella. Gnutella is a generic term used to identify those P2P systems that use the Gnutella protocol. There is no single interpretation of what the protocol is, actually. However, there are certain common elements that manifest in Gnutella-based systems. Chief among those is that Gnutella does away with the central server. In this system, each client continuously keeps track of other clients by pinging known clients in the system. Distributed searches are propagated from one client to its immediate neighbors in ever-increasing circles until answers are found, or the search times out. Search responses are propagated back to the searcher in the same manner.

Like Napster, Gnutella-based systems are also not web-based, and run as applications in client environments. Gnutella is a truly anonymous resource sharing system. No server is used to facilitate searches, clients must establish ad-hock peer information. The searcher does not know the identity of the responder, and vice-versa. Thus there are no authentication or authorization checks, trust is implicitly assumed.

A serious problem in Gnutella-based systems is their reputation for being unreliable. Lacking a central server that keeps track of which client is connected, and which is not, there is no way for a client to know if all its neighbors are alive and connected. This leads to less than reliable performance.

The third approach to P2P systems is referred to as Web Mk. This is more of an approach than an actual product, and is described in a Gartner Report on the emergence of P2P computing entitled The Emergence of Distributed Content Management and Peer-to-Peer Content Networks, January 2001. Said report is hereby incorporated by reference. This is a web-based approach that uses web servers and web browsers. The web browsers would be

configurable by users and would integrate resource-sharing features. The servers will maintain multiple indexes and allow access to different forms of data. This type of system would use software agents or Bots to provide services such as extraction and consolidation of multiple resources, chat facilities, and notifications of changes. Search requests could be stored in the server and set to run in real-time or as a batch process, and alert the appropriate clients of the results.

What is needed is a system that adapts the advantages of the P2P network while resolving disadvantages of current P2P systems. What is needed is a P2P network that takes advantage of the reduced central server requirements of a pure P2P network without sacrificing the efficiencies of the central server. What is further needed is a P2P network that provides secure access and control to client resources without the requirement of a central server.

Brief Summary of the Invention

In a first aspect, the present invention provides a method of securely conducting a resource search initiated by a first client in a peer-to-peer network, the resource search included with a search request having a credentials signal indicative of the first client, the method comprising the steps of: communicating the search request from the first client to a second client, the second client having a multiplicity of second resources, each of the multiplicity of second resources having at least one corresponding access attribute; at the second client, selectively searching the multiplicity of second resources in response to comparison of the credentials signal and the at least one access attribute of each of the multiplicity of second resources; communicating the search request from the second client to a third client, the third client having a multiplicity of third resources, each of the multiplicity of third resources having at least one corresponding access attribute; and at the third client, selectively searching the multiplicity of third resources in response to comparison of the credentials signal and the at least one access attribute of each of the multiplicity of third resources.

The method preferably further comprises the steps of: at the third client, determining a matching resource in response to said step of selectively searching the multiplicity of third resources; and communicating a matching signal indicative of the matching resource from the third client to the first client.

Preferably, the credentials signal includes an identification signal indicative of the first client and the access attributes of the second and third resources includes an authorization signal indicative of at least one of a plurality of clients, the plurality of clients including the first client, and further said step of selectively searching the second multiplicity of resources searches one of the second multiplicity of resources if the identification signal substantially matches the authorization signal included with the corresponding access attributes, and said step of selectively searching the third multiplicity of resources searches one of the third multiplicity of resources if the identification signal substantially matches the authorization signal included with the corresponding access attributes.

Preferably, the credentials signal includes an identification signal indicative of the first client and the access attributes of the second and third resources includes an authorization signal indicative of at least one of a plurality of clients, the plurality of clients including the first client, and said step of selectively searching the second multiplicity of resources further includes the steps of: communicating from the second client to an authentication process external to the first, second and third clients the identification signal; receiving from the authentication process an authenticated signal indicative of the first client in response thereto; and searching one of the second multiplicity of resources if the authenticated signal substantially matches the authorization signal included with the corresponding access attributes, and said step of selectively searching the third multiplicity of resources further includes the steps of: communicating from the third client to the authorization process the identification signal; receiving from the authorization process the authenticated signal indicative of the first client in response thereto; and searching one of the third multiplicity of resources if the authenticated signal substantially matches the authorization signal included with the corresponding access attributes.

The method prefeerably further comprises the steps: at the second client, storing the identification signal and the received authenticated signal in a cache memory at the second client; and at the second client searching the cache memory for the identification signal and the received authentication signal prior to said step communicating from the second client to the authentication process, wherein said step communicating from the second client to the authentication process is not performed if said step of searching the cache memory finds the identification signal and the received authentication signal stored therein, and said step of searching

one of the second multiplicity of resources uses the authenticated signal stored in the cache memory, thereby reducing communication between the second client and the authentication process.

The method preferably further comprises the steps: at the third client, storing the identification signal and the received authenticated signal in a cache memory at the third client; and at the third client searching the cache memory for the identification signal and the received authentication signal prior to said step communicating from the third client to the authentication process, wherein said step communicating from the third client to the authentication process is not performed if said step of searching the cache memory finds the identification signal and the received authentication signal stored therein, and said step of searching one of the third multiplicity of resources uses the authenticated signal stored in the cache memory, thereby reducing communication between the third client and the authentication process.

Preferably, said step of communicating the search request from the second client to the third client and said step of selectively searching the multiplicity of third resources are not performed if the authentication signal is not received from the authentication process by the second client.

Preferably, the credentials signal includes an identification signal indicative of the first client and the access attributes of the second and third resources includes an authorization signal indicative of at least one of a plurality of client classes, wherein said step of selectively searching the second multiplicity of resources further includes the steps of: communicating from the second client to an authorization process external to the second client the identification signal; receiving from the authorization process a client class signal indicative which of the plurality of client classes are associated with the identification signal; and searching one of the second multiplicity of resources if the client class signal substantially matches the authorization signal included with the corresponding access attributes, and said step of selectively searching the third multiplicity of resources further includes the steps of: communicating from the third client to the authorization process external to the third client the identification signal; receiving from the authorization process the client class signal indicative which of the plurality of client classes are associated with the identification signal; and searching one of the third multiplicity of

Ex.1002 / Page 199 of 1173
Cisco Systems, Inc.

resources if client class signal substantially matches the authorization signal included with the corresponding access attributes.

The method preferably further comprises the steps: at the second client, storing the identification signal and the received client class signal in a cache memory at the second client; and at the second client searching the cache memory for the identification signal and the received client cache signal prior to said step communicating from the second client to the authorization process, wherein said step communicating from the second client to the authorization process is not performed if said step of searching the cache memory finds the identification signal and the received client cache signal stored therein, and said step of searching one of the second multiplicity of resources uses the client cache signal stored in the cache memory, thereby reducing communication between the second client and the autorization process.

The method preferably further comprises the steps: at the third client, storing the identification signal and the received client class signal in a cache memory at the third client; and at the third client searching the cache memory for the identification signal and the received client cache signal prior to said step communicating from the third client to the authorization process, wherein said step communicating from the third client to the authorization process is not performed if said step of searching the cache memory finds the identification signal and the received client class signal stored therein, and said step of searching one of the third multiplicity of resources uses the client class signal stored in the cache memory, thereby reducing communication between the third client and the authentication process.

Preferably, the peer-to-peer network further including a multiplicity of clients including the first, second and third clients, each of the multiplicity of clients having a unique client address, and a server having a list of client addresses, said method further comprising the steps of: communicating from the server to the first client a first seed list comprising a first portion of the list of client addresses; and communicating from the server to the second client a second seed list comprising a second portion of the list of client addresses, the first seed list including a second client address corresponding to the second client and the second seed list including a third client address corresponding to the third client, wherein said step of communicating the search request from the first client to the second client communicates to the second client in response to the second client address included in the

Ex.1002 / Page 200 of 1173
Cisco Systems, Inc.

first seed list, and said step of communicating the search request from the second client to the third client communicates to the third client in response to the third client address included in the second seed list.

Preferably, each of the multiplicity of clients may be either connect to or disconnect from the peer-to-peer network at any time, and the method further comprising the steps of: at the server, determining which of the multiplicity of clients is connected to the peer-to-peer network; at the server, generating a list of connected client addresses in response said step of determining; and at the server, generating the first and second seed lists from the list of connected client addresses.

The method preferably further comprises the steps: communicating a connection signal from one of the multiplicity of clients to the server in response to the one of the multiplicity of clients connecting to the peer-to-peer network; and at the server, adding a newly connected client address corresponding to the one of the multiplicity of clients to the list of connected client addresses in response thereto.

In a second aspect, the present invention provides a client included in a peer-to-peer network having a multiplicity of clients, the client comprising: a peer-to-peer network dispatcher for receiving a resource search request from a second client of the multiplicity of clients, the search request initiating from an initiating client of the multiplicity of clients, the search request including a credentials signal having an identification signal indicative of the initiating client; a memory for storing a plurality of resources, each of the plurality of resources having at least one corresponding access attribute; and a search engine for selectively searching at least one of the plurality of resources in response to a comparison of the credentials signal and the at least one access attribute of each of the plurality of resources.

Preferably, said peer-to-peer network dispatcher communicates the identification signal to an authentication process external to the client and receives an authenticated signal if the identification signal is authenticated by the authentication process, and said search engine does not search any of the plurality of resources if the authenticated signal is not received from the authentication process.

Preferably, said peer-to-peer network dispatcher communicates the resource search request to a third client of the multiplicity of clients if the authenticated signal is received from the authentication process,

Ex.1002 / Page 201 of 1173
Cisco Systems, Inc.

or does not communicate the resource search request to the third client if the authenticated signal is not received from the authentication process.

Preferably, the access attribute is indicative of a class of clients permitted to access to the corresponding resource, said peer-to-peer network dispatcher communicates the identification signal to an authorization process external to the client and receives a client class signal in response thereto, and said search engine selectively searches the at least one of the plurality of resources in response to a comparison of the client class signal and the at least one access attribute of each of the plurality of resources.

Preferably, the peer-to-peer network further includes a server and each of the multiplicity of clients has a unique client address, the client further comprises a seed list receiver for receiving and storing a seed list of client address from the server, and said peer-to-peer network search dispatcher forwards the resource search request to client addresses of the seed list.

It is suitable to have a method of securely conducting a resource search initiated by a first client in a peer-to-peer network, the resource search included with a search request having a credentials signal indicative of the first client, the method comprising the steps of: communicating the search request from the first client to a second client; communicating the search request from the second client to a third client, the third client having a multiplicity of third resources, each of the multiplicity of third resources having at least one corresponding access attribute; and at the third client, selectively searching the multiplicity of third resources in response to comparison of the credentials signal and the at least one access attribute of each of the multiplicity of third resources.

Preferably, the peer-to-peer network further including a multiplicity of clients including the first, second and third clients, each of the multiplicity of clients having a unique client address, and a server having a list of client addresses, said method further comprising the steps of: communicating from the server to the first client a first seed list comprising a first portion of the list of client addresses; and communicating from the server to the second client a second seed list comprising a second portion of the list of client addresses, the first seed list including a second client address corresponding to the second client and the second seed list including a third client address

corresponding to the third client, wherein said step of communicating the search request from the first client to the second client communicates to the second client in response to the second client address included in the first seed list, and said step of communicating the search request from the second client to the third client communicates to the third client in response to the third client address included in the second seed list.

One preferred embodiment of the invention provides a method in a peer-to-peer network for securely conducting a resource search initiated by a first client, the resource search included with a search request having a credentials signal indicative of the first client. The method comprising the steps of communicating the search request from the first client to a second client, communicating the search request from the second client to a third client, the third client having a multiplicity of third resources, each of the multiplicity of third resources having at least one corresponding access attribute; and at the third client, selectively searching the multiplicity of third resources in response to comparison of the credentials signal and the at least one access attribute of each of the multiplicity of third resources.

Another embodiment of the invention provides a client included in a peer-to-peer network having a multiplicity of clients. The client comprises a peer-to-peer network dispatcher for receiving a resource search request from a second client of the multiplicity of clients, the search request initiating from an initiating client of the multiplicity of clients, the search request including a credentials signal having an identification signal indicative of the initiating client. The client also comprises a memory for storing a plurality of resources, each of the plurality of resources having at least one corresponding access attribute and a search engine for selectively searching at least one of the plurality of resources in response to a comparison of the credentials signal and the at least one access attribute of each of the plurality of resources.

Another embodiment of the invention provides a method in a peer-to-peer network a for securely conducting a resource search initiated by a first client, the resource search included with a search request having a credentials signal indicative of the first client. The method comprises the step of communicating the search request from the first client to a second client, the second client having a multiplicity of second resources, each of the multiplicity of second resources having at least one corresponding access attribute. The method further comprises the

Ex.1002 / Page 203 of 1173
Cisco Systems, Inc.

step of at the second client, selectively searching the multiplicity of second resources in response to comparison of the credentials signal and the at least one access attribute of each of the multiplicity of second resources. The method further comprises the step of communicating the search request from the second client to a third client, the third client having a multiplicity of third resources, each of the multiplicity of third resources having at least one corresponding access attribute. The method further comprises the step of at the third client, selectively searching the multiplicity of third resources in response to comparison of the credentials signal and the at least one access attribute of each of the multiplicity of third resources.

Brief Description of the Drawings

FIG. 1 shows a block diagram of a P2P network and system operating in accordance with a preferred embodiment of the present invention

FIG. 2 shows a block diagram a server of the P2P network and system operating in accordance with a preferred embodiment of the present invention.

FIG. 3 shows a block diagram of an authentication and authorization process of the P2P network and system operating in accordance with a preferred embodiment of the present invention.

FIG. 4 shows a block diagram of a client of the P2P network and system operating in accordance with a preferred embodiment of the present invention..

FIG. 5 shows a process flow diagram including interactions between a client and server for generating and maintaining seed lists in accordance with the a preferred embodiment of the present invention.

FIG. 6 shows a process flow diagram of PING, SEARCH and GET request processing by a client in accordance with a preferred embodiment of the present invention.

FIG. 7 shows a process flow diagram of an authentication process that does not require communication with an authentication process external to the client.

FIG. 8 shows a process flow diagram of communication between a client and an authentication process external to the client in accordance with a preferred embodiment of the present invention.

FIG. 9 shows a process flow diagram of a communication between a client and an authorization process external to the client in accordance with a preferred embodiment of the present invention.

Detailed Description of the Invention

It is important to note, that these embodiments are only examples of the many advantageous uses of the innovative teachings herein. In general, statements made in the specification of the present application do not necessarily limit any of the equivalent and various claimed inventions. Moreover, some statements may apply to some inventive features but not to others. In general, unless otherwise indicated, singular elements may be in the plural and visa versa with no loss of generality.

The preferred embodiment is directed towards peer-to-peer (P2P) resource sharing within a corporate intranet environment. The preferred embodiment is a hybrid system for P2P resource sharing. It consists of both a server and a client component. It supports the features of the three aforementioned P2P architectures, as well as some additional characteristics.

The client is an application running in the client computer, and acts as a modified pure P2P client. The system includes reliable IP repository, security integration through enterprise systems, an enhanced client side database for better search results and some basic network activity reduction. Together these qualities provide P2P services for the corporate environment.

Characteristics of the preferred embodiment include:

Reliable IP Repository – Each client first "announces itself' to the server, and requests a list of IP addresses of connected clients. The server sends a seed list of the connected clients. (The term seed list is used because each client needs to know only a limited number of other connected clients). The server maintains a current list of connected clients by maintaining a list of clients, and pinging each client periodically.

Ex.1002 / Page 205 of 1173
Cisco Systems, Inc.

Authentication and authorization – Metadata associated with each resource includes file descriptions as well as security and access control information. The security checks can be local account based or enterprise level security based.

Enhanced client database – Each client maintains a database of resources that it shares. The database will preferably not only contain names and characteristics of the files, but also user-defined metadata describing the files.

Reduced Network Activity – Unlike a pure P2P network, clients need not ping the other clients continuously. Instead, a client maintains awareness of other connected clients by downloading the list of IP addresses from the server periodically. Each client sends a handshake to each of the clients in the list received. If an acknowledgement is received from another client, that client is added to the original client's list.

Pure P2P Protocol Based – Like most of the packet communications, search and search response is accomplished among clients using a protocol similar to a pure P2P protocol.

This approach enables use of the central server concept within a P2P environment that results in a highly enhanced P2P resource sharing system. This system thus builds upon existing P2P approaches and provides additional functionality.

FIG. 1 shows a block diagram of a P2P network and system operating in accordance with a preferred embodiment of the present invention. An intranet backbone 100 couples a P2P server 102 and an authentication and authorization process 104 to a multiplicity of clients 1 - Y 106 - 120. Each client has a corresponding address indicative of the client as shown by IP 1 through IP Y. The intranet 100 also facilitates communication between the clients thereby enabling the P2P communications.

FIG. 2 shows a block diagram a server of the P2P network and system operating in accordance with a preferred embodiment of the present invention. Server 102 is coupled to intranet backbone 100 through a network interface 202 that facilitates communication with the intranet and the clients. When a client connects to the intranet, a client connect signal is received by the network interface 202 and process by the client connect function 204 which adds the address of the connected client to the

connected client list 206. In response to the connect signal, seed list generator 208 generates a seed list for the connected client. The seed list being a member of a multiplicity of seed lists 210 that the server has provided to the clients. The seed list is shown being stored in a memory having all seed lists, in the preferred embodiment. The memory storage is optional. Seed lists may be randomly generated or generated in response to a number of criteria. Example criterion include geographic and client characterization. For example, seed lists may be limited to connected clients in a specific country or regions such as the United States or Europe. Alternatively seed lists may be limited to connected clients classes sharing a common attribute such as engineering or sales. Seed lists may also be generated in response to distance from client, distance including network response time, where clients that are close are included in the seed list. In another embodiment seed lists may be generated in response to prior seed lists in order to generate an optimal network interconnection in an effort to maximize searched clients within a search time. Such a method could be further used to create search islands within a P2P network. Server 102 also maintains the connected client IP addresses 206 by testing for an expected acknowledgement signal from the connected clients. If an acknowledgement signal is not received, then the client address is removed from the list. Preferably the server periodically send a PING signal to connected clients and if an acknowledgement PONG signal is not received within a predetermined time the server determines the client is disconnected and removes the address of the client from list 206.

FIG. 3 shows a block diagram of an authentication and authorization process of the P2P network and system operating in accordance with a preferred embodiment of the present invention. Authentication and authorization process 104 preferably resides in a separate network security server but may alternatively reside in server 102. The authentication and authorization process is coupled to intranet backbone 100 through a network interface 302 that facilitates communication with the intranet and the clients. Before a client performs a resource search, the client may request that the authentication and authorization process provide authentication and/or authorization of the resource search.

If authentication is required, the client sends an authentication request signal to process 104. Network interface 302 receives the authentication request and communicates it to authentication credential check 304. The credentials are indicative of a client initiating a SEARCH request and included in the SEARCH request signal. When a client receives

Ex.1002 / Page 207 of 1173
Cisco Systems, Inc.

the SEARCH request and desires authentication of the requesting client, the credentials are communicated to process 104. The credentials preferably include a client ID of the client initiating the search and a corresponding password. Process 104 has a table of predetermined client identifications and passwords. If the client ID 306 and password 308 match those included in the authentication request signal, then the requesting client is verified and the process 104 sends an authentication signal back to the requesting client. Those familiar with the art appreciate that numerous other authentication processes are known and may be substituted for the authentication process described above.

If authorization is required, the client sends an authorization request signal to process 104. Network interface 302 receives the authorization request and communicates it to authorization process 310. The credentials are indicative of the client initiating the SEARCH request and included in the SEARCH request signal. When a client receives the SEARCH request and desires to determine which resources the requesting client is authorized to access, the credentials are communicated to process 104. The credentials preferably include a client ID of the client initiating the SEARCH. Process 104 has a table of predetermined client identifications 312 and access controls 314. In response to the authorization request, process 104 sends an authorization signal having the corresponding access control signals back to the requesting client. Access control signals 314 are indicative of the type of resources or client classes a client is permitted to search on its peers. Examples of various access controls or client classes include engineering resources, marketing resources and managerial resources. Each access control may have a number of subcategories, for example engineering may include network, integrated circuit and operating system subcategories. Each client may have authorization to access unique to each subcategory. For example, a client in an engineering department may not be authorized to search for managerial resources related to personnel issues or engineering integrated circuit resources while authorized to search engineering network and operating system resources.

In the preferred embodiment, both authentication and authorization processes are performed by a single request signal from the client, and may be performed for both SEARCH and GET requests. In alternative embodiments, only authorization or only authentication may be used. Furthermore, the authentications and/or authorizations may be held in the cache of a client in order to eliminate duplicate authentication and/or

Ex.1002 / Page 208 of 1173
Cisco Systems, Inc.

authorization communications of subsequent SEARCH and GET requests, thereby reducing network traffic.

FIG. 4 shows a block diagram of a client of the P2P network and system operating in accordance with a preferred embodiment of the present invention. The client is preferably a process operating in a personal computer coupled to intranet backbone 100. In alternate embodiments the process is operable in other computing devices such as laptop PCs, PDAs, and interactive consumer devices such as set top boxes, televisions, stereos, cell phones or other types of resource storing devices. Dispatcher and network interface 402 facilitates communication with the server, authentication and authorization process and other clients via the intranet backbone 100. The dispatcher responds to at least three signals received on the intranet backbone. The three signals are PING, SEARCH and GET. The client is also able to initiate PING, SEARCH and GET commands as well as communicate with the server 102 and authentication and authorization process 104. In responding to commands, the dispatcher 402 routs PING commands to ping/pong process 404 which responds to reception of a PING command with an acknowledging PONG command. SEARCH and GET commands are routed by dispatcher 402 to search and get processors 405 and 406. However, before a SEARCH or GET command is processed, the command is evaluated by the authentication and authorization process 408. Process 408 has at least three components, all of which are optional. The first component of authorization is predetermined and based upon the identification of the requesting client. This embodiment does not require the external authentication process 104. The second and third components are authentication and authorization performed by the external authentication and authorization 104. Numerous embodiments may be realized by various combinations of these three components. Authentication and authorization also includes an optional cache for storing authorized client identifications and or access controls associated with a client ID 412. Storage of this information in cache 410 reduces repeated authentication and/or authorization request to the process of FIG. 3.

If a SEARCH request is not authenticated, it need not be propagated to a subsequent peer in the P2P system, thereby reducing network traffic. Furthermore, the failure of the authentication need not be communicated to the requesting client, thereby deterring intranet hacking because the search requester will not know why the search yielded no results - either the resource was not found or the searcher not authenticated. If the SEARCH request is authenticated, then memory 320 of the client is searched for resource 422 matching the SEARCH request. Resources are preferably

Ex.1002 / Page 209 of 1173
Cisco Systems, Inc.

searched by searching metadata 424 which includes access controls and resource attributes. Search process 404 determines which resources may be searched by comparing the authorized access controls with the access controls associated with each resource. If there is a match, then the resource may be searched. Searching is preferably performed by searching attributes of the resource, the attributes including file type, file size, date or author. The attributes may also include comments or abstracts, for example manually generated by the author, providing additional information about the resource, thereby facilitating keyword searches. Alternatively, a more exhaustive search of the resource itself may be conducted. If a match is found, then a positive signal is propagated back to the client initiating the search.

A GET request is typically initiated by a client having initiated a SEARCH request and further having received a positive search result from the client receiving the GET request. The GET request may be both authorized and/or authenticated prior to execution by get process 406. Thereafter, the particular resource identified by the GET request is communicated to the requesting client.

Note that dispatcher 402 directly routs PING commands, however SEARCH and GET requests are in effect hidden behind a custom firewall 408. All requests, PING, SEARCH and GET appear to any other client as available. However, no response from the client may also mean there were security measures protecting GET or SEARCH. For example, a failed search does not send back a "no items found" signal. So if a client does not receive a response from a search, it does not know if the items were protected or if the items simply do not exist.

The client of FIG. 4 may also initiate SEARCH and GET requests. When a SEARCH request is initiated, the terms of the search are received typically from an operator of the client. The SEARCH and GET request processor 430 packages the terms of the search along with the credentials of the client 432 including a client ID and password as well as its IP address. The search request is then communicated to clients having an IP address included in its seed list 434, seed list 434 having IP addresses received from server 102. Credentials 432 are used in the aforementioned authentication and authorization processes. If a particular resource in a particular client is desired as a result of the search, then the SEARCH and GET request processor 430 packages the resource identification along with credential information into a GET request and sends the GET request to the corresponding client.

As a further part of the P2P search propagation process, a SEARCH request processed by search process 405 is also communicated to other addresses included in the seed list 434. This provides a peer-to-peer network search dispatcher for forwarding a resource search to client address of the seed list. However, the SEARCH request may not be propagated if there is a timeout or if there is a failure of the authentication process.

FIG. 5 shows a process flow diagram including interactions between a client and server for generating and maintaining seed lists in accordance with the a preferred embodiment of the present invention. For clarity, processes performed within the client are on the left and processes performed within the server are on the right. Beginning at step 500, the client stays at step 500 until it connects to the network. Connection preferably involves executing a program facilitating coupling to the P2P network. Such a program may be executed in a desktop personal computer client after it is powered ON. Similarly, such a program may be executed in a portable laptop personal computer client after it is physically coupled to the backbone.

Thereafter, the client sends a connect signal including the address of the client to the server at step 502. The server receives the connect signal at step 504 and adds the client address to the connected client address list, step 506. Step 508 generates a seed list for the client using any method including the aforementioned seed list generation methods. The seed list is sent from the server at step 510 and received by the client at step 512. Step 512 further sends a PING signal to the clients on the seed list to verify their connection to the P2P network. Non-acknowledging clients will be removed from the seed list at step 522. If the client has been disconnected at step 514, the process returns to step 500 awaiting reconnection. Disconnection can result at any time and be the result of a number of different events such as the client being powered OFF or the operator terminating the client's P2P program. It is not necessary for the client to actively signal the server that it is disconnected from the network. If still connected the client acknowledges any PING signal received as step 516. PING signals may be received from the server or other clients and are typically acknowledged with a PONG signal. Step 520 communicates with other clients performing PING, SEARCH and GET requests. If a client on the seed list does not respond to a PING, SEARCH or GET request, or may not otherwise be coupled or bound to, the client is determined to have been disconnected from the network and is removed from the seed list at step 522. Step 524 determines if the seed

Ex.1002 / Page 211 of 1173
Cisco Systems, Inc.

list should be refreshed, and if so sends the server a request to refresh the seed list at step 526. The seed list may be refreshed for any of several reasons including removal of one or more clients at step 522. Alternatively the seed list can be refreshed in response to a specific input from the operator, initiation of a new search, or after a certain period of time or inactivity. In other embodiments the server may initiate a refresh in order to reconfigure network behaviors. Seed list refresh may be a total or partial refresh. For example, if a seed list initially contained ten clients and it was determined that four of the clients had disconnected then the seed list refresh could request four new client addresses. Alternatively, if a first initiated search was based in engineering resources and a second initiated search was based in sales resources, an entire seed list could be replaced accordingly to optimize searching for a different type of resource. At the server, step 528 maintains the connected client address list. This is done by periodically sending a PING signal from the server to the clients on the connected list. If an expected acknowledgement signal, such as a PONG signal, is not received, then the client is removed from the connected client list. Then step 530 determines if the server has received a seed list refresh request and if not returns to step 504. Otherwise the server generates a seed list refresh from the connected client IP address list at step 532 and sends the seed list to the requesting client at step 534. The client receives the refreshed seed list at step 536 and sends a PING signal to new clients. Any non-acknowledging new clients are removed from the seed list at step 522. By the process of FIG. 5, seed lists are established and maintained at the client and the connected client IP address list is maintained at the server. It should be appreciated that in alternate embodiments the server may remove a client from the connected lists in response to any non-acknowledgement including non-response to a PING signal. For example clients could periodically send an acknowledgement signal without requiring PING from the server and if the acknowledgement signal is not received within a predetermined time, then step 528 removes the client from the connected list. Alternatively the client could actively send a disconnect signal, conditions permitting, and the server remove the client from the connected list in response thereto. Note in the preferred embodiment clients on the seed list are not regularly sent PING requests because the PING requests of steps 512 and 536 are sufficient. This has the advantage of significantly reducing network traffic in a distributed search P2P network.

FIG. 6 shows a process flow diagram of PING, SEARCH and GET request processing by a client in accordance with a preferred embodiment of the

Ex.1002 / Page 212 of 1173
Cisco Systems, Inc.

present invention. If a PING is received by a client at step 600 then a PONG is sent by the client at step 602. If a SEARCH request is received at step 604 then authentication is performed at step 606 and a search time out is checked at step 608. Authentication will be described in more detail below. If authentication passes and the search has not timed out, then step 610 forwards the search request to other clients in the seed list. Step 612 determines which resources may be searched by the client requesting or initiating the search. Of the selected or authorized resources, step 614 searches resource metadata for a match with the search request. If there is a resource match at step 616 then the client replies with a signal indicative of the matching resource at step 608 for propagation back to the requesting computer. From either of steps 604, 606, 608, 616 or 618 the process proceeds to step 620 to determine if a GET request is received. A GET request is typically initiated by a client after initiating a SEARCH request and receiving a match signal generated at step 618. If a GET request is received then step 622 determines if the requesting client is authorized to receive the resource. If authorized, step 624 sends the resource to the client initiating the GET request. It should be appreciated that the search is not propagated in response to a time out at step 608 or in response to an authentication failure at step 606. It should further be appreciated by one familiar with the art that the authentication process of step 606 may be combined with the determination process of step 612 while inhibiting search propagation in response to failure of authentication.

FIG. 7 shows a process flow diagram of an authentication process that does not require communication with an authentication process external to the client. The process of FIG. 7 occurs at the client at steps 612 and 622 of FIG. 6. At step 700 the identification credentials of the client initiating the search request are checked. The credential check could be a simple comparison of the client ID with a predetermined list, determination of the IP address of the requesting client, verification of a check sum, an encryption technique, security certificate or other method that does not require authentication through a process external to the client in response to a SEARCH or GET request. At step 702, resource access limitations are compared with the credentials of the initiating client. For example, it may be predetermined that client 1 has access to resources 2 and 3 while client 2 has access to resources 5 and 6. Alternatively it may be predetermined that clients from a certain IP gateway have limited access while other clients have unlimited access to resources. In response step 704 determines which specific resources may be searched or sent to the requesting client. The process shown in FIG. 7 has

Ex.1002 / Page 213 of 1173
Cisco Systems, Inc.

the advantage of providing for selective resource sharing in a distributed P2P network without the requirement of an external authorization and/or authentication process, the selection being in response to credentials indicative of the requesting client.

FIG. 8 shows a process flow diagram of communication between a client and an authentication process external to the client in accordance with a preferred embodiment of the present invention. For clarity, the client processes occur on the left side of FIG. 8 and the external authentication processes occur on right side of FIG. 8. The processes of FIG. 8 provide more detail to the processes shown in steps 612 or 622 of FIG. 6. Step 800 examines the client cache for a prior authentication of identification credentials performed in a prior SEARCH or GET request. If no prior authentication, then step 802 sends the identification credentials to an external authentication process, such as process 104 of FIG. 1. The external authentication process receives the credentials at step 804 and determines if the name and password included in the credentials matches a name and password stored at the authentication process. If there is a match, the authentication signal is returned to the client at step 806. Otherwise authentication is denied. The authentication signal is received by the client at step 808 and stored in the client cache along with the credentials received in the SEARCH or GET request at step 810. Thereafter, resource access controls are compared with identification credentials at step 812. For example it may be predetermined that client 1 has access to resources 2 and 3 while client 2 has access to resources 5, and 6. Alternatively it may be predetermined that clients from a certain IP gateway have limited access while other clients have unlimited access to resources. Step 814 determines which resources may be searched or sent to the requesting client. The process shown in FIG. 8 has the advantage of providing for selective resource sharing in a distributed P2P network using a centrally controlled authentication process. In a large organization where employees routinely are hired or terminated, central control of authentication allows for secure control of who may conduct a search in a distributed search P2P network system. Furthermore, caching of prior authentications significantly reduces authentication network traffic.

FIG. 9 shows a process flow diagram of a communication between a client and an authorization process external to the client in accordance with a preferred embodiment of the present invention. For clarity, the client processes occur on the left side of FIG. 9 and the external authorization processes occur on right side of FIG. 9. The processes of

Ex.1002 / Page 214 of 1173
Cisco Systems, Inc.

FIG. 9 provide more detail to the processes shown in steps 612 or 622 of FIG. 6. Step 900 examines the client cache for prior authorization access limitations of identification credentials performed in a prior SEARCH or GET request. If no prior authorization, then step 902 sends the identification credentials to an external authorization process, such as process 104 of FIG. 1. The external authorization process receives the credentials at step 904 and determines which access controls are associated with the identification credentials. In response an authorization access control signal is returned to the client at step 906. The authorization access control signal is received by the client at step 908 and stored in the client cache along with the credentials received in the SEARCH or GET request at step 910. Thereafter, authorization access controls associated with the requesting client are compared with resource access controls at step 912. Step 914 determines which resources may be searched or sent to the requesting client. The process shown in FIG. 9 has the advantage of providing for selective resource sharing in a distributed P2P network using a centrally controlled authorization process. In a large organization where employees regularly change job functions, thereby requiring access to differing types of information, central control of authorization allows for secure control of the type of resource one may search in a distributed search P2P network system. Furthermore, caching of prior authorizations significantly reduces authorization network traffic.

Thus, what is provided is a system that adapts the advantages of the P2P network while resolving disadvantages of current P2P systems. The P2P network takes advantage of the reduced central server requirements of a pure P2P network without sacrificing the efficiencies of the central server. Furthermore, the P2P network provides secure access and control to client resources without the requirement of a central server. The server function and security functions can operate independently. For example, the P2P network of FIG. 1 may be operated without the authentication and authorization functions 104 to provide server enhanced P2P search propagation. Alternately, the P2P network of FIG. 1 may be operated without the P2P server 102 providing a P2P search propagation with authentication and/or authorization functionality. The server 102 and authentication and authorization 104, when combined produce an efficient and secure P2P search propagation network. Such a combined system finds advantageous application in intranet application for global or other large organizations.

The present invention, as would be known to one familiar with the art, could be produced in hardware or software, or in a combination of

Ex.1002 / Page 215 of 1173
Cisco Systems, Inc.

hardware and software. The system, or method, according to the inventive principles as disclosed in connection with the preferred embodiment, may be produced in a single computer system having separate elements for performing the individual functions or steps described or claimed or one or more elements combining the performance of any of the functions or steps disclosed or claimed, or may be arranged in a distributed computer system, interconnected by any suitable means as would be known by one familiar with the art.

According to the inventive principles as disclosed in connection with the preferred embodiment, the invention and the inventive principles are not limited to any particular kind of computer system but may be used with any general purpose computer, as would be known to one familiar with the art, arranged to perform the functions described and the method steps described. The operations of such a computer, as described above, may be according to a computer program contained on a medium for use in the operation or control of the computer, as would be known to one familiar with the art. The computer medium that may be used to hold or contain the computer program product, may be a fixture of the computer such as an embedded memory or may be on a transportable medium such as a disk, as would be known to one familiar with the art.

The invention is not limited to any particular computer program or logic or language, or instruction but may be practiced with any such suitable program, logic or language, or instructions as would be known to one familiar with the art. Without limiting the principles of the disclosed invention any such computing system can include, inter alia, at least a computer readable medium allowing a computer to read data, instructions, messages or message packets, and other computer readable information from the computer readable medium. The computer readable medium may include nonvolatile memory, such as ROM, Flash memory, floppy disk, Disk drive memory, CDROM, and other permanent storage. Additionally, a computer readable medium may include, for example, volatile storage such as RAM, buffers, cache memory, and network circuits.

Furthermore, the computer readable medium may include computer readable information in a transitory state medium such as a network link and/or a network interface, including a wired network or a wireless network, that allow a computer to read such computer readable information.

Although a specific embodiment of the invention has been disclosed. It will be understood by those familiar with the art that changes can be made

to this specific embodiment without departing from the spirit and scope of the invention. The scope of the invention is not to be restricted, therefore, to the specific embodiment, and it is intended that the appended claims cover any and all such applications, modifications, and embodiments within the scope of the present invention.

Ex.1002 / Page 217 of 1173
Cisco Systems, Inc.

CLAIMS

1. In a peer-to-peer network a method of securely conducting a resource search initiated by a first client, the resource search included with a search request having a credentials signal indicative of the first client, the method comprising the steps of:

communicating the search request from the first client to a second client, the second client having a multiplicity of second resources, each of the multiplicity of second resources having at least one corresponding access attribute;

at the second client, selectively searching the multiplicity of second resources in response to comparison of the credentials signal and the at least one access attribute of each of the multiplicity of second resources;

communicating the search request from the second client to a third client, the third client having a multiplicity of third resources, each of the multiplicity of third resources having at least one corresponding access attribute; and

at the third client, selectively searching the multiplicity of third resources in response to comparison of the credentials signal and the at least one access attribute of each of the multiplicity of third resources.

2. The method according to claim 1 further comprising the steps of:

at the third client, determining a matching resource in response to said step of selectively searching the multiplicity of third resources; and

communicating a matching signal indicative of the matching resource from the third client to the first client.

3. The method according to claim 1 or claim 2 wherein

the credentials signal includes an identification signal indicative of the first client and

the access attributes of the second and third resources includes an authorization signal indicative of at least one of a plurality of clients, the plurality of clients including the first client, and further wherein

said step of selectively searching the second multiplicity of resources searches one of the second multiplicity of resources if the identification signal substantially matches the authorization signal included with the corresponding access attributes, and

said step of selectively searching the third multiplicity of resources searches one of the third multiplicity of resources if the identification signal substantially matches the authorization signal included with the corresponding access attributes.

4. The method according to any preceding claim wherein the credentials signal includes an identification signal indicative of the first client and

the access attributes of the second and third resources includes an authorization signal indicative of at least one of a plurality of clients, the plurality of clients including the first client, wherein

said step of selectively searching the second multiplicity of resources further includes the steps of:

communicating from the second client to an authentication process external to the first, second and third clients the identification signal;

receiving from the authentication process an authenticated signal indicative of the first client in response thereto; and

searching one of the second multiplicity of resources if the authenticated signal substantially matches the authorization signal included with the corresponding access attributes, and

said step of selectively searching the third multiplicity of resources further includes the steps of:

communicating from the third client to the authorization process the identification signal;

receiving from the authorization process the authenticated signal indicative of the first client in response thereto; and

searching one of the third multiplicity of resources if the authenticated signal substantially matches the authorization signal included with the corresponding access attributes.

5. The method according to claim 4 further comprising the steps:

at the second client, storing the identification signal and the received authenticated signal in a cache memory at the second client; and

at the second client searching the cache memory for the identification signal and the received authentication signal prior to said step communicating from the second client to the authentication process, wherein

said step communicating from the second client to the authentication process is not performed if said step of searching the cache memory finds the identification signal and the received authentication signal stored therein, and

said step of searching one of the second multiplicity of resources uses the authenticated signal stored in the cache memory, thereby reducing communication between the second client and the authentication process.

6. The method according to claim 4 further comprising the steps:

at the third client, storing the identification signal and the received authenticated signal in a cache memory at the third client; and

at the third client searching the cache memory for the identification signal and the received authentication signal prior to said step communicating from the third client to the authentication process, wherein

said step communicating from the third client to the authentication process is not performed if said step of searching the cache memory finds the identification signal and the received authentication signal stored therein, and

said step of searching one of the third multiplicity of resources uses the authenticated signal stored in the cache memory, thereby reducing communication between the third client and the authentication process.

7. The method according to claim 4 wherein said step of communicating the search request from the second client to the third client and said step of selectively searching the multiplicity of third resources are not performed if the authentication signal is not received from the authentication process by the second client.

8. The method according to any preceding claim wherein

the credentials signal includes an identification signal indicative of the first client and

the access attributes of the second and third resources includes an authorization signal indicative of at least one of a plurality of client classes, wherein

said step of selectively searching the second multiplicity of resources further includes the steps of:

communicating from the second client to an authorization process external to the second client the identification signal;

receiving from the authorization process a client class signal indicative which of the plurality of client classes are associated with the identification signal; and

searching one of the second multiplicity of resources if the client class signal substantially matches the authorization signal included with the corresponding access attributes, and

said step of selectively searching the third multiplicity of resources further includes the steps of:

communicating from the third client to the authorization process external to the third client the identification signal;

receiving from the authorization process the client class signal indicative which of the plurality of client classes are associated with the identification signal; and

searching one of the third multiplicity of resources if client class signal substantially matches the authorization signal included with the corresponding access attributes.

9. The method according to claim 8 further comprising the steps:

at the second client, storing the identification signal and the received client class signal in a cache memory at the second client; and

at the second client searching the cache memory for the identification signal and the received client cache signal prior to said step communicating from the second client to the authorization process, wherein

said step communicating from the second client to the authorization process is not performed if said step of searching the cache memory finds the identification signal and the received client cache signal stored therein;

said step of searching one of the second multiplicity of resources uses the client cache signal stored in the cache memory, thereby reducing communication between the second client and the autorization process;

at the third client, storing the identification signal and the received client class signal in a cache memory at the third client; and

at the third client searching the cache memory for the identification signal and the received client cache signal prior to said step communicating from the third client to the authorization process, wherein

said step communicating from the third client to the authorization process is not performed if said step of searching the cache memory finds the identification signal and the received client class signal stored therein, and

said step of searching one of the third multiplicity of resources uses the client class signal stored in the cache memory, thereby reducing communication between the third client and the authentication process.

10. A client included in a peer-to-peer network having a multiplicity of clients, the client comprising:

a peer-to-peer network dispatcher for receiving a resource search request from a second client of the multiplicity of clients, the search request initiating from an initiating client of the multiplicity of clients, the search request including a credentials signal having an identification signal indicative of the initiating client;

a memory for storing a plurality of resources, each of the plurality of resources having at least one corresponding access attribute; and

a search engine for selectively searching at least one of the plurality of resources in response to a comparison of the credentials signal and the at least one access attribute of each of the plurality of resources.

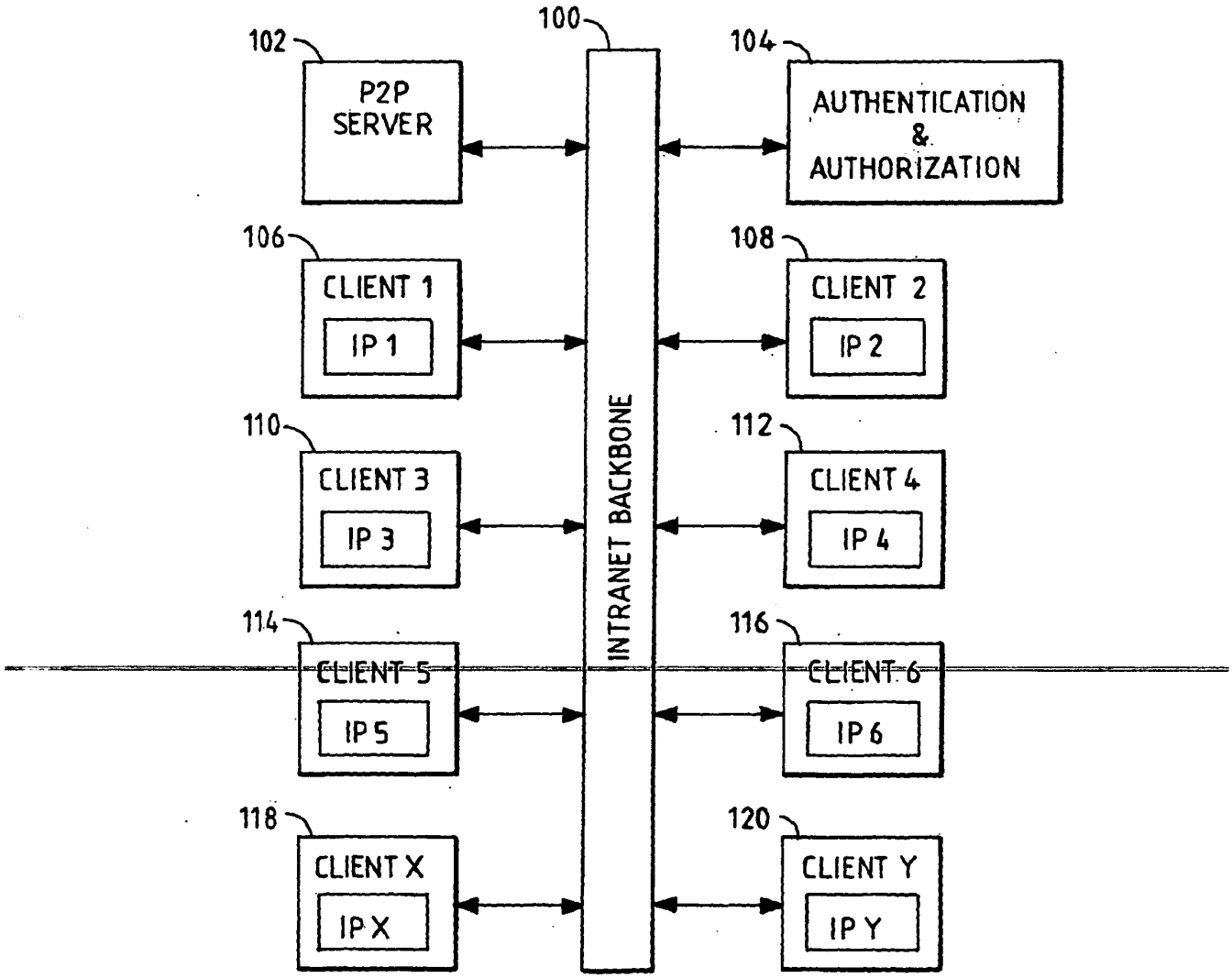

100
102
P2P SERVER
104
AUTHENTICATION & AUTHORIZATION
106
CLIENT 1
IP 1
108
CLIENT 2
IP 2
110
CLIENT 3
IP 3
112
CLIENT 4
IP 4
114
CLIENT 5
IP 5
116
CLIENT 6
IP 6
118
CLIENT X
IP X
120
CLIENT Y
IP Y
INTRANET BACKBONE

FIG. 1

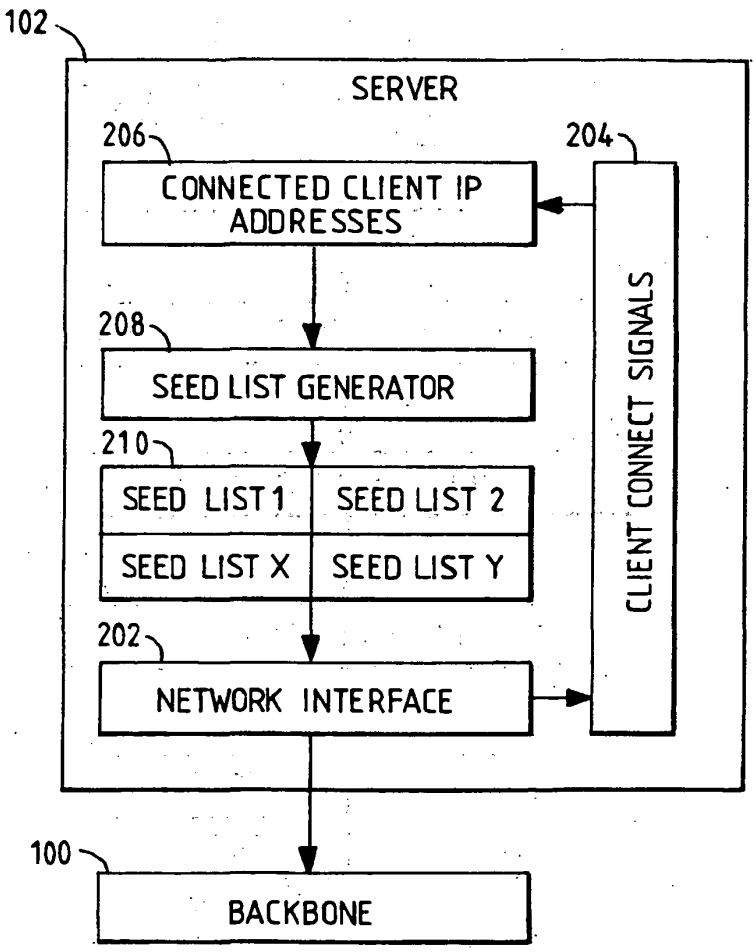


FIG. 2

Ex.1002 / Page 225 of 1173
Cisco Systems, Inc.

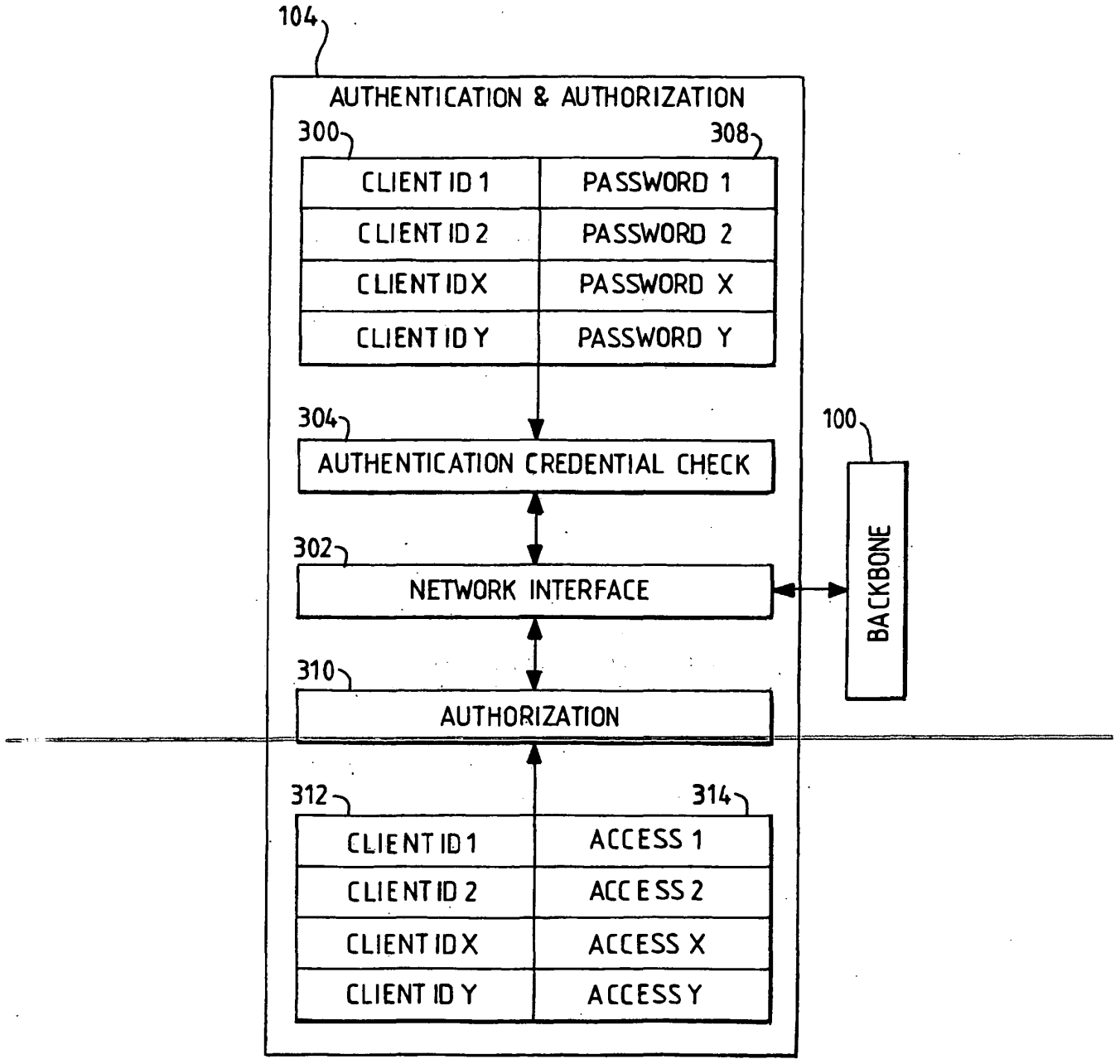

104
AUTHENTICATION & AUTHORIZATION
300
308
CLIENT ID 1
PASSWORD 1
CLIENT ID 2
PASSWORD 2
CLIENT ID X
PASSWORD X
CLIENT ID Y
PASSWORD Y
304
AUTHENTICATION CREDENTIAL CHECK
100
BACKBONE
302
NETWORK INTERFACE
310
AUTHORIZATION
312
314
CLIENT ID 1
ACCESS 1
CLIENT ID 2
ACCESS 2
CLIENT ID X
ACCESS X
CLIENT ID Y
ACCESS Y

FIG. 3

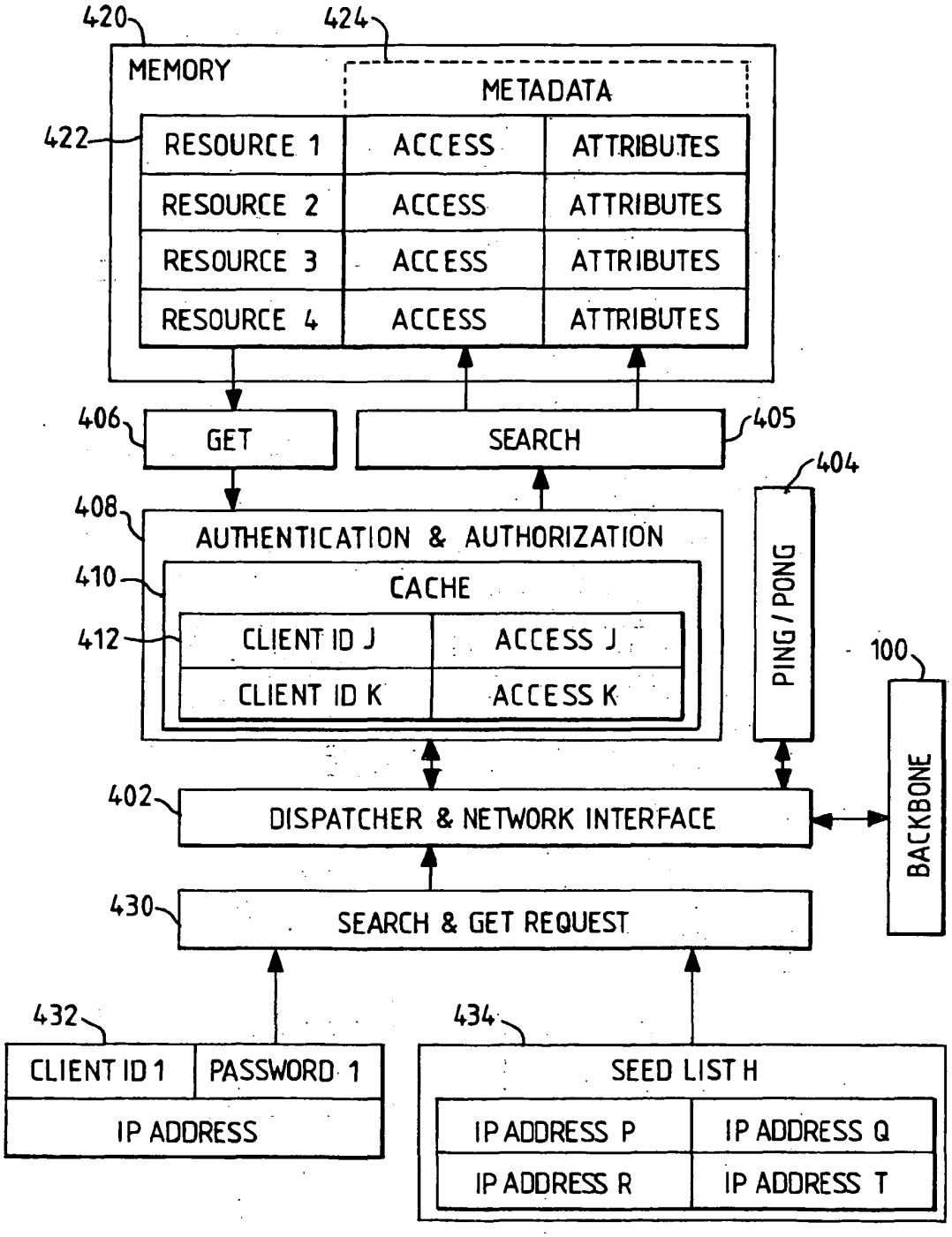

420
424
MEMORY
METADATA
422
RESOURCE 1
ACCESS
ATTRIBUTES
RESOURCE 2
ACCESS
ATTRIBUTES
RESOURCE 3
ACCESS
ATTRIBUTES
RESOURCE 4
ACCESS
ATTRIBUTES
406
GET
SEARCH
405
404
408
AUTHENTICATION & AUTHORIZATION
410
CACHE
412
CLIENT ID J
ACCESS J
CLIENT ID K
ACCESS K
PING / PONG
100
BACKBONE
402
DISPATCHER & NETWORK INTERFACE
430
SEARCH & GET REQUEST
432
CLIENT ID 1
PASSWORD 1
IP ADDRESS
434
SEED LIST H
IP ADDRESS P
IP ADDRESS Q
IP ADDRESS R
IP ADDRESS T

FIG. 4

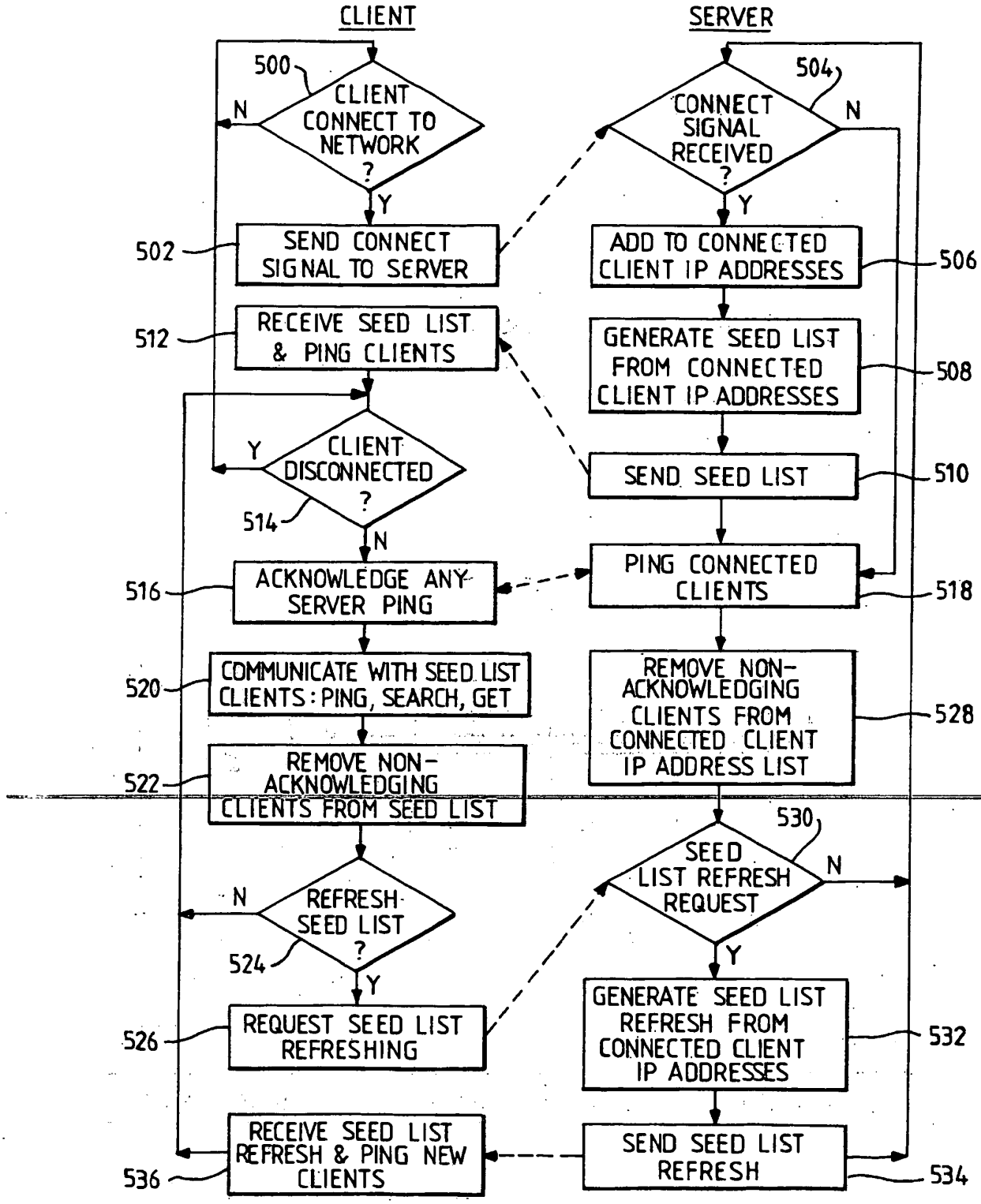


FIG. 5

BNSDOCID: <WO_____03079635A1_I_>

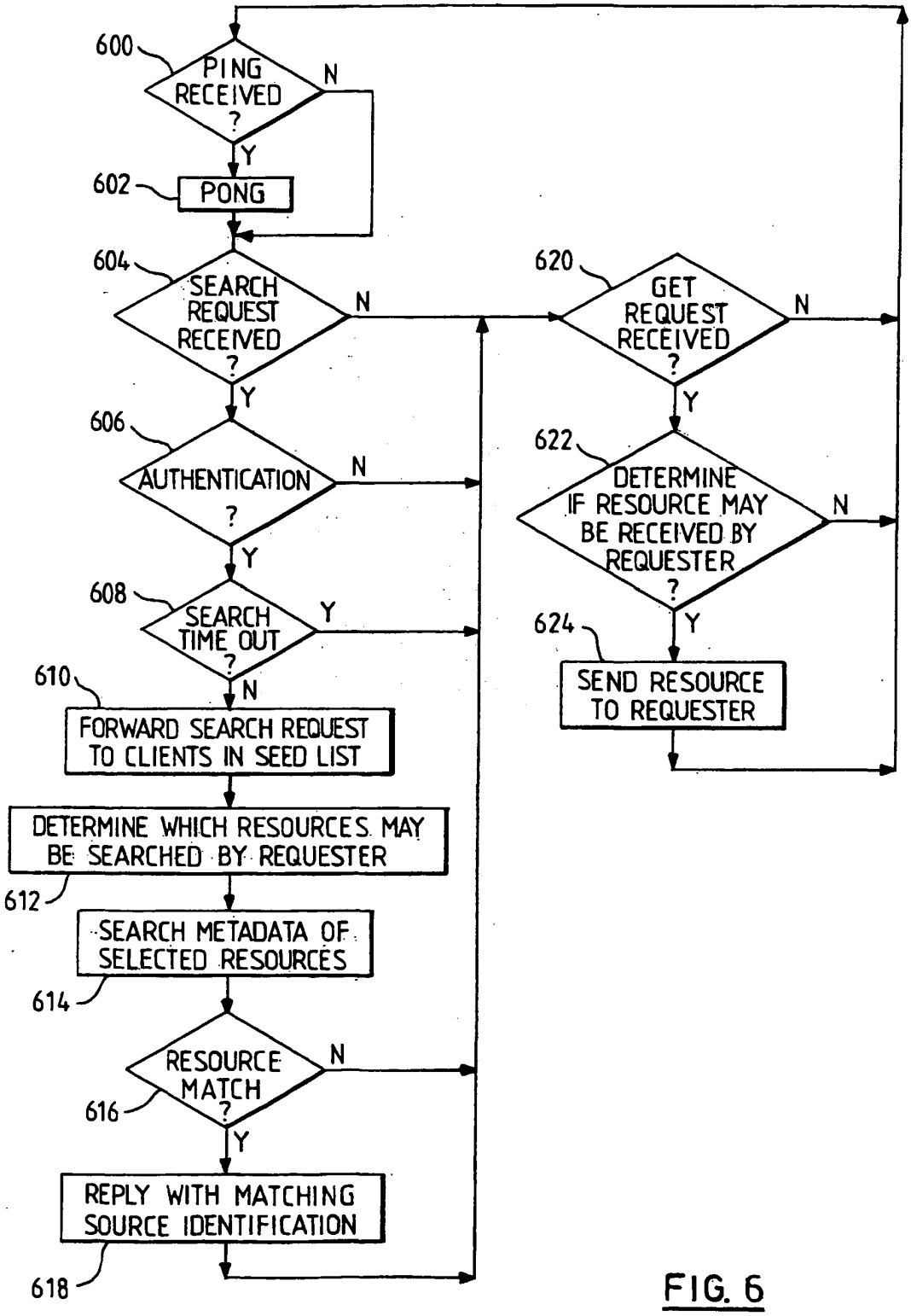

600
PING RECEIVED ?
N
Y
602
PONG
604
SEARCH REQUEST RECEIVED ?
N
Y
606
AUTHENTICATION ?
N
Y
608
SEARCH TIME OUT ?
Y
N
610
FORWARD SEARCH REQUEST TO CLIENTS IN SEED LIST
DETERMINE WHICH RESOURCES MAY BE SEARCHED BY REQUESTER
612
SEARCH METADATA OF SELECTED RESOURCES
614
RESOURCE MATCH ?
N
616
Y
REPLY WITH MATCHING SOURCE IDENTIFICATION
618
620
GET REQUEST RECEIVED ?
N
Y
622
DETERMINE IF RESOURCE MAY BE RECEIVED BY REQUESTER ?
N
Y
624
SEND RESOURCE TO REQUESTER

FIG. 6

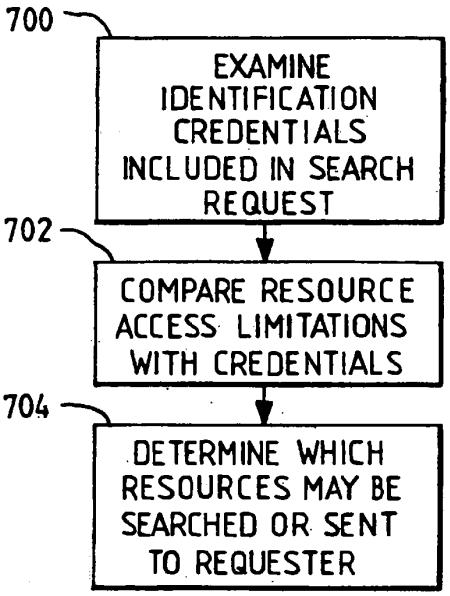

700
EXAMINE IDENTIFICATION CREDENTIALS INCLUDED IN SEARCH REQUEST
702
COMPARE RESOURCE ACCESS LIMITATIONS WITH CREDENTIALS
704
DETERMINE WHICH RESOURCES MAY BE SEARCHED OR SENT TO REQUESTER

FIG. 7

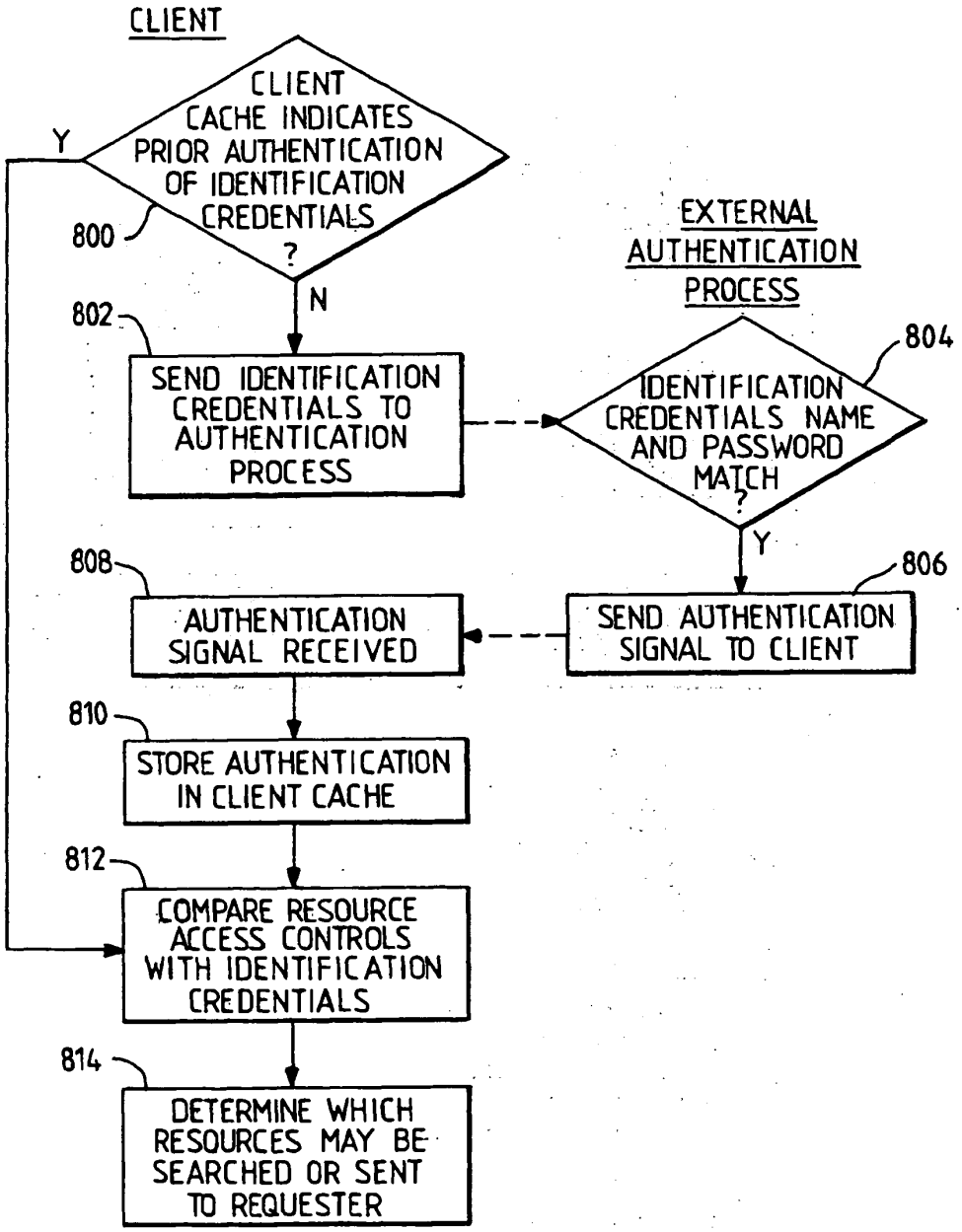

CLIENT
CLIENT CACHE INDICATES PRIOR AUTHENTICATION OF IDENTIFICATION CREDENTIALS ?
800
Y
N
802
SEND IDENTIFICATION CREDENTIALS TO AUTHENTICATION PROCESS
EXTERNAL AUTHENTICATION PROCESS
804
IDENTIFICATION CREDENTIALS NAME AND PASSWORD MATCH ?
Y
806
SEND AUTHENTICATION SIGNAL TO CLIENT
808
AUTHENTICATION SIGNAL RECEIVED
810
STORE AUTHENTICATION IN CLIENT CACHE
812
COMPARE RESOURCE ACCESS CONTROLS WITH IDENTIFICATION CREDENTIALS
814
DETERMINE WHICH RESOURCES MAY BE SEARCHED OR SENT TO REQUESTER

FIG. 8

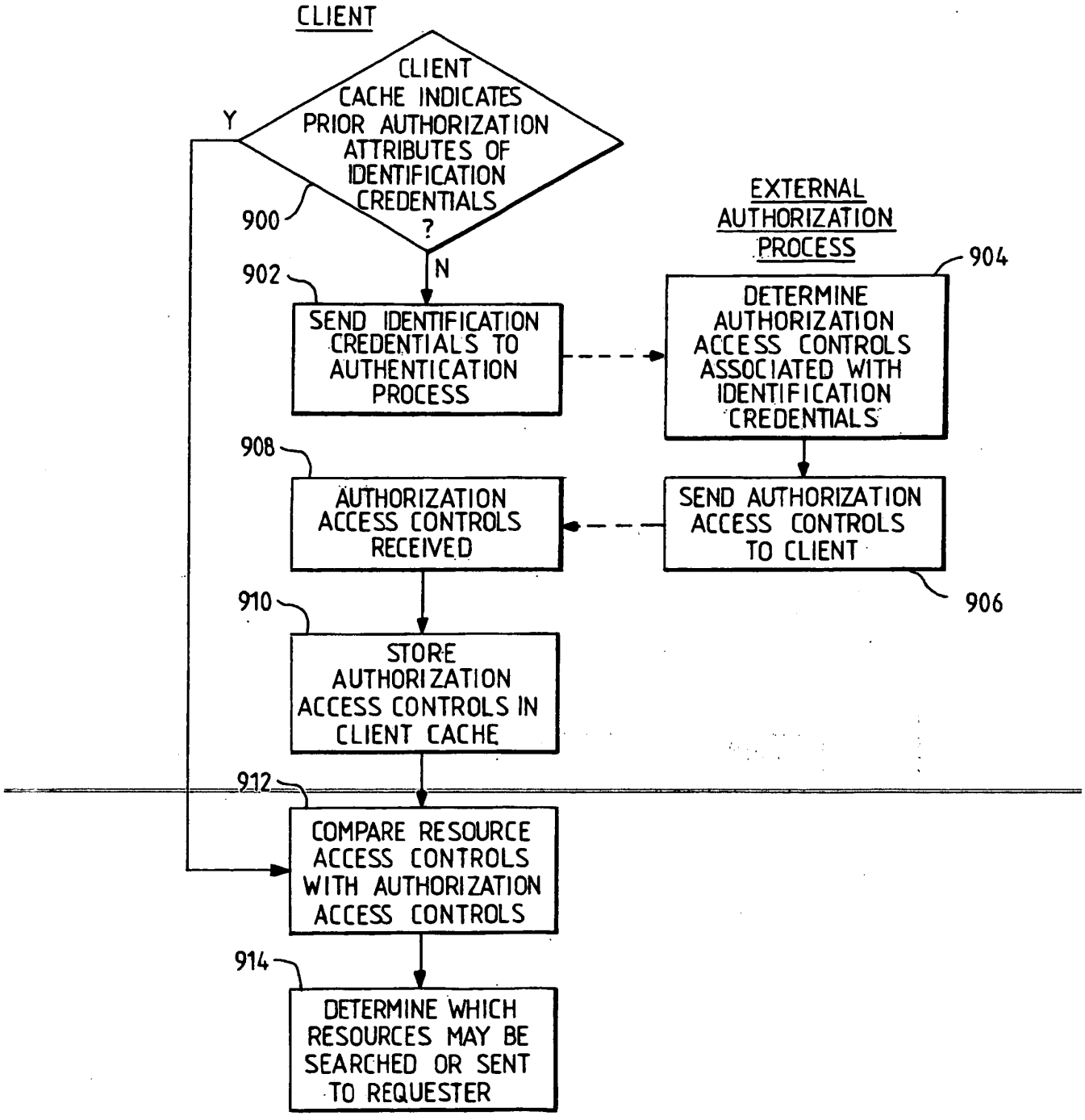


FIG. 9

BNSDOCID: <WO_____03079635A1_I >

INTERNATIONAL SEARCH REPORT

Internati Application No
PCT/GB 03/00776

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 H04L29/08

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 H04L

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, PAJ, WPI Data, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WOOYOUNG KIM ET AL: "A secure platform for peer-to-peer computing in the Internet" PROCEEDINGS OF THE 35TH ANNUAL HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES, PROCEEDINGS OF THE 35TH ANNUAL HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES, BIG ISLAND, HI, USA, 7-10 JAN. 2002, 'Online! pages 3948-3957, XP002251810 2002, Los Alamitos, CA, USA, IEEE Comput. Soc, USA ISBN: 0-7695-1435-9 Retrieved from the Internet: <URL:7198204> 'retrieved on 2003-08-14! Abstract 2.3 Queries 2.4 Communication 3.3 Capability-based Access Control -/--	1-10

[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
21 August 2003	01/09/2003

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	Bertolissi, E

Form PCT/ISA/210 (second sheet) (July 1992)

ISDOCID: <WO_____03079635A1_I_>

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	5. Advertising Service and Ad Hoc Discovery --- ADVANCED REALITY: "Advanced Reality Introduces Peer-to-Peer Collaboration Platform that Makes Any Application Collaborative " ADVANCED REALITY PRESS RELEASE, 'Online! 10 December 2001 (2001-12-10), XP002251811 Retrieved from the Internet: <URL:http://www.advancedreality.com/news_and_events/Press_Releases/2001/Presence-AR%20Press%20Release%20121001.pdf> 'retrieved on 2003-08-14! Page 2, Enterprise Level Security	
X		1-10
	--- ADVANCED REALITY : "Presence-AR Technology Overview " ADVANCED REALITY INTERNET PUBLICATION, 'Online! 20 March 2002 (2002-03-20), XP002251812 Retrieved from the Internet: <URL:http://www.advancedreality.com/Resource_Library/Presence-AR_Technology_Overview.pdf> 'retrieved on 2003-08-14! pages 9-10, Security	
P,X		1-10
	--- UMA S CHATHAPURAM: "Security in Peer-to-Peer Networks" INTERNET PUBLICATION, 'Online! 8 August 2001 (2001-08-08), XP002251813 Retrieved from the Internet: <URL:http://netserver.cerc.wvu.edu/classes/cs491h_summer2_2001/sankaran_securityoverview/security-uma.doc> 'retrieved on 2003-08-14! Page 3, Introduction Page 7, Availability	
X		1,10
	--- WO 01 13201 A (SARNOFF CORP) 22 February 2001 (2001-02-22) abstract	
A		1,10
	--- EP 1 229 442 A (SUN MICROSYSTEMS INC) 7 August 2002 (2002-08-07) abstract paragraph '0285! - paragraph '0303!	
P,X		1,10
	--- WO 02 091239 A (SUN MICROSYSTEMS INC) 14 November 2002 (2002-11-14) abstract page 35, line 22 - line 28 page 41, line 25 - line 31	
P,X		1,10
	--- -/--	

Ex.1002 / Page 234 of 1173
Cisco Systems, Inc.

INTERNATIONAL SEARCH REPORT

Internati Application No
PCT/GB 03/00776

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2000 112860 A (MITSUBISHI ELECTRIC CORP) 21 April 2000 (2000-04-21) abstract paragraph '0001! - paragraph '0017!	1-10

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

ISDOCID: <WO_____03079635A1_I_>

INTERNATIONAL SEARCH REPORT

Internati Application No
PCT/GB 03/00776

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0113201 A	22-02-2001	AU 6522200 A	05-03-2001
		AU 6537400 A	13-03-2001
		EP 1203479 A2	08-05-2002
		WO 0111817 A2	15-02-2001
		WO 0113201 A2	22-02-2001
EP 1229442 A	07-08-2002	EP 1229442 A2	07-08-2002
		EP 1229443 A2	07-08-2002
		WO 02057917 A2	25-07-2002
		US 2002143944 A1	03-10-2002
		US 2002143855 A1	03-10-2002
		US 2002184310 A1	05-12-2002
		US 2002184357 A1	05-12-2002
		US 2002184311 A1	05-12-2002
		US 2003002521 A1	02-01-2003
		US 2002152299 A1	17-10-2002
		US 2002184358 A1	05-12-2002
		US 2002188657 A1	12-12-2002
		US 2002147810 A1	10-10-2002
		US 2002147771 A1	10-10-2002
		US 2002156893 A1	24-10-2002
		US 2003041141 A1	27-02-2003
		EP 1282289 A2	05-02-2003
		US 2003028585 A1	06-02-2003
		US 2003070070 A1	10-04-2003
		US 2003055894 A1	20-03-2003
		US 2003055898 A1	20-03-2003
WO 02091239 A	14-11-2002	US 2003088544 A1	08-05-2003
		US 2003126120 A1	03-07-2003
		WO 02091238 A2	14-11-2002
		WO 02091239 A2	14-11-2002
		WO 02091107 A2	14-11-2002
		WO 02091241 A2	14-11-2002
		WO 02091242 A2	14-11-2002
		WO 02091243 A2	14-11-2002
		US 2003050959 A1	13-03-2003
		US 2003050924 A1	13-03-2003
		US 2003055818 A1	20-03-2003
JP 2000112860 A	21-04-2000	NONE	

Form PCT/ISA/210 (patent family annex) (July 1992)

BNSDOCID: <WO_____03079635A1_I_>

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 July 2004 (29.07.2004)

PCT

(10) International Publication Number
WO 2004/063843 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number:
PCT/JP2004/000261

(22) International Filing Date: 15 January 2004 (15.01.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/342,304 15 January 2003 (15.01.2003) US
10/372,218 25 February 2003 (25.02.2003) US

(71) Applicant *(for all designated States except US)*: **MATSUSHITA ELECTRIC INDUSTRIAL CO.,LTD.** [JP/JP]; 1006, Oaza Kadoma, Kadoma-shi, Osaka 5718501 (JP).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **TAKEDA, Yutaka** [/]. **BOIRI, Youssef, Kamal** [/].

(74) Agents: **MAEDA, Hiroshi** et al.; Honmachi-nakajima Bldg., 4-8,, Utsubohonmachi 1-chome, Nishi-ku, Osaka-shi, Osaka 5500004 (JP).

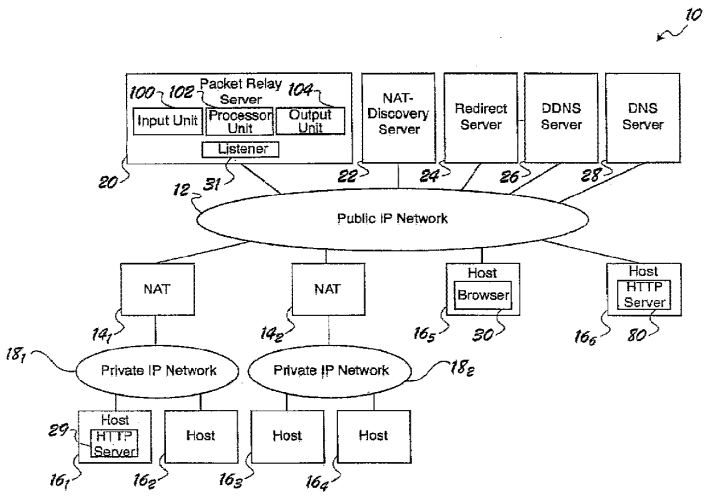
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, 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 *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI (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: PEER-TO-PEER (P2P) CONNECTION DESPITE NETWORK ADDRESS TRANSLATOR (NATs) AT BOTH ENDS



(57) Abstract: Methods of operating a first endpoint device (ED) facilitate the making of a peer-to-peer (P2P) connection between the first ED and a second ED despite intervening network address translators (NATs) at both ends. The P2P connection extends across a system compliant with the internet protocol (IP) whose architecture that includes a first network (having at least the first ED and a first NAT), a second network (having at least the second ED and a second NAT) and a third network. The first ED connects to the third network via the first NAT while the second ED connects to the third network via the second NAT. A first such method includes: providing the second ED with the first IP-address/port pair; and providing the second ED with first type-information regarding the type of the first NAT.

WO 2004/063843 A2

DESCRIPTION

PEER-TO-PEER (P2P) CONNECTION DESPITE NETWORK ADDRESS TRANSLATOR (NATs) AT BOTH ENDS

BACKGROUND ART

In the last decade, the number of computers connected to the Internet has increased by an enormous order of magnitude. High growth in the number of Internet connections has put severe pressure on the available address-space of routable internet protocol (IP) addresses. To overcome the problem of limited and diminishing IP address-space, it became imperative to have a solution that would allow multiple users to share a single routable internet address. The commonly used solution for sharing a single IP address is known as a Network Address Translator (NAT). Operation of a typical NAT is described next.

The basic concept underlying a NAT is to have a device or software module that allows sharing of one or more routable Internet Protocol (IP) addresses by multiple computers. A typical NAT is connected to the public internet on one side and has at least one global or public IP address for receiving and sending data packets from and to the public internet. On the other side of the typical NAT is a private network, in which each network node (computer) is assigned a local arbitrary address. Typically, the NAT assigns arbitrary addresses to the nodes of the private network using a Dynamic host Control Protocol (DHCP) or alternatively the NAT assigns static translation addresses.

According to Simple Traversal of UDP through NAT ("STUN", where UDP is the acronym for User Datagram Protocol), there are five basic types of NAT in the Background Art. It is helpful to discuss the differences between the types of NAT, which will be done in terms of the simplistic system block diagrams of Background Art Figs. 4A - 4E.

Fig. 4A depicts a system 400 according to the Background Art that includes: an endpoint device 404; an endpoint device 406 having an IP address X and ports p and q; an endpoint device 408 having an IP address Y and ports p and q; and a full cone type of NAT 404. Devices 404, 406 and 408 are described as "endpoint" devices because they can be the endpoints of a communication session, e.g., between device 404 and device 406 or between device 404 and device 408. While there will be at least one intermediary device, namely the NAT 402, between the endpoint devices, the endpoints themselves are not intermediary devices for the purposes of this explanation.

The endpoint devices 404, 406 and 408, respectively, can be, e.g., a host of server such as an HTTP server, a host of browser such as an HTTP browser, an IP video camera, etc. Typically, the endpoint device 404 is part of a first network 418, and the endpoint devices 406 and 408 are part of a second network 419. The full-cone NAT 402 can be considered as part of each of the first network 418 and the second network 419. The endpoint devices 406 and 408 communicate with the endpoint device 404 via the full-cone NAT 402, and vice-versa, respectively.

In general, any type of the four types of NAT will allocate or map an address and port-number pair to the endpoint device 404. As a practical matter, this address/port pair makes it seem to devices on the second network 419 as if the endpoint device 404 is directly connected to the second network 419. In particular, the full-cone NAT 402 will accept a packet from any device on the second network 419, e.g., endpoint devices 406 or 408.

In Fig. 4A, a packet (not depicted) can be sent from the endpoint device 404 to the endpoint device 406 through the full-cone NAT 402 using the destination address/port pair X,p, as indicated by path 410. Not surprisingly, a packet (not depicted) sent by the endpoint device 406 to the endpoint device 404 using the source address/port pair X,p will

be accepted by the full-cone NAT 402 (and passed along to the endpoint device 404), as indicated by the path 412.

The nature of the full-cone NAT 402 is to accept a packet whose destination address/port pair is the address/port pair mapped to the endpoint device 404, regardless of the packet's source address, i.e., regardless of whether the source address and/or source port of the received packet matches a destination address of a packet previously sent from the endpoint device 404 via the full-cone NAT 402 to the second network 419. As such, packets (not shown) having the following source address/port pairs will also be accepted by the full-cone NAT 402: X,q as indicated by path 413; Y,p as indicated by path 414; and Y,q as indicated by path 416.

In contrast, other types of NAT depicted in Figs. 4B, 4C, 4D and 4E each exhibit greater restrictions upon what types of packets coming from the second network 419 will be accepted.

Fig. 4B depicts a system 420 that is similar to the system 400 except that an address-restricted cone type of NAT 422 is present instead of the full-cone NAT 402.

In Fig. 4B, a packet (not depicted) can be sent from the endpoint device 404 to the endpoint device 406 through the address-restricted NAT 422 using the destination address/port pair X,p, as indicated by path 424. Not surprisingly, a packet (not depicted) sent by the endpoint device 406 to the endpoint device 404 using the source address/port pair X,p will be accepted by the address-restricted NAT 422 (and passed along to the endpoint device 404), as indicated by the path 424.

The more-restricted nature of the address-restricted NAT 422 is to accept a packet whose destination address/port pair is the address/port pair mapped to the endpoint device 404 so long as the source address in the received packet matches a destination address of a packet previously sent from the endpoint device 404 via the address-restricted NAT 422 to

the second network 419, regardless of whether the source port matches the destination port of the packet previously sent from the endpoint device 404 via the full-cone NAT 422 to the second network 419. As such, a packet (not shown) having the address/port pair X,q will be also be accepted by the full-cone NAT 422, as indicated by path 426.

But packets having the following source address/port pairs will not be accepted (i.e., will be blocked) by the full-cone NAT 402: Y,p as indicated by path 430; and Y,q as indicated by path 432. Again, this is because the source addresses of the packets of path 430 and 432 do not match a destination address of a packet previously sent by the address-restricted NAT 422, e.g., such as the destination address of the packet of path 424.

Fig. 4C depicts a system 440 that is similar to the system 420 except that an address&port-restricted ("port-restricted") cone type of NAT 442 is present instead of the address-restricted NAT 422.

In Fig. 4C, a packet (not depicted) can be sent from the endpoint device 404 to the endpoint device 406 through the port-restricted NAT 442 using the destination address/port pair X,p, as indicated by path 444. Not surprisingly, a packet (not depicted) sent by the endpoint device 406 to the endpoint device 404 using the source address/port pair X,p will be accepted by the port-restricted NAT 442 (and passed along to the endpoint device 404), as indicated by the path 446.

The further-restricted nature of the port-restricted NAT 442 is to accept a packet whose destination address/port pair is the address/port pair mapped to the endpoint device 404 so long as the source port as well as the source address in the received packet matches a destination address/port pair of a packet previously sent from the endpoint device 404 via the port-restricted NAT 442 to the second network 419. Consequently, packets having the following source address/port pairs will not be accepted (i.e., will be blocked) by the port-

restricted NAT 442: X,q as indicated by path 448; Y,p as indicated by path 450; and Y,q as indicated by path 452.

Again, though the packet of path 448 has a source address that matches the destination address for the packet of path 444, the source port does not match a destination port of a packet previously sent via the port-restricted NAT 442. And both of the source addresses and source ports of the packets of paths 450 and 452, and hence their respective address/port pairs, fail to match the address/port of a packet previously sent via the port-restricted NAT 442.

Fig. 4D depicts a system 460 that is similar to the system 440 except that a symmetric and port-sensitive ("SYM_S") type of NAT 462 is present instead of the port-restricted NAT 442. For the purposes of this explanation, it is assumed that the SYM_S 462 has mapped two address/port pairs to the endpoint device 404; namely: a first address/port pair having the address of the SYM_S 462 and port:v; and a second pair having the same address but using port:w.

In Fig. 4D, a packet (not depicted) can be sent from the endpoint device 404 to the endpoint device 406 through port-v of the SYM_S 462 using the destination address/port pair X,p, as indicated by path 464. Not surprisingly, a packet (not depicted) sent by the endpoint device 406 to the endpoint device 404 using the source address/port pair X,p and the destination port-v will be accepted by the SYM_S 462 (and revised and then passed along to the endpoint device 404), as indicated by the path 466.

The yet further-restricted nature of the SYM_S 462 is similar to the port-restricted NAT 442, albeit with a significant difference. For each different destination address/port pair that the endpoint device 404 sends a packet, the SYM_S 462 allocates/maps a separate address/port pair. For a packet to be accepted from the second network 419 by the SYM_S 442, the packet's combination of destination port and source address/port pair should

match the combination of source port and destination address/port pair, respectively, of a packet sent to the second network 419 via the SYM_S NAT 462.

It is assumed for the purposes of explanation that a packet will be sent from the endpoint device 404 to each of the endpoint devices 406 (specifically at port:p) and 408 (specifically at port:q) via the SYM_S 462.

For use with respect to port:p of the endpoint device 406 (address/port pair X,p), the SYM_S 462 maps its port:v to the endpoint device 404. Similarly, for use with respect to port:q of the endpoint device 408 (address/port pair Y,q), the SYM_S 462 maps its port:w to the endpoint device 404. The packet (not depicted) sent to port:p of the endpoint device 406 through port:v of the SYM_S 462 is indicated by path 464, while the packet (not depicted) sent to port:q of the endpoint device 408 through port:w of the SYM_S 462 is indicated by path 470. Not surprisingly, a packet (not depicted) sent by the endpoint device 406 to the endpoint device 404 using the source address/port pair X,p will be accepted by the SYM_S 462 (and revised and then passed along to the endpoint device 404), as indicated by the path 466. Similarly, a packet (not depicted) sent by the endpoint device 408 using the source address/port pair Y,q will be accepted by the SYM_S 462, as indicated by the path 472.

But packets having the following source address/port pairs will not be accepted (i.e., will be blocked) by the SYM_S 462: X,q as indicated by path 468; and Y,q as indicated by path 474. Again, though the address portion of the source address/port pair of the packet of path 468 matches an address portion of a packet previously sent via the SYM_S 462, the port portion (namely port:q) of the source address/port pair does not match.

Fig. 4E depicts a system 480 that is similar to the system 460 except that a symmetric and port-insensitive ("SYM_I") type of NAT 482 is present instead of the port-restricted NAT 462. For the purposes of this explanation, it is assumed that the SYM_I 482

has mapped two address/port pairs to the endpoint device 404; namely: a first address/port pair having the address of the SYM_I 462 and port:v; and a second pair having the same address but using port:w.

In Fig. 4E, a packet (not depicted) can be sent from the endpoint device 404 to the endpoint device 406 through port-v of the SYM_I 462 using the destination address/port pair X,p, as indicated by path 484. Not surprisingly, a packet (not depicted) sent by the endpoint device 406 to the endpoint device 404 using the source address/port pair X,p and the destination port-v will be accepted by the SYM_I 462 (and revised and then passed along to the endpoint device 404), as indicated by the path 486.

The further-restricted nature of the SYM_I 482 is similar to the port-restricted NAT 462, albeit with a significant difference that makes the SYM_I 482 somewhat similar also to the address-restricted NAT 422. For each different destination address (not address/port pair as with the SYM_S NAT 462) that the endpoint device 404 sends a packet, the SYM_I 462 allocates/maps a separate address/port pair. The SYM_I type of NAT 462 can have two implementations: loose (not separately depicted); and tight (not separately depicted). Depending upon the particular implementation, one of two initialization scenarios, namely tightly initialized or loosely initialized, will describe what sort of initialization should take place before a packet from the second network 419 will be accepted by the SYM_I NAT 482.

First, the loosely initialized scenario for a loose SYM_I NAT 482 will be described. For a packet to be accepted from the second network 419 by the loose SYM_I NAT 482, the packet's combination of destination port and source address (but not also source port) should match the combination of source port and destination address, respectively, of a packet sent to the second network 419 via the loose SYM_I NAT 482. In terms of an example, despite the loose SYM_I NAT 482 having not sent a packet to port:q of the endpoint device 406 (again, address X) via port:v (of the NAT 482), a packet having

source address/port pair X,q (i.e., coming from port:q of the endpoint device 406) nevertheless will be accepted by the loose SYM_I NAT 482 (e.g., at its port:v) if the SYM_I NAT 482 has been loosely initialized. Being loosely initialized should be understood as meaning that a packet previously has been sent (in the context of this example) to the endpoint device 406 at another port, e.g., port:p (destination address/port pair X,p) via the SYM_I NAT 482.

The tightly initialized scenario for a tight SYM_I NAT 482 will now be described. For a packet to be accepted from the second network 419 by the tight SYM_I NAT 482, the packet's combination of destination port and source address/port pair (i.e.. the combination of source port and source address) should match the combination of source port and destination address/port pair, respectively, of a packet sent to the second network 419 via the tight SYM_I NAT 482. In terms of an example, a packet having source address/port pair X,q (i.e., coming from port:q of the endpoint device 406) will be accepted by the tight SYM_I NAT 482 (e.g., at its port:v) if the SYM_I NAT 482 has been tightly initialized. Being tightly initialized should be understood as meaning that a packet previously has been sent (in the context of this example) to the endpoint device 406 at the same port, e.g., port:q (destination address/port pair X,q) via the SYM_I NAT 482.

After initialization, the loose and tight implementations of the SYMI NAT 482 behave the same. For a packet to be accepted from the second network 419 by the SYMI NAT 482 after initialization, the packet's combination of destination port and source address (but not also source port as with the SIM_S NAT 462) should match the combination of source port and destination address, respectively, of a packet sent to the second network 419 via the SYMI NAT 482. In other words, similar to the address-sensitive NAT 422, for each port on the SYM_I NAT 482, the SYM_I NAT 482 (again, after initialization) will accept packets from different source ports so long as their source

address is the same as a packet previously sent to the second network 419 via the SYM_I NAT 482.

It is assumed for the purposes of explanation that a packet will be sent from the endpoint device 404 to each of the endpoint devices 406 (specifically at port:p) and 408 (specifically at port:q) via the SYM_I NAT 482.

For use with respect to the endpoint device 406 (address X), the SYM_I NAT 482 maps its port:v to the endpoint device 404. Similarly, for use with respect to the endpoint device 408 (address Y), the SYM_I NAT 482 maps its port:w to the endpoint device 404. The packet (not depicted) sent to port:p of the endpoint device 406 through port:v of the SYM_I NAT 482 is indicated by path 484, while the packet (not depicted) sent to port:q of the endpoint device 408 through port:w of the SYM_I NAT 482 is indicated by path 490.

Not surprisingly, a packet (not depicted) sent by the endpoint device 406 to the endpoint device 404 using the source address/port pair X,p will be accepted by the SYM_I NAT 482 (and revised and then passed along to the endpoint device 404), as indicated by the path 486. Similarly, a packet (not depicted) sent by the endpoint device 408 using the source address/port pair Y,q will be accepted by the SYM_I NAT 482 (again, after initialization), as indicated by the path 492. Moreover, packets having the following source address/port pairs will also be accepted (i.e., will not be blocked) by the SYM_I NAT 482 (again, after initialization): X,q as indicated by path 488; and Y,q as indicated by path 494.

The full cone NAT 402, the address-restricted NAT 422 and the port-restricted NAT 442 each permits a ratio of 1:N (where N can be any positive integer) between one of its own ports and source addresses or source address/port pairs, respectively, on the second network 419. The 1:N ratio is what gives rise to each of the NATs 402, 422 and 442 being described with the term "cone."

In contrast, each of the SYM_I NAT 482 and the SIM_S NAT 462 permits only a ratio of 1:1 between one of its own ports and a source address or a source address/port pair, respectively, on the second network 419. The 1:1 ratio is what gives rise to each of the NATs 482 and 462 being described with the term "symmetric."

An analogy will be provided to aid the explanation of how the various NATs operate.

The analogy is couched in terms of a doorman to a building (corresponding to the first network 418) in which endpoint device 404 is located. Each of the NATs 402, 422, 442 and 462 can act as a wall of the building. Until the NAT allocates/maps an address/port pair to the endpoint device 404, there are no doors in any of the walls of the building by which a packet from the second network 419 could gain entry or a packet from the endpoint device 404 could leave.

When the NAT allocates/maps an address/port pair to the endpoint device 404, the effect is as if the NAT creates a door in the wall that it represents. From the perspective of the second network 419, the NAT will act as a doorman relative to the doors that it has created.

The NAT (as doorman) keeps the door it created (for the endpoint device 404) closed until the endpoint device 404 sends a packet to the second network 419 via the NAT. In other words, the NAT (as doorman) will not let through packets (from the second network 419) appearing at the door (i.e., where the packet has a destination address the address/port pair allocated/mapped to the endpoint device 404) until the NAT opens the door.

When the endpoint device 404 finally does send a packet to the second network 419 via the NAT, initially the packet's indicated source address is the address on the first network 418 of the endpoint device 404. The NAT revises it so that the packet's indicated

source address information becomes the address/port pair which the NAT has allocated to the endpoint device 404, and then passes along the revised packet to the second network 419. In revising and passing along the packet, the effect is as if the NAT (as doorman) opens the door that it has created so that certain packets (depending upon the type of NAT) coming from the second network can pass through the doorway.

The full-cone NAT 402, in its role as doorman, will let through the door any packet appearing at the door (i.e., received by the NAT 402) that is intended for the endpoint device 404 (i.e., whose destination address is the address/port pair that the NAT 402 has mapped to the endpoint device 404). The NAT 402 (as doorman) is the least discriminating type of NAT about what packets it lets through its opened doors. The other NATs 422, 442 and 462 are increasingly more discriminating in their roles as doorman, respectively, checking more than just the packet's destination address/port pair.

The other NATs 422, 442, 462 and 482 treat the packets sent out from the endpoint device 404 as invitations corresponding to a guest list. In their roles as doormen, NATs 422, 442, 462 and 482 act as though they check whether packets appearing at their doors are on a guest list. As should be expected, the guest lists of the NATs 422, 442, 462 and 482 are more selective, respectively, than the full-cone NAT 402.

To be on the guest list for a door opened by the address-restricted NAT 422, a packet from the second network 419 should also have a source address (but not necessarily a source port) that matches a destination address of an invitation (packet) previously sent by the endpoint device via the NAT 422. To be on the guest list for a door opened by the port-restricted NAT 442, a packet from the second network 419 should also have a source address/source port pair that matches a destination address/port pair of a previously sent invitation packet.

Like the port-restricted NAT 442, being on a guest list maintained by the SYM_S 462 in its role as doorman requires that a packet from the second network 419 should also have a source address/source port pair that matches a destination address/port pair of an invitation (packet) previously sent by the endpoint device via the NAT 422. The port-restricted NAT 442 opens only one door for the endpoint device 404 (through which packets of varying destination address can be sent). As such, the port-restricted NAT 442 maintains only one guest list for the endpoint device 404.

In contrast, the SYM_S 462 creates/opens a door for each destination address to which the endpoint device 404 sends a packet. Accordingly, the SYM_S 462 (as doorman) maintains a separate guest list for each door it creates/opens for the endpoint device 404. So in Fig. 4D, a packet having destination port:v and source address/port pair Y,q would not be on either the guest list corresponding to door:v (port:v) or door:w (port:w). This is because the endpoint device 404 never sent a packet to source address/port pair Y,q via port:v. Rather, the packet sent to source address/port pair Y,q was sent via port:w (again, see path 470).

Like the SYM_S NAT 462, the SYM_I NAT 462 (as doorman) maintains a separate guest list for each door it creates/opens for the endpoint device 404. But unlike the SYM_S NAT 462, the SYM_I NAT 462 (as doorman) creates/opens only one door for each address on the second network 419, i.e., different ports of the same address use the same door created/opened by the SYM_I NAT 462 albeit after initialization.

So in Fig. 4E, after initialization, the packet (not depicted) of path 488 having destination port:v and source address/port pair Y,q is on the guest list corresponding to door:v (port:v). Similarly after initialization, the packet (not depicted) of path 494 having destination port:w and source address/port pair Y,p is on the guest list corresponding to door:w (port:w).

This concludes explanation of the analogy.

The NAT provides a convenient way of providing shared and transparent communication between the public internet and the computers (attached to a private network) having a non-globally-unique IP address, i.e., an IP address that is not globally-unique. However, not all forms of communications are operable over a NAT. This is a problem. Many types of applications require a globally-unique IP address as a termination point or require IP address consistency over the whole communication cycle. For example, an IP enabled phone will typically require a globally-unique IP address to receive and send voice-transmission using the IP. The presence of a NAT at the receiving end of the IP phone call may block the receiver (the endpoint device) from receiving the phone IP packets.

The presence of NATs in a network poses another type of problem as described next. There is no simple and convenient way to access a server type of device located behind a NAT from the public internet side of the NAT. For example, if a Hypertext Transfer Protocol (HTTP) webserver is located behind a NAT, then it has a private address which is invisible to the outside world through the public internet. On the contrary, a typical webserver, e.g., an HTTP server, which is not behind a NAT, is readily accessible from the public internet if it has an IP address that can be resolved using common methods like the Domain Name System (DNS).

TCP/IP allows multiple applications to run on a single computer using a variety of port numbers. When a NAT is used by a private network to share an IP address, then the port addresses are shielded behind the NAT from the outside network. This situation can be further complicated by presence of a firewall with a security policy that does not allow access to specific ports of the computers on the private network as described next.

A port-forwarding solution creates a "tunnel" through the firewall so that external users from the public internet can access a specific computer in the private network using the designated port for the tunnel. Typically, a port forwarding solution has a maximum number of about five forwarded port entries. But many applications like network-gaming, instant messaging and collaboration software may require access to previously "unopened" specific TCP/UDP ports from the external public internet. Creating all the required tunnels for such applications can be an impractical task for a typical user, since the tunnel configuration process can be complicated and confusing. Port forwarding is typically a kind of functionality provided by a router, hence it typically raises a need for a specific router that has an inbuilt port forwarding capability.

The presence of a NAT may not affect the network much if the transport connections are initiated from the clients that are behind the NAT. But if a server is located behind a NAT, then IP requests originating from the public network may not be able to access the server due to the presence of the NAT. An approach to solve this problem and its drawbacks are discussed next. In a Dynamic Domain Name System (DDNS) the users attempting to access a server located behind a NAT using a Fully Qualified Domain Name (FQDN) may face problems. Such problems result from the situation when a server or device behind a NAT is assigned a private IP address by a NAT which is invisible. A DDNS trying to route packets to an IP address due to a FQDN access request will fail since the NAT-assigned private address is invisible to the public internet side of the NAT.

Attempts have been made to define protocols for solving the NAT traversal problem described above. For example, protocols such as TURN (Traversal Using Relay NAT), STUN (Simple Traversal of UDP through NAT), SPAN-A (Simple Protocol for Augmenting NATs), etc., provide an approach that does not require routers to have the

specific functionality of supporting NAT traversal. However, these protocols do not provide a complete NAT traversal mechanism. These protocols are to be handled by an application known as SIP (Session Initiation Protocol).

Gnutella is a Peer-To-Peer (P2P) file-sharing system. The Gnutella protocol ("The Gnutella Protocol Specification v0.4 Document Revision 1.2") is widely used by Gnutella clone systems such as Kazaa, BearShare, etc. Unlike a centralized server network, the Gnutella protocol does not rely on a central server to keep track of all shared files. The Gnutella protocol uses multiple nodes known as "servents" each of which can become both a server and a client. The Gnutella protocol uses TCP protocol for a communication between the servents.

Once a servent finds an IP address of another servent which has a file the servent wants to download, it starts downloading the file through the TCP connection between the two. The Gnutella protocol can accommodate the presence of one NAT between two servents. If a servent is behind a NAT, other servents cannot initiate a TCP connection. In this case, the other servents send a "Push" descriptor to tell the server behind the NAT to initiate the TCP connection back to the other servents.

DISCLOSURE OF INVENTION

Embodiments of the invention provide methods of operating a first endpoint device (ED) facilitate the making of a peer-to-peer (P2P) connection between the first ED and a second ED despite intervening network address translators (NATs) at both ends. The P2P connection extends across a system compliant with the internet protocol (IP) whose architecture that includes a first network (having at least the first ED and a first NAT), a second network (having at least the second ED and a second NAT) and a third network. The first ED connects to the third network via the first NAT while the second ED connects to the third network via the second NAT.

One such embodiment according to the invention provides a facilitation method that includes: providing the second ED with the first IP-address/port pair; and providing the second ED with first type-information regarding the type of the first NAT.

Another such embodiment provides a facilitation method that includes: generating a session description protocol (SDP) message including an SDP attribute that describes the type of the NAT; and sending the SDP message to the second network from the first network.

Another such embodiment provides a facilitation method, for determining a port increment size (Δp) for a symmetric network address translator (NAT), that includes: requesting the symmetric NAT to map a plurality of port identification numbers (IDs); receiving information regarding the plurality of port IDs; and comparing the information to determine an increment size (Δp) of the NAT.

Another such embodiment provides a facilitation method that includes: receiving an indication of increment size (Δp) used by the second NAT to allocate/map new port numbers; and predicting, based upon the indication of increment size (Δp), at least one predicted destination port identification number ("ID") that would be used by the second NAT for the P2P connection between the first ED and a second ED.

Other embodiments provide the corresponding software and the corresponding devices that perform the methods, respectively.

Further areas of applicability of the invention will become apparent from the detailed description provided hereinafter. It should be understood that the detailed description and specific examples, while indicating the preferred embodiment of the invention, are intended for purposes of illustration only and are not intended to limit the scope of the invention.

BRIEF DESCRIPTION OF DRAWINGS

Figure 1 shows a network configuration according to an embodiment of the invention;

Figure 2 is a sequence diagram of operations according to an embodiment of the invention; and

Figure 3 is a sequence diagram of operations by which a P2P connection can be facilitated according to embodiments of the invention.

Figures 4A-4E are block diagram depictions of various types of NATs according to the Background Art.

Fig. 5A is a table showing how possible combinations of NAT-types can be organized into classes according to an embodiment of the invention.

Fig. 5B is a more detailed version of Fig. 5A that shows how Class V can be further organized into subclasses according to another embodiment of the invention.

Figs. 6A-6B, 7A-7C, 8A-8C, 9A-9C, 10A-10C, 11, 12, 13A-13B, 14A-14C, 15A-15D, 16A-16D, 17A-17C, 18A-18D and 19A-19C are hybrid block-sequence diagram that further the discussion of how to handle the classes of Fig. 5B, according to embodiments of the invention, respectively.

Figure 20 depicts a table that organizes actions, according to an embodiment of the invention, which can be taken toward establishing a P2P connection, depending upon the classes and subclasses described in Fig. 5B.

Fig. 21 is a flowchart, related to the table of Fig. 20, depicting actions relative to the classes and subclasses described in Fig. 5B that can be taken by an endpoint device, e.g., an endpoint server, according to embodiments of the invention.

Fig. 22 is a flowchart, related to the table of Fig. 20, depicting actions relative to the classes and subclasses described in Fig. 5B that can be taken by an endpoint device, e.g., a browser, according to embodiments of the invention.

BEST MODE FOR CARRYING OUT THE INVENTION

The following description of the example embodiment(s) is merely exemplary in nature and is in no way intended to limit the invention, its application, or uses.

The following acronyms are used below: UDP = User Datagram Protocol; NAT = Network Address Translation (Translator); IETF = Internet Engineering Task Force; STUN = Simple Traversal of UDP through NAT; TURN = Traversal Using Relay NAT; P2P = Peer-To-Peer (as opposed to 'server and client'); DNS = Domain Name Server; DDNS = Dynamic DNS; FQDN = Fully Qualified Domain Name; HTTP = Hyper Text Transfer Protocol; HTML = Hyper Text Markup Language; URI = Uniform Resource Indicator; URL = Uniform Resource Locator (a subset of all URIs, couched in terms of primary access technique); IP = Internet Protocol; TCP = Transmission Control Protocol; RTP = Real-time Transfer Protocol; and SDP = Session Description Protocol.

Until noted below, the following section briefly discusses some aspects of a prior patent application (U.S. Patent Application, Serial No. 10/342,304, filed January 15, 2003 and having the same inventor).

Figure 1 shows a network configuration 10 according to an embodiment of the invention of the prior patent application. Network configuration 10 includes a public IP network 12 that can be, e.g., the Internet.

Included as being attached to the public network 12 are: a packet relay server 20, a NAT-discovery server 22, e.g., a STUN (Simple Traversal UDP (User Datagram Protocol) through NATs) server, a redirect server 24, a dynamic DNS (DDNS) server 26, a DNS

(domain name system) server 28, a host computing device 16_5, a host computing device 16_6, a network address translator (NAT) 14_1 and a NAT 14_2.

The network configuration 10 further includes a private network 18_1 and a private network 18_2. Host computing devices 16_1 and 16_2 connect to the network 18_1 while host computing devices 16_3 and 16_4 connect to the network 18_2.

For the purposes of subsequent discussion, it can be helpful to think in terms of examples in which there is: an application, e.g., a web browser 30, that runs on the host 16_5; an application, e.g., an HTTP server 29, that runs on the host 16_1; an input unit 100, a processing unit 102 and an output unit 104 in the relay server 20; an application, e.g., a listener 31, that runs on the packet relay server 20; and an application, e.g., an HTTP server 80, that runs on the host 16_6.

Host 16_1 is indirectly connected to the public network 12 via the NAT 14_1 and the private IP network 18_1. In contrast, host 16_5 is directly connected to the public IP network 12.

Network configuration 10 described above including the hosts, NATs and private IP networks is a non-limiting example of how the network configuration 10 can be implemented in an embodiment of the invention of the prior patent application. As a practical matter, the presence of NAT 14_1 will not allow a typical client, e.g., the browser 30, to directly access the HTTP server 29 on host 16_1, since the browser 30 is most unlikely to have the port number of host 16_1 that was assigned by the NAT 14_1. This problem is known as the NAT traversal problem. To perform a NAT traversal, network configuration 10 according to an embodiment of the invention of the prior patent application includes additional elements as described next.

After booting up, the HTTP server 29 running on the host 16_1 performs a NAT-discovery process, e.g., a STUN test, resulting in an indication that the NAT 14_1 is present in the connection between the host 16_1 and the STUN server 22.

After positively determining the presence of a NAT, the host 16_1 connects to the packet relay server 20, which is operable to receive and forward IP packets. Host 16_1 initiates a TCP (Transmission Control Protocol) session and sends a packet relay initiation request to the input unit 100 of the relay server 20. In response, the processing unit 102 of the relay server 20 can run a TCP application known as a listener 31.

The output unit 104 of the relay server 20 returns to the host 16_1 a global IP address (namely, the IP address of the packet relay server 20) and a port on which it (namely, the packet relay server 20 running the listener 31) will receive and send packets on behalf of the host 16_1.

Hosts connected to the public IP network 12 such as the Internet can send packets to the IP address and port number designated by the relay server 20 as the listener 31. The listener 31 in turn forwards such packets to the host 16_1. Similarly, the host 16_1 can send packets to the relay server 20, and the relay server 20 can rewrap the payloads and transmit them to the specific forwarding IP address given in the packets.

After obtaining the set of global IP address and port number from the relay server 20, the host 16_1 via the NAT 14_1 provides the redirect server 24 with the IP address and port number of the listener 31. Then the redirect server 24 can redirect HTTP requests from the public IP network 12 seeking the HTTP server 29 to the global IP address and port number of the listener 31 on the relay server 20.

The HTTP server 29 on host 16_1 is assigned a FQDN, which is statically associated with a global IP address on the redirect server 24. The redirect server 24 adaptively maps the FQDN to the dynamic IP address and port number of the listener 31. Hence, when a

user (not depicted) makes a request via the browser 30 to access the FQDN, the request from the browser 30 will first be received by the redirect server 24. The redirect server 24 can use multiple methods to redirect the HTTP request to the listener 31 on the relay server 20, e.g., by providing a "splash page" (not depicted) to the browser 30 that can include a hyperlink to the listener 34 or by automatically redirecting the HTTP request to the listener 34 using the "307 Temporary Redirect" feature of the HTTP 1.1 protocol or by using a combination of a splash page with an automatic JAVA-script-based redirect method.

Figure 2 is a sequence diagram of operations according to an embodiment of the invention of the prior patent application. Figure 2 does not strictly conform to the conventions of UML-type sequence diagrams. After booting-up, the HTTP server 29 running on the host 16_1 sends a message 70 initiating a NAT-discovery process, e.g., a STUN test. The message 70 is sent to the NAT-discovery server, e.g., STUN server 22, via the NAT 14_1. The intervening role of the NAT 14_1 is indicated by the dot 72 at the intersection of the message 70 and the lifeline 74 of the NAT 14_1. Such a dot convention will be used for other messages passing via the NAT 14_1. The NAT-discovery server 22 sends a return message 76 to indicate the presence of the NAT 14_1 to the host 16_1.

Host 16_1 sends a message 32 to the packet relay server 20 requesting it to open a listener 31. The packet relay server 20 sends back a message 34 to the host 16_1 indicating the global IP address (of the packet relay server 20) and the port number (on the packet relay server 20) assigned to the listener 31. The host 16_1 then updates the redirect server 24 by a message 36 to register the global IP address and port number of the listener 31 on the relay server 20. The redirect server 24 will authenticate the message 36 and update its database to associate the IP address and port number of the listener 31 with the FQDN of the HTTP server 29. After the above initiation process is over, the user can access the, e.g., of the browser 30 on the host 16_5, HTTP server 29 running on the host 16_1.

Harkening back to the example, it is to be noted that the browser 30 on the host 16_5 is representative of any computer or IP-enabled device connected to the public IP network 12 (shown in Fig. 1). When the user of the browser 30 types in the URL (Universal Resource Locator), e.g., FQDN, of the HTTP server 29, the browser 31 on the host 16_5 sends a message 38 to the DNS server 28 with the FQDN in order to obtain the DNS entry of the entered URL. The DNS server 28 sends back a message 40 to the host 16_5 with the IP address of the redirect server 24. It may be necessary for the DNS server 28 to communicate (not shown as a message in Fig. 2) with the DDNS server 26 in order to collectively provide the IP address of the redirect server 24 to the browser 30.

The typical browser 30 on the host 16_5 can then initiate an HTTP request to the IP address of the redirect server 24 on the default port 80 (for HTTP protocol communications) via a message 42. The redirect server 24 in turn checks its database to find a set of IP address and port number of the listener 31 on the relay server 20 that correspond to the requested URL or URI (Universal Resource Indicator).

Host 16_5 (as part of hosting the browser 30) then sends an HTTP request to the relay server 20 as indicated by the message 46 based on the redirection IP address and port number received from the redirect server 24. The relay server 20 in turn sends a message 48 to the host 16_1 with which it has maintained a live TCP session.

On the return side, the host 16_1 (as part of hosting the HTTP server 29) will send a response to the packet relay server 20 as message 50. Further, the relay server 20 transmits the response to the browser 30 on the host 16_5. Thus, an HTTP session is established where the browser 30 on the host 16_5 can access the HTTP server 29 on the host 16_1 even though the host 16_1 is located behind the NAT 14_1, i.e., even though the NAT 14_1 is located between the browser 30 and the HTTP server 29.

Such NAT traversal is achieved above without the browser 30 on the host 16_5 having knowledge of the private IP address of the HTTP server 29 shielded by the NAT 14_1. No manual step or configuration is required at the host 16_5, i.e., on the user side of the HTTP access operation.

The preceding section, as noted above, briefly discusses some aspects of the prior patent application.

An embodiment of the invention, in part, represents the recognition of the following: SIP (again, Session Initiation Protocol) does not provide a way to establish a P2P connection through NATs at both ends where one of the following NAT combinations is present: A symmetric NAT and an address-restricted NAT; a symmetric NAT and port-restricted NAT; and a symmetric NAT and a symmetric NAT. Also, the "Push" scheme of the Gnutella protocol does not work in the circumstance that each of the endpoints has one or more NATs.

An embodiment of the invention is, in part, the recognition of the following. Based upon the NAT traversal mechanism described above, a client (e.g., an HTTP browser) can reach an endpoint device (e.g., an HTTP server) regardless of whether or not both the server and client are behind NATs. However, all the traffic would have to go through the packet relay server. In the circumstance of the packet content being data, e.g., multimedia data, that consumes large bandwidth, e.g., where the server is an IP video camera, the traffic load on packet relay server can be significant.

An embodiment of the invention provides multiple relay servers as a solution to the recognized problem, namely large bandwidth data overly loading a packet relay server being used for NAT traversal. A concern can be, from a business point of view, that providing multiple relay servers could potentially be prohibitively expensive.

Another embodiment of the invention solves the recognized problem mentioned above (again, large bandwidth data overly loading a packet relay server being used for NAT traversal) by changing the way that the data is exchanged after the packet-relay-server-based connection has been established, e.g., by providing a method that facilitates the making of a peer-to-peer (P2P) connection (e.g., using the STUN protocol) between two endpoint devices (e.g., an HTTP server and would-be client of the server) through one or more NATs interposed between the two.

Different types of NATs exhibit different circumstances under which incoming UDP packets (from a first, e.g., public, network that are to be forwarded via the NAT into a second, e.g., private, network) will be accepted by the NAT. By accounting for such differences, embodiments of the invention can establish P2P connections through NATs even though NATs are at both ends of the connection. A NAT-discovery process, e.g., such as provided by the STUN protocol, can be used not only to detect the presence of a NAT, but also to analyze the type of NAT. Knowledge of the NATs at one or both ends will determine what the two endpoint devices, e.g., the server and the client, should do to establish the P2P connection.

Fig. 5A is a table showing possible combinations of NAT-types (including the absence, or no, NAT) interposed as part of a connection between two endpoint devices. Fig. 5A also shows how such combinations can be organized into classes according to an embodiment of the invention. In particular, the rows represent possible types of NAT adjacent to a first endpoint device, e.g., an HTTP server, while the columns represent possible types of NAT adjacent to a second endpoint device, e.g., an HTTP client such as a browser.

Fig. 5B is a more detailed version of Fig. 5A that shows how Class V can be further organized into subclasses V1, V2 and V3 according to another embodiment of the invention.

Each of the classes of Fig. 5B will now be discussed in view of Figs. 6A- 19C. To further the explanation, each of Figs. 6A-17C assumes the following. The first endpoint device 629 is an HTTP server (hereafter "endpoint server"), e.g., an IP video camera, and that the second endpoint device 630 is a host/PC running an HTTP client such as a browser. In this regard, the HTTP server corresponds to the server 29 of Fig. 2 and the HTTP browser corresponds to the browser 630 of Fig.2. Further, it is assumed that a packet-relay-server-based connection exists between the first endpoint device 629 and the second endpoint device 630 via a relay server (not depicted) (hereafter "implied relay server"), e.g., taking the form of a TURN server. The relay sever can correspond to the relay sever 20 of Fig. 2. Also, a NAT-discovery server 622, e.g., taking the form of a STUN server, is assumed to be present. The NAT-discovery server 622 can correspond to the NAT-discover server 22 of Fig. 2. It is noted that the first endpoint device, the second endpoint device, the relay server and the NAT-discovery server 622 can take other forms.

Class I will now be discussed in terms of Figs. 6A-6B.

Conditions Of Class 1:

endpoint server side	Any Type Of NAT.
browser side	No NAT. (Open to the Internet)

To further the context of the explanation, Figs. 6A-6B assume that the endpoint server 629 connects via a NAT 602 (of any of the types discussed above) to an IP network

606 including the NAT-discovery server 622, the implied relay server and the browser 630. The browser is not associated with a NAT. In Fig. 6A, the endpoint server 629 receives (via the implied relay server and the NAT 602) information from the browser 630 as to the local address/port pair of the browser 630, as indicated by path 604. In Fig. 6B, the endpoint server 629 sends a stream of packets (e.g., a video stream where the endpoint server 629 is an IP video camera) over a UDP type of P2P connection to the browser 630, as indicated by path 605.

Class II will now be discussed in terms of Figs. 7A-7C.

Conditions of Class II:

endpoint server side	Any Type Of NAT (except a symmetric NAT in the case where the browser side has a port-restricted NAT).
browser side	Full / Address-Restricted / Port-restricted cone NAT

To further the context of the explanation, Figs. 7A-7C assume that: the endpoint server 629 connects to an IP network 706 (that includes the implied relay server and the NAT-discovery server 622) via a NAT 702; and the browser 630 connects to the network 706 via a NAT 704. The NAT 704 can be any of the following types: full cone; address-restricted; or port-restricted. The NAT 702 can be any type of NAT except a symmetric NAT in the case where the NAT 704 is a port-restricted NAT.

In Fig. 7A, the endpoint server 629 communicates with the NAT-discovery server 622 (via the NAT 702) to determine the address/port pair mapped by the NAT 702 to the endpoint server 629 and what type the NAT 702 is, as indicated by path 707A. Similarly,

the browser 630 communicates with the NAT-discovery server 622 (via the NAT 704) to determine the address/port pair mapped by the NAT 704 to the browser 630 and what type the NAT 704 is, as indicated by path 707B. Information as to the type of NAT and how an endpoint device determines that information will be discussed below.

An endpoint device, such as the endpoint server 629 or the browser 630, can determine the type of the NAT through which it communicates using a NAT type-discovery process, for example the STUN discovery process disclosed in the document entitled "STUN - Simple Traversal of UDP Through Network Address Translators," J. Rosenberg et al., Internet Engineering Task Force, draft-ietf-midcom-stun-02.txt, dated August 22, 2002 (expires February 2003) (the entirety of which is hereby incorporated by reference), see, e.g., section 10.1 and Fig. 2.

The endpoint server 629 receives from the browser 630 (via the NAT 704, the implied relay server and the NAT 702) information regarding the address/port pair mapped by the NAT 704 to the browser 630 and what type the NAT 704 is, as indicated by path 708. Similarly, the browser 630 receives from the endpoint server 629 (via the NAT 702, the implied relay server and the NAT 704) information regarding the address/port pair mapped by the NAT 702 to the endpoint server 629 and what type the NAT 702 is, as indicated by path 710.

Fig. 7B assumes the circumstance that the NAT 704 is either a full-cone NAT, an address-restricted NAT or a port-restricted NAT. So in Fig. 7B, the browser 630 sends a break-out packet ("BOP") to the endpoint server 629, as indicated by path 712. The BOP might or might not be blocked by the NAT 702 depending upon what type of NAT it is. The purpose of the BOP of path 712 is not thwarted if it is blocked by the NAT 702. Rather, a purpose of sending the BOP of path 712 is to open the door in the NAT 704 to packets from the endpoint server 629 sent via the NAT 702.

In Fig. 7C, the endpoint server 629 sends a stream of packets (e.g., a video stream where the endpoint server 629 is an IP video camera) over a UDP type of P2P connection to the browser 630, as indicated by path 714. Because the door at the NAT 704 was previously opened via the BOP of path 712, the NAT 704 accepts the stream of packets of path 714.

Class III will now be discussed in terms of Figs. 8A-8C.

Condition of Class III:

endpoint server side	No NAT. (Open to the Internet)
browser side	Symmetric NAT

To further the context of the explanation, Figs. 8A-8C assume that: the endpoint server 629 is part of a network 806 (that includes the implied relay server) and is not associated with a NAT; and the browser 630 connects to the network 806 via a symmetric NAT 804.

In Fig. 8A, the browser 630 communicates with the NAT-discovery server 622 (via the NAT 804) to determine the address/port pair mapped by the NAT 804 to the browser 630 and what type the NAT 804 is, as indicated by path 807. The endpoint server 629 receives from the browser 630 (via the NAT 804) information regarding the address/port pair mapped by the NAT 804 to the browser 630 and what type the NAT 804 is, as indicated by path 808.

In Fig. 8B, the browser 630 sends a break-out packet ("BOP") to the endpoint server 629, as indicated by path 812. A purpose of the BOP of path 812 is to open the door in the NAT 804 to packets from the endpoint server 629. Here, another purpose is that the

endpoint server 629 records (as indicated by item 813) the address/source pair mapped by the NAT 804 to the browser 630.

In Fig. 8C, the endpoint server 629 sends a stream of packets (e.g., a video stream where the endpoint server 629 is an IP video camera) over a UDP type of P2P connection to the browser 630, as indicated by path 814. Because the door at the NAT 804 was previously opened via the BOP of path 812, the NAT 804 accepts the stream of packets of path 814.

Class IV will now be discussed in terms of Figs. 9A-9C.

Conditions of Class IV:

endpoint server side	Full / Address-restricted cone NAT
browser side	Symmetric NAT

To further the context of the explanation, Figs. 9A-9C assume that: the endpoint server 629 connects to an IP network 906 (that includes the implied relay server and the NAT-discovery server 622) via a NAT 902; and the browser 630 connects to the network 906 via a symmetric NAT 904. The NAT 902 can be a full cone type or address-restricted cone type of NAT.

In Fig. 9A, the endpoint server 629 communicates with the NAT-discovery server 622 (via the NAT 902) to determine the address/port pair mapped by the NAT 902 to the endpoint server 629 and what type the NAT 902 is, as indicated by path 907A. Similarly, the browser 630 communicates with the NAT-discovery server 622 (via the NAT 904) to determine the address/port pair mapped by the NAT 904 to the browser 630 and what type the NAT 904 is, as indicated by path 907B.

A path 910 indicates that: the endpoint server 629 receives from the browser 630 (via the NAT 904, the implied relay server and the NAT 902) information regarding the address/port pair mapped by the NAT 904 to the browser 630 and what type the NAT 904 is; and the browser 630 receives from the endpoint server 629 (via the NAT 902, the implied relay server and the NAT 904) information regarding the address/port pair mapped by the NAT 902 to the endpoint server 629 and what type the NAT 902 is.

In the circumstance that the NAT 902 is an address-restricted NAT, the endpoint server 629 sends a BOP via the NAT 902 to the browser 630, as indicated by path 908. A purpose of the BOP of path 908 is to open a door in the NAT 902 to packets from the browser 630 that will come directly to the NAT 902 from the NAT 904 rather via the implied relay server.

In Fig. 9B, the browser 630 sends a BOP to the endpoint server 629, as indicated by path 912. A purpose of the BOP of path 912 is to open a door in the NAT 904 to packets from the endpoint server 629 that will come directly to the NAT 904 from the NAT 902 rather via the implied relay server. Here, because it is symmetric, the NAT 904 will allocate/map a separate port (door) for use with the address/pair mapped to the endpoint server 629 by the NAT 902. As such, another purpose of the BOP of path 912 is that the endpoint server 629 records (as indicated by item 913) the address/source pair mapped by the NAT 904 to the browser 630.

In Fig. 9C, the endpoint server 629 sends a stream of packets (e.g., a video stream where the endpoint server 629 is an IP video camera) over a UDP type of P2P connection to the browser 630, as indicated by path 914. Because the door at the NAT 904 was previously opened via the BOP of path 912, the NAT 904 accepts the stream of packets of path 914.

Class V has three subsets of conditions to which Figs. 10A-12 correspond.

The second subset (of the three) will be discussed first in terms of Figs. 10A-10C. The second (of three) subsets of conditions of Class V, referred to as subclass V_2, is:

endpoint server side	Port restricted-cone NAT
browser side	Symmetric NAT

To further the context of the explanation, Figs. 10A-10C assume that: the endpoint server 629 connects to an IP network 1006 (that includes the implied relay server and the NAT-discovery server 622) via a NAT 1002 that is of the port-restricted cone type; and the browser 630 connects to the network 1006 via a symmetric NAT 1004.

In Fig. 10A, the endpoint server 629 communicates with the NAT-discovery server 622 (via the NAT 1002) to determine the address/port pair mapped by the NAT 1002 to the endpoint server 629 and what type the NAT 1002 is, as indicated by path 1007A. Similarly, the browser 630 communicates with the NAT-discovery server 622 (via the NAT 1004) to determine the address/port pair mapped by the NAT 1004 to the browser 630 and what type the NAT 1004 is, as indicated by path 1007B.

A path 1010 indicates that: the endpoint server 629 receives from the browser 630 (via the NAT 1004, the implied relay server and the NAT 1002) information regarding the address/port pair mapped by the NAT 1004 to the browser 630 and what type the NAT 1004 is; and the browser 630 receives from the endpoint server 629 (via the NAT 1002, the implied relay server and the NAT 1004) information regarding the address/port pair mapped by the NAT 1002 to the endpoint server 629 and what type the NAT 1002 is. For simplicity, it is assumed that port:a was mapped by the NAT 1004 to the browser 630. The symmetric nature of the NAT 1004 should be kept in mind, i.e., only packets having as a

source address the address/port pair of the NAT-discovery server 622 will be accepted at port:a by the symmetric NAT 1004.

In Fig. 10B, the browser 630 sends a break-out packet ("BOP") to the endpoint server 629 that goes from the NAT 1004 to the NAT 1002 without going via the implied relay server, as indicated by path 1012. A purpose of the BOP of path 1012 is to open a door in the symmetric NAT 1004 to packets from the endpoint server 629 that will come directly to the symmetric NAT 1004 from the NAT 1002 rather than by way of the implied relay server. Here, because it is symmetric, the NAT 1004 will allocate/map a separate port (door), e.g., port:b, for use with the address/pair mapped to the endpoint server 629 by the NAT 1002.

The port-restricted NAT 1002 blocks the packet of path 1012 because a packet has not yet been sent via the NAT 1002 from the endpoint server 629 to port:b of the symmetric NAT 1004 (which is the port allocated to the browser 630 by the NAT 1004 for use with the endpoint server 629). Because the NAT 1002 is of the port-restricted type, the packet previously sent via the NAT 1002 from the endpoint server 629 to port:a of the NAT 1004 (which is a port allocated to the browser 630 by the symmetric NAT 1004, albeit for use with the address/port pair of the implied relay server) will not open the door to a packet from the browser 630 sent via port:b of the symmetric NAT 1004.

Because the packet of path 1012 was blocked by the NAT 1002, the endpoint server 629 was not able to examine the packet and so is not able to determine what port has been assigned by the symmetric NAT 1004 to the browser 630 for packets from the endpoint server 629 that will come directly to the symmetric NAT 1004 from the NAT 1002 rather than by way of the implied relay server. In Fig. 10C, the attempt by the endpoint server 629 to send a BOP to the browser 630 fails, as indicated by path 1016 not

reaching the symmetric NAT 104, because the endpoint server 629 does not know that it is port:b which the endpoint server 629 should be using.

Until the endpoint server 629 can successfully send BOP corresponding to path 1016, endpoint server 629 will not be able to send a stream of packets (e.g., a video stream where the endpoint server 629 is an IP video camera) over a UDP type of P2P connection to the browser 630. A technique to overcome this problem is discussed below.

Again, class V has three subsets of conditions. The first subset (of the three) will now be discussed in terms of Fig. 11.

The first (of three) subsets of conditions of Class V, referred to as subclass V_1, is:

endpoint server side	Symmetric NAT
browser side	Port restricted-cone NAT

To further the context of the explanation, Fig. 11 assumes that: the endpoint server 629 connects to an IP network 1106 (that includes the implied relay server and the NAT-discovery server 622) via a symmetric NAT 1102; and the browser 630 connects to the network 1106 via a NAT 1104 that is of the port-restricted cone type.

In Fig. 11, the endpoint server 629 communicates with the NAT-discovery server 622 (via the NAT 1102) to determine the address/port pair mapped by the NAT 1102 to the endpoint server 629 and what type the NAT 1102 is, as indicated by path 1107A. Similarly, the browser 630 communicates with the NAT-discovery server 622 (via the NAT 1104) to determine the address/port pair mapped by the NAT 1104 to the browser 630 and what type the NAT 1104 is, as indicated by path 1107B.

Similar to path 1010 of Fig. 10A (though a corresponding path is not depicted in Fig. 11 for brevity), the following occurs: the endpoint server 629 receives from the browser 630 (via the NAT 1104, the implied relay server and the NAT 1102) information regarding the address/port pair mapped by the NAT 1104 to the browser 630 and what type the NAT 1104 is; and the browser 630 receives from the endpoint server 629 (via the NAT 1102, the implied relay server and the NAT 1104) information regarding the address/port pair mapped by the NAT 1102 to the endpoint server 629 and what type the NAT 1102 is.

For simplicity, it is assumed that port:a was mapped by the NAT 1102 to the endpoint server 629 for use with the NAT-discovery server 622. The symmetric nature of the NAT 1104 should be kept in mind, i.e., only packets having as a source address the address/port pair of the NAT-discovery server 622 will be accepted at port:a by the symmetric NAT 1102.

In Fig. 11, the browser 630 would like to send a BOP to the endpoint server 629, as indicated by path 1112. A purpose of the BOP of path 1112 would be to open the door in the port-restricted NAT 1104 to packets from the endpoint server 629 that will come directly to the port-restricted NAT 1104 from the NAT 1102 rather than by way of the implied relay server. But the browser 630 knows that the NAT 1102 is a symmetric NAT which will assign a port other than port:a for use with packets from it (the browser 630) that will come directly to the symmetric NAT 1102 from the NAT 1104 rather than by way of the implied relay server. Unfortunately, the browser 630 only knows of port:a, at which only packets from the address/port pair of the NAT-discovery server 622 are accepted by the symmetric NAT 1102. Thus, the browser 630 is prevented from actually sending the BOP of path 1112.

In Fig. 11, the attempt by the browser 630 to send a BOP to the endpoint server 629 fails, as indicated by path 1112 not reaching the symmetric NAT 104, because the endpoint

server 629 does not know that it is port:b to which it (the endpoint server 629) should be sending.

Until the browser 630 can successfully send BOP corresponding to path 1112, the endpoint server 629 will not be able to send a stream of packets (e.g., a video stream where the endpoint server 629 is an IP video camera) over a UDP type of P2P connection to the browser 630 because the door/port on the NAT 1104 will not be open to packets coming from the endpoint sever 629 by way of port:b of the NAT 102. A technique to overcome this problem is discussed below.

Yet again, class V has three subsets of conditions. The third subset (of the three) will now be discussed in terms of Figs. 12.

The third (of three) subset of conditions of Class V, referred to as subclass V_3, is:

endpoint server side	Symmetric NAT
browser side	Symmetric NAT

To further the context of the explanation, Fig. 12 assumes that: the endpoint server 629 connects to an IP network 1206 (that includes the implied relay server and the NAT-discovery server 622) via a symmetric NAT 1202; and the browser 630 connects to the network 1206 via a symmetric NAT 1204.

In Fig. 12, the endpoint server 629 communicates with the NAT-discovery server 622 (via the NAT 1202) to determine the address/port pair mapped by the NAT 1202 to the endpoint server 629 and what type the NAT 1202 is, as indicated by path 1207A. Similarly, the browser 630 communicates with the NAT-discovery server 622 (via the

NAT 1204) to determine the address/port pair mapped by the NAT 1204 to the browser 630 and what type the NAT 1204 is, as indicated by path 1207B.

Similar to path 1010 of Fig. 10A (though a corresponding path is not depicted in Fig. 12 for brevity), the following occurs: the endpoint server 629 receives from the browser 630 (via the NAT 1204, the implied relay server and the NAT 1202) information regarding the address/port pair mapped by the NAT 1204 to the browser 630 and what type the NAT 1204 is; and the browser 630 receives from the endpoint server 629 (via the NAT 1202, the implied relay server and the NAT 1204) information regarding the address/port pair mapped by the NAT 1202 to the endpoint server 629 and what type the NAT 1202 is.

For simplicity, it is assumed that port:a was mapped by the NAT 1202 to the endpoint server 629 for use with the implied relay server and, similarly, port:a was mapped by the NAT 1204 to the browser 630 for use with the implied relay server. The symmetric nature of the NATs 1202 and 1204 should be kept in mind, i.e., only packets having as a source address the address/port pair of the NAT-discovery server 622 will be accepted at port:a by each of the symmetric NATs 1202 and 1204.

Similar to what is described above relative to path 1112 of Fig. 11, the attempt by the browser 630 to send a BOP to the endpoint server 629 fails, as indicated by path 1212. The circumstance of path 1212 is sufficient to prevent the endpoint server 629 from sending a stream of packets (e.g., a video stream where the endpoint server 629 is an IP video camera) over a UDP type of P2P connection to the browser 630. There is a further problem of subclass V_3 to be overcome.

In Fig. 12, the endpoint server 629 would also like to send a send a stream of packets (e.g., again, a video stream where the endpoint server 629 is an IP video camera) over a UDP type of P2P connection to the browser 630. But the endpoint server 629 knows that the NAT 11204 is a symmetric NAT which will assign a port other than port:a

for use with packets from it (the endpoint server 629) that will come directly to the symmetric NAT 1202 from the NAT 1204 (such as with the P2P connection) rather than by way of the implied relay server. Unfortunately, the endpoint server 629 only knows of port:a, at which only packets from the address/port pair of the NAT-discovery server 622 are accepted by the symmetric NAT 1204.

In Fig. 12, the attempt by the endpoint server 629 to make the P2P connection to the browser 630 fails, as indicated by path 1216 not reaching the symmetric NAT 104, because the endpoint server 629 does not know that it is port:b to which it (the endpoint server 629) should be sending.

Until the endpoint server 629 can determine the port on the NAT 1204 that it (the endpoint server 629) should use to make a P2P connection, the endpoint server 629 will be prevented from making the P2P connection. A technique to overcome this problem is discussed below.

In the context of a first endpoint device, its associated NAT (the "first NAT"), a counterpart endpoint device and its counterpart NAT (that happens to be a symmetric NAT), an embodiment of the invention, in part, is a recognition of the following: the otherwise unknown particular identification number ("ID") of a port which will be assigned/mapped/bound to the counterpart endpoint device by the counterpart symmetric NAT (see the problems of subclasses V_1, V_2 and V_3 discussed above) can be predicted; and, accordingly, BOPs can be sent to predicted port IDs of the counterpart symmetric NAT by the first endpoint device via the first NAT in order to open doors in the first NAT in anticipation of receiving packets sourced through the predicted port IDs of the counterpart NAT.

An embodiment of the invention, in part, is the recognition that symmetric NATs assign/map ports, i.e., bind a particular port ID to an IP address or address/port pair, using a substantially constant increment size (Δp).

An embodiment of the invention provides a method to determine the substantially constant increment size (Δp) of a port-sensitive symmetric NAT, e.g., SIM_S NAT 462 of Background Art Fig. 4D. Such a method will be explained in terms of Fig. 13A. It is noted that such a method can be applied to a negative increment size, i.e., a decrement size.

In Fig. 13A, an endpoint device 1302, e.g., such as the endpoint device 629 or the browser 630, connects to a network 1304 via a SIM_S NAT 1306. The endpoint device 1302 will determine the increment size (Δp) by discovering the port IDs which the SIM_S NAT 1306 allocates/maps (or binds) to various destination address/port pairs to which the endpoint device 1302 attempts to send test packets; and then calculating the differences between successive ones of the port IDs. If a consistent value among the differences emerges, then this number can be treated as the increment size (Δp). The endpoint device 1302 can discover the port IDs by performing a NAT-discovery process, as e.g., a STUN test, in conjunction with a NAT discover server such as the NAT-discovery server 622.

The endpoint device 1302 sends packets via the SIM_S NAT 1306 to destinations in the network 1304 having the address/port pairs X,p (as indicated by arrow 1308), X,q (as indicated by arrow 1310), Y,p (as indicated by arrow 1312) and Y,q (as indicated by arrow 1314). To simplify the explanation, example port IDs will be assumed for the ports of the SIM_S NAT 1306 allocated/mapped/bound to the destinations of 1308 -1314, namely: port 49152 for destination X,p (path 1308); port 49153 for destination X,q (path 1310); port 49154 for destination Y,p (path 1312); and port 49155 for destination Y,q (path 1314). Here, the differences between successive ones of the port IDs are always one, hence $\Delta p=1$. In actuality, Δp can be 1, or 2 or a greater integer.

Also, it is noted that the destination X,p of path 1308 and the destination X,q of path 1310 differ only in port number, which is also true of destinations Y,p (path 1312) and Y,q (path 1314). Because associated port IDs (namely 49152 & 49153 and 49154 & 49155, respectively) are different, the endpoint device will recognize the symmetric NAT 1302 as a SIM_S type of NAT. This knowledge is useful because, where a counterpart NAT is the SIM_S-type, there is little benefit (in effect) to the endpoint device 1302 sending more than one prediction-based BOP, as will be discussed in more detail below.

Another embodiment of the invention provides a method to determine the substantially constant increment size (Δp) of a port-insensitive symmetric NAT, e.g., SYM_I NAT 482 of Background Art Fig. 4E. Such a method will be explained in terms of Fig. 13B.

Fig. 13B is similar to Fig. 13A except that the SIM_S NAT 1326 has been replaced with a SYM_I NAT 1326. The endpoint device 1302 will determine the increment size (Δp) as before by discovering and analyzing the port IDs which the SYM_I NAT 1326 allocates/maps (or binds) to various destination address/port pairs to which the endpoint device attempts to send test packets.

The endpoint device 1302 again sends packets via the SIM_S NAT 1326 to destinations in the network 1304 having the address/port pairs X,p (as indicated by arrow 1328), X,q (as indicated by arrow 1330), Y,p (as indicated by arrow 1332) and Y,q (as indicated by arrow 1334). To simplify the explanation, again example port IDs will be assumed for the ports of the SYM_I NAT 1326 allocated/mapped/bound to the destinations of 1328 -1334, namely: port 49152 for destinations X,p (path 1328) and X,q (path 1330); and port 49153 for destinations Y,p (path 1332) and Y,q (path 1334).

For the SIM_S NAT 1326, there is no difference in port ID for different ports at the same destination address, namely X,p (path 1328) and X,q (path 1330) have port 49152,;

and Y,p (path 1332) and Y,q (path 1334) have the same port 49153. But port 49152 for destinations having address X (paths 1328 and 1330) differs by one from port 49153 for destinations having address Y (paths 1332 and 1334). As such, the endpoint device 1302 will determine that $\Delta p=1$. In actuality, Δp can be 1, or 2 or a greater integer. Also, the endpoint device 1302 will recognize the symmetric NAT 1326 as a SYM_I type of NAT. This knowledge is useful because, where a counterpart NAT is the SYM_I-type, there can be significant benefit to the endpoint device 1302 sending more than one prediction-based break-out packet ("BOP"), as will be discussed in more detail below.

When the endpoint device 1302 receives information indicating that a NAT (not depicted) associated with another endpoint device (not depicted) (hereafter the "counterpart NAT" associated with the "counterpart endpoint device") is a SIM_S or SYM_I type of NAT, the endpoint device 1302 will also be provided with the estimate of the counterpart NAT's Δp. The endpoint device 1302 predicts port numbers at the counterpart symmetric NAT, in succession, by adding Δp to the port ID mapped by the counterpart symmetric NAT to the counterpart endpoint device.

There will be a time lag between when the counterpart NAT allocates/maps/binds a port number (the "previous" port number) to the counterpart endpoint device for use with the NAT-discovery server 622 and when the counterpart NAT allocates/maps/binds a port number to the counterpart endpoint device for use with the endpoint device 1302. During the time lag, the counterpart NAT might allocate/map/bind one or more successive port IDs to one or more applications other than the counterpart endpoint device might create another binding on the same Symmetric NAT.

This creates a problem that the next port number to be assigned by the counterpart NAT for use relative to the endpoint device 1302 might not be +1 to the previous port number, but instead +2 or greater. To minimize the effect of this problem, the counterpart

endpoint device can be configured to minimize a delay between when it receives information about the NAT (the "home NAT") associated with the endpoint device 1302 and when a port ID on the counterpart NAT is allocated/mapped/bound for use with the endpoint device 1302 exclusive of a relay server.

The port ID assigned by a NAT typically lies within a predetermined port range, e.g., 0xC000 to 0xCFFF (hexadecimal notation). Occasionally, as a symmetric NAT assigns subsequent port IDs, the symmetric NAT will reach the upper boundary 0xCFFF. Because port IDs can be recycled, then the symmetric NAT will recycle to the beginning of the address range (0xC000) in order to obtain available port IDs. But the difference between a port ID at the end of the range and a port ID at the beginning of the range is enormous. In this situation, the NAT will treat the difference as an anomaly and will repeat the Δp determination process.

If the port ID at the counterpart NAT that is mapped/bound to the counterpart endpoint device is not what the endpoint device 1302 predicted, the result is that the endpoint device 1302 will send a prediction-based packet either (i) to an unbound port ID of the counterpart NAT, or (ii) to a port ID mapped/bound to an application other than the counterpart endpoint device or (iii) to a port mapped/bound to the counterpart endpoint device albeit for use relative to a different port ID of the home NAT. In case (i), the sent packet will be discarded by the counterpart NAT because there is no such port ID has been mapped/bound. In case (ii) and (iii), where the counterpart NAT is of the symmetric type (which does not receive an incoming packet from an unknown IP address and/or port number), the prediction-based packet will be discarded by the counterpart NAT and should have no affect on the counterpart endpoint device or the other applications.

Next, prediction-based P2P connection facilitation will be discussed for subclass V_1 in terms of Figs. 14A-14C.

To further the context of the explanation, Fig. 14A assumes that: the endpoint server 629 connects to an IP network 1406 (that includes the implied relay server and the NAT-discovery server 622) via a symmetric NAT 1402; and the browser 630 connects to the network 1406 via a NAT 1404 that is of the port-restricted cone type. It should be observed that Fig. 14A is similar to Fig. 11. Here, also to further the explanation, example port IDs and a value for Δp are assumed which should not be viewed as limiting the scope of this disclosure.

In Fig. 14A, the endpoint server 629 communicates with the NAT-discovery server 622 (via the NAT 1402) to determine the address/port pair (for example, the port ID is 49152) mapped by the NAT 1402 to the endpoint server 629, what type the NAT 1402 is and the increment size, Δp (here, Δp=+1), as indicated by path 1407A. Similarly, the browser 630 communicates with the NAT-discovery server 622 (via the NAT 1404) to determine the address/port pair (here, the port ID is 60004) mapped by the NAT 1404 to the browser 630 and what type the NAT 1404 is, as indicated by path 1407B.

The endpoint server 629 receives from the browser 630 (via the NAT 1404, the implied relay server and the NAT 1402) information regarding the address/port pair mapped by the NAT 1404 to the browser 630 and what type the NAT 1404 is, as indicated by path 1408. The browser 630 receives from the endpoint server 629 (via the NAT 1402, the implied relay server and the NAT 1404) information regarding the address/port pair mapped by the NAT 1402 to the endpoint server 629 and what type the NAT 1402 is (including Δp), as depicted by path 1410.

In Fig. 14B, the browser 630 would like to send one or more break-out packets ("BOPs") to the endpoint server 629. A purpose of the BOP of path 1412 would be to

open the door in the port-restricted NAT 1404 to packets from the endpoint server 629 that will come directly to the port-restricted NAT 1404 from the NAT 1402 rather than by way of the implied relay server. But the endpoint server 629 knows that the NAT 1404 is a symmetric NAT which will assign a new port ID other than port ID=49152 for use with packets from it (the endpoint server 629) that will come directly to the symmetric NAT 1404 from the NAT 1402 rather than by way of the implied relay server. Using the knowledge that $\Delta p=+1$ for the NAT 1504, the endpoint server 629 can predict a possible value of the new port ID. To improve the chances of successfully predicting the new port ID, the browser 630 can make more than one prediction. Then, the browser 630 can generate one or more corresponding multiple prediction-based BOPs ("p-BOPs").

The browser 630 predicts port IDs and sends corresponding p-BOPs as follows: port ID 49153 over path 1410; port ID 49154 over path 1412; port ID 49155 over path 1414; and port ID 49156 over path 1416. The p-BOPs of paths 1410-1416 are blocked because the symmetric NAT 1402 has not yet sent a packet directly to port 6004 of the NAT 1404. But that does not thwart the purpose of the p-BOPs because a purpose of their being sent is to open the port 60004 in the NAT 1404 to packets from the endpoint server 629 sent via the predicted ports of the NAT 1402.

Continuing in terms of the example port IDs, it is assumed that the NAT 1402 assigns port ID 49154 for use with packets coming/going directly between the port-restricted NAT 1404 and the NAT 1402 rather than by way of the implied relay server. Port ID 49154 corresponds to the packet of path 1412, hence door (port ID 60004) at the NAT 1404 is already open to packets originating through port ID 49154 that do not arrive by way of the implied relay server. As such, in Fig. 14C, the endpoint server 629 sends a stream of packets (e.g., a video stream where the endpoint server 629 is an IP video camera) over a UDP type of P2P connection to the browser 630, as indicated by path 1420.

Next, prediction-based P2P connection facilitation will be discussed for subclass V_2 in terms of Figs. 15A-15C.

To further the context of the explanation, Fig. 15A assumes that: the endpoint server 629 connects to an IP network 1506 (that includes the implied relay server and the NAT-discovery server 622) via a port-restricted cone type NAT 1502; and the browser 630 connects to the network 1506 via a symmetric NAT 1504. It should be observed that Fig. 15A is similar to Fig. 10A. Here, also to further the explanation, example port IDs and a value for Δp are assumed which should not be viewed as limiting the scope of this disclosure.

In Fig. 15A, the endpoint server 629 communicates with the NAT-discovery server 622 (via the NAT 1502) to determine the address/port pair (for example, the port ID is 60004) mapped by the NAT 1502 to the endpoint server 629, what type the NAT 1502 is, as indicated by path 1507A. Similarly, the browser 630 communicates with the NAT-discovery server 622 (via the NAT 1504) to determine the address/port pair (here, the port ID is 49152) mapped by the NAT 1504 to the browser 630 and what type the NAT 1504 is and the increment size, Δp (here, Δp=+1), as indicated by path 1507B.

The endpoint server 629 receives from the browser 630 (via the NAT 1504, the implied relay server and the NAT 1502) information regarding the address/port pair mapped by the NAT 1504 to the browser 630 and what type the NAT 1504 is (including Δp), as indicated by path 1508. The browser 630 receives from the endpoint server 629 (via the NAT 1502, the implied relay server and the NAT 1504) information regarding the address/port pair mapped by the NAT 1502 to the endpoint server 629 and what type the NAT 1502 is, as depicted by path 1510.

In Fig. 15B, the endpoint server 629 would like to send a break-out packet ("BOP") to the endpoint server 629, as indicated by path 1512. A purpose of the BOP of path 1512 would be to open the door in the port-restricted NAT 1502 to packets from the browser 630 that will come directly to the port-restricted NAT 1502 from the NAT 1504 rather than by way of the implied relay server. But the endpoint server 629 knows that the NAT 1504 is a symmetric NAT which will assign a new port ID other than port ID=49152 for use with packets from it (the endpoint server 629) that will come directly to the symmetric NAT 1504 from the NAT 1502 rather than by way of the implied relay server. Using the knowledge that $\Delta p=+1$ for the NAT 1504, the browser 630 can predict a possible value of the new port ID. To improve the chances of successfully predicting the new port ID, the browser 630 can make more than one prediction. Then, the browser can generate one or more corresponding multiple prediction-based BOPs ("p-BOPs").

The endpoint server 629 predicts port IDs and sends corresponding p-BOPs as follows: port ID 49153 over path 1510; port ID 49154 over path 1512; port ID 49155 over path 1514; and port ID 49156 over path 1516. The p-BOPs of paths 1510-1516 are blocked because the symmetric NAT 1504 has not yet sent a packet directly to port 6004 of the NAT 1504. But that does not thwart the purpose of the p-BOPs because a purpose of their being sent is to open the existing port 60004 in the NAT 1502 to packets from the browser 630 sent via the predicted ports of the NAT 1504.

Continuing in terms of the example port IDs, it is assumed that the NAT 1504 assigns port ID 49154 for use with packets coming/going directly between the port-restricted NAT 1502 and the NAT 1504 rather than by way of the implied relay server. Port ID 49154 corresponds to the packet of path 1512, hence door (port ID 60004) at the NAT 1502 is already open to packets originating through port ID 49154 that do not arrive by way of the implied relay server. But the endpoint server 629 does not yet know which

of its predictions was successful, i.e., which of the predicted ports 49153-49156 corresponds to the new port. In Fig. 15C, the browser 630 sends a break-out packet ("BOP") to the endpoint server 629, as indicated by path 1518. A purpose of the BOP of path 1518 would be to open the door (port ID 49154) in the symmetric NAT 1504 to packets from the endpoint server 629 that will come directly to the symmetric NAT 1504 from the NAT 1502 rather than by way of the implied relay server.

Upon receiving the p-BOP of path 1518, the endpoint server 629 records its port ID 49154 (and the IP address) for use in making a P2P connection with the browser 630, as indicated by item 1519. Then, in Fig. 15D, the endpoint server 629 sends a stream of packets (e.g., a video stream where the endpoint server 629 is an IP video camera) over a UDP type of P2P connection to the browser 630, as indicated by path 1520.

Next, prediction-based P2P connection facilitation will be discussed for subclass V_3. As there are two types of symmetric NAT as discussed above, namely SYM_S and SYM_I, there are four sub-classes of sub-class V_3, i.e., four sub-sub-classes: V_{3A}; V_{3B}; V_{3C}; and V_{3D}. The following table, as an example, assumes that a first endpoint device is an endpoint server, e.g., 629, and that the second endpoint device is a browser, e.g., 630.

		Browser Side	
		SYM_I NAT	SYM_S NAT
Endpoint Server Side	SYM_I NAT	**$V3_A$**	**$V3_C$**
	SYM_S NAT	**$V3_B$**	**$V3_D$**

Sub-sub-class V_{3A} will now be discussed in terms of Figs. 16A-16D.

To further the context of the explanation, Fig. 16A assumes that: the endpoint server 629 connects to an IP network 1606 (that includes the implied relay server and the NAT-discovery server 622) via a port-insensitive symmetric ("SYM_I") NAT 1602; and the

browser 630 connects to the network 1606 also via a SYM_I NAT 1604. Here, also to further the explanation, example port IDs and a value for Δp are assumed which should not be viewed as limiting the scope of this disclosure.

In Fig. 16A, the endpoint server 629 communicates with the NAT-discovery server 622 (via the NAT 1602) to determine the address/port pair (for example, the port ID is 50012) mapped by the NAT 1602 to the endpoint server 629, what type the NAT 1602 is and the increment size, Δp (here, Δp=+2), as indicated by path 1607A. Similarly, the browser 630 communicates with the NAT-discovery server 622 (via the NAT 1604) to determine the address/port pair (here, the port ID is 49152) mapped by the NAT 1604 to the browser 630 and what type the NAT 1604 is and the increment size, Δp (here, Δp=+1), as indicated by path 1607B.

The endpoint server 629 receives from the browser 630 (via the NAT 1604, the implied relay server and the NAT 1602) information regarding the address/port pair mapped by the NAT 1604 to the browser 630 and what type the NAT 1604 is (including Δp), as indicated by path 1608. The browser 630 receives from the endpoint server 629 (via the NAT 1602, the implied relay server and the NAT 1604) information regarding the address/port pair mapped by the NAT 1602 to the endpoint server 629 and what type the NAT 1602 is, as depicted by path 1610.

In Fig. 16B, the endpoint server 629 would like to send a break-out packet ("BOP") to the browser 630. A purpose of such a BOP would be to open the door in the SYM_I NAT 1602 to packets from the browser 630 that will come directly to the SYM_I NAT 1602 from the NAT 1604 rather than by way of the implied relay server. But the endpoint server 629 knows that the NAT 1604 is a symmetric NAT which will assign a new port ID other than port ID=49152 for use with packets from it (the endpoint server 629) that will come directly to the symmetric NAT 1604 from the NAT 1602 rather than by way of the implied

relay server. Using the knowledge that $\Delta p=+1$ for the NAT 1604, the browser 630 can predict a possible value of the new port ID.

Because the NAT 1602 is a SYM_I NAT rather than a SYM_S NAT, once it has sent a packet to an address/port pair, the SYM_I NAT 1602 will not assign a new port ID for any other port at the same IP address to which it sends a packet. Hence, the NAT 1602 can send multiple prediction-based BOPs ("p-BOPs") to multiple ports from just one of its own ports, thereby improving the chances of successfully predicting the new port ID. In the example of Fig. 16B, it is assumed that the endpoint server 629 will generate multiple prediction-based BOPs ("p-BOPs").

The endpoint server 629 predicts port IDs and sends corresponding p-BOPs as follows: port ID 49153 over path 1610; port ID 49154 over path 1612; port ID 49155 over path 1614; and port ID 49156 over path 1616. The p-BOPs of paths 1610-1616 are blocked because the symmetric NAT 1604 has not yet sent a packet directly to port 6004 of the NAT 1604. But that does not thwart the purpose of the p-BOPs because a purpose of their being sent is to open the existing port 50012 in the NAT 1602 to packets from the browser 630 sent via the predicted ports of the NAT 1604.

Continuing in terms of the example port IDs, it is assumed that the NAT 1604 assigns port ID 49154 for use with packets coming/going directly between the port-restricted NAT 1602 and the NAT 1604 rather than by way of the implied relay server. Port ID 49154 corresponds to the packet of path 1612, hence door (port ID 60004) at the NAT 1602 is already open to packets originating through port ID 49154 that do not arrive by way of the implied relay server. But the endpoint server 629 does not yet know which of its predictions was successful, i.e., which of the predicted ports 49153-49156 corresponds to the new port.

The browser 630 also would like to send one or more break-out packets ("BOPs") to the endpoint server 629. A purpose of the BOP of path 1612 would be to open the door (port ID=49154) in the symmetric NAT 1604 to packets from the endpoint server 629 that will come directly to the symmetric NAT 1604 from the NAT 1602 rather than by way of the implied relay server. But the browser 630 knows that the NAT 1602 is a symmetric NAT which will assign a new port ID other than port ID=50012 for use with packets from it (the browser 630) that will come directly to the symmetric NAT 1602 from the NAT 1604 rather than by way of the implied relay server. Using the knowledge that $\Delta p=+2$ for the NAT 1604, the browser 630 can predict a possible value of the new port ID.

Because the NAT 1604 is a SYM_I NAT rather than a SYM_S NAT, once it has sent a packet to an address/port pair, the SYM_I NAT 1602 will not assign a new port ID for any other port at the same IP address to which it sends a packet. Hence, the NAT 1604 can send multiple prediction-based BOPs ("p-BOPs") to multiple ports from just one of its own ports, thereby improving the chances of successfully predicting the new port ID. In the example of Fig. 16C, it is assumed that the browser 630 will generate multiple prediction-based BOPs ("p-BOPs").

The browser 630 predicts port IDs and sends corresponding p-BOPs as follows: port ID 50014 over path 1630; port ID 50016 over path 1632; port ID 50018 over path 1634; and port ID 50020 over path 1636. The p-BOPs of paths 1630-1636 are blocked because the symmetric NAT 1602 has not yet sent a packet directly to port 49154 of the NAT 1604. But that does not thwart the purpose of the p-BOPs because a purpose of their being sent is to open the port 49154 in the NAT 1604 to packets from the endpoint server 629 sent via the predicted ports of the NAT 1602.

Continuing in terms of the example port IDs, it is assumed that the NAT 1602 assigns port ID 50014 for use with packets coming/going directly between the symmetric

NAT 1602 and the symmetric NAT 1604 rather than by way of the implied relay server. Port ID 50014 corresponds to the packet of path 1630, hence door (port ID 49154) at the NAT 1604 is already open to packets originating through port ID 50014 that do not arrive by way of the implied relay server.

Upon receiving the p-BOP of path 1630, the endpoint server 629 records its port ID 49154 (and the IP address) for use in making a P2P connection with the browser 630, as indicated by item 1639. Then, in Fig. 16D, the endpoint server 629 sends a stream of packets (e.g., a video stream where the endpoint server 629 is an IP video camera) over a UDP type of P2P connection to the browser 630, as indicated by path 1640.

Sub-sub-class V_{3B} will now be discussed in terms of Figs. 17A-17C.

To further the context of the explanation, Fig. 17A assumes that: the endpoint server 629 connects to an IP network 1706 (that includes the implied relay server and the NAT-discovery server 622) via a port-sensitive symmetric ("SYM_S") NAT 1702; and the browser 630 connects to the network 1706 via a port-insensitive symmetric (SYM_I) NAT 1704. Here, also to further the explanation, example port IDs and a value for Δp are assumed which should not be viewed as limiting the scope of this disclosure.

In Fig. 17A, the endpoint server 629 communicates with the NAT-discovery server 622 (via the NAT 1702) to determine the address/port pair (for example, the port ID is 50012) mapped by the NAT 1702 to the endpoint server 629, what type the NAT 1702 is and the increment size, Δp (here, Δp=+2), as indicated by path 1707A. Similarly, the browser 630 communicates with the NAT-discovery server 622 (via the NAT 1704) to determine the address/port pair (here, the port ID is 49152) mapped by the NAT 1704 to the browser 630 and what type the NAT 1704 is and the increment size, Δp (here, Δp=+1), as indicated by path 1707B.

The endpoint server 629 receives from the browser 630 (via the NAT 1704, the implied relay server and the NAT 1702) information regarding the address/port pair mapped by the NAT 1704 to the browser 630 and what type the NAT 1704 is (including Δp), as indicated by path 1708. The browser 630 receives from the endpoint server 629 (via the NAT 1702, the implied relay server and the NAT 1704) information regarding the address/port pair mapped by the NAT 1702 to the endpoint server 629 and what type the NAT 1702 is, as depicted by path 1710.

Continuing in terms of the example port IDs, it is assumed that the NAT 1704 assigns port ID 49153 for use with packets coming/going directly between the port-restricted NAT 1702 and the NAT 1704 rather than by way of the implied relay server. The browser 630 would like to send one or more break-out packets ("BOPs") to the endpoint server 629. A purpose of the BOP of path 1712 would be to open the door (port ID=49153) in the symmetric NAT 1704 to packets from the endpoint server 629 that will come directly to the symmetric NAT 1704 from the NAT 1702 rather than by way of the implied relay server. But the browser 630 knows that the NAT 1702 is a symmetric NAT which will assign a new port ID other than port ID=50012 for use with packets from it (the browser 630) that will come directly to the symmetric NAT 1702 from the NAT 1704 rather than by way of the implied relay server. Using the knowledge that Δp=+2 for the NAT 1704, the browser 630 can predict a possible value of the new port ID.

Because the NAT 1704 is a SYM_I NAT rather than a SYM_S NAT, once it has sent a packet to an address/port pair, the SYM_I NAT 1702 will not assign a new port ID for any other port at the same IP address to which it sends a packet. Hence, the NAT 1704 can send multiple prediction-based BOPs ("p-BOPs") to multiple ports from just one of its own ports, thereby improving the chances of successfully predicting the new port ID. In the

example of Fig. 17C, it is assumed that the browser 630 will generate multiple prediction-based BOPs ("p-BOPs").

The browser 630 predicts port IDs and sends corresponding p-BOPs as follows: port ID 50014 over path 1730; port ID 50016 over path 1732; port ID 50018 over path 1734; and port ID 50020 over path 1736. The p-BOPs of paths 1730-1736 are blocked because the symmetric NAT 1702 has not yet sent a packet directly to port 49154 of the NAT 1704. But that does not thwart the purpose of the p-BOPs because a purpose of their being sent is to open the port 49154 in the NAT 1704 to packets from the endpoint server 629 sent via the predicted ports of the NAT 1702.

Continuing in terms of the example port IDs, it is assumed that the SYM_S NAT 1702 assigns port ID 50014 (=50012+2) for use with packets coming/going directly between the SYM_S NAT 1702 and the SYM_I NAT 1704 rather than by way of the implied relay server. The endpoint server 629 predicts that the port ID on the SYM_I NAT 1704 will be ID=49153 (=49153+1). In Fig. 17D, the endpoint server 629 sends a stream of packets (e.g., a video stream where the endpoint server 629 is an IP video camera) over a UDP type of P2P connection to the browser 630 using predicted port ID=49153, as indicated by path 1740. If the prediction is wrong, then the endpoint server 629 can predict another port ID and resend the stream iteratively until the prediction is successful and the P2P connection is established.

Sub-sub-class V_{3C} will now be discussed in terms of Figs. 18A-18D.

To further the context of the explanation, Fig. 18A assumes that: the endpoint server 629 connects to an IP network 1806 (that includes the implied relay server and the NAT-discovery server 622) via a port-insensitive symmetric (SYM_I) NAT 1802; and the browser 630 connects to the network 1806 via a port-sensitive symmetric ("SYM_S") NAT

1804. Here, also to further the explanation, example port IDs and a value for Δp are assumed which should not be viewed as limiting the scope of this disclosure.

In Fig. 18A, the endpoint server 629 communicates with the NAT-discovery server 622 (via the NAT 1802) to determine the address/port pair (for example, the port ID is 50012) mapped by the NAT 1802 to the endpoint server 629, what type the NAT 1802 is and the increment size, Δp (here, Δp=+2), as indicated by path 1807A. Similarly, the browser 630 communicates with the NAT-discovery server 622 (via the NAT 1804) to determine the address/port pair (here, the port ID is 49152) mapped by the NAT 1804 to the browser 630 and what type the NAT 1804 is and the increment size, Δp (here, Δp=+1), as indicated by path 1807B.

In Fig. 18B, the endpoint server 629 would like to send a break-out packet ("BOP") to the browser 630. A purpose of such a BOP would be to open the door in the SYM_I NAT 1802 to packets from the browser 630 that will come directly to the SYM_I NAT 1802 from the NAT 1804 rather than by way of the implied relay server. But the endpoint server 629 knows that the NAT 1804 is a symmetric NAT which will assign a new port ID other than port ID=49152 for use with packets from it (the endpoint server 629) that will come directly to the symmetric NAT 1804 from the NAT 1802 rather than by way of the implied relay server. Using the knowledge that Δp=+1 for the NAT 1804, the browser 630 can predict a possible value of the new port ID.

Because the NAT 1802 is a SYM_I NAT rather than a SYM_S NAT, once it has sent a packet to an address/port pair, the SYM_I NAT 1802 will not assign a new port ID for any other port at the same IP address to which it sends a packet. Hence, the NAT 1802 can send multiple prediction-based BOPs ("p-BOPs") to multiple ports from just one of its own ports, thereby improving the chances of successfully predicting the new port ID. In the

example of Fig. 18B, it is assumed that the endpoint server 629 will generate multiple prediction-based BOPs ("p-BOPs").

The endpoint server 629 predicts port IDs and sends corresponding p-BOPs as follows: port ID 49153 over path 1810; port ID 49154 over path 1812; port ID 49155 over path 1814; and port ID 49156 over path 1816. The p-BOPs of paths 1810-1816 are blocked because the symmetric NAT 1804 has not yet sent a packet directly to port 50014 of the NAT 1804. But that does not thwart the purpose of the p-BOPs because a purpose of their being sent is to open the existing port 50014 in the NAT 1802 to packets from the browser 630 sent via the predicted ports of the NAT 1804.

Continuing in terms of the example port IDs, it is assumed that the NAT 1804 assigns port ID 49154 for use with packets coming/going directly between the port-restricted NAT 1802 and the NAT 1804 rather than by way of the implied relay server. Port ID 49154 corresponds to the packet of path 1812, hence door (port ID 50014) at the NAT 1802 is already open to packets originating through port ID 49154 that do not arrive by way of the implied relay server. But the endpoint server 629 does not yet know which of its predictions was successful, i.e., which of the predicted ports 49153-49156 corresponds to the new port.

In Fig. 18C, the browser 630 sends a predicted break-out packet ("p-BOP") to the endpoint server 629, as indicated by path 1818. A purpose of the BOP of path 1818 would be to open the door (port ID 49154) in the SYM_S NAT 1804 to packets from the endpoint server 629 that will come directly to the SYM_S NAT 1804 from the SYM_I NAT 1802 rather than by way of the implied relay server.

Upon receiving the p-BOP of path 1818, the endpoint server 629 records its port ID 49154 (and the IP address) for use in making a P2P connection with the browser 630, as indicated by item 1819. Then, in Fig. 18D, the endpoint server 629 sends a stream of

packets (e.g., a video stream where the endpoint server 629 is an IP video camera) over a UDP type of P2P connection to the browser 630, as indicated by path 1820.

Sub-sub-class V_{3D} will now be discussed in terms of Figs. 19A-19C.

To further the context of the explanation, Fig. 19A assumes that: the endpoint server 629 connects to an IP network 1906 (that includes the implied relay server and the NAT-discovery server 622) via a port-sensitive symmetric ("SYM_S") NAT 1902; and the browser 630 connects to the network 1906 also via a SYM_S NAT 1904. Here, also to further the explanation, example port IDs and a value for Δp are assumed which should not be viewed as limiting the scope of this disclosure.

In Fig. 19A, the endpoint server 629 communicates with the NAT-discovery server 622 (via the NAT 1902) to determine the address/port pair (for example, the port ID is 50012) mapped by the NAT 1902 to the endpoint server 629, what type the NAT 1902 is and the increment size, Δp (here, Δp=+2), as indicated by path 1907A. Similarly, the browser 630 communicates with the NAT-discovery server 622 (via the NAT 1904) to determine the address/port pair (here, the port ID is 49152) mapped by the NAT 1904 to the browser 630 and what type the NAT 1904 is and the increment size, Δp (here, Δp=+1), as indicated by path 1907B.

In Fig. 19B, the browser 630 sends a predicted break-out packet ("p-BOP") to the endpoint server 629, as indicated by path 1918. A purpose of the BOP of path 1918 would be to open the door (port ID 49153) in the SYM_S NAT 1904 to packets from the endpoint server 629 that will come directly to the SYM_S NAT 1904 from the SYM_S NAT 1902 rather than by way of the implied relay server.

Using the knowledge that Δp=+2 for the NAT 1904, the browser 630 can predict a possible value of the new port ID.

The browser 630 predicts the port ID to be ID=50014 sends corresponding p-BOP over path 1918. The p-BOP of paths 1918 is blocked because the symmetric NAT 1902 has not yet sent a packet directly to port 49154 of the SYM_S NAT 1904. But that does not thwart the purpose of the p-BOP because a purpose of it being sent is to open the port 49153 in the SYM_S NAT 1904 to packets from the endpoint server 629 sent via the predicted port of the SYM_S NAT 1902.

Continuing in terms of the example port IDs, it is assumed that the SYM_S NAT 1902 actually does assign port ID 50014 (=50012+2) for use with packets coming/going directly between the SYM_S NAT 1902 and the SYM_I NAT 1904 rather than by way of the implied relay server. The endpoint server 629 predicts that the port ID on the SYM_I NAT 1904 will be ID=49153 (=49153+1). In Fig. 19C, the endpoint server 629 sends a stream of packets (e.g., a video stream where the endpoint server 629 is an IP video camera) over a UDP type of P2P connection to the browser 630 using predicted port ID=49153, as indicated by path 1920. If the prediction is wrong, then the endpoint server 629 can repeat the process, starting with the paths 1907A, 1907B, etc., albeit including the following differences: the endpoint server 629 and the browser 630 can cause the respective NATs to make new bindings by communicating to the NAT-discovery server 622 using different source port IDs, respectively.

According to another embodiment of the invention, an extension to the Session Description Protocol ("SDP"), namely a new attribute, is provided by which information as to the type of a NAT can be exchanged. Alternatively, techniques other than an SDP-message can be used to exchange NAT-type information.

SDP is suitable for use with HTTP because, e.g., SDP is text-based and/or because it is commonly used as a voice-over-IP protocol. Over HTTP, an SDP message having

NAT-type information can be sent as some or all of the content/body of a request (e.g., using HTTP's POST method) and a response (e.g., using HTTP's message 200 OK) message.

Such an SDP NAT-type attribute can be as follows.

- Content-Type: application/sdp
- Use a= field: (ex. a=<attribute>:<value>)
- Attribute name: nat
- Attribute value (see following table):

Open	OPEN (default)
Full-cone NAT	F
Address-restricted cone NAT	R
Port-restricted-cone NAT	PR
Port-sensitive Symmetric NAT	SYM
Port-INsensitive Symmetric NAT	SYMI
UDP_BLOCKED	UB

The following is an example SDP-message that can be used to exchange NAT-type information. This example will treat the characters, //, and every subsequent character encountered until the end of a line as a comment, i.e., as not being part of the SDP message.

POST /P2PRequest HTTP/1.1	//HTTP header, request line
Content-Type: application/sdp	//HTTP header, attribute line
Content-Length: 89	///HTTP header, attribute line
	//Intentional SDP Blank line
v=0	//Version number of SDP
s=P2P Viewer	//Name of browser
c=IN IP4 67.105.5.125	//IPV4 scheme, browser's //address
a=recvonly	//browser receive only not also //send
m=video 61003 RTP/AVP 26	//forthcoming P2P content //(media)
a=nat:F	//Specific example of extension // to SDP according to an //embodiment of the invention, // here NAT type is full cone (F)

In the case that the NAT is a symmetric NAT, the attribute value will have a second field in addition to the type field (e.g., for a symmetric NAT, the type field will be "SYM" or "SYMI"). The second field represents the value of the increment size (Δp). As an example, a SYM_I NAT having $\Delta p=+2$ can be represented as: a=nat:SYMI 2. As another example, a SYM_S NAT having $\Delta p=+1$ can be represented as: a=nat:SYM 1.

Figure 20 depicts a table that organizes actions, according to an embodiment of the invention, which can be taken toward establishing a P2P connection between a first endpoint device and a second endpoint device after these devices have exchanged NAT-mapped address and NAT-type information via a relay-server-based connection, depending upon the class (I, II, III, IV and V_1, V_2, V_{3A}, V_{3B}, V_{3C} and V_{3D}) of NAT-combination. As in the explanations above, the first endpoint device can be, e.g., an endpoint server such as 629, and the second endpoint device can be, e.g., a browser such as 630. In Fig. 20, the legend "SR" indicates source port recording. There, the endpoint server can record the

source port number of an incoming packet to be used as a destination port to send UDP packets.

Fig. 21 is a flowchart, related to the table of Fig. 20, depicting actions that can be taken by the first endpoint device, e.g., (again), an endpoint server such as 629, according to embodiments of the invention. The various classes (I, II, III, IV and V_1, V_2, V_{3A}, V_{3B}, V_{3C} and V_{3D}) of NAT-combination, indicated generally at item 2102, enter the flowchart of Fig. 21 at different locations. Classes IV, V_2, V_{3A}, and V_{3C} enter box 2104, where the first endpoint device sends one or more BOPs and/or p-BOPs. For classes V_2, V_{3A}, V_{3B}, V_{3C} and V_{3D}, the first endpoint device might send multiple p-BOPs to destinations predicted using the increment size (Δp) of the second endpoint device's NAT.

Flow moves in Fig. 21 from box 2104 to decision box 2106, where the first endpoint device waits to receive a packet from the second endpoint device. It is noted that class III enters the flowchart by entering decision box 2106. If a packet is received by the first endpoint device, then flow moves from box 2106 to box 2108, where the first endpoint device records the packet's source port (and IP address).

Flow moves further in Fig. 21 from box 2108 to box 2110, where the first endpoint device sends a stream of packets over a UDP type of P2P connection. It is noted that classes I, II, V_1, V_{3B}, and V_{3D} enter the flowchart by entering decision box 2104. After the P2P connection is finished, flow moves from box 2110 to box 2112, where flow ends. If a packet is not received by the first endpoint device after waiting a predetermined time, T1 (e.g., T1 = 10 seconds), a failure/exception is considered to have occurred and flow moves from box 2106 to box 2114, where the first endpoint device carries out appropriate exception/failure procedures. Flow moves from box 2114 to box 2112.

Fig. 22 is a flowchart, related to the table of Fig. 20 (and the flowchart of Fig. 21), depicting actions that can be taken by the second endpoint device, e.g., (again), a browser

such as 630, according to another embodiment of the invention. The various classes (I, II, III, IV and V1, V2, V3A, V3B, V3C and V3D) of NAT-combination, indicated generally item at 2202, enter the flowchart of Fig. 22 at different locations. Classes I, II, III, IV and V1, V2, V3A, V3B, V3C and V3D (i.e., all except class I) enter box 2204, where the second endpoint device sends one or more BOPs and/or p-BOPs. For classes V_2, V_{3A} or V_{3B}, the second endpoint device might send multiple p-BOPs to destinations predicted using the increment size (Δp) of the first endpoint device's NAT.

Flow moves from box 2204 to decision box 2206, where the second endpoint device waits to receive a packet from the first endpoint device. If a packet is received by the second endpoint device, then flow in Fig. 22 moves from box 2206 to box 2210, where the second endpoint device attempts receives a stream of packets over a UDP type of P2P connection. It is noted that class I enters the flowchart by entering decision box 2210. After the P2P connection is finished, flow moves from box 2210 to box 2212, where flow ends.

In Fig. 22, if a packet is not received by the second endpoint device after waiting a predetermined time, T2 (e.g., T2 = 10 milliseconds), flow moves or loops from box 2206 back to box 2204. If a packet is not received by the second endpoint device after waiting a concurrently-elapsing predetermined time, T1 (e.g., T1 = 10 seconds), a failure/exception is considered to have occurred and flow moves from box 2206 to box 2214, where the second endpoint device carries out appropriate exception/failure procedures. Flow moves from box 2214 to box 2212.

Figure 3 is a sequence diagram of operations by which a P2P connection can be facilitated according to embodiments of the invention. Figure 23 does not strictly conform to the conventions of UML-type sequence diagrams. Figure 3 is similar to Fig. 2 in that it includes: an endpoint server 629; a first NAT 2314_1 corresponding to 14_1; a NAT-

discovery server 2322 corresponding to 22; a packet relay server 2320 corresponding to 20; a redirect server 2324 corresponding to 24; a second NAT 2314_2 corresponding to 14_2; and a browser 630. The endpoint server 629 and the browser 630, again, are examples of endpoint devices; other types of endpoint devices can be used.

Further, Figure 3 is similar to Fig. 2 in its sequence of messages up through a point at which the packet-relay-based connection is established, as indicated by item 2362. As such, messages 2330, 2332, 2334, 2336, 2342, 2344, 2346, 2348, 2350 and 2352 of Figure 3 correspond to messages 30, 32, 34, 36, 42, 44, 46, 48, 50 and 52 of Fig. 2, respectively, and will be described further, if at all, merely with brief comments, for the sake of brevity. Comments, as indicated by items 2391 and 2393, have been listed in Figure 3 for messages 2332 and 2336, respectively. Messages corresponding to 38 and 40 can take place in Figure 3, but are not depicted for brevity. The intervening roles of the NATs 2314_1 and 2314_2 are indicated by the dots 72 at the intersections of messages and the lifelines 2373 and 2375.

Messages 2330, 2332, 2334 and 2336 can be described as occurring during a boot-up phase (as indicated by item 2359) of the endpoint server 629. An additional message 2360 is sent by the endpoint server 629 during the boot-up phase 2359, namely message 2360 sent after message 2330 but before message 2332. Message 2360 is a NAT-discovery-over-UDP test initiated by the endpoint server 629 to determine information about what type the NAT 2314_1 is and to gather data by which the endpoint server 629 can determine the value of the increment size (Δp) of the NAT 2314_1.

Messages 2342, 2344, 2346, 2348, 2350 and 2352 can be described as occurring during a redirect phase (as indicated by item 2361). Message 2342, as an example, assumes 'URL:http://www.cam1.mweb.com' as an address mapped by the NAT 2314_1 to the endpoint server 629. Messages 2344, 2350 and 2352 each, as an example, assumes a

response that includes the HTTP message "200 OK". The HTTP session between the endpoint server 629 and the browser 630 via the relay server 2320 as intermediary becomes established after message 2352.

Figure 3 further includes the following phases: a browser-status-check phase (as indicated by item 2363) which the browser 630 undergoes, corresponding to messages 2364, 2366 and 2368; an SDP-message-exchange phase (as indicated by item 2365) including messages 2370, 2371, 2374, 2376, 2378 and 2389; and a priming phase (as indicated by item 2367) including messages 2382 and 2384. After the priming phase 2367, the endpoint server 629 and the browser 630 are ready to make a P2P connection, as indicated by item 2388.

The browser-status-check phase 2363 will now be described in more detail. After receiving the message 2352, the browser 630 sends a message 2364, which is a NAT-discovery-over-UDP test to determine information about what type the NAT 2314_2 is and to gather data by which the endpoint server 629 can determine the value of the increment size (Δp) of the NAT 2314_2. Message 2364 corresponds to message 2360. A typical browser 630 does not have the capability to perform a NAT-discovery-over-UDP test. Such capability can be added to the browser 630 via a plug-in module, an active-X control, an applet, etc. provided to the browser 630, e.g., as an additional part of the messages 2350 and 2352.

Then, the browser 630 sends message 2366, e.g., a STUN allocate request, by which the browser 630 requests the port allocated/mapped to it (the browser 630) by the NAT 2314_2 for a forthcoming P2P connection with the endpoint server 629. The NAT-discovery server 2322 responds in the form of message 2368, e.g., a STUN Mapped-Address indicating at least a port ID if not an address/port pair.

The SDP-message-exchange phase 2365 will now be described in more detail. After message 2368, the browser 630 sends message 2370, e.g., an SDP on HTTP message, to the endpoint server 629 via the relay server 2320, which relays message 2370 as message 2371 to the endpoint server 629. Aspects of the messages 2370 and 2371 can include: an indication that browser 630 wants to set-up a P2P connection; an indication of what type the NAT 2314_2 is; and an indication of what is the value of the increment size (Δp), e.g., using the NAT-type attribute extension to SDP discussed above. For example, the sample SDP-type message discussed above, namely "POST/P2PRequest HTTP/1.1 ...", uses the "POST" method available in SDP to convey information. Among other things, the text string "P2PRequest" (in the field known as the "requested URI" field) indicates that the browser 630 (as the sender of the message) wants to set-up a P2P connection with the recipient of the message, namely the endpoint server 629. Other SDP methods could be used to convey such information.

The endpoint server 629 responds by sending message 2374, e.g., a STUN allocate request, by which the endpoint server 629 requests the port allocated/mapped to it (the browser 630) by the NAT 2314_2 for a forthcoming P2P connection with the browser 630. The NAT-discovery server 2322 responds in the form of message 2376, e.g., a STUN Mapped-Address indicating at least a port ID if not an address/port pair. The endpoint server 629 sends message 2378, e.g., an SDP on HTTP message, to the browser 630 via the relay server 2320, which relays message 2378 as message 2380 to the endpoint server 629. The messages 2378 and 2380, similar to messages 2370 and 2371, indicate what type the NAT 2314_1 is as well as what is the value of the increment size (Δp), e.g., using the NAT-type attribute extension to SDP discussed above.

It is noted that the SDP exchange phase can be carried out in ways other than the messages 2370 - 2389. Alternatively, the NAT-type information, etc., can be exchanged

between the browser 630 and the endpoint server 629 via the existing relay-server-based HTTP session, a separate MODEM-supported communication channel,; a wireless connection, a ping-pong Gnutella-type-protocol session, etc.

The priming phase 2367 will now be described in more detail. If the characteristics of the two NATs 2314_1 and 2314_2 correspond to one of classes III, IV or V, then the endpoint server 629 sends one or more BOPs or p-BOPs to the browser 630. Then, if the characteristics of the two NATs 2314_1 and 2314_2 correspond to one of classes II, III, IV or V, the browser 630 sends one or more BOPs or p-BOPs to endpoint server 629. And if the characteristics of the two NATs 2314_1 and 2314_2 correspond to one of classes III, IV or V, then the endpoint server 629 also records the port ID allocated/mapped by the NAT 2314_2 to the browser 630 for the forthcoming P2P connection, as indicated by note 2386. It is noted that a trigger for causing the endpoint server 629 to send one or more BOPs can be the P2P request included in message 2371/2370. Similarly, a trigger for the browser 630 to send one or more BOPs can be the message 2378/2380 that responds to the P2P request.

After message 2384 and (in some cases) the source port recording 2386, the endpoint server 629 and the browser 630 are ready to establish a P2P connection. As indicated by message 2390, the endpoint server 629 then sends a stream of packets (e.g., a video stream where the endpoint server 629 is an IP video camera) over a UDP type of P2P connection to the browser 630.

The description of the invention is merely exemplary in nature and, thus, variations that do not depart from the gist of the invention are intended to be within the scope of the invention. Such variations are not to be regarded as a departure from the spirit and scope of the invention.

CLAIMS

1. A method of operating a first endpoint device (ED) to facilitate a peer-to-peer (P2P) connection between the first ED and a second ED despite intervening network address translators (NATs) at both ends of the connection, for use with a system compliant with the internet protocol (IP),

the system having an architecture that includes a first network, a second network and a third network,

the first network having at least the first ED and a first NAT, the first ED being connected to the third network via the first NAT, the first NAT allocating a first pair of an IP address and port number for communication from the third-network-side of the first NAT with the first ED via the first NAT,

the second network having at least the second ED and a second NAT, the second ED being connected to the third network via the second NAT, the second NAT allocating a second IP-address/port pair for communication from the third-network-side of the second NAT with the second ED via the second NAT,

the method comprising:

providing the second ED with the first IP-address/port pair; and

providing the second ED with first type-information regarding the type of the first NAT.

2. The method of claim 1, further comprising:

determining the first type-information.

3. The method of claim 2, wherein the first type-information is determined by performing a NAT-discovery test.

4. The method of claim 3, wherein the NAT-discovery test is a STUN test over the UDP.

5. The method of claim 1, further comprising:

receiving the second IP-address/port pair from the second ED; and

receiving second type-information regarding the type of the second NAT from the second ED.

6. The method of claim 1, wherein at least one of the first IP-address/port pair and the first type-information is provided to the second ED via one of: an HTTP session with the second ED; a separate MODEM-supported communication channel with the second ED; a wireless connection to the second ED; and ping-pong type-protocol session with the second ED.

7. The method of claim 6, wherein the first type-information is provided via an SDP-on-HTTP message.

8. The method of claim 7, wherein the SDP-on-HTTP message includes an SDP attribute representing the type of a NAT.

9. The method of claim 8, wherein content of the attribute can indicate that the NAT is one of the following types: full-cone; restricted cone; port-restricted cone; genus symmetric; species port-sensitive symmetric; species port-insensitive symmetric; and UDP-blocked.

10. The method of claim 1, wherein one of the first and second EDs is a server and the other ED is a would-be client of the server.

11. The method of claim 1, wherein the server is an HTTP server and the would-be client is a browser.

12. The method of claim 1, wherein the first network and the second network are each private networks and the third network is a public network.

13. The method of claim 12, wherein the public network is the internet.

14. A method of communicating information about a network address translator (NAT), where the NAT connects a first network to a second network, the method comprising:

generating a session description protocol (SDP) message;

including an SDP attribute in the message that describes the type of the NAT; and

sending the SDP message to the second network from the first network via the NAT.

15. The method of claim 14, wherein the SDP is an SDP on HTTP message.

16. The method of claim 14, wherein content of the attribute can indicate that the NAT is one of the following types: full-cone; restricted cone; port-restricted cone; genus symmetric; species port-sensitive symmetric; species port-insensitive symmetric;; and UDP-blocked.

17. A first endpoint device (ED) for use with a system compliant with the internet protocol (IP),

the system having an architecture that includes a first network, a second network and a third network,

the first network having at least the first ED and a first NAT, the first ED being connected to the third network via the first NAT, the first NAT allocating a first pair of an IP address and port number for communication from the third-network-side of the first NAT with the first ED via the first NAT,

the second network having at least a second ED and a second NAT, the second ED being connected to the third network via the second NAT, the second NAT allocating a second IP-address/port pair for communication from the third-network-side of the second NAT with the second ED via the second NAT,

the first ED being operable to facilitate a peer-to-peer (P2P) connection between the first ED and the second ED, despite the intervening first and second NATs at both ends of the connection, by performing the method of any one of claims 1, 14, 20 and 27.

18. The first endpoint device of claim 17, wherein the first ED is one of a server and a would-be client of a server.

19. The first endpoint device of claim 18, wherein the server is an HTTP server and the would-be client is a browser.

20. A method of determining a port increment size (Δp) for a symmetric network address translator (NAT), the method comprising:

requesting the symmetric NAT to map a plurality of port identification numbers (IDs);

receiving information regarding the plurality of port IDs; and

comparing the information to determine an increment size (Δp) of the NAT.

21. The method of claim 20, wherein the information is compared by

calculating the difference between port IDs allocated, respectively, by the NAT in response to successive requests for mappings; and

analyzing the resulting distribution of differences to estimate increment size (Δp).

22. The method of claim 20, further comprising:

determining whether the symmetric NAT is port-sensitive or port-insensitive.

23. The method of claim 22, wherein, if two mapping requests to the NAT for different destination port IDs on the same destination IP address are mapped to the same port on the NAT, then the NAT is port-insensitive.

24. The method of claim 20, wherein

the NAT is a first NAT; and

the receiving and comparing of the information is done by a first endpoint device (ED) being used with a system compliant with the internet protocol (IP),

the system having an architecture that includes a first network, a second network and a third network,

the first network having at least the first ED and the first NAT, the first ED being connected to the third network via the first NAT, the first NAT allocating a first pair of an IP address and port number for communication from the third-network-side of the first NAT with the first ED via the first NAT,

the second network having at least the second ED and a second NAT, the second ED being connected to the third network via the second NAT, the second NAT allocating a second IP-address/port pair for communication from the third-network-side of the second NAT with the second ED via the second NAT,

the method further comprising:

sending an indication of the increment size (Δp) from the first ED to the second ED.

25. The method of claim 24, wherein the indication of increment size (Δp) is sent via a packet-relay-server-based connection between the first ED and the second ED.

26. The method of claim 24, wherein the indication of increment size (Δp) is represented via an SDP message having a NAT-type attribute.

27. A method of operating a first endpoint device (ED) to facilitate a peer-to-peer (P2P) connection between the first ED and a second ED despite intervening network address translators (NATs) at both ends of the connection, for use with a system compliant with the internet protocol (IP),

the system having an architecture that includes a first network, a second network and a third network,

the first network having at least the first ED and a first NAT, the first ED being connected to the third network via the first NAT, the first NAT allocating a first pair of an IP address and port number for communication from the third-network-side of the first NAT with the first ED via the first NAT,

the second network having at least the second ED and a second NAT, the second ED being connected to the third network via the second NAT, the second NAT allocating a second IP-address/port pair for communication from the third-network-side of the second NAT with the second ED via the second NAT,

the method comprising:

receiving an indication of increment size (Δp) used by the second NAT to allocate/map new port numbers; and

predicting, based upon the indication of increment size (Δp), at least one predicted destination port identification number ("ID") that would be used by the second NAT for the P2P connection between the first ED and a second ED.

28. The method of claim 27, further comprising:

generating at least one predicted break-out packet ("p-BOP") corresponding to the one predicted destination port, respectively.

29. The method of claim 28, further comprising:

sending the at least one p-BOP to the second ED via the first NAT.

30. The method of claim 27, wherein the increment size (Δp) is received from the second ED.

31. The method of claim 30, wherein the increment size (Δp) is received via a packet-relay-server-based connection between the first ED and the second ED.

32. The method of claim 30, wherein the indication of increment size (Δp) is represented via an SDP message having a NAT-type attribute.

33. A computer-readable medium having code portions embodied thereon that are readable by a first endpoint device (ED), the first ED being usable with a system compliant with the internet protocol (IP),

the system having an architecture that includes a first network, a second network and a third network,

the first network having at least the first ED and a first NAT, the first ED being connected to the third network via the first NAT, the first NAT allocating a first pair of an IP address and port number for communication from the third-network-side of the first NAT with the first ED via the first NAT,

the second network having at least a second ED and a second NAT, the second ED being connected to the third network via the second NAT, the second NAT allocating a second IP-address/port pair for communication from the third-network-side of the second NAT with the second ED via the second NAT,

the code portions embodied on the computer-readable medium, when read by the first ED, causing the first ED to perform any one of the methods of claims 1, 14, 20 and 27, thereby making the first ED operable to facilitate a peer-to-peer (P2P) connection between the first ED and the second ED, despite the intervening first and second NATs at both ends of the connection.

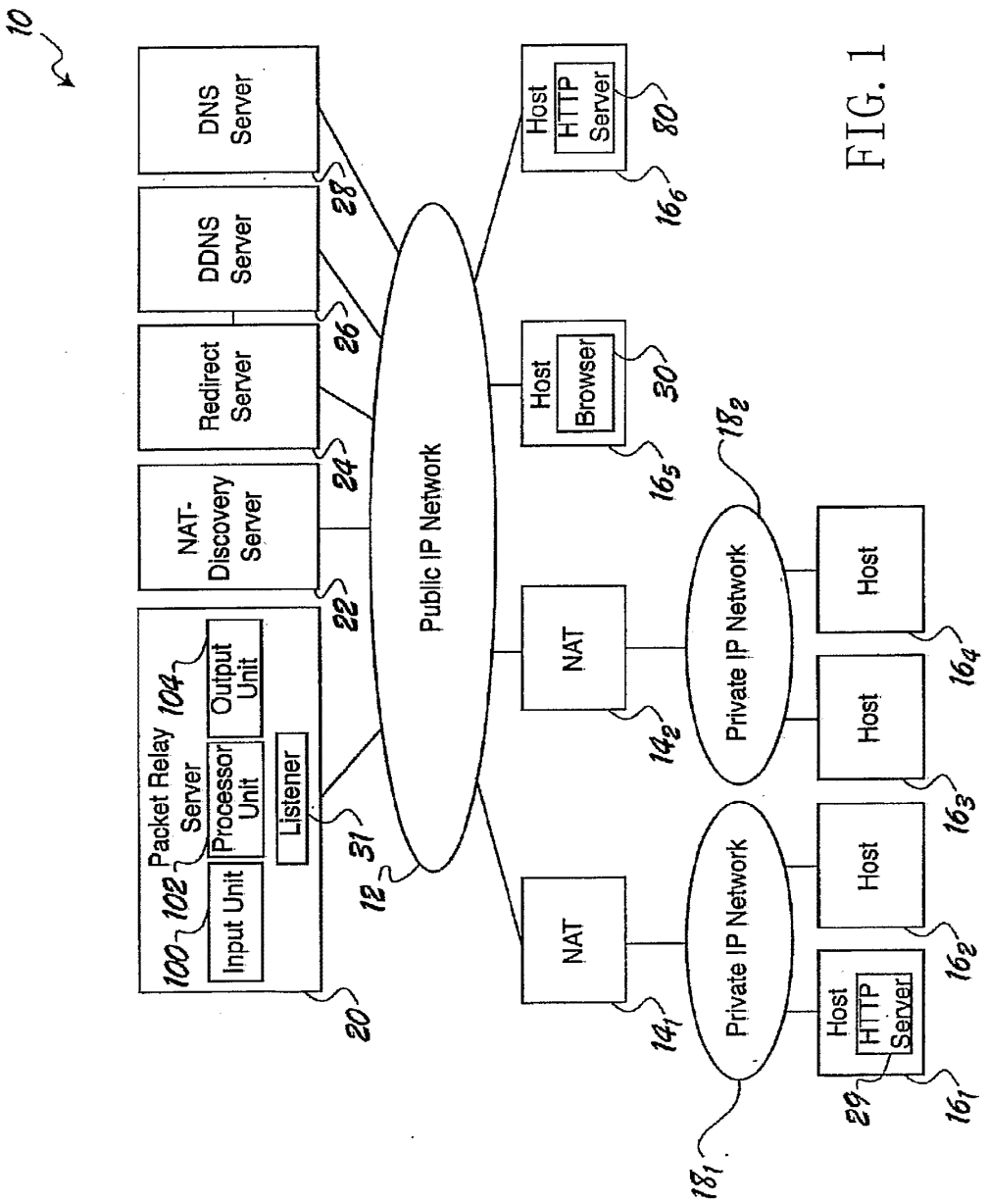

10
DNS Server
DDNS Server
Redirect Server
NAT-Discovery Server
Packet Relay Server
Input Unit
Processor Unit
Output Unit
Listener
Public IP Network
Host HTTP Server
Host Browser
NAT
Private IP Network
Host
Host HTTP Server
20
22
24
26
28
30
31
80
100
102
104
12
141
142
161
162
163
164
165
166
181
182

FIG. 1

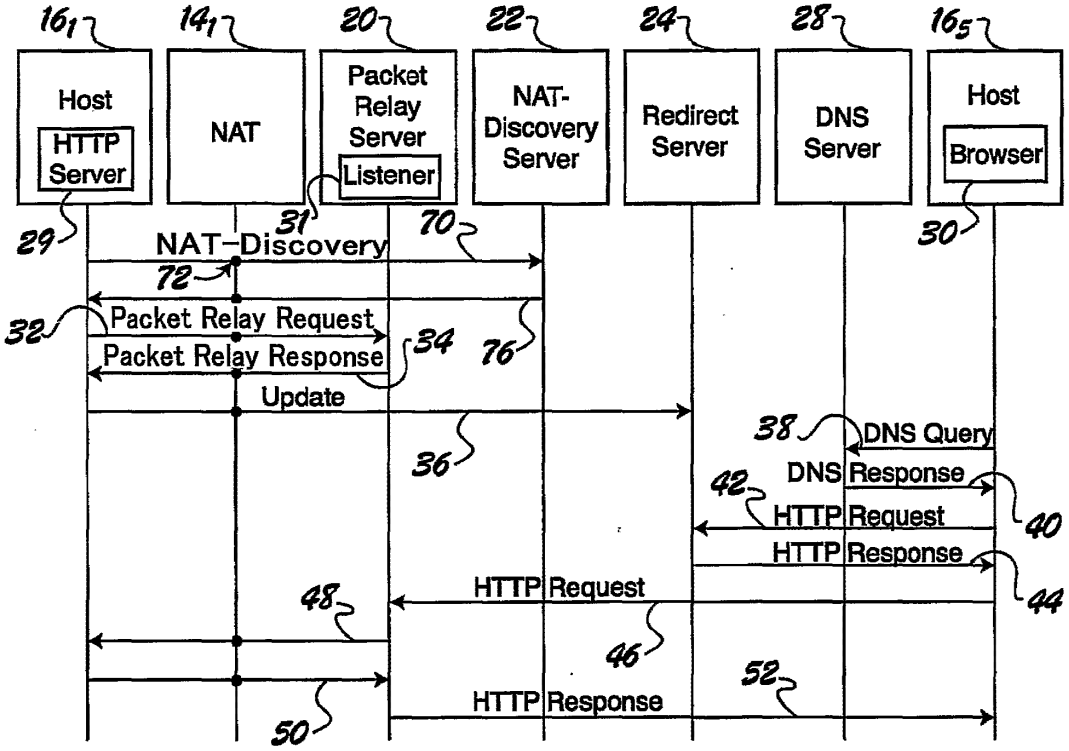

16₁
14₁
20
22
24
28
16₅
Host
HTTP Server
NAT
Packet Relay Server
Listener
NAT-Discovery Server
Redirect Server
DNS Server
Host
Browser
29
31
70
30
NAT-Discovery
72
32
Packet Relay Request
Packet Relay Response
34
76
Update
36
38
DNS Query
DNS Response
42
HTTP Request
40
HTTP Response
44
48
HTTP Request
46
52
50
HTTP Response

FIG. 2

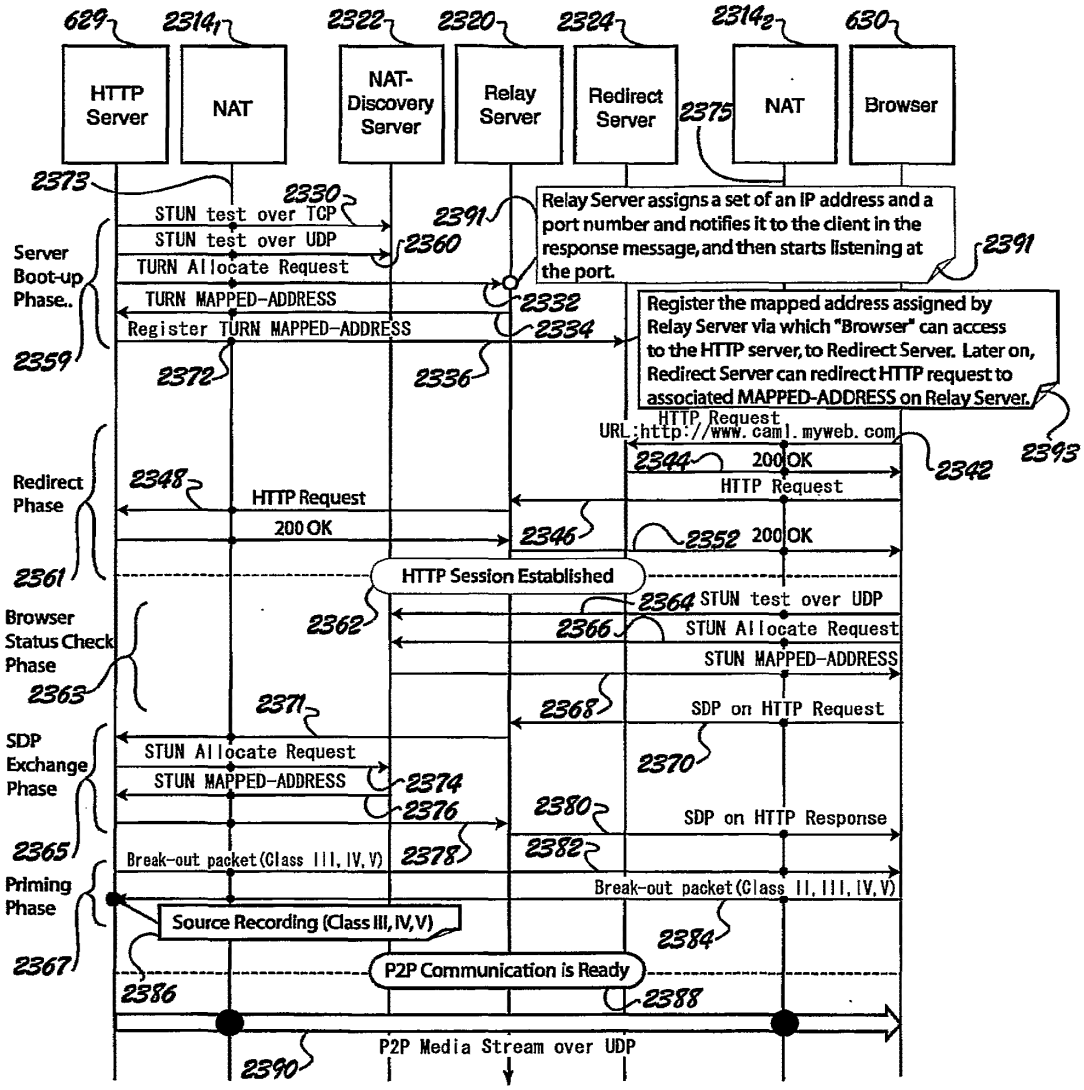

HTTP Server
NAT
NAT-Discovery Server
Relay Server
Redirect Server
NAT
Browser
STUN test over TCP
STUN test over UDP
TURN Allocate Request
TURN MAPPED-ADDRESS
Register TURN MAPPED-ADDRESS
Relay Server assigns a set of an IP address and a port number and notifies it to the client in the response message, and then starts listening at the port.
Register the mapped address assigned by Relay Server via which "Browser" can access to the HTTP server, to Redirect Server. Later on, Redirect Server can redirect HTTP request to associated MAPPED-ADDRESS on Relay Server.
Server Boot-up Phase..
HTTP Request
URL:http://www.cam1.myweb.com
200 OK
HTTP Request
Redirect Phase
HTTP Request
200 OK
200 OK
HTTP Session Established
STUN test over UDP
STUN Allocate Request
STUN MAPPED-ADDRESS
Browser Status Check Phase
SDP on HTTP Request
SDP Exchange Phase
STUN Allocate Request
STUN MAPPED-ADDRESS
SDP on HTTP Response
Break-out packet(Class III, IV, V)
Break-out packet(Class II, III, IV, V)
Priming Phase
Source Recording (Class III, IV, V)
P2P Communication is Ready
P2P Media Stream over UDP

FIG. 3

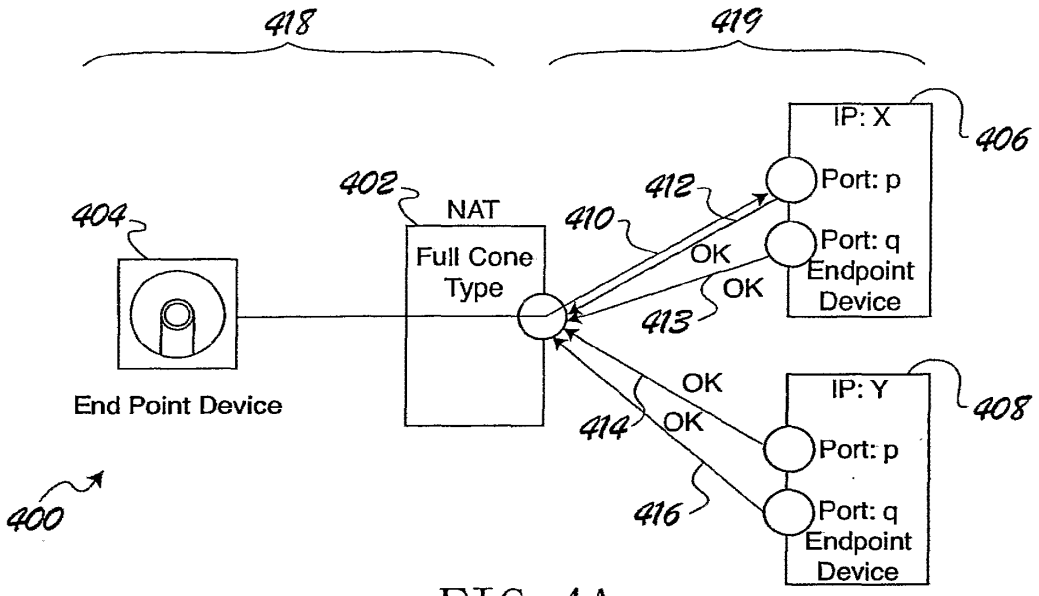


FIG. 4A
(Background Art)

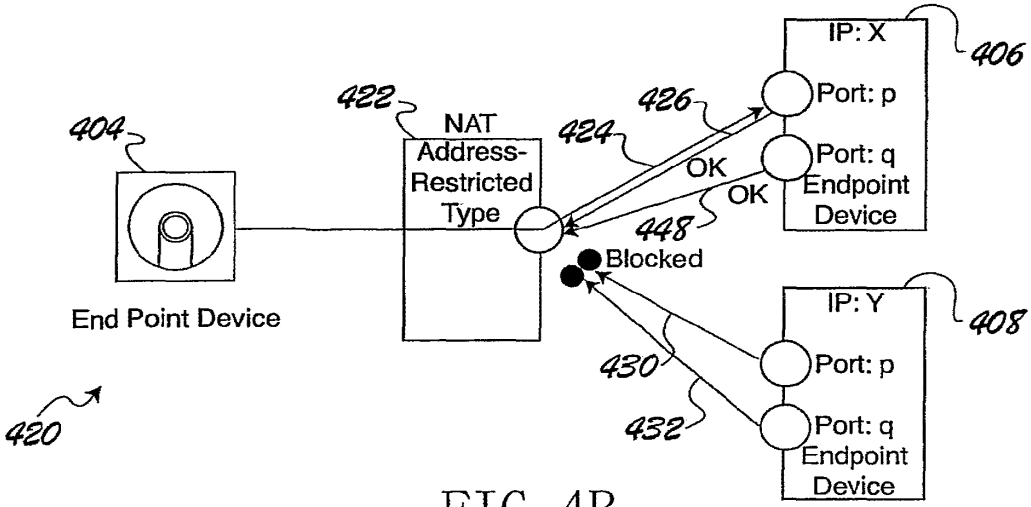


FIG. 4B
(Background Art)

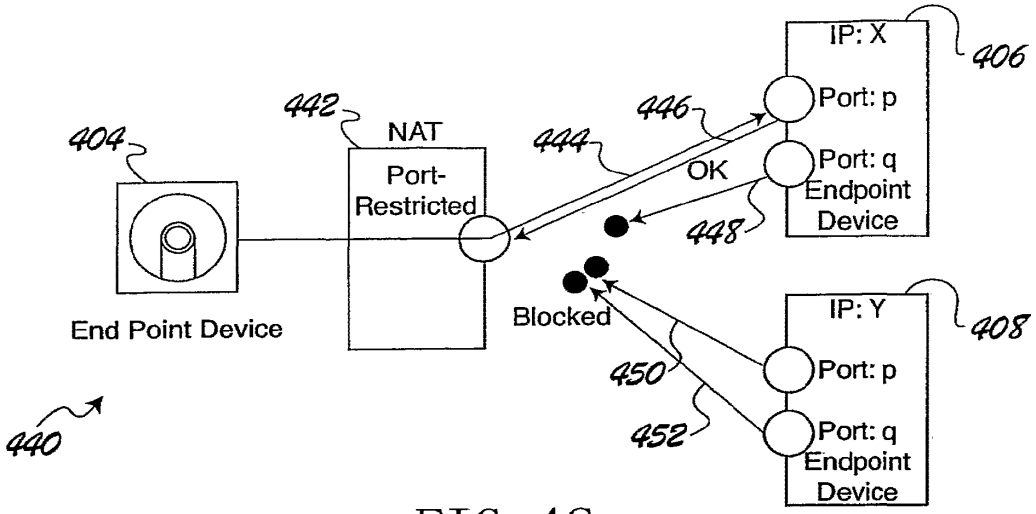


FIG. 4C
(Background Art)

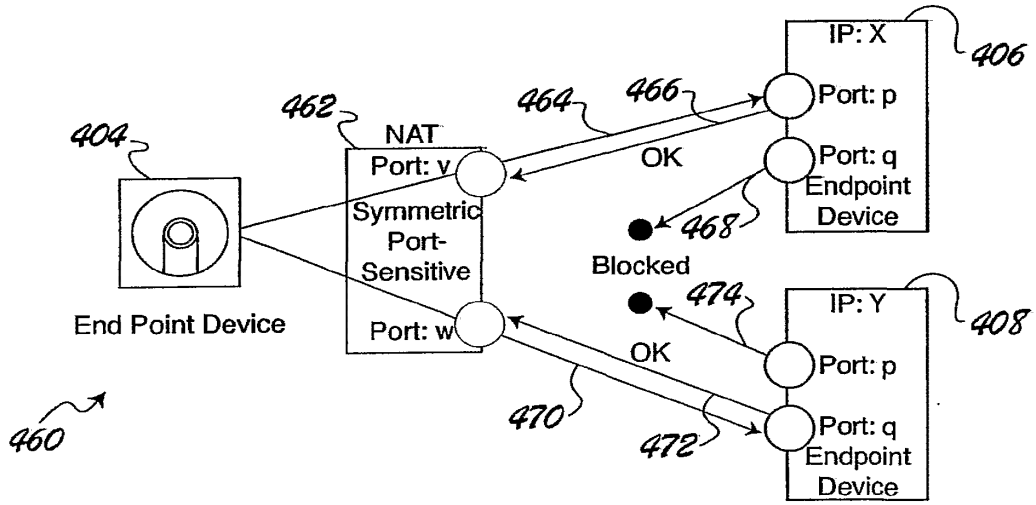


FIG. 4D
(Background Art)

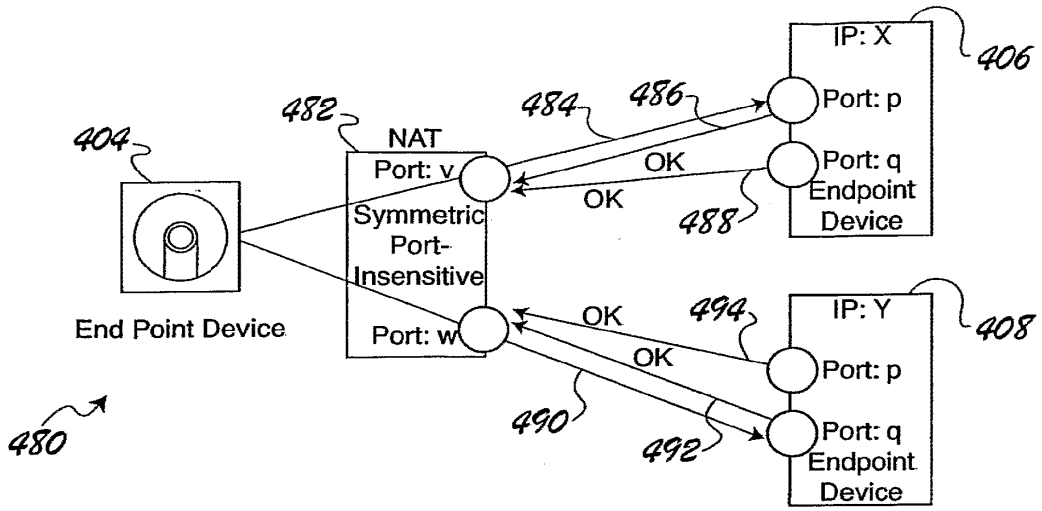


FIG. 4E
(Background Art)

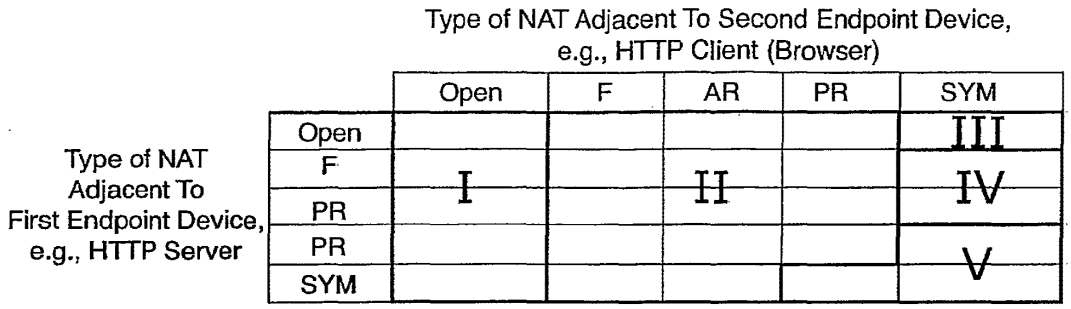

Type of NAT Adjacent To Second Endpoint Device, e.g., HTTP Client (Browser)
Open
F
AR
PR
SYM
Type of NAT Adjacent To First Endpoint Device, e.g., HTTP Server
Open
F
PR
PR
SYM
I
II
III
IV
V

FIG. 5A

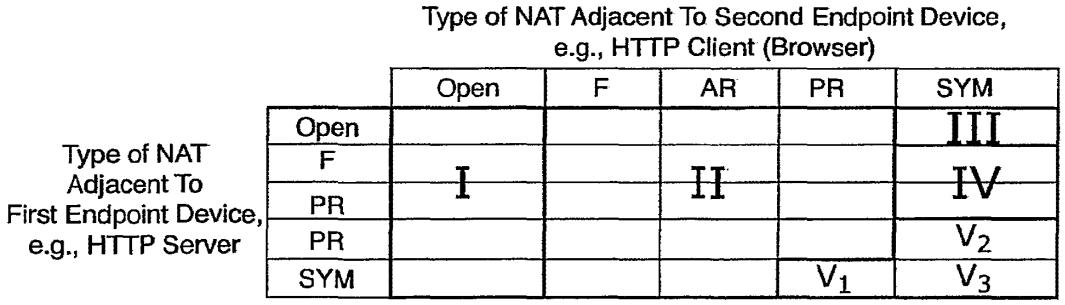

Type of NAT Adjacent To Second Endpoint Device, e.g., HTTP Client (Browser)
Open
F
AR
PR
SYM
Type of NAT Adjacent To First Endpoint Device, e.g., HTTP Server
Open
F
PR
PR
SYM
I
II
III
IV
V2
V1
V3

FIG. 5B

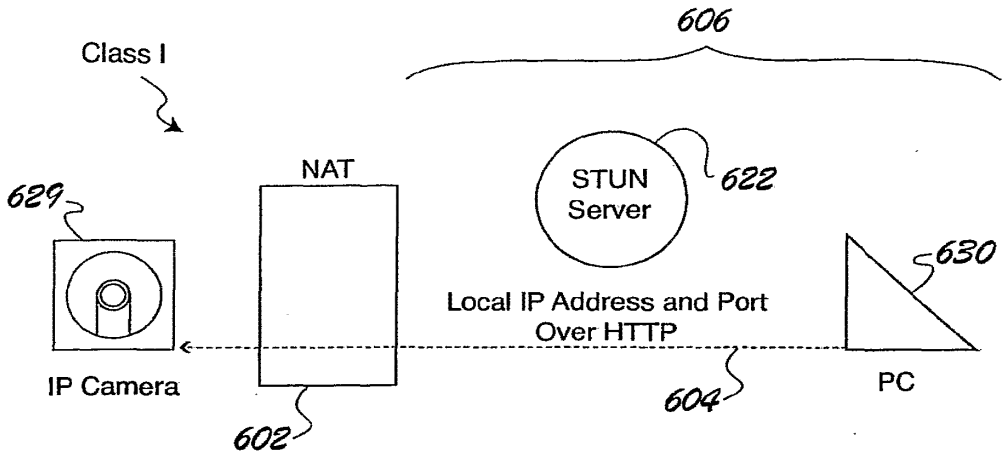

606
Class I
NAT
STUN
Server
622
629
630
Local IP Address and Port
Over HTTP
IP Camera
604
PC
602

FIG. 6A

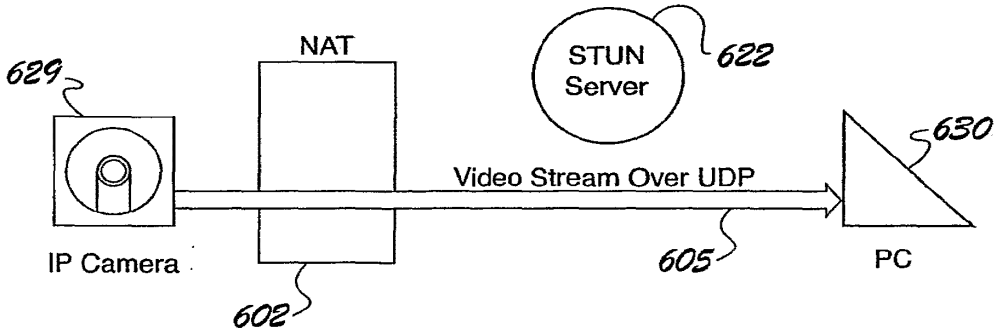

NAT
STUN
Server
622
629
630
Video Stream Over UDP
IP Camera
605
PC
602

FIG. 6B

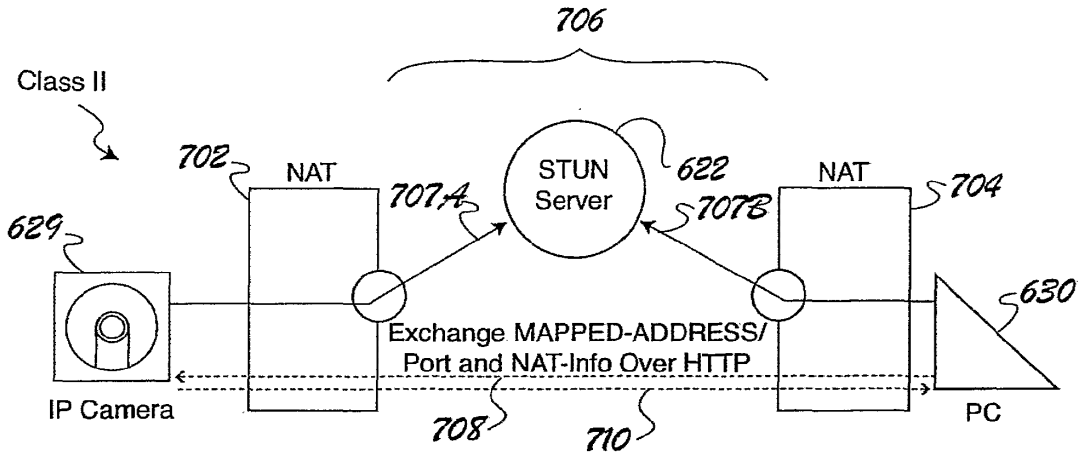


FIG. 7A

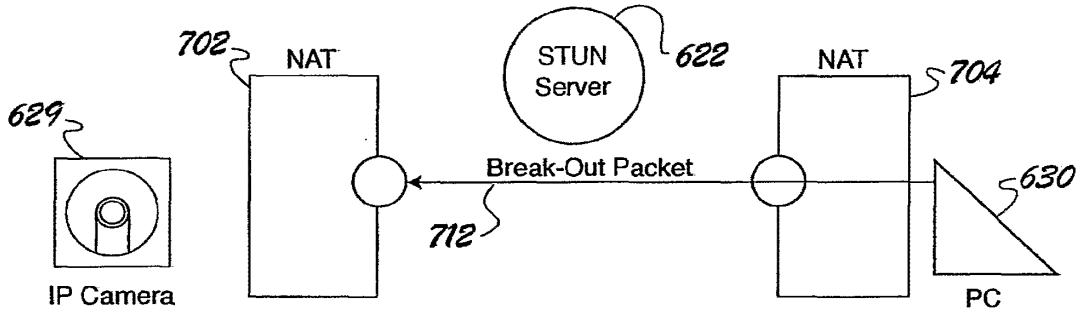


FIG. 7B

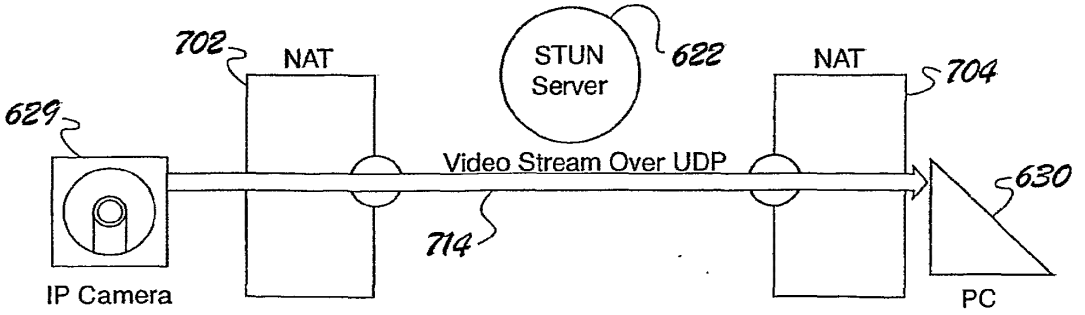


FIG. 7C

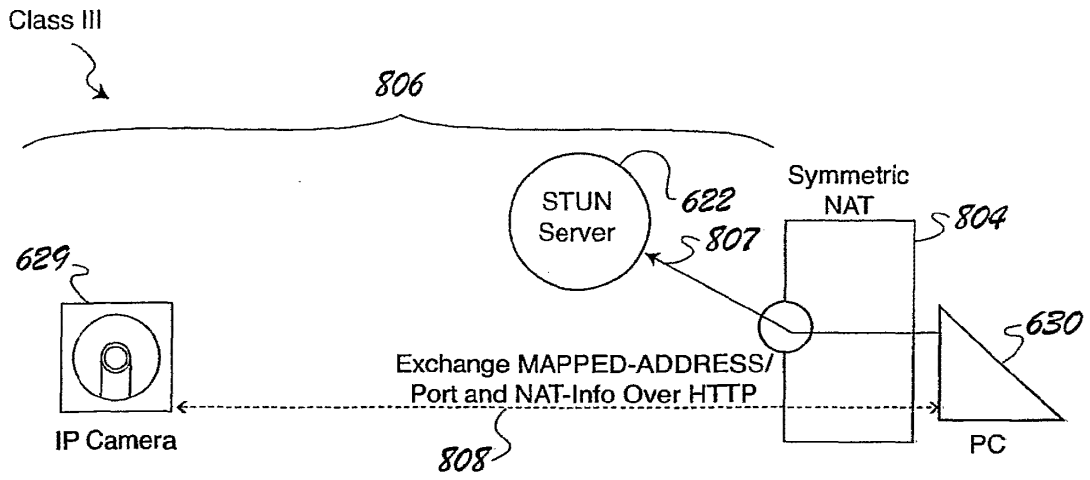


FIG. 8A

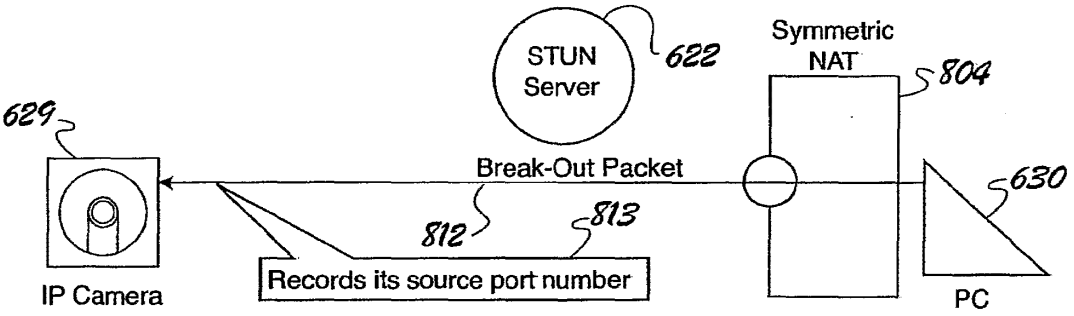


FIG. 8B

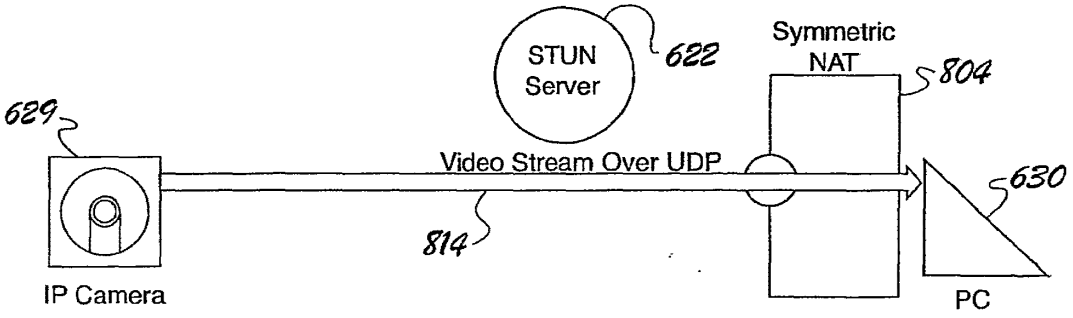


FIG. 8C

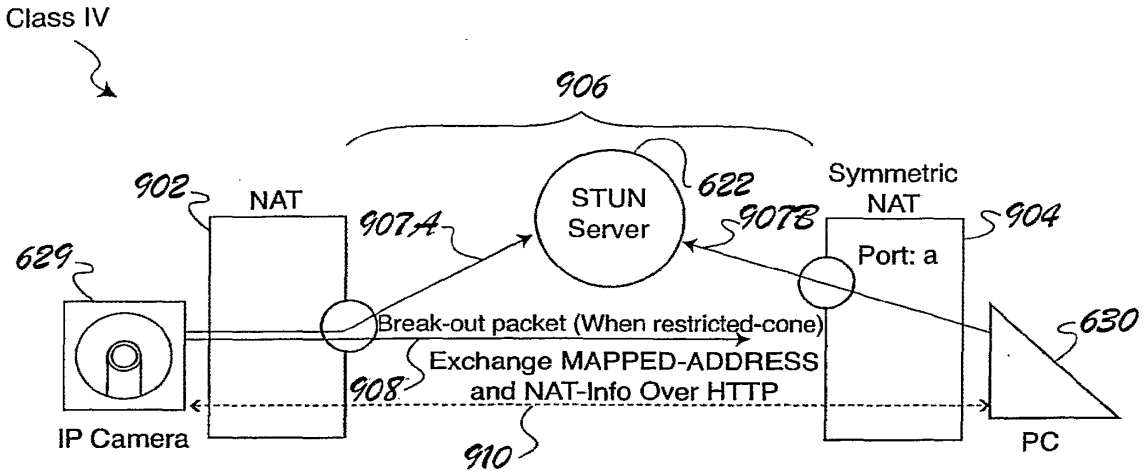


FIG. 9A

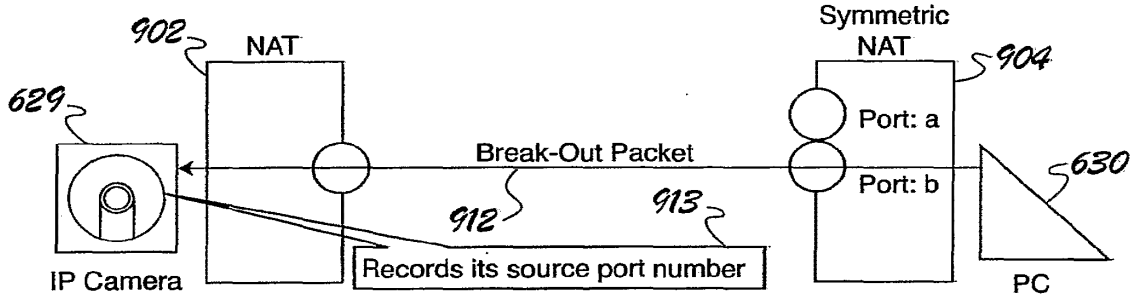


FIG. 9B

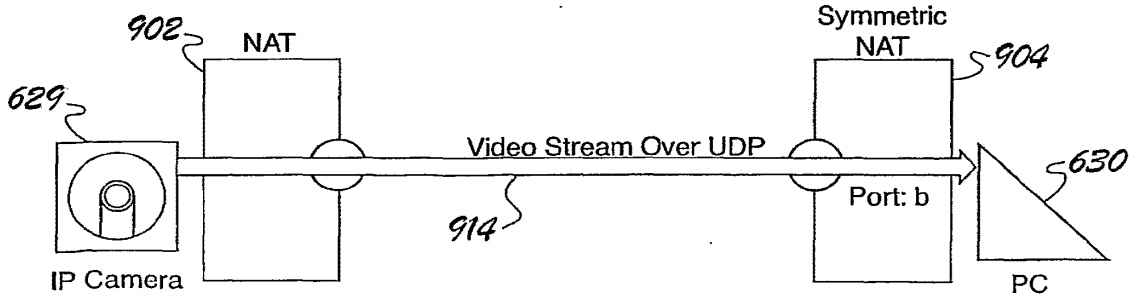


FIG. 9C

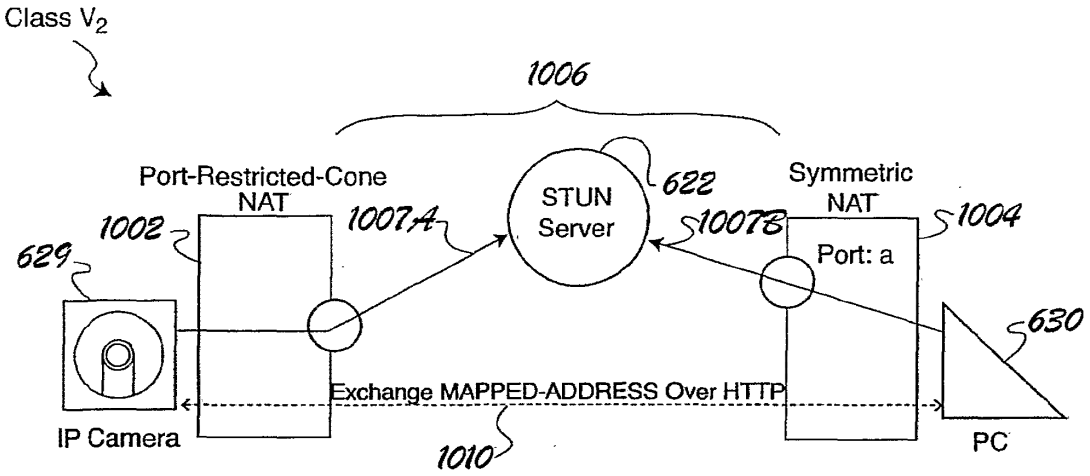


FIG. 10A

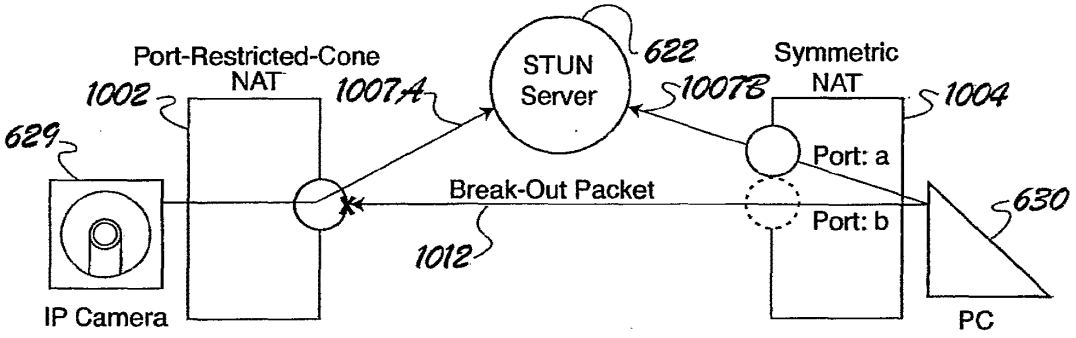


FIG. 10B

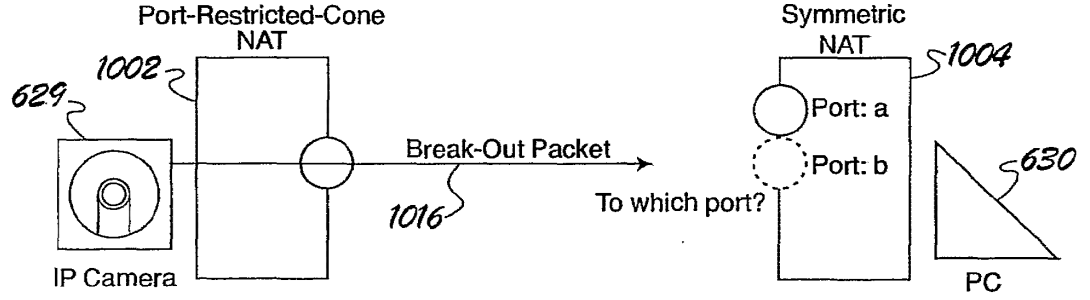


FIG. 10C

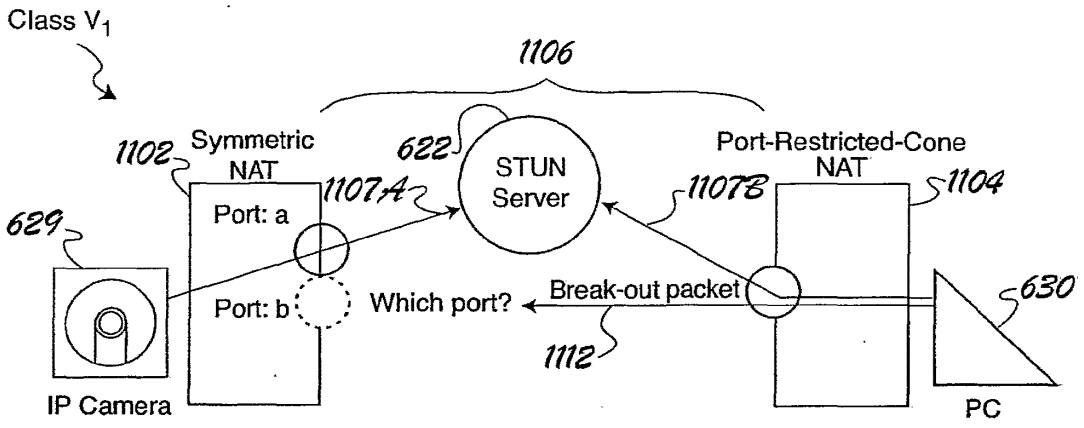

Class V_1
1106
1102
Symmetric NAT
622
STUN Server
Port-Restricted-Cone NAT
1104
1107A
1107B
629
Port: a
Port: b
Which port?
Break-out packet
1112
630
IP Camera
PC

FIG. 11

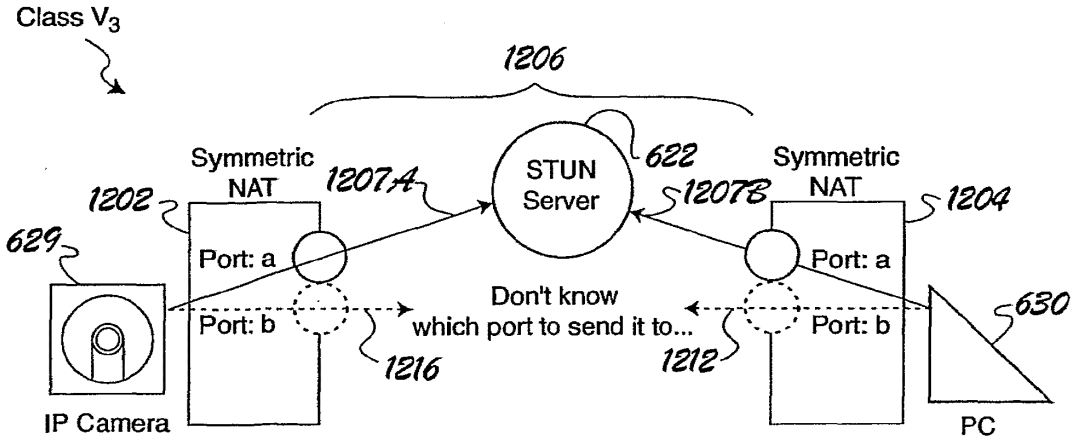

Class V_3
1206
622
Symmetric NAT
1207A
STUN Server
1207B
Symmetric NAT
1202
1204
629
Port: a
Port: a
Don't know
which port to send it to...
Port: b
Port: b
1216
1212
630
IP Camera
PC

FIG. 12

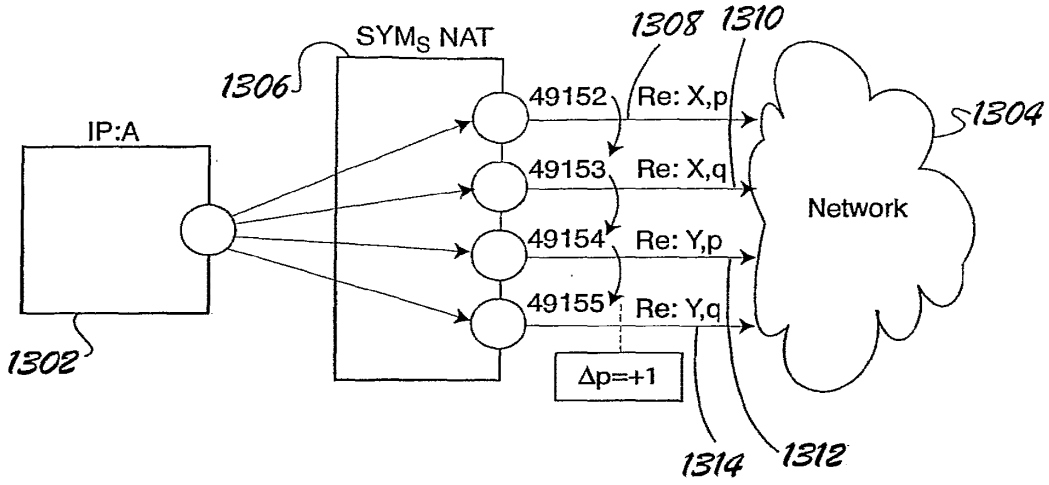


FIG. 13A

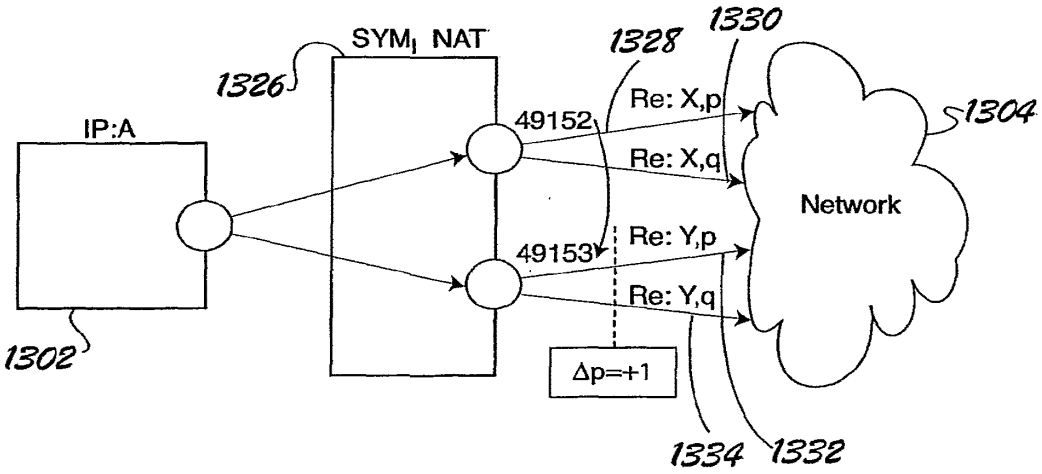


FIG. 13B

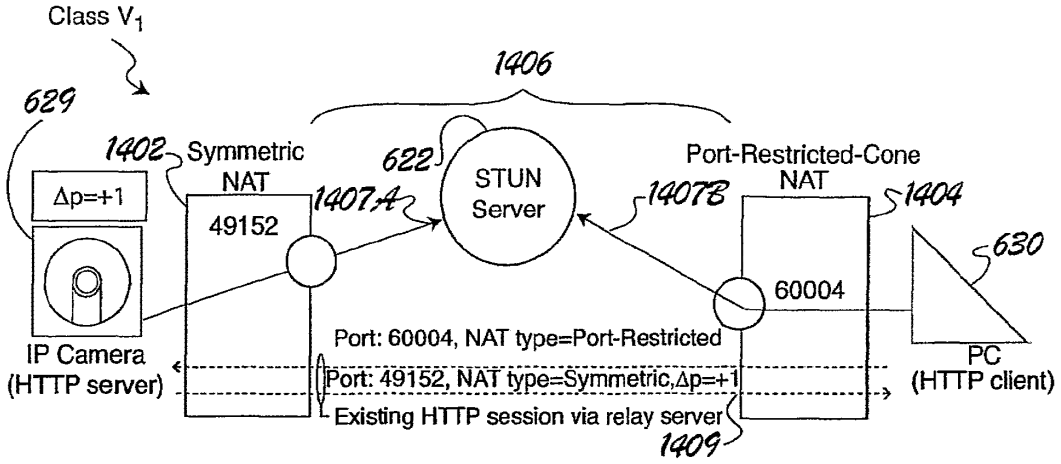


FIG. 14A

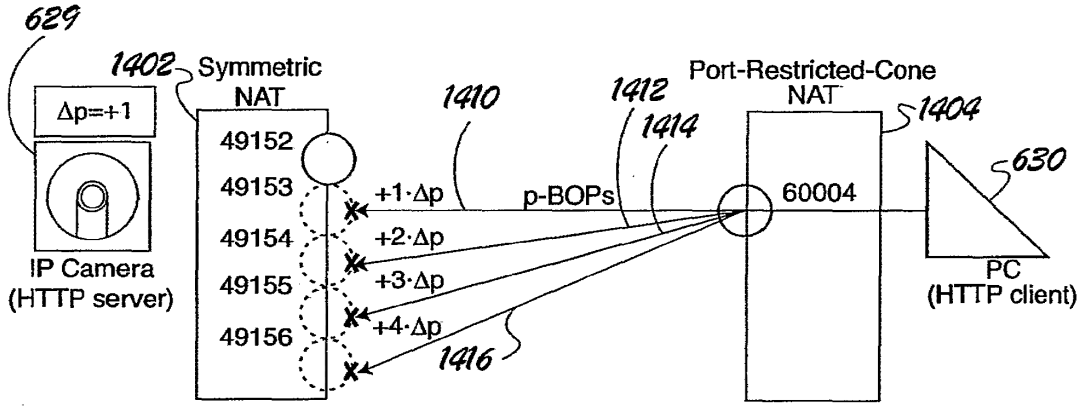


FIG. 14B

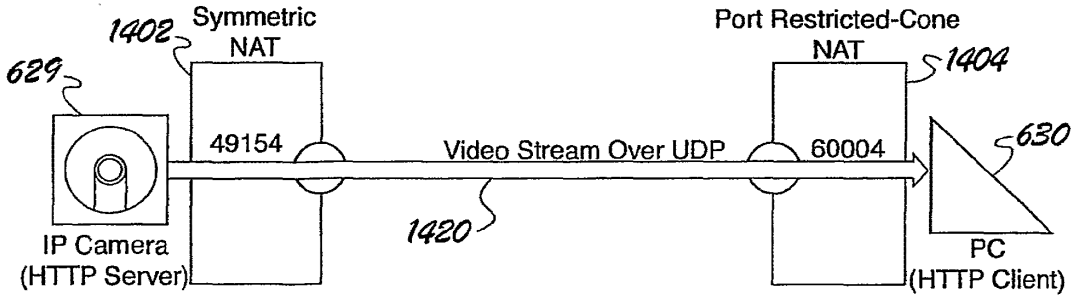


FIG. 14C

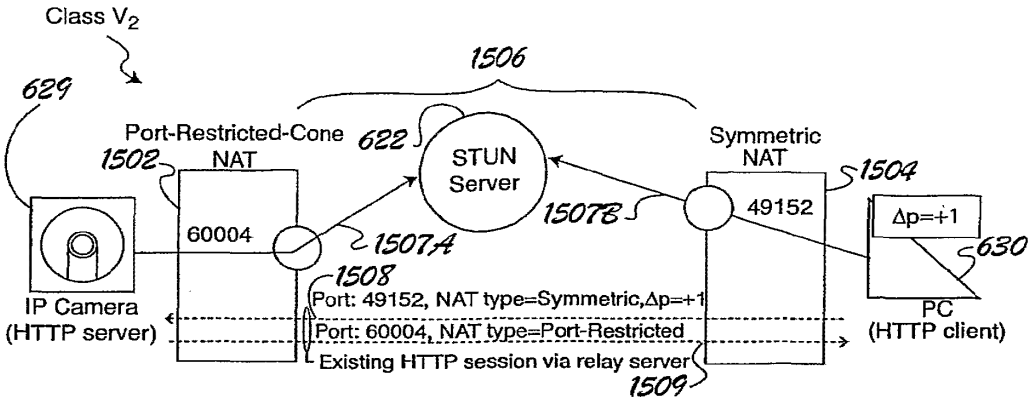


FIG. 15A

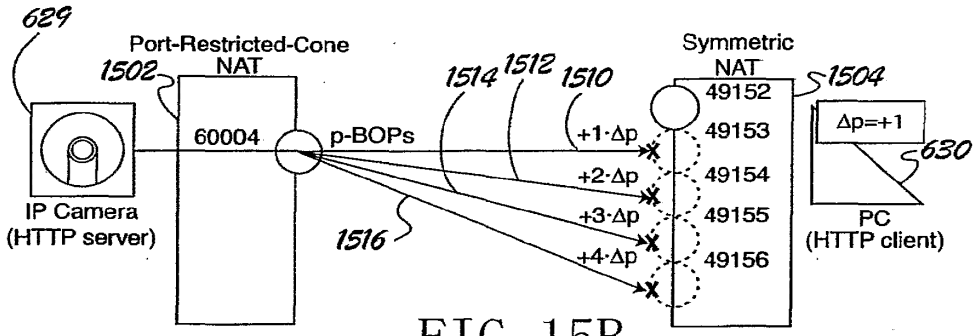


FIG. 15B

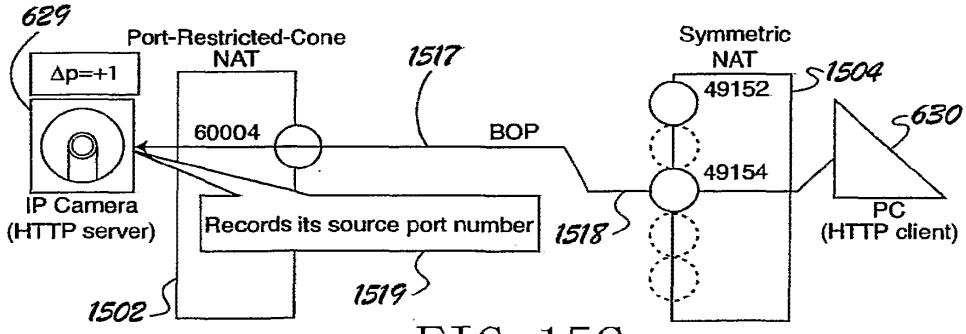


FIG. 15C

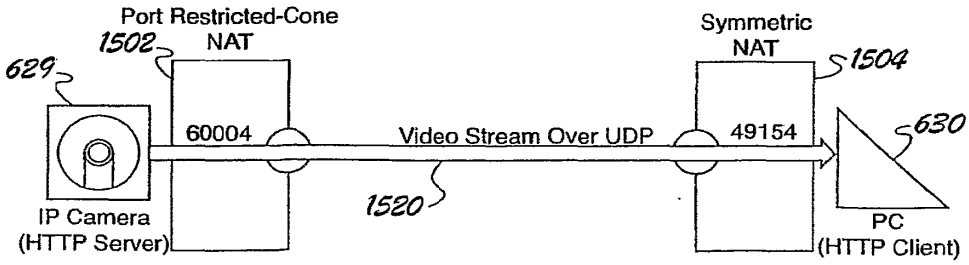


FIG. 15D

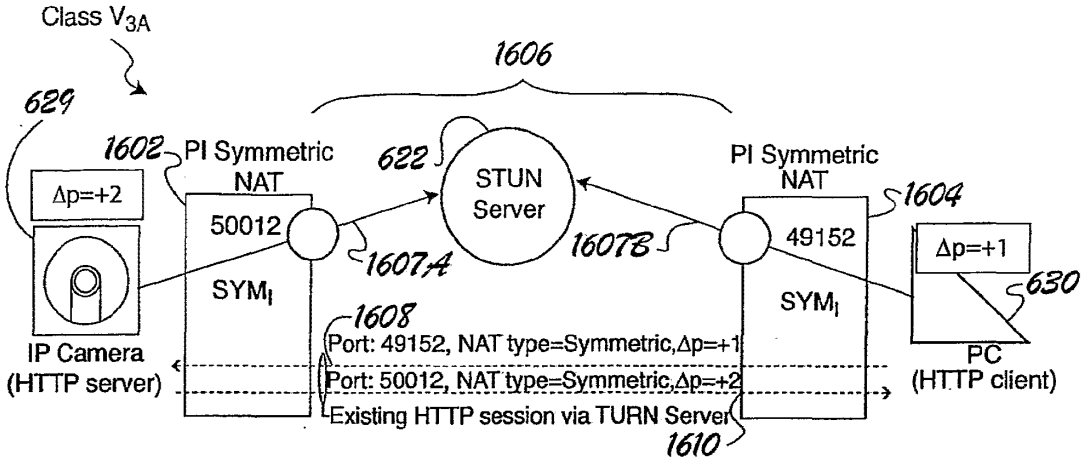


FIG. 16A

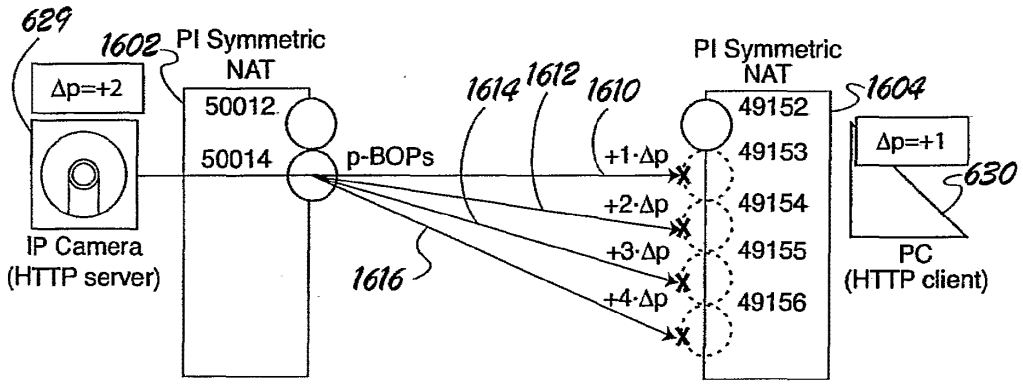


FIG. 16B

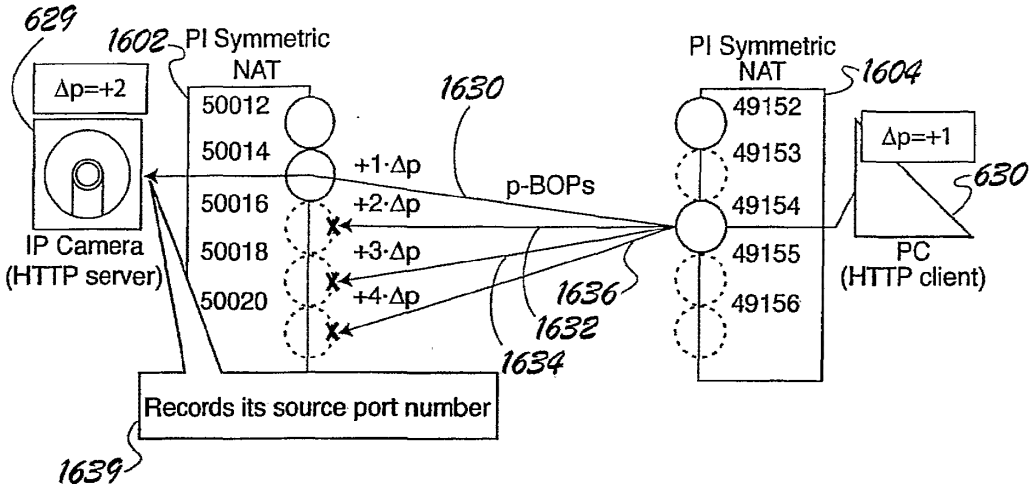


FIG. 16C

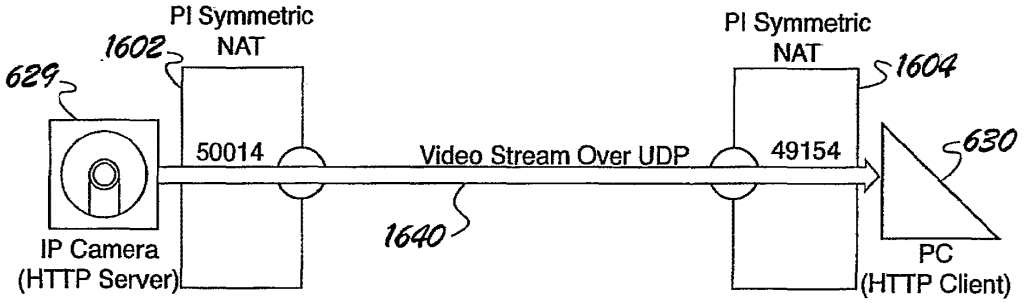


FIG. 16D

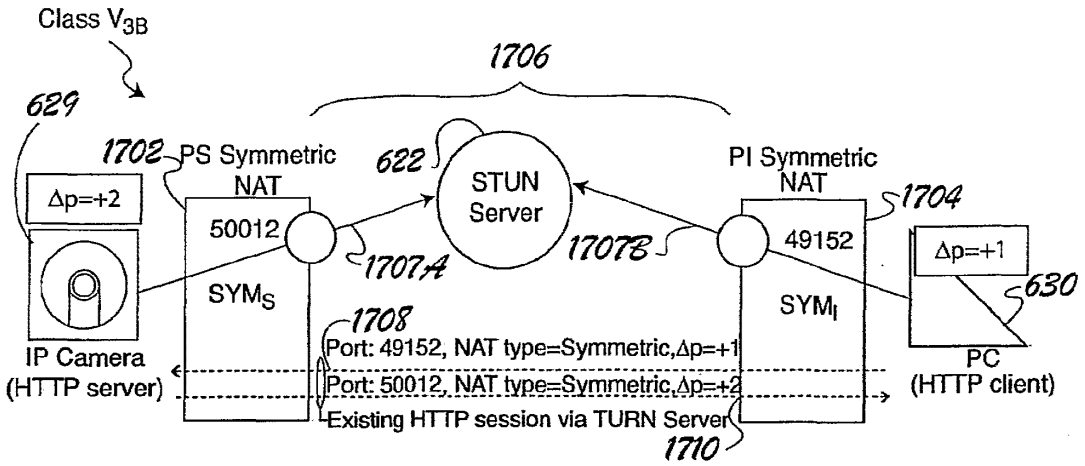


FIG. 17A

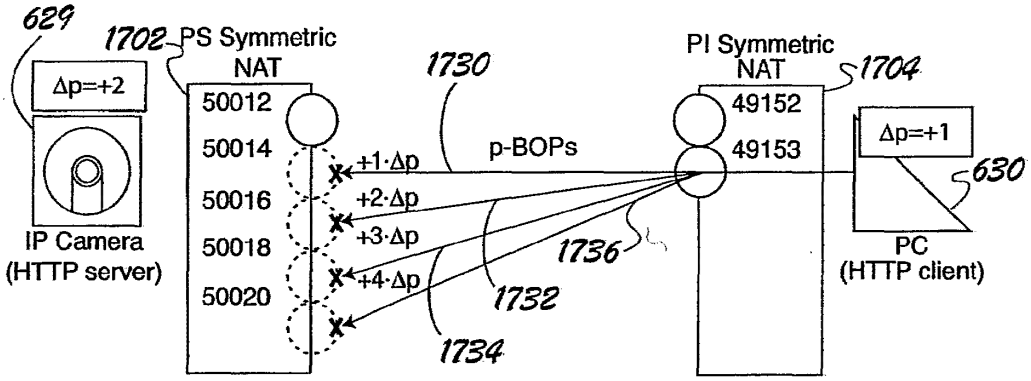


FIG. 17B

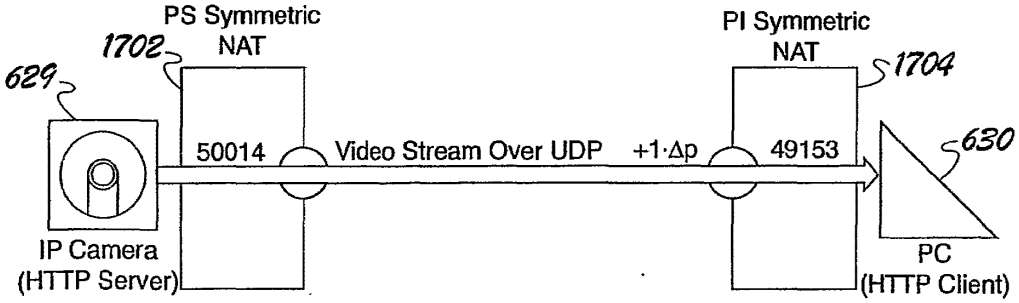


FIG. 17C

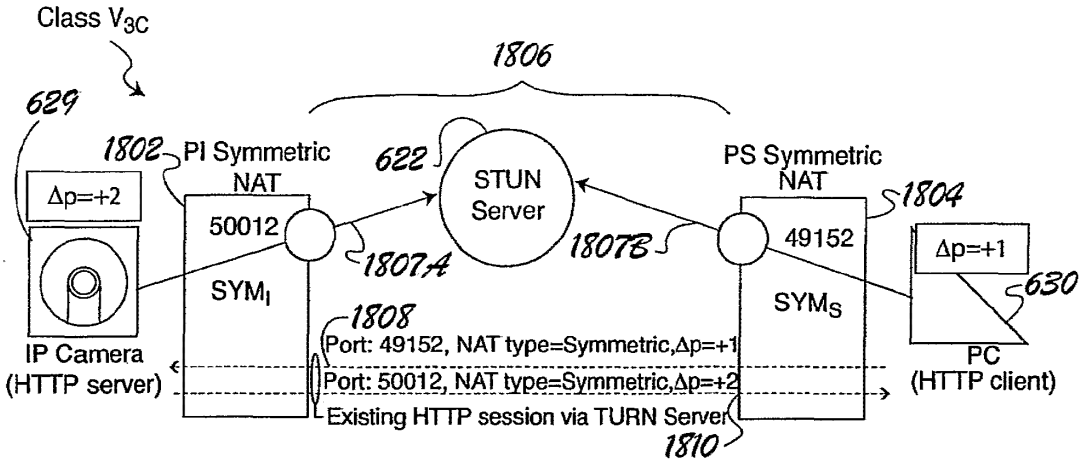


FIG. 18A

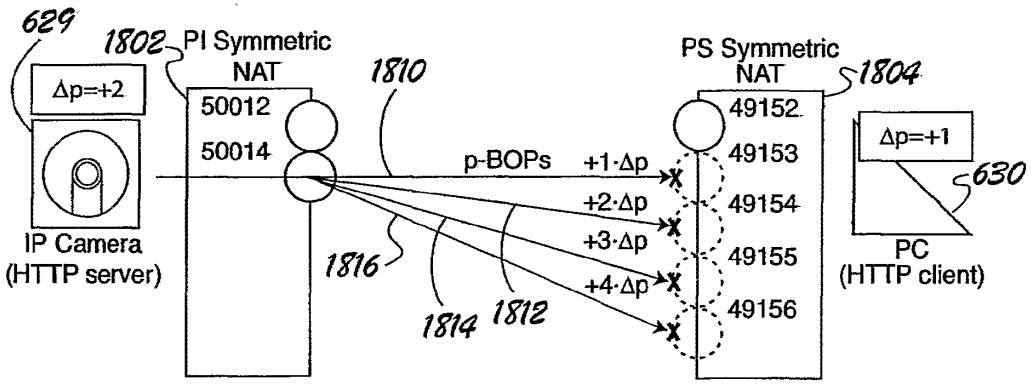


FIG. 18B

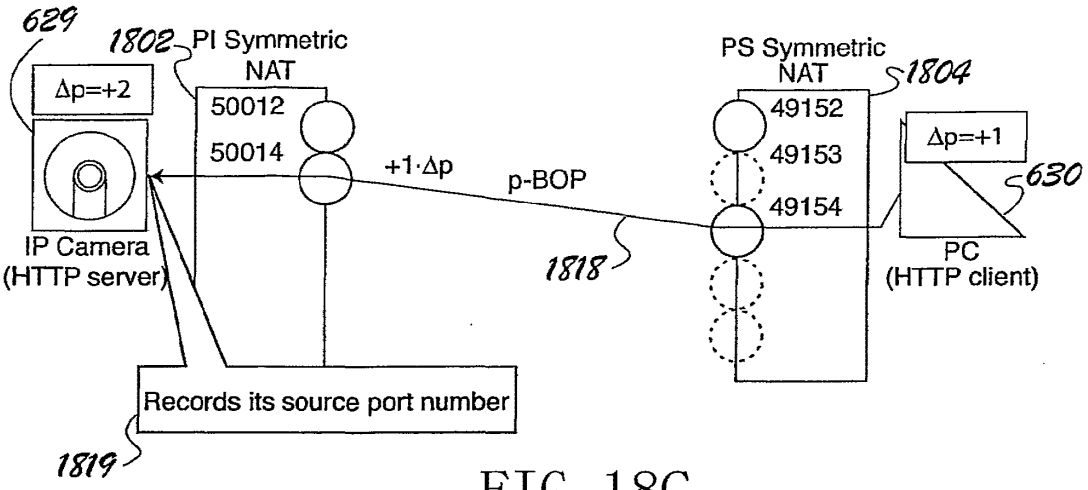


FIG. 18C

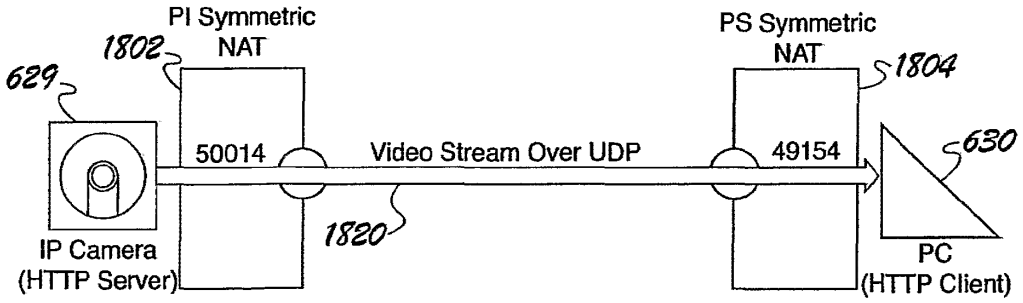


FIG. 18D

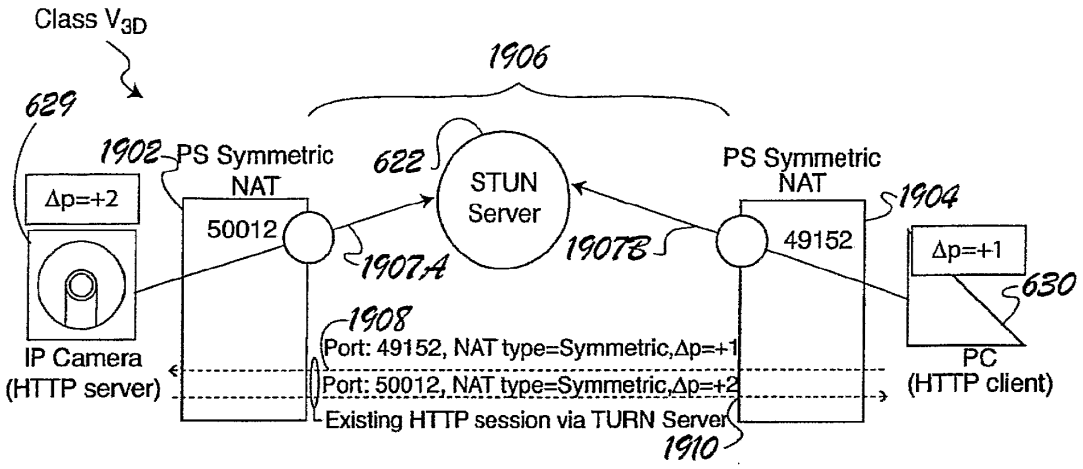


FIG. 19A

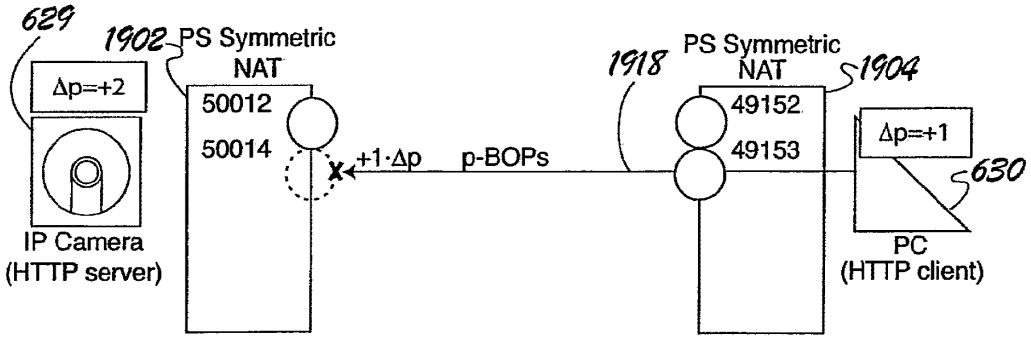


FIG. 19B

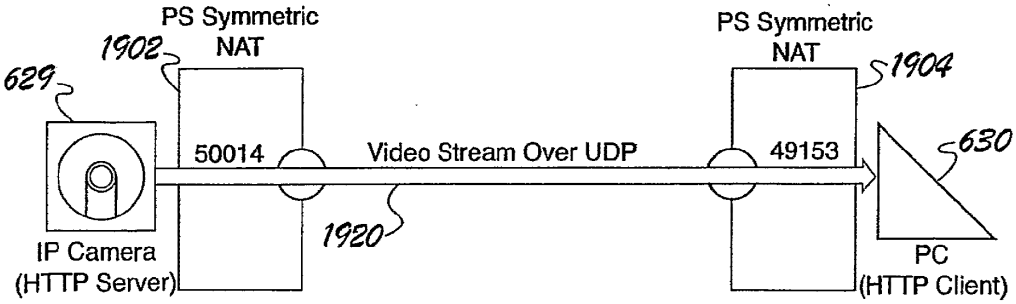


FIG. 19C

Class			Endpoint Server				Browser Client
			BOP	SR	Note	BOP	Note
I			-	-		-	
II			-	-		X	
III			-	X		X	Send a BOP repeatedly until it receives a packet.
IV						X	
V	V_1		-	-		X	Sends N p-BOPs to predetected ports with Dp, repeatedly until it receives a packet. (+n·Δp; n=1..N)
	V_2		X	X	May send N p-BOPs to subsequent ports. (+n·Δp; n=1..N)	X	Sends a p-BOP repeatedly until it receives a packet
	V_3	V_{3A}	X	X	May send N BOPs to predetected ports with Δp.. (+n·Δp; n=1..N)	X	Sends N p-BOPs to predetected ports with Dp, repeatedly until it receives a packet. (+n·Δp; n=1..N)
		V_{3B}	-	-		X	
		V_{3C}	X	X	May send N p-BOPs to subsequent ports. (+n·Δp; n=1..N)	X	Sends a p-BOP repeatedly until it receives a packet.
		V_{3D}	-	-		X	

SR: Source port recording

FIG. 20

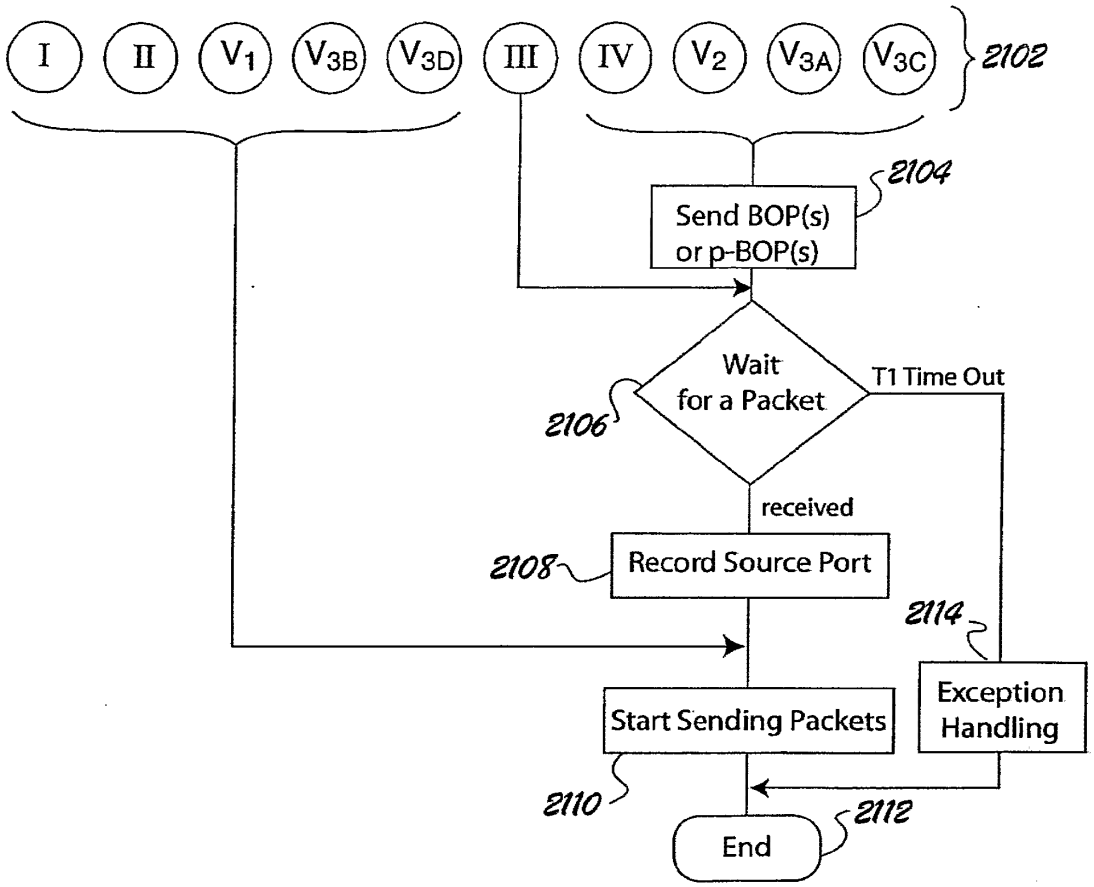

I
II
V1
V3B
V3D
III
IV
V2
V3A
V3C
2102
2104
Send BOP(s) or p-BOP(s)
Wait for a Packet
2106
T1 Time Out
received
2108
Record Source Port
2114
Exception Handling
Start Sending Packets
2110
2112
End

FIG. 21

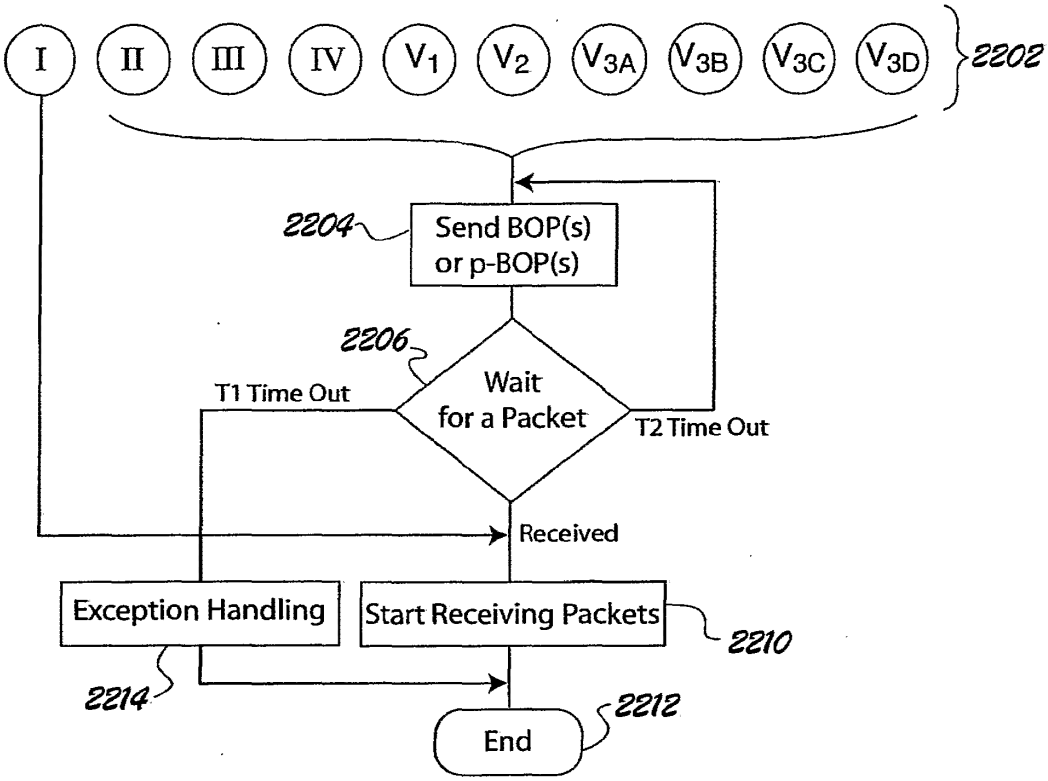

I
II
III
IV
V1
V2
V3A
V3B
V3C
V3D
2202
2204
Send BOP(s) or p-BOP(s)
2206
Wait for a Packet
T1 Time Out
T2 Time Out
Received
Exception Handling
Start Receiving Packets
2210
2214
2212
End

FIG. 22

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 January 2005 (27.01.2005)

PCT

(10) International Publication Number
WO 2005/009019 A2

(51) International Patent Classification[7]: H04M 7/00, 3/38, 15/00, H04L 29/06, 9/00

(21) International Application Number: PCT/IB2004/002282

(22) International Filing Date: 14 July 2004 (14.07.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/487,242 16 July 2003 (16.07.2003) US

(71) Applicant *(for all designated States except US)*: **SKYPER LTD.** [GB/GB]; 28-30 The Parade, St. Helier, Jersey FE4 8XY, Channel Islands (GB).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **HEINLA, Ahti** [EE/EE]; Juhkentali 8-5, EE10132 Tallinn (EE). **KASESALU, Priit** [EE/EE]; Mahtra 25-57, EE13811 Tallinn (EE).

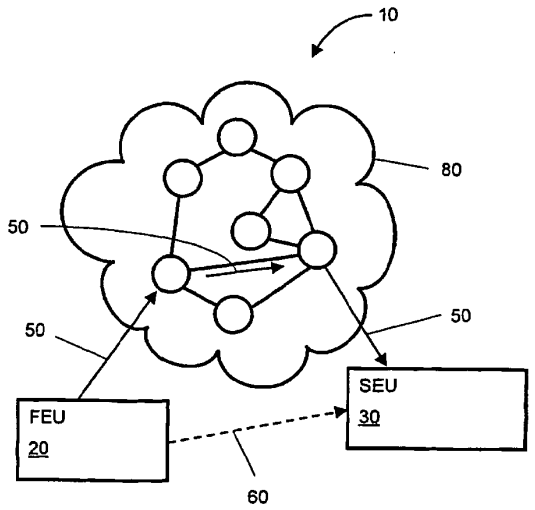
(74) Agent: **PLOUGMANN & VINGTOFT A/S**; Sundkrogsgade 9, Post Office Box 831, DK-2100 Copenhagen Ø (DK).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, 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, NA, 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 *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: PEER-TO-PEER TELEPHONE SYSTEM



(57) Abstract: There is provided a peer-to-peer telephone system (10) comprising a plurality of end-users (20, 30) and a communication structure (80) through which one or more end-users (20, 30) are couplable for communication purposes. The system (10) is distinguished in that: (a) the communication structure (80) is substantially de-centralized with regard to communication route switching therein for connecting said one or more end-users (20, 30); (b) said one or more end-users (20, 30) are operable to establish their own communication routes through the structure (80) based on exchange of one or more authorisation certificates, namely User Identity Certificates (UIC), to acquire access to the structure (80); and (c) said structure (80) includes an administration arrangement (100) for issuing said one or more certificates to said one or more end-users (20, 30).

WO 2005/009019 A2

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.

PEER-TO-PEER TELEPHONE SYSTEM

Field of the invention

The present invention relates to telecommunications systems, for example to telephone systems as well as to decentralized telecommunications systems operating according to a peer-to-peer principle. Moreover, the invention also relates to methods of operating such telephone systems and telecommunications systems.

Background to the invention

Contemporary telecommunications systems presently deployed, for example "public switched telephony network" (PSTN), mobile telephone and "Voice over Internet protocol" (VoIP), are substantially centralized in nature. They often employ central exchanges linked to users through trunk lines, local metro-rings and similar distribution structures. More recently, software-operated end-user devices have become available for connecting to such contemporary telephone systems, for example desk telephones, mobile telephones and VoIP devices. However, for performing almost any function offered by the telephony service provider, end-user devices are obliged to communicate with a central telephone exchange and/or branch exchange which executes one or more desired functions for them. In most cases, two end-user telephones of such a contemporary telephone system are not able to communicate directly to one another without a central exchange of the system linking the two end-user telephones together. For example, two people using their mobile telephones to converse together is facilitated by their two telephones communicating by radio via one or more mobile base stations, such base station communication being required even when the two people and their associated mobile telephones are in the same building. In another example, two people using "Voice over IP" software to converse together over the public Internet is facilitated by their software applications communicating via a central server, such server being required even though a connection can be established directly between the two people.

The use of centralized telephone systems places considerable demands on central switching exchanges. Such central exchanges are increasingly dependent on wide bandwidth optical connections employing dense wavelength division multiplexing (DWDM) with up to 120 optical channels distributed into wavelength bands of 50 GHz frequency spacing at an optical carrier frequency in the order of 300 THz. Such centralized exchanges are extremely costly and complex items of equipment which are susceptible to occasional malfunction, such malfunction potentially resulting in loss of communication traffic therethrough with potential corresponding compensation payments due to

customers. Moreover, the cost of operating such central exchanges scales proportionally with the number of end users.

The inventors of the present invention have appreciated that such a centralized approach is sub-optimal in many situations and that advantages arise from the deployment of other alternative telephone system architectures.

In order to address issues arising from adoption of such alternative architectures, the inventors have devised the present invention.

Summary of the invention

A first object of the invention is to provide a substantially decentralized telephone network system.

A second object of the invention is to provide such a decentralized telephone system in which subscriber authentication, network access control and accounting are performable in a more robust and reliable manner.

A third object of the invention is to provide a decentralised telephone system operable to reduce concentration of communication traffic therein by transferring responsible for establishing connections to end-users of the system.

According to a first aspect of the present invention, there is provided a peer-to-peer telephone system comprising a plurality of end-users and a communication structure through which one or more end-users are couplable for communication purposes, characterised in that:

(a) the communication structure is substantially de-centralized with regard to communication route switching therein for connecting said one or more end-users;

(b) said one or more end-users are operable to establish their own communication routes through the structure based on verification of one or more authorisation certificates to acquire access to the structure; and

(c) said structure includes administrating means for issuing said one or more certificates to said one or more end-users.

The invention is of advantage in that it is capable of addressing at least one of the aforementioned objects of the invention.

The invention is capable of addressing issues associated with less-centralized architectures, namely issues of control and user-authorisation, for example for billing/invoicing purposes to which the present invention is directed.

Preferably, in the system, the administrating means is operable to administer at least one of end-user sign-up and end-user payment for access to the communication structure.

More preferably, for example to try to circumvent unauthorised free and/or fraudulent use of the system, the administrating means is operable to generate one or more private-public key pairs, the administrating means being operable to maintain said one or more private keys secret and to distribute said one or more corresponding public keys within the system for certificate authentication purposes. Yet more preferably in the system, the administrating means is operable to generate private-public key pairs using a Rivest-Shamir-Adelman (RSA) method.

Preferably, for purposes of enhancing network robustness in the system, the structure includes a peer-to-peer communication network through which the end-users are mutually connectable. More preferably, the peer-to-peer network is implemented as a combination of interfacing nodes and storage nodes, said storage nodes being configured in one or more slots for database access purposes. Beneficially, the structure is implemented by way of a proprietary Global Index peer-to-peer network technology.

Preferably, in the system, the administrating means is arranged to perform one or more of:

(a) providing an end-user accounts database;
(b) providing a synchronizing time reference for the communication structure;
(c) providing globally-configurable settings for the system;
(d) providing peer discovery during bootstrap of the structure;
(e) handling new end-user registration; and
(f) monitoring operation of the structure for controlling desired modes of operation thereof.

Preferably, in the system, a plurality of end-users are operable to mutually exchange their authorisation certificates prior to commencing communication therebetween where at least one of said certificates is identified to be authentic.

Preferably, for example to assist adoption of the system in practice, the structure is arranged to support end-user free-trial use of the system, such free-trial use being subject to administration from the administrating means by repeated issuing of authorisations.

Ex.1002 / Page 338 of 1173
Cisco Systems, Inc.

Preferably, the administrating means is operable to invoice one or more end-users on a flat-fee rate substantially irrespective of use of the system exercised by said one or more end-users.

Preferably, in order to promote usage of the system in existing deployed equipment, the system is arranged to be configurable to operate concurrently with POTS and/or PSTN. Abbreviations POTS and PSTN correspond to "Plain Old Telephone System" and "Public Switch Telephone Network" respectively.

Preferably, the administrating means is implemented by way of one or more central computer servers. Such an implementation is especially beneficial when the system is configured in conjunction with the public Internet. Alternatively, the administrating means is otherwise susceptible to being implemented in a substantially de-centralized manner.

Preferably, the administrating means is operable to apply an heuristics fraud detection analysis of end-user registration and system usage data for detecting fraudulent access to the system by end-users.

According to a second aspect of the present invention, there is provided a method of operating a peer-to-peer telephone system comprising a plurality of end-users and a communication structure through which one or more end-users are couplable for communication purposes, characterised in that the method includes steps of:

(a) arranging for the communication structure to be substantially de-centralized with regard to communication route switching therein for connecting said one or more end-users;

(b) arranging for said one or more end-users to be operable to establish their own communication routes through the structure based on verification of one or more authorisation certificates to acquire access to the structure; and

(c) arranging for said structure to include administrating means for issuing said one or more certificates to said one or more end-users.

The method is of advantage in that its application to the system is capable of addressing at least one of the objects of the invention.

Preferably, in the method, the administrating means is operable to administer at least one of end-user sign-up and end-user payment for access to the communication structure.

Preferably, in the method, the administrating means is operable to generate one or more private-public key pairs, the administrating means being operable to maintain said one or more private keys secret and to distribute said one or more corresponding public keys within the system for certificate authentication purposes.

Preferably, in the method, the administrating means is operable to generate private-public key pairs using a Rivest-Shamir-Adelman (RSA) method. However, other approaches to private-public key generation are also susceptible to being used in the method.

Preferably, in the method, the structure includes a peer-to-peer communication network through which the end-users are mutually connectable. More preferably, the peer-to-peer network is implemented as a combination of interfacing nodes and storage nodes, said storage nodes being configured in one or more slots for database access purposes.

Preferably, in the method, the administrating means is arranged to perform one or more of:

(a) providing an end-user accounts database;
(b) providing a synchronizing time reference for the communication structure;
(c) providing globally-configurable settings for the system;
(d) providing peer discovery during bootstrap of the structure;
(e) handling new end-user registration; and
(f) monitoring operation of the structure for controlling desired modes of operation thereof.

Preferably, in the method, a plurality of end-users are operable to mutually exchange their authorisation certificates prior to commencing communication therebetween where at least one of said certificates is identified to be authentic.

Preferably, to encourage adoption of the system, the method is implemented such that the structure is arranged to support end-user free-trial use of the system, such free-trial use being subject to administration from the administrating means by repeated issuing of authorisations.

Preferably, in the method, the administrating means is operable to invoice one or more end-users on a flat-fee rate substantially irrespective of use of the system exercised by said one or more end-users.

Preferably, in order to encourage use of the system where existing telephone infrastructure exists, the method is implemented such that the system is arranged to be configurable to operate concurrently with POTS and/or PSTN. Abbreviations POTS and PSTN correspond to "Plain Old Telephone System" and "Public Switched Telephone Network" respectively.

Preferably, in the method, the administrating means is implemented by way of one or more central computer servers.

Ex.1002 / Page 340 of 1173
Cisco Systems, Inc.

Preferably, in order to avoid fraudulent use of the system when implementing the method, the administrating means is operable to apply an heuristics fraud detection analysis of end-user registration and system usage data for detecting fraudulent access to the system by end-users.

According to a third aspect of the present invention, there is provided software operable to implement at least part of the telephone system according to the first aspect of the invention.

According to a fourth aspect of the invention, there is provided software operable to execute at least part of the method according to the second aspect of the invention.

It will be appreciated that features of the invention are susceptible to being combined in any combination without departing from the scope of the invention.

Diagrams of embodiments of the invention

Embodiments of the invention will now be described, by way of example only, with reference to the following diagrams wherein:

Figure 1 is a schematic diagram of a telephone system according to the present invention; and

Figure 2 is a schematic representation of a per-to-peer structure of the system of Figure 1.

Description of embodiments of the invention

A telephone system according to the present invention is substantially a decentralised structure comprising a spatially distributed array of end-users connected by way of a peer-to-peer communication network. The structure is substantially devoid of any form of centralized exchange except for one or more administration nodes for performing some specific network administration functions such as subscriber sign-up and payment for communication network usage. In the decentralised structure, most routine functions, for example placing a telephone call, are handled entirely by end-user devices operable to communicate substantially directly to each other or via some form of local exchange such as an optical metro ring or distributed relay nodes on the public Internet.

In a system according to the present invention, the system indicated generally by 10 in Figure 1, a first end-user (FEU) 20 of the system 10 desiring to send a message to a second end-user (SEU) 30 thereof adopts a method of communication as follows:

(a) the first end-user 20 locates the second end-user 30; such location is executed by way of peer-to-peer technologies, for example using a "Global Index" (GI) proprietary peer-to-peer technology which will be described later and/or contemporary "Distributed Hash Table" technology, arranged to provide node look-up functionality;

(b) the first end-user 20 receives information regarding the address of the second end-user 30 and also details of one or more communication path-ways 50, 60 which may be used for making a connection from the first end-user 20 to the second end-user 30; and

(c) the first end-user 10 then follows a protocol to establish the one or more communication pathways 50, 60 to the second end-user 30.

In the GI peer-to-peer technology, there is provided a network of participating nodes interlinked through a distributed communication network. The participating nodes are allocated to be either interfacing nodes or storage nodes. Preferably, the number of storage nodes is arranged to be considerably less than the number of interfacing nodes, for example 100 times more interfacing nodes than storage nodes. Moreover, the storage nodes are responsible for storing data records whereas the interfacing nodes are responsible for processing queries and sending requests to the storage nodes for sending data records therefrom in response to the queries. Moreover, the interfacing nodes are also responsible for receiving data records to be stored and determining one or more appropriate groups of storage nodes to receive the data records for storage therein. The storage nodes are arranged in groups known as slots wherein association of a given storage node with a particular slot is dependent upon address data held in each of the storage nodes. The GI technology is described in a patent application approximately contemporary with the present patent application, the contents of the GI technology patent application herewith being incorporated by reference for purposes of describing the telephone system of the present invention.

In the system 10, there is a considerable requirement for subscriber authentication, access control and accounting. Using major system functions of the system 10 is only possible if one or more end-users thereof have paid or otherwise have authorized access to such functions. In a contemporary conventional telephone system, end-user access to one or more major system functions is checked by a central office thereof in a manner of centralised control. In contradistinction, in the system 10, access is checked by end-user devices using public-key cryptography. In such cryptography, each end-user, also referred to as subscriber, has associated therewith a cryptography key pair which is created by the end-user's device. Upon subscriber sign-up or payment, a central office of

Ex.1002 / Page 342 of 1173
Cisco Systems, Inc.

the system 10 issues to the subscriber a digital certificate, such certificate also being referred to as a User Identity Certificate (UIC), whereby the central office certifies that the owner of this key pair is an authorised subscriber.

In step (c) of the aforementioned method, when the first end-user 20 communicates with other subscriber devices, namely the second end-user 30, the first end-user 20 provides the certificate, namely the aforementioned UIC, as a proof of subscription. In the system 10, end-user devices are arranged to refuse to mutually communicate where there exists an absence of such proof of subscription. Moreover, using public-key cryptography, end-user devices of the system 10 are arranged to be operable to verify each other's certificates (UIC's) without needing to communicate with the aforesaid central office of the system 10 responsible for issuing certificates (UIC's). The system 10 thus functions in a de-centralized manner on account of the end-users 20, 30 not needing to communicate with the central office of the system 10 when establishing a communication route between the end-users 20, 30.

When a subscribing device of the system, for example the first end-user 20, has located a recipient, for example the second end-user 30, they will subsequent need to mutually communicate. Such communication is preferably by a direct route, for example along the path-way 60 illustrated in Figure 1. However, for example for reasons of spatial separation and/or terrain, such a direct route is not always technically feasible; for example, if communication is desired from the first end-user 20 to the second end-user 30 via the public Internet, such communication is not feasible when the second end-user 30 has a private address that is not accessible from outside a local network of the system 10. In a situation where direct communication is not feasible, the system 10 is operable to route communication via one or more peer nodes in its peer-to-peer structure 80 to assist the first and second end-users 20, 30 to mutually communicate. These one or more peer nodes are preferably implemented by subscriber devices that need not necessarily belong to the first and second end-users 20, 30 involved in making a telephone call therebetween. Thus, for example, in such a scenario where direct connection is not feasible, a subscriber communicates to another device that is directly accessible, and this other device communicates directly with the final recipient.

Architectural aspects of the system 10 will now be described in further detail. The peer-to-peer structure 80 is subdivided into two sections as illustrated in Figure 2, namely central servers (CS) 100 on the one hand and a peer-to-peer network (P2PN) 110 on the other hand.

The central servers 100 are preferably operated by the proprietor of the structure 80. These servers 100 are arranged to execute one or more of the following tasks:

(i) providing an end-user accounts database for recording end-users' accounting details;

(ii) providing a synchronizing time reference for the structure 80;

(iii) providing globally-configurable settings for the system 10;

(iv) providing peer discovery during bootstrap of the structure 80 and handling new end-user registration;

(v) electronically signing critical information pertinent to the system 10, for example signing end-user identities as described in the foregoing, for example the aforementioned User Identity Certificates (UIC's), using digital signatures using secret cryptographic keys known only to the proprietor of the system 10;

(vi) providing add-on services from one or more of the proprietor's infrastructure, rented infrastructure and outsourced infrastructure; and

(vii) monitoring operation of the central servers 100 and the network 110 for ensuring desired modes of operation thereof.

The add-on services referred in (vi) above relate to one or more of:

(1) "Public Switched Telephone Network" (PSTN) and/or "plain old telephone system" (POTS) connectivity, to "Voice over Internet Protocol " (VoIP) traffic termination and reverse thereof, for example from POTS to the proprietor's system 10;

(2) handling "Instant Message" (IM) to "Short Message Service" (SMS) connectivity; and

(3) handling end-user conferencing, voicemail and similar activities couplable to back-end servers included within the central servers 100.

The peer-to-peer network 110 preferably comprises end-user computing devices arranged to execute thereon software provided by the proprietor of the system 10. The network 110 is also preferably based on a version of the aforementioned GI protocol customized by the proprietor of the system 10. The network 110 is operable to perform functions preferably including one or more of:

(a) administering end-user buddy lists;

(b) handling end-user preferences, for example buddy online/offline notification;

(c) providing end-user identification by way of one or more of the following: node identification (ID), username, end-user profile data;

(d) maintaining basic statistics, for example a number of end-users currently actively communicating within the system 10; and

(e) maintaining firewall and/or "Network Address Translation" (NAT) traversal via random peer nodes within the network 110 functioning as ad hoc proxies supporting communication therethrough.

In (c) above pertaining to the peer-to-peer network 110, the username is effectively useable as a "telephone number" within the system 10. Moreover, the end-user profile data relates to data records if provided by the end-users, such records including one or more of: real name (e.g. Roger Smith, Annie Hansen), spatial location (e.g. Washington USA; Copenhagen, Denmark), date of birth and e-mail address.

The inventors have appreciated that operation of the system 10 is dependent on security provided by, for example, the use of public key encryption therein. In devising the system 10, the inventors have further anticipated that a peer-to-peer IM/VoIP system is inherently less secure than POTS or any comparable telephone system reliant on one or more central servers; as in the foregoing, abbreviations IM, VoIP and POTS refer to "Instant Messaging", "Voice over Internet Protocol" and "Plain Old Telephone System" respectively. In the system 10, the inventors have arranged for the use of contemporary Rivest-Shamir-Adelman (RSA) public key encryption and associated digital signatures to cater for most basic security requirements within the system 10. However, it will be appreciated that other types of public-private key encryption are susceptible to being employed in the system 10.

Upon an end-user, for example one of the end-users 20, 30, seeking registration at the central servers 100, the end-user proceeds to generate a RSA encryption key pair, namely complementary private and public keys wherein said private key is not derivable from said public key and vice versa. The end-user's public key appears in the User Identity Certificate (UIC) provided to the end-user, whereas the private key is stored locally at the end-users premises.

During a call set-up from the first end-user 20 to the second end-user 30, similarly during an Instant Message (IM) sending, prior to commencing communication, both end-users 20, 30 present their User Identity Certificate (UIC), or Temporary Identification Number (TIN) where the system 10 is set up to accept these, as appropriate to the other; if they have a user name, they present their UIC. If a UIC is presented from a primary one of the end-users 20, 30 to a secondary one thereof, the secondary end-user verifies the signature provided by the primary end-user, such verification not requiring any contact with the central servers 100. Moreover, the secondary end-user verifies that the primary end-user has the corresponding secret key by issuing a challenge data packet for the primary end-user's public key and checks that the primary end-user is capable of decrypting it. After completion of such activities, the primary end-user is in a position to safely believe that the primary end-user legitimately has the username it claims to hold.

When calls are made within the system 10, additional checking is required because calls require payment unless permission for a limited trial period has been granted. In the system 10, it is difficult to monitor in a secure manner duration of calls or number of calls

made; in this respect, the inventors have appreciated that it is advantageous to employ a time-based subscription as a basis of billing/invoicing within the system 10. Thus, in order to implement such time-based subscription, User Identity Certificate (UIC) privileges are checked and non-trial calls are not communicated through the peer-to-peer network 110 if neither of the end-users 20, 30 in the above example has a User Identity Certificate (UIC) with non-expired subscription privileges. In other words, a call will propagate through the peer-to-peer network 110 if one or more of the end-users 20, 30 has a valid subscription or trial.

To keep their subscriptions from expiring, end-users of the system 10 are obliged to renew their User Identity Certificate (UIC) periodically for instance by paying a fee for a coming month/year; it will be appreciated that other payment periods are possible or that UICs may be extended based on other criteria than payment. Upon receipt of renewal payments, the central servers 100 are operable to issue new UIC's in response in the earlier end-users' names, the new UIC's having associated new subscription privilege expiry details. When credit/debit card billing/invoicing has been authorised by one or more of the end-users of the system 10, billing/invoicing is susceptible to being performed automatically by the central servers 100 without the need for associated end-user intervention.

Thus, in the system 10, a preferred method of payment for calls made is by flat-fee monthly or yearly subscription entitling the user to an unlimited number of calls in the system 10. Such a billing/invoicing arrangement is acceptable in the system 10 from a business perspective because calls made do not incur operating expenses to the proprietor of the system 10 as central exchange resources are substantially not utilized when making such calls. In contradistinction, calls to or from POTS/PSTN incur real per-minute operating costs and are therefore appropriately charged separately and distinctly from calls made according to the invention in the system 10.

When the peer-to-peer structure 80 is implemented in the manner of the aforementioned GI protocol, the end-users 20, 30 in Figure 1 together with other end-users not shown, the central servers 100 and the peer-to-peer network 110 are effectively participating nodes. In such a configuration, each end-user advertises its presence to GI storage nodes by periodically sending thereto its information about its identity or Temporary Identification Number (TIN) when the system 10 is configured to accept such TIN's. When one or more end-users make GI queries, for example akin to telephone directory enquiries, the storage nodes are responsive to send such stored User Identity Certificates (UIC) or Temporary Identification Numbers (TIN) as data packets in response to such queries.

In the case of UIC's, corresponding data packets despatched by the GI storage nodes are received at end-users which sign off the data packets with their end-user private keys;

Ex.1002 / Page 346 of 1173
Cisco Systems, Inc.

one or more querying end-users are thereby capable of verifying authenticity of the data packets received thereat, for example in response to making an enquiry, using a corresponding public key. Such an arrangement is advantageous because it is substantially capable of guaranteeing that no-one is able to fake User Identity Certificate (UIC) end-user directory entries. The rationale of such an approach is that a participating node who owns a User Identity Certificate (UIC) is operable, for example when advertising its presence, to send its private-key-signed data packets corresponding to its UIC to one or more storage nodes and another participating node if required. The signed UIC received from one or more of the storage nodes and stored therein for subsequent release is verifiable at an enquiring participating node by using a corresponding public key. Such an arrangement is capable of circumventing tampering with UIC and even faked UIC's.

The system 10 is further provided with a free-trial facility, such a facility being of commercial advantage for purposes of attracting new end-users to the system 10. Preferably, such a free-trial facility pertains to X_1 free days or, alternatively or additionally, X_2 free calls. For such free-trial days or calls, the central servers 100 are required to provide explicit permission for each free call made. Preferably, all permissions given or requested are recorded in a database of the system 10, for example for heuristic fraud detection purposes as described later. If the end-user has already used up free days and/or free calls allocated thereto, permission is not granted from the central servers 100 and the end-user is subsequently requested to pay if it still desires to make calls within the system 10.

The system 10 is capable of being operated concurrently within, or in combination with, a conventional telephone system, for example a conventional telephone system capable of implementing the Internet.

The aforementioned free-trial permission scheme is intended by the inventors only to pertain to the system 10. For conventional paid subscription calls undertaken in connection with the system 10, a normal conventional subscription regime applies and per-call permissions are neither requested nor recorded. For PSTN calls, a free-trial scheme does not pertain although it is potentially capable of being provided in connection with the system 10.

For each free-call permission request received in the system 10, the central servers 100 are operable to record at least one of the following parameters with regard to a call:

(a) calling end-user's identity in the form of a username or Temporary Identification Number (TIN);

(b) calling end-user's computer identification (ID);

(c) calling end-user's Internet Protocol (IP) address;

(d) called end-user's identity in the form of a username or TIN;
(e) called end-user's computer ID;
(f) called end-user's IP address;
(g) time and date of the call;
(h) whether or not permission was granted for the call.

Thus, in the system 10, a "trial user" explicit status is not accommodated; preferably, there is merely a need for an end-user to make some free calls from a defined starting date D. Any end-user is entitled to make free calls if its first free calls were less than X_1 days ago (or the end-user has not yet exercised a free-call option within the system 10). Alternatively, the system 10 may be set up in such a way as to allow a free-trial period to consist of X number of free calls as opposed to X days.

Hacked version of system 10 software enables fraudulent end-users to omit free-trial permission asking and permission checking provisions employed within the system 10. However, on account of the system 10 implementing both calling end-user and called end-user permission checking, such hacking only enables fraudulent end-users to call other fraudulent end-users free of charge; in other words, pirated fraudulent end-user software is only capable of providing very limited benefit when employed on the system 10. In many cases, such limited fraudulent use of the system 10 can be accommodated without significant financial loss to the proprietor of the system 10.

The inventors have appreciated that a major opportunity of fraud exists in the system 10 when a hacker attempts to fake a username or computer ID and repetitively starts new free trials. Such a major opportunity of fraud requires the hacker to omit from system 10 compatible software all local shareware-type checks. In order to counteract such fraud, the central servers 100 are programmed to perform heuristic fraud detection to identify repetitive fraud patterns. For example, the central servers 100 are operable to detect a fraudulent end-user seeking free-call provisions Z times and then subsequently seeking with the same IP address and new computer ID for new free-call permission to call the same people. Since explicit permission for free calls in the system 10 is required from the central servers 100, there is considerable information available within the system 10 for input to such heuristics fraud detection software executing within the system 10. However, the inventors are aware that such heuristics fraud detection is unlikely to detect all cases of hacking occurring within the system 10.

It will be appreciated that embodiments of the invention described above are susceptible to being modified without departing from the scope of the invention.

In the foregoing, the system 10 is described as being able to support the use of Temporary Identification Numbers (TINs). However, the system 10 is capable of being

Ex.1002 / Page 348 of 1173
Cisco Systems, Inc.

modified so that TINs are not utilized therein, such that user names and associated User Identity Certificates (UIC's) with associated time-limited substantially cost-free privileges are employed for free-trial purposes. If required, the system 10 is even susceptible to being configured so that free-trial usage as described earlier is not provided to end-users; alternatively, other arrangements for free trials can be utilized, for example reimbursement of initial paid subscription fee.

The system 10 is preferably implemented, at least in part, using software executable on computing hardware. Such software can be distributed to users via a communication network such as the Internet and/or via the software stored on a suitable data carrier such as a CD ROM supplied to users.

In the foregoing description of embodiments of the invention relating to the telephone system 10, it will be appreciated that the invention is relevant to telecommunications systems in general and the term "telephone" should therefore be construed accordingly. Specifically, other forms of communication susceptible to being performed with the system include video calls, conference calls and text messaging.

In the foregoing, terms such as "contain", "include", comprise", "have", "has", "is", "are", "incorporate" and "encompass" are intended to be construed as being non-exclusive, namely other items not disclosed are also potentially present.

CLAIMS

1. A peer-to-peer telephone system (10) comprising a plurality of end-users (20, 30) and a communication structure (80) through which one or more end-users (20, 30) are couplable for communication purposes, characterised in that:

(a) the communication structure (80) is substantially de-centralized with regard to communication route switching therein for connecting said one or more end-users (20, 30);

(b) said one or more end-users (20, 30) are operable to establish their own communication routes through the structure (80) based on verification of one or more authorisation certificates to acquire access to the structure (80); and

(c) said structure (80) includes administrating means (100) for issuing said one or more certificates to said one or more end-users (20, 30).

2. A system (10) according to Claim 1, wherein the administrating means (100) is operable to administer at least one of end-user sign-up and end-user payment for access to the communication structure (80).

3. A system (10) according to Claim 1 or 2, wherein the administrating means (100) is operable to generate one or more private-public key pairs, the administrating means (100) being operable to maintain said one or more private keys secret and to distribute said one or more corresponding public keys within the system (10) for certificate authentication purposes.

4. A system (10) according to Claim 3, wherein the administrating means (100) is operable to generate private-public key pairs using a Rivest-Shamir-Adelman (RSA) method.

5. A system (10) according to Claim 1, 2, 3 or 4, wherein the structure (80) includes a peer-to-peer communication network (110) through which the end-users (20, 30) are mutually connectable.

6. A system (10) according to Claim 5, wherein the peer-to-peer network (110) is implemented as a combination of interfacing nodes and storage nodes, said storage nodes being configured in one or more slots for database access purposes.

7. A system (10) according to any one of the previous claims, wherein the administrating means (100) is arranged to perform one or more of:

(a) providing an end-user (20, 30) accounts database;

(b) providing a synchronizing time reference for the communication structure (80);
(c) providing globally-configurable settings for the system (10);
(d) providing peer discovery during bootstrap of the structure (80);
(e) handling new end-user (20, 30) registration; and
(f) monitoring operation of the structure (80) for controlling desired modes of operation thereof.

8. A system (10) according to any one of the preceding claims, wherein a plurality of end-users are operable to mutually exchange their authorisation certificates prior to commencing communication therebetween where at least one of said certificates is identified to be authentic.

9. A system (10) according to any one of the preceding claims, wherein the structure (80) is arranged to support end-user free-trial use of the system (10), such free-trial use being subject to administration from the administrating means (10) by repeated issuing of authorisations.

10. A system (10) according to any one of the preceding claims, wherein the administrating means (100) is operable to invoice one or more end-users (20, 30) on a flat-fee rate substantially irrespective of use of the system (10) exercised by said one or more end-users (20, 30).

11. A system (10) according to any one of the preceding claims arranged to be configurable to operate concurrently with POTS and/or PSTN.

12. A system (10) according to any one of the preceding claims, wherein the administrating means (100) is implemented by way of one or more central computer servers.

13. A system (10) according to any one of the preceding claims, wherein the administrating means (100) is operable to apply an heuristics fraud detection analysis of end-user registration and system (10) usage data for detecting fraudulent access to the system (10) by end-users (20, 30).

14. A method of operating a telephone system (10) comprising a plurality of end-users (20, 30) and a communication structure (80) through which one or more end-users (20, 30) are couplable for communication purposes, characterised in that the method includes steps of:
(a) arranging for the communication structure (80) to be substantially de-centralized with regard to communication route switching therein for connecting said one or more end-users (20, 30);

(b) arranging for said one or more end-users (20, 30) to be operable to establish their own communication routes through the structure (80) based on exchange of one or more authorisation certificates to acquire access to the structure (80); and

(c) arranging for said structure (80) to include administrating means (100) for issuing said one or more certificates to said one or more end-users (20, 30).

15. A method according to Claim 1, wherein the administrating means (100) is operable to administer at least one of end-user sign-up and end-user payment for access to the communication structure (80).

16. A method according to Claim 14 or 15, wherein the administrating means (100) is operable to generate one or more private-public key pairs, the administrating means (100) being operable to maintain said one or more private keys secret and to distribute said one or more corresponding public keys within the system (10) for certificate authentication purposes.

17. A method according to Claim 16, wherein the administrating means (100) is operable to generate private-public key pairs using a Rivest-Shamir-Adelman (RSA) method.

18. A method according to Claim 14, 15, 16 or 17, wherein the structure (80) includes a peer-to-peer communication network (110) through which the end-users (20, 30) are mutually connectable.

19. A method according to Claim 18, wherein the peer-to-peer network (110) is implemented as a combination of interfacing nodes and storage nodes, said storage nodes being configured in one or more slots for database access purposes.

20. A method according to any one of Claims 14 to 19, wherein the administrating means (100) is arranged to perform one or more of:

(a) providing an end-user (20, 30) accounts database;

(b) providing a synchronizing time reference for the communication structure (80);

(c) providing globally-configurable settings for the system (10);

(d) providing peer discovery during bootstrap of the structure (80);

(e) handling new end-user (20, 30) registration; and

(f) monitoring operation of the structure (80) for controlling desired modes of operation thereof.

21. A method according to any one of Claims 14 to 20, wherein a plurality of end-users are operable to mutually exchange their authorisation certificates prior to

commencing communication therebetween where at least one of said certificates is identified to be authentic.

22. A method according to any one of Claims 14 to 21, wherein the structure (80) is arranged to support end-user free-trial use of the system (10), such free-trial use being subject to administration from the administrating means (10) by repeated issuing of authorisations.

23. A method according to any one of the Claims 14 to 22, wherein the administrating means (100) is operable to invoice one or more end-users (20, 30) on a flat-fee rate substantially irrespective of use of the system (10) exercised by said one or more end-users (20, 30).

24. A method according to any one of Claims 14 to 23 wherein the system (10) is arranged to be configurable to operate concurrently with POTS and/or PSTN.

25. A method according to any one of the preceding Claims 14 to 24, wherein the administrating means (100) is implemented by way of one or more central computer servers.

26. A method according to any one of Claims 14 to 25, wherein the administrating means (100) is operable to apply an heuristics fraud detection analysis of end-user registration and system (10) usage data for detecting fraudulent access to the system (10) by end-users (20, 30).

27. Software for implementing at least a part of the system (10) according to Claim 1.

28. Software executable on computing hardware for implementing one or more steps of the method according to Claim 14.

29. Software according to Claim 27 or 28 communicable to end-users (20, 30) via a communication network and/or stored on a data carrier.

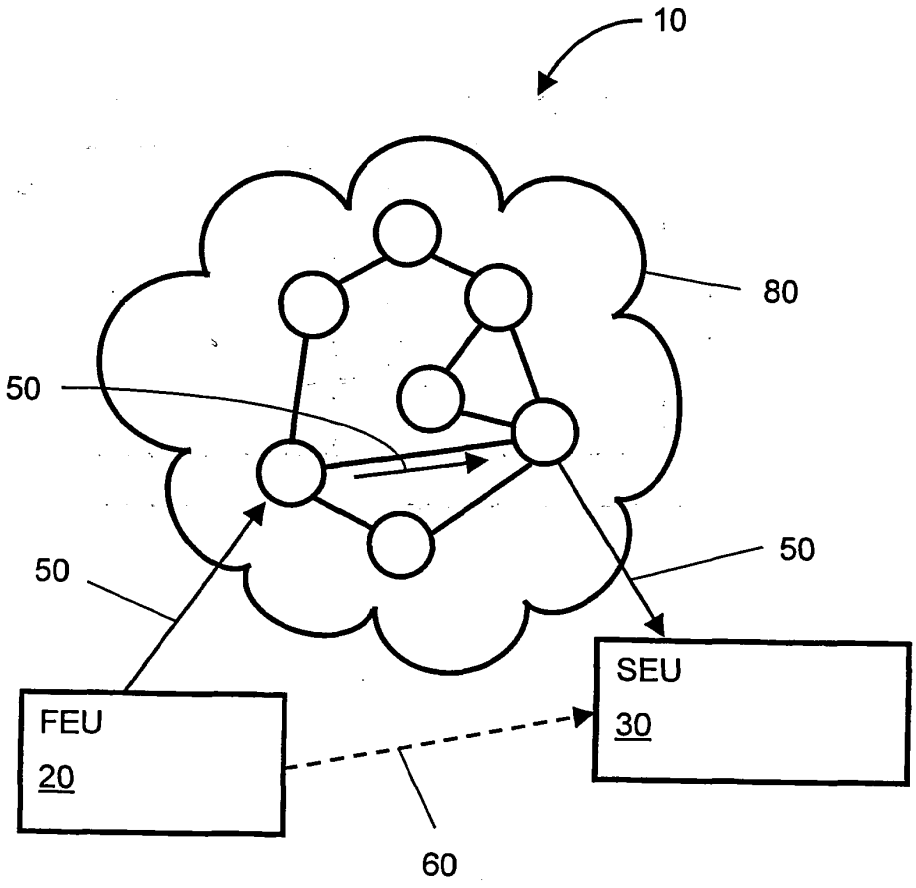


Fig. 1

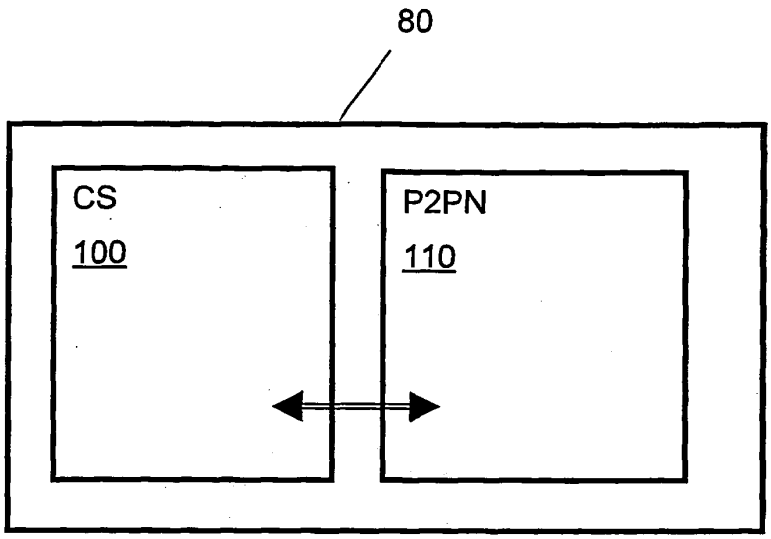


Fig. 2

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 January 2005 (27.01.2005)

PCT

(10) International Publication Number
WO 2005/009019 A3

(51) International Patent Classification[7]: H04M 7/00, 3/38, 15/00, H04L 29/06, 9/00

(21) International Application Number: PCT/IB2004/002282

(22) International Filing Date: 14 July 2004 (14.07.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/487,242 16 July 2003 (16.07.2003) US

(71) Applicant *(for all designated States except US)*: **SKYPER LTD.** [GB/GB]; 28-30 The Parade, St. Helier, Jersey FE4 8XY, Channel Islands (GB).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **HEINLA, Ahti** [EE/EE]; Juhkentali 8-5, EE10132 Tallinn (EE). **KASESALU, Priit** [EE/EE]; Mahtra 25-57, EE13811 Tallinn (EE).

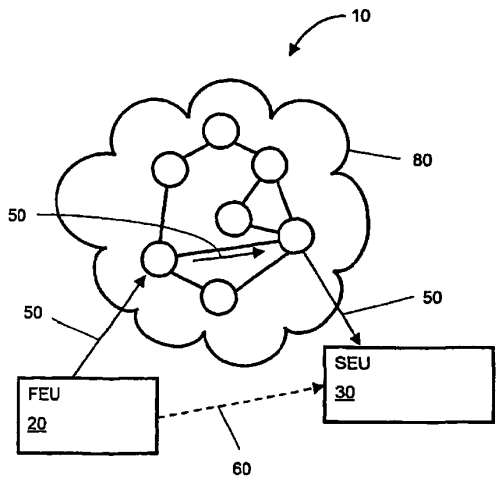
(74) Agent: PLOUGMANN & VINGTOFT A/S; Sundkrogsgade 9, Post Office Box 831, DK-2100 Copenhagen Ø (DK).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, 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, NA, 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 *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: PEER-TO-PEER TELEPHONE SYSTEM AND METHOD



(57) Abstract: There is provided a peer-to-peer telephone system (10) comprising a plurality of end-users (20, 30) and a communication structure (80) through which one or more end-users (20, 30) are couplable for communication purposes. The system (10) is distinguished in that: (a) the communication structure (80) is substantially de-centralized with regard to communication route switching therein for connecting said one or more end-users (20, 30); (b) said one or more end-users (20, 30) are operable to establish their own communication routes through the structure (80) based on exchange of one or more authorisation certificates, namely User Identity Certificates (UIC), to acquire access to the structure (80); and (c) said structure (80) includes an administration arrangement (100) for issuing said one or more certificates to said one or more end-users (20, 30).

WO 2005/009019 A3

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*

(88) Date of publication of the international search report:
28 April 2005

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.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB2004/002282

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04M7/00 H04M3/38 H04M15/00 H04L29/06 H04L9/00

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 H04M H04L

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, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CHARAS P: "Peer-to-peer mobile network architecture" PEER-TO-PEER COMPUTING, 2001. PROCEEDINGS. FIRST INTERNATIONAL CONFERENCE ON LINKOPING, SWEDEN 27-29 AUG. 2001, LOS ALAMITOS, CA, USA,IEEE COMPUT. SOC, US, 27 August 2001 (2001-08-27), pages 55-61, XP010583975 ISBN: 0-7695-1503-7 paragraph '03.5! paragraphs '04.2! - '04.3!	1-29
A	US 6 061 794 A (DRISCOLL DAN J ET AL) 9 May 2000 (2000-05-09) column 6, line 65 - column 7, line 38 column 9, line 48 - column 10, line 43 -/--	1-29

[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
9 March 2005	17/03/2005

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	Willems, B

Form PCT/ISA/210 (second sheet) (January 2004)

ISDOCID: <WO_____2005009019A3_I_>

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB2004/002282

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 03/014955 A (GIGAMEDIA ACCESS CORP) 20 February 2003 (2003-02-20) abstract	
P,X	WO 03/079635 A (IBM UK ;IBM (US)) 25 September 2003 (2003-09-25) page 13, line 27 - line 36; figures 1,3	1-29
P,X	ES 2 192 942 A (VIARGA VAI S L) 16 October 2003 (2003-10-16) the whole document	1-29
A	US 2002/184311 A1 (ABDELAZIZ MOHAMED M ET AL) 5 December 2002 (2002-12-05) The whole document	
P,X	US 2003/163697 A1 (PABLA KULDIP SINGH ET AL) 28 August 2003 (2003-08-28) paragraph '0013!	1,14
A	CHATHAPURAM U S: "Security in Peer-to-Peer Networks" PEER-TO-PEER COMPUTING, 'Online! 8 August 2001 (2001-08-08), XP002251813 Retrieved from the Internet: URL:http://netserver.cerc.wvu.edu/classes/cs491h_summer2_2001/sankaran_securityoverv> 'retrieved on 2003-08-20! the whole page	
A	WO 01/13201 A (SARNOFF CORP) 22 February 2001 (2001-02-22) the whole document	

Form PCT/ISA/210 (continuation of second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/IB2004/002282

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6061794 A	09-05-2000	NONE	
WO 03014955 A	20-02-2003	EP 1423796 A1	02-06-2004
		WO 03014955 A1	20-02-2003
		US 2003105812 A1	05-06-2003
WO 03079635 A	25-09-2003	US 2003177186 A1	18-09-2003
		AU 2003207337 A1	29-09-2003
		CA 2477197 A1	25-09-2003
		WO 03079635 A1	25-09-2003
ES 2192942 A	16-10-2003	ES 2192942 A1	16-10-2003
US 2002184311 A1	05-12-2002	US 2002156893 A1	24-10-2002
		EP 1229442 A2	07-08-2002
		EP 1229443 A2	07-08-2002
		WO 02057917 A2	25-07-2002
		US 2002143944 A1	03-10-2002
		US 2002143855 A1	03-10-2002
		US 2002184310 A1	05-12-2002
		US 2002184357 A1	05-12-2002
		US 2003002521 A1	02-01-2003
		US 2002152299 A1	17-10-2002
		US 2002184358 A1	05-12-2002
		US 2002188657 A1	12-12-2002
		US 2002147810 A1	10-10-2002
		US 2002147771 A1	10-10-2002
		US 2003041141 A1	27-02-2003
		EP 1282289 A2	05-02-2003
		US 2003028585 A1	06-02-2003
		US 2003070070 A1	10-04-2003
		US 2003055894 A1	20-03-2003
		US 2003055898 A1	20-03-2003
US 2003163697 A1	28-08-2003	NONE	
WO 0113201 A	22-02-2001	AU 6522200 A	05-03-2001
		AU 6537400 A	13-03-2001
		EP 1203479 A2	08-05-2002
		JP 2003529126 T	30-09-2003
		WO 0111817 A2	15-02-2001
		WO 0113201 A2	22-02-2001

ISDOCID: <WO_____2005009019A3_I_>

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2005-094600
(43)Date of publication of application : 07.04.2005

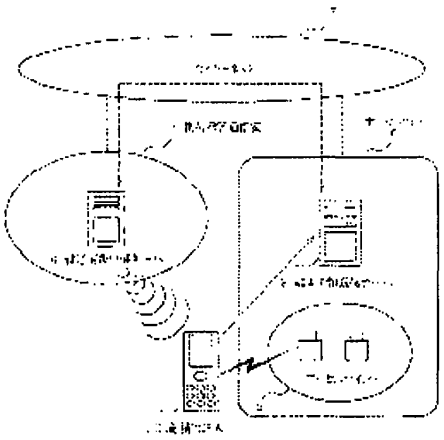
(51)Int.Cl. H04L 12/28
H04Q 7/38

(21)Application number : 2003-327855
(22)Date of filing : 19.09.2003

(71)Applicant : NEC CORP
(72)Inventor : MURATSU FUMITAKE

(54) AUTOMATIC WIRELESS LAN CONNECTION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an automatic wireless LAN connection system wherein setup information required for connection to a wireless LAN system is automatically transferred to a radio information terminal by giving notice of a terminal ID by the radio information terminal.
SOLUTION: A wireless information terminal 1 is connected to the Internet 7, LAN services and the like. An access point 2 associates the wireless information terminal 1 and provides connection of a wireless LAN level. A terminal information transmission server 3 acquires the terminal ID of the radio information terminal 1 and notifies the outside of setting information for connection to a hot spot service and the terminal ID. A setup information relay server 4 receives the ID of the wireless information terminal 1 and the setup information, determines a transmission destination on the basis of the terminal ID and transmits the setup information to the wireless information terminal 1. A cellular phone communication network 5 includes the setup information relay server 4. A hot spot 6 includes the access point 2 and the terminal information transmission server 3.



(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2006 年7 月20 日 (20.07.2006)

PCT

(10) 国際公開番号
WO 2006/075677 A1

(51) 国際特許分類:
H04L 12/56 (2006.01) *H04Q 7/38* (2006.01)

(21) 国際出願番号: PCT/JP2006/300324

(22) 国際出願日: 2006 年1 月13 日 (13.01.2006)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2005-009301 2005 年1 月17 日 (17.01.2005) JP

(71) 出願人 (米国を除く全ての指定国について): シャープ株式会社 (SHARP KABUSHIKI KAISHA) [JP/JP]; 〒5458522 大阪府大阪市阿倍野区長池町２２番２２号 Osaka (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 山田 昇平 (YAMADA, Shohei) [JP/JP]; 〒2610004 千葉県千葉市美浜区高洲３－６－２－７０４ Chiba (JP). 森脇 鉄朗 (MORIWAKI, Tetsuro) [JP/JP]; 〒3300071 埼玉県さいたま市浦和区上木崎５－１４－２５ Saitama (JP). 日比 慶一 (HIBI, Keiichi) [JP/JP]; 〒2700034 千葉県松戸市新松戸３－３２８ Ｂ－２１１ Chiba (JP).

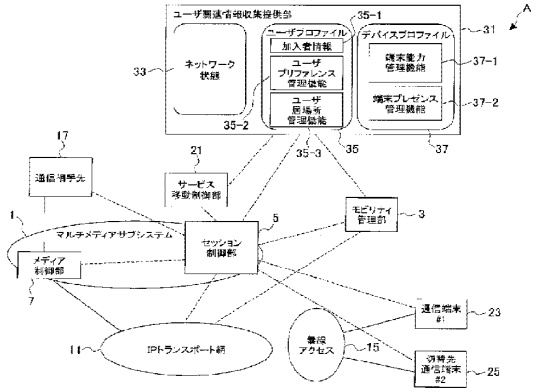
(74) 代理人: 平木 祐輔 (HIRAKI, Yusuke); 〒1050001 東京都港区虎ノ門４丁目３番２０号 神谷町ＭＴビル１９階 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK,

[続葉有]

(54) Title: COMMUNICATION NETWORK CONTROL SYSTEM

(54) 発明の名称: 通信ネットワーク制御システム



31 USER-ASSOCIATED INFORMATION COLLECTING/PROVIDING UNIT
33 NETWORK STATE
35 USER PROFILE
35-1 SUBSCRIBER INFORMATION
35-2 USER PREFERENCE MANAGEMENT FUNCTION
35-3 USER LOCATION MANAGEMENT FUNCTION
37 DEVICE PROFILE
37-1 TERMINAL ABILITY MANAGEMENT FUNCTION
37-2 TERMINAL PRESENCE MANAGEMENT FUNCTION
17 COMMUNICATION PARTNER
21 SERVICE SHIFT CONTROL UNIT
3 MOBILITY MANAGEMENT UNIT
1 MULTIMEDIA SUBSYSTEM
7 MEDIA CONTROL UNIT
5 SESSION CONTROL UNIT
11 IP TRANSPORT NETWORK
15 RADIO ACCESS
23 COMMUNICATION TERMINAL #1
25 SWITCHING DESTINATION COMMUNICATION TERMINAL #2

(57) **Abstract:** A communication network control system realizes a smooth and seamless terminal switching guaranteeing continuity of communication in the application level. The communication network control system includes: a mobility management unit (3) for setting and managing a physical and logical transmission route with a communication terminal (23) and a communication partner (17) by performing route control of the data packet transmission; a session control unit (5) for controlling a session with a communication terminal (23) and a communication partner (17) on the transmission path; a service shift control unit (21) for transmitting a session switching request signal instructing switching of the session from the communication terminal (23) to a switching destination communication terminal (25), to the session control unit (5); and a user-associated information collecting/providing unit (31) for collecting a user profile including user location information, a user network state, and user's hobby and taste, and a device profile including a device type and a device network connection state, from various function elements of the network , the user, the user terminal, and a user peripheral device so as to provide user-associated information.

[続葉有]

WO 2006/075677 A1

LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約:

アプリケーションのレベルでの通信の連続性を保証したスムーズでシームレスな端末切り替えを実現する。

データパケット転送の経路制御を行って通信端末２３と通信相手先１７との物理的、論理的な伝送経路を設定し管理するモビリティ管理部３と、伝送経路上で通信端末２３と通信相手先１７とのセッションを制御するセッション制御部５と、セッションを通信端末２３から切替先通信端末２５へ切替えることを指示するセッション切替要求信号をセッション制御部５に対し送信するサービス移動制御部２１と、ユーザの居場所情報とユーザのネットワーク状態とユーザの趣味趣向を含むユーザプロファイルとデバイスの種類や各デバイスのネットワーク接続状態を含むデバイスプロファイルとをネットワークの各機能要素やユーザやユーザ端末やユーザの周辺デバイスから収集し、ユーザ関連情報を提供するユーザ関連情報収集提供部３１と、を備える。

明 細 書

通信ネットワーク制御システム

技術分野

[0001] 本発明は、移動通信サービスを提供する通信ネットワークにおける端末切り替え技術に関し、より詳細には、ユーザが、利用している端末を通信中に異なる端末に切り替えた際にも、途切れることなく通信を継続できるシームレスな端末切り替え技術に関する。

背景技術

[0002] 近年、インターネットに代表されるネットワークサービスや、携帯電話の急速な普及拡大により、更に高度な通信サービスの実現が期待されている。携帯電話では、ユーザが端末を持ちながら移動しても通信が継続される、いわゆるハンドオーバ機能、モビリティ管理機能が提供されているが、この機能を更に発展、高度化させて、通信中に端末を変更しても通信が継続できる機能の実現などが望まれている。

[0003] 通信ネットワークが拡大、発展して、様々な端末がネットワークに接続可能になると、ユーザは通信ネットワークに接続可能な多種の通信端末を所有するようになる。これらの通信端末としては、携帯電話のような可搬型の端末だけでなく、例えばテレビ受像機のような家庭内に設置される据え置き型の家電機器などの情報機器(以下、情報機器と称する)も通信端末として用いられるようになると考えられる。

[0004] 一方、通信ネットワーク側では、インターネットの発展によって構築されたIP(Internet Protocol)通信技術を活用した共通IPバックボーンを設けることによって、無線、有線などのアクセス手段や、ネットワークのオペレータ、サービスのプロバイダの違いを意識せずに各種の通信端末で共通のサービスを享受することが容易となる。

[0005] このようになると、ユーザは、例えば、移動通信端末、PDA、パーソナルコンピュータなどの情報機器などの自己が所有する通信端末を、ユーザの現在状況や好みなどに応じて自由に使い分けることができるようになると、同じサービスであっても、その時点で自分が保有、選択する端末によって当該サービスを利用したいとの要求が生じる。さらに、通信中に、端末を別の端末に切り替えたい場面も想定さる。その際には

、通信を一旦切断して、別の端末から改めて接続するのではなく、通信の状態を維持したままで途切れることなくシームレスに別の端末へ切り替えたいというユーザの要求を実現する必要がある。

[0006] 具体的には、自宅のパーソナルコンピュータにより映像コンテンツをストリーミング配信で視聴していたが、外出時には、受信端末を移動通信端末やPDAに切り替えて、外出先へ携帯する端末で同一コンテンツを引き続き視聴する例がある。また、外出中にテレビ電話で相手と通信している途中で帰宅したため、自宅のテレビに切り替えて相手とのテレビ電話の通信を継続する例なども考えられる。

[0007] 上述したようなシームレスな端末切り替えを実現するにあたり、マルチキャスト型の配信を受信している場合は、送信側端末から同一コンテンツのデータが複数(不特定多数)の通信端末に向けて同時に配信されているため、切り替え先の端末でも当該データを受信するように当該受信端末をその送信側端末へ接続すれば良く、比較的容易に端末切り替えが実現できる。

[0008] しかしながら、ある特定の端末だけに配信されるユニキャスト型配信、あるいは1対1の通信の場合には、送信側端末に対して、一旦通信の中断を指示して、切り替え先の端末をその送信側端末に接続してから、受信側の端末を切り替えたことを通知した上で、通信を再開するという手順が必要となる。

[0009] このような従来の通信ネットワークの制御システムにおける端末切り替えの例を図7に示す。図7の例では、ユーザは、通信に利用していた通信端末(＃1)203を通信端末(＃2)205に切り替える場合を示す。まず、ユーザは、データを受信中の通信端末(＃1)203から配信側のサーバ装置201に対して、矢印221で示すように制御情報を送信して、配信の中断を指示する。次に、通信ネットワーク内の制御装置213に対して、サーバ装置201との通信接続の切断を要求する矢印224aに示す制御情報を送出して、通信を切断する。

[0010] 次に、ユーザは、切り替え先である通信端末(＃2)205から通信ネットワークの制御装置213に対して、矢印225に示すように前述のサーバ装置201への接続要求を送出すると、制御装置213は通信ネットワーク内に通信端末(＃2)205とサーバ装置201との通信経路を設定して、当該装置間での接続を設定する。続いて通信端末(＃

2)213からサーバ装置201に対して、矢印224bに示す配信の再開を指示する制御情報を送出すると、サーバ装置201は、上記配信を中断された時点からのデータを送出することによって、ユーザは通信端末(＃2)205を用いて、続きのデータを受信することができ、すなわち端末切り替えが実行できる。

[0011] ここで、切り替え先の通信端末(＃2)205がサーバ装置201と接続するためのサーバ装置201のアドレス情報は、電話番号やURLなどの形式により、ユーザが通信端末(＃2)205を操作して入力するなどの手段によって指定される。この例では、通信ネットワークの制御装置213は、通信端末(＃1)203または通信端末(＃2)205とサーバ装置201との間の接続および切断のみを行い、端末を切り替えるための制御機能を有しておらず、通信端末およびサーバ装置における通信の中断、再開機能によって端末の切り替えが実現される。

[0012] 端末切り替えのもう一つの方法の従来例を、図8に示す。受信側の通信端末(＃1)303は、端末の切り替えにあたって、矢印321に示すように配信側サーバ装置301に対して配信の中断を指示する制御情報を送出する。サーバ装置301との通信が保留された後にユーザが転送操作を行なうと、通信端末(＃1)303は、矢印332に示すように通信ネットワークの制御装置313に対して、サーバ装置301との間の接続を通信端末(＃2)305へ転送することを要求する制御情報を送出する。

[0013] その制御情報を受信した制御装置313は、矢印333に示すように通信端末(＃2)305に対してサーバ装置301との接続を指示する制御情報を送出することによって通信端末(＃2)305へ発呼して、矢印334に示すように通信端末(＃2)305が当該発呼に対して応答すると、通信端末(＃2)305とサーバ装置301との間に通信経路を設定することによって接続を確立する。

[0014] その後、矢印335に示すように、転送元の通信端末(＃1)303と制御装置313との間での制御情報の送受によって、通信端末(＃1)303とサーバ装置301との接続が切断されると共に、通信端末(＃2)305は上記サーバ装置301に対して、矢印324に示す保留中の通信の再開を要求する制御情報を送出することによって、通信端末(＃2)305が続きのデータを受信する。この例においては、通信ネットワーク内の制御装置313は、呼を別の端末へ転送するための制御機能は有しているものの、当該

制御装置313は、通信端末／サーバ装置間でのデータ送受信の中断、再開を制御する機能は備えておらず、通信の連続性、即ちシームレスな切り替えを保証するものではない(非特許文献1)。

[0015] また、従来の通信ネットワーク構成として、3GPPで規格が定められている第三世代移動体通信の構成例を図2に示す。IMS(IP Multimedida CN Subsystem)は、IPマルチメディアサービスをパケット交換システムで提供することを目的としており、そのためにネットワーク101内にセッション制御機能を配置する。セッション制御プロトコルとしてはSIP(Session Initiation Protocol)が採用されている。CSCF105は呼状態制御機能であり、SIPの登録サーバとしてHSS103(Home Subscriber Server)とやり取りし、ユーザ登録処理を行なうとともに、セッション情報を転送し、呼接続制御を行う。また、サービスを提供するために、アプリケーションサーバとやり取りを行うインターフェイスも持つ。また、HSS103は、ユーザの加入者情報や、ロケーション情報を管理する。MRF107(Media Resource Function)は、メディアストリームのリソース制御を行い、マルチメディア会議などでのメディア合成や、メディアストリームの変換などを行う。また、MGCF(MediaGateway Control Function)とMGW(MediaGateway)とにより、PSTN(Public Switched Telephone Network)と接続する際のメディア変換を行う。しかし、通信相手先117とネットワーク101、パケット網111を介して無線アクセス115を行う端末123／125に対して変更後もサービスを提供し続けるという仕組みはない(非特許文献2参照)。

非特許文献1:藪崎他「モバイルネットワークAll－IP化特集」、NTT DoCoMo テクニカルジャーナル Vol. 10 No. 4 2003年1月、p. 6－34。

非特許文献2:3GPP TS22. 228 V5. 6. 0。

発明の開示

発明が解決しようとする課題

[0016] しかしながら、上述したいずれの従来例においても、端末切り替え時には、通信端末とサーバ装置との間、すなわち、エンド・エンド間での通信の保留と再開とによって連続性が確保されているものであり、途切れのないシームレスな切り替えを保証する技術ではない。つまり、上述したいずれの従来例も、サーバ装置に通信、即ちデータ

伝送を保留する機能を設けておき、保留にした後に別の通信端末からデータ伝送の再開を要求することによって、見かけ上、端末切り替えを実現しているだけである。サーバ装置に蓄積されたコンテンツを通信端末へ一方向に配信するような場合や、テレビ電話のような1対1の双方向型のリアルタイム通信を行なう場合などには、ある程度の機能を実現できる。

[0017] しかしながら、上位の通信アプリケーションが伝送データに応じた状態を持つ場合、例えば、通信型のゲームの続きを別の端末で実行したり、通信しながら同一文書を編集する共同作業を行ったりする場合には、上記通信アプリケーションの状態を切り替え先の端末へ通知することが困難であるという問題点があった。

[0018] すなわち、テレビ電話やコンテンツ配信のようなサービスであっても、多数のメディアを同時に利用するアプリケーションや、各種のコンテンツ／情報を連携して利用するアプリケーションなど、エンド・エンドのアプリケーション間で複数の通信（コネクション）を設定している場合には、別の端末への切り替えの処理、手順が煩雑になるという問題点があった。

[0019] 加えて、以下のような問題点がある。

[0020] 1）端末の切り替えに併せて、端末能力に応じた最適な通信形態（ビットレート、解像度など）でコンテンツを受信するために、ネットワークのサービス品質（ビットレート、遅延、その他）を適切に制御するような通信ネットワーク制御と連携したサービスの提供が困難である。

[0021] 2）また、上記のサービス品質の適切な切替をネットワーク制御側で行うのか、通信相手側で行うのか判断を行なったり、ユーザの好みに合わせてサービス品質の切替を決定することが困難である。

[0022] 3）また、周辺にどのような端末が存在し、どの端末に切り替えるべきか制御するようなサービスの提供が困難であるという問題があった。

[0023] 本発明は、ユーザは従来型の有線・無線のネットワークやサービスの違い、通信端末の種別の違い等を意識する必要がない、シームレスでユビキタスなサービス環境を提供することを目的とする。

課題を解決するための手段

[0024] 本発明に係る通信ネットワークの制御システムは、データパケット転送の経路制御を行って前記通信端末と通信相手先との物理的、論理的な伝送経路を設定し管理するモビリティ管理手段と、前記伝送経路上で前記通信端末と通信相手先とのセッションを制御するセッション制御手段と、セッションを前記通信端末から切替先通信端末へ切替えることを指示するセッション切替要求信号を前記セッション制御手段に対し送信するサービス移動制御手段と、を有する通信ネットワークシステムにおいて、ネットワーク状態とユーザの居場所情報とユーザの趣味趣向とを含むユーザプロファイルと、デバイスの種類や各デバイスのネットワーク接続状態を含むデバイスプロファイルと、をネットワークの各機能要素やユーザやユーザ端末やユーザの周辺デバイスから収集し、ユーザ関連情報を提供するユーザ関連情報収集提供手段と、を備えている。

[0025] 前記サービス移動制御手段は、前記通信端末から端末切替要求信号を受信するかまたは前記ユーザ関連情報に基づいて端末切替を行うか判断することにより、セッション切替要求信号を生成し、前記セッション制御手段は、セッション切替要求信号を受信して、セッションを中断する機能と、前記モビリティ管理手段に対して前記切替先通信端末との伝送経路を設定するよう指示する機能と、前記切替先通信端末との間でセッションを確立する機能と、前記セッション確立後、前記通信相手先との間でセッションを再開する機能と、を発揮する。これにより通信端末間の通信を中断させることなく、当該通信を行っている少なくとも一つの通信端末を、前記通信を行っていない他の通信端末へ切替えて前記通信を継続させる制御を行うことができ、通信ネットワークにおいて、データの伝送経路を設定、管理する機能に加えて、エンド・エンドでのセッション、即ち伝送されたデータを利用するアプリケーション間での論理的な伝送路の管理、制御機能と前記セッションの転送機能が発揮されるので、セッションおよびアプリケーションの状態管理まで含めた通信端末のスムーズかつシームレスな切り替えを実現することが可能となる。

[0026] また、ユーザの環境に適応して、端末切替を行うか否かの判断が可能となり、ユーザの居場所やネットワークの状態に応じて、ネットワーク側でサービスの制御を提供することが可能となる。また、サービスに関するユーザ関連情報やサービスの提供を

維持しながら端末を切り替える指示を行う手段と端末間でのセッションを張る手段を分離することにより、より効率的なネットワーク制御が可能となる。さらに既存の3GPPのシステムでのセッション制御を行うCSCFに対し、サービス移動制御手段を追加することにより実現が可能となる。

[0027] また、本発明に係る通信ネットワークの制御システムは、前記サービス移動制御手段は、前記ユーザ関連情報から前記通信端末と前記切替先端末のデバイスプロファイルと、前記通信相手先からメディア切替能力情報を取得し、メディアの変換をメディア制御手段にて行うか、前記通信相手先にセッションを変更するように指示するか判断するメディア変換先判定機能と、どのようなメディア変換を行うかを判断するメディア変換処理判定機能を有し、前記サービス移動制御手段は前記メディア変換先判定と前記メディア変換処理判定に基づき、セッションの変更指示メディア変換指示情報を生成すること特徴としている。

[0028] これにより、通信相手先のメディア切替能力と、通信端末と切替先通信端末の端末能力を考慮して、ネットワーク側でメディアの変換を行うべきか、通信相手先で行うべきか、よりサービスの状態が保たれるように自動的に判断することが可能となる。

[0029] また、本発明に係る通信ネットワークの制御システムは、前記ユーザ関連情報収集提供手段は、ユーザのメディア変換先とメディア変換処理に対する判定基準をユーザプリファレンスとして管理し、前記サービス移動制御手段は、ユーザプリファレンスに基づいてメディア変換指示情報を生成することを特徴としている。

[0030] これにより、ユーザが予め自分の好みを設定して、どのサービス提供者にメディア変換をしてもらいたいのか、どのようなメディア変換処理をしてほしいのかを設定することができ、ユーザに対してもサービス提供者に対しても拡張性、柔軟性のあるサービスを提供できる。

[0031] また、本発明に係る通信ネットワークの制御システムは、前記通信端末は、前記切替先通信端末との通信を行う手段を有し、前記切替先通信端末から前記切替先通信端末の状態やアドレスを示す端末プレゼンス情報と前記切替先通信端末の種別、属性、処理および利用可能なビットレート、メディア種別、およびコーデック種別を含む端末能力情報を取得し、前記端末切替要求信号は、前記切替先通信端末の端末

プレゼンス情報と端末能力情報を含み、サービス移動制御手段は、前記端末切替要求信号に基づいて前記セッション切替要求信号を生成するとともに端末プレゼンス情報と端末能力情報とをデバイスプロファイルに登録することを特徴としている。

[0032] これにより、通信ネットワーク側で切替先通信端末の情報を持っていない場合でも、セッションの制御が可能となり、新たなデバイス登録も同時に行うことができる。

[0033] また、本発明に係る通信ネットワークの制御システムは、前記通信端末は、前記切替先通信端末として動作し、端末切替要求信号にて端末の切替ではなく接続経路の変更のみを要求する指示を送信するかまたは前記ユーザ関連情報に基づいて経路切替を行うか判断することにより、前記サービス移動制御手段は、前記通信端末内のセッションの切替を行うように指示するセッション切替信号を生成し、セッション制御部に送信することを特徴としている。

[0034] これにより、通信端末にて、異なるアクセス方法や異なるオペレータのネットワークに接続を切り替える際に、サービスを維持したまま切替が可能となる。

発明の効果

[0035] 本発明によれば、ユーザは、自己の状況の変化に応じて、切替要求時の簡単なボタン操作などだけで、使用する通信端末の切り替えを、従来に比べて大幅に操作の手間と時間的なロスを軽減して実現することができ、より高度なサービスを享受することができる。また、配信側のサーバ装置においても特別に新規の機能を実装しなくても配信サービスが続けられるという利点がある。さらに、受信側の通信端末間の能力が異なっても、データ形式が個々の通信端末に応じて最適化されて伝送されるので、通信端末側にもサーバ装置側にも負荷を与えることがないという利点がある。こうしたサービス提供基盤の共通化により、ユーザは従来型の有線・無線のネットワークやサービスの違い、通信端末の種別の違い等を意識することがなくなり、シームレスでユビキタスなサービス環境を享受可能となる。

図面の簡単な説明

[0036] [図1]本発明の第1の実施の形態による通信ネットワークの制御システムの概略構成例を示す図である。

[図2]従来の通信ネットワークの制御システムの構成例の概略図である。

[図3]ユーザ関連情報収集提供部のデータベース構成例を示す図である。

[図4]本実施の形態による通信ネットワークの制御システムにおける端末切替の実行手順を示す図である。

[図5]本発明の第2の実施の形態によるアクセス方法の切替に関する通信ネットワークの制御システムの概略図である。

[図6]本実施の形態のアクセス方法の切替に係る通信ネットワークの制御システムにおける経路切替の実現手順を示す図である。

[図7]通信ネットワークの制御システムにおける端末切り替えの例を示す図である。

[図8]通信ネットワークの制御システムにおける端末切り替えの例を示す図である。

符号の説明

[0037] A…通信ネットワークの制御システム、3…モビリティ管理部、5…セッション制御部、11…IPトランスポート網、21…サービス移動制御部、31…ユーザ関連情報収集提供部、33…ネットワーク状態、35…ユーザプロファイル、37…デバイスプロファイル。

発明を実施するための最良の形態

[0038] 本発明に係る通信ネットワークの制御システムは、通信ネットワーク内の制御装置に、データの伝送経路を設定、管理する機能に加えて、エンド・エンドでのセッション、即ち伝送されたデータを利用するアプリケーション間での論理的な伝送路の管理、制御機能と前記セッションの転送機能を発揮する。これらの機能によって、セッションおよびアプリケーションの状態管理まで含めた通信端末のスムーズかつシームレスな切り替えを実現する。

[0039] また、本発明に係る通信端末は、端末切り替えを実行するためにセッション、アプリケーションの状態を通知する機能、および、前記通知された状態に基づいてセッション、アプリケーションを当該状態に設定して、再開する機能を発揮する。これらの機能によって、セッションの状態を的確に保持したままでのスムーズかつシームレスな端末切り替えを実現する。

[0040] 更に、移動通信ネットワークなどで提供されている通信端末の位置やアドレス情報の変更に追従して伝送経路を適切に切り替えていくハンドオーバ、モビリティ管理機能を活用し、上記セッション制御機能と連携させることによって、通信端末を切り替え

る際の伝送経路の設定機能を、従来技術からの最小限の変更で実現する。そして、柔軟性、拡張性が高いセッション制御機能を実現する。

[0041] 次世代の移動通信ネットワークにおいては、すべてのデータがIPパケットの形で伝送、交換されるオールIPベースのプラットフォームを構築して利用することが想定されている。また、データ伝送の機能と、呼設定、ルーティング管理などの制御機能とを明確に分離した、いわゆる呼制御分離型のアーキテクチャとすることが検討されている。このようなアーキテクチャでは、下位層であるトランスポート層がデータ、即ち、IPパケットを高速かつ効率的に伝送する機能に専念し、経路(ルーティング)制御やトラフィック制御などの機能は接続制御層に分担させて、その接続制御層からトランスポート層に対してIPパケットのルーティング、リソース割り当て等を指示する構成とすることによって、システム全体としての高速化、高効率化を図っている。また、オールIPベースのプラットフォームでは、呼制御などの制御信号、シグナリングもIPパケットの形で伝送されることが想定されている。

[0042] さらに、オールIPベースの上記アーキテクチャでは、ネットワークの高度化、高付加価値化を図り、様々な通信サービスを柔軟かつ自由に提供できるようにするためのサービスサポート機能を設けることが検討されている。これは、以前の音声電話を中心としたネットワークでは、エンド・エンドでの物理的、論理的な伝送経路(パス)を設定する呼制御機能が主体であったのに対し、次世代のネットワークでは、エンド・エンドの通信アプリケーション間の論理的な接続であるセッション制御の機能をネットワーク内に設けることを意味している。

[0043] ここで、呼あるいは呼接続とは、エンド・エンドの端末間で相手へデータを伝送するための物理的、論理的なパス(が設定されていること)を示し、セッションとは、端末の通信アプリケーションが通信相手の端末上のアプリケーションからのデータを受信して処理できる(処理している)状態にあることを示す。つまり、相手端末との間でデータの送受信はできるが、どのアプリケーションを用いるかが決定していないか準備ができていない状態は、呼接続されているがセッションが接続されていない状態であり、反対に、アプリケーションはデータの送受信の準備ができているが、データ伝送パスが失われた(例えば、携帯電話機が圏外へ移動するなど)状態は、セッションは接続

されているが呼接続されていない状態ということとなる。

[0044] ここまでは、主として呼接続について説明してきた。従来の音声電話では、呼接続とセッションとは特に区別されないが、マルチメディア通信やデータ通信などの場合には、呼接続の設定後にエンド・エンドで確立された伝送経路上で通信端末のアプリケーション間でのセッションが設定される。次世代の移動通信ネットワークでは、ネットワーク内にセッション制御機能を含めることが検討されている。これは、通信の多様化、高度化により様々な通信の形態、モード、メディアなどに応じた接続制御、通信制御などの機能をネットワークから提供する必要が生じてきたためである。例えば、音声のみの通話かテレビ電話かの区別や、テレビ電話における解像度やビットレートなどの品質、端末能力を指定して相手に発呼するようなケースでは、これらの要求に合致した端末を指定するためのアドレス解決、適切な品質の伝送路の設定(呼制御、経路制御)など、エンド・エンドのネゴシエーションでは不充分な機能をネットワークの能力によって実現する必要がある。

[0045] そこで、セッション制御を行うセッション制御部を設け、セッション、即ち、エンド・エンドのアプリケーション間の通信状態、モードなどを管理、制御すると共に、そのセッション制御機能からモビリティ管理部の呼制御機能や経路制御機能に対して、適切な帯域、品質での伝送パスを設定するように指示、制御を行なうように構成する。この時、通信端末のアプリケーションからの接続要求(セッション設定要求)は、前記セッション制御機能へ送られて、処理されることとなる。

[0046] 図1に本発明の第1の実施の形態による通信ネットワークの制御システムの一構成例を示す。図1に示すように、本実施の形態による通信ネットワークの制御システムAは、IPパケットを転送するIPトランスポート網11と、IPトランスポート網11を制御し、上述したように通信端末の物理的な位置の管理、呼制御、ハンドオーバ制御(経路制御)を行なうモビリティ管理部3およびセッションの確立・管理するセッション制御部5と、セッションを維持させながら通信端末を切り替えるなどのユーザの高度な要求への対応を担当するサービス移動制御部21を含んでいる。

[0047] モビリティ管理部3は、図2におけるIMSのHSS103に相当し、特にIPトランスポート網の制御に特化した機能要素である。セッション制御部5は、図2におけるIMSのC

SCF105に相当し、サービス移動制御部21は、図2におけるIMSに対して新たな機能要素である。但し、サービス移動制御部21は図2におけるCSCF105の機能拡張によって実現されたと解釈することも可能である。サービス移動制御部21は、サービスを継続しながら端末切替を行うために、端末から端末切替の指示がセッション制御部に要求され、端末切替要求をセッション制御部から受け、セッション制御部にセッション切替要求信号を送信したり、ユーザの状態をユーザ関連情報収集提供部31とやり取りして、ユーザの状態に応じて自動的にセッション切替要求信号を送信したりすることができる。

[0048] ユーザ関連情報収集提供部31は、ネットワーク状態33と、ユーザに関するユーザプロファイル35と、デバイスに関するデバイスプロファイル37と、を管理し、様々なネットワークの機能要素から情報収集を行い、各サービスやネットワークの機能要素に対して情報を提供する。これは、図2に示すIMS101のHSS103をさらに拡張した機能であり、モビリティ管理部3と統合して、図2に示すHSS103の機能を拡張することによって実現されてもよい。ユーザプロファイル35は、加入者情報35－1、ユーザのプリファレンス管理機能35－2、ユーザの居場所管理機能35－3、からなる。ユーザの居場所に関する情報は、モビリティ管理部3からのアクセスポイントの情報や移動速度情報やその周辺のRFIDや通信端末に搭載したGPSなどの情報により取得することができる。

[0049] ユーザの趣味趣向は、ユーザの居場所や移動速度や使用デバイスの種類に対応した無線アクセスの種類やサービスの種類やローミングの方法やメディア変換の実行先やメディア変換の方法を、ユーザが予め設定するか、ネットワーク側で上記のような利用の履歴を管理し、履歴から判断してユーザの趣味趣向を推定して設定するなどの方法で管理される。

[0050] デバイスプロファイル37は、端末の形状、データ変換方式、動画対応、画面サイズなどを含む端末能力情報37－1と、端末の現在状況（居場所）を含む端末プレゼンス情報37－2とを有している。デバイスプロファイル37は、ユーザが予め登録するか、端末をネットワークに接続した際に、端末から情報を送信し、ネットワーク側で自動的に管理することにより取得される。また、切替先通信端末が登録されていない場合

は、近距離通信を利用して、切替先通信端末の端末能力情報を取得し、端末切替要求信号に含めて通信端末から送信され、デバイスプロファイル37に登録されるようにすることもできる。

[0051] デバイスプロファイル37とユーザプロファイル35とは、ユーザの居場所情報、デバイス所有者情報に応じて関連付けられる。従って、ユーザの所有デバイスではない公共のデバイスや共有デバイスとユーザとが関連付けられる場合もある。

[0052] 端末能力管理機能37－1が管理する端末能力に関する端末能力情報は、端末の種別、属性、処理、IPアドレスおよび利用可能なビットレート、メディア種別およびコーデック種別、画面サイズ、CPU能力、接続可能ネットワークなどを示す情報である。端末プレゼンス管理機能37－2が管理する端末プレゼンス情報は、現在実行中のアプリケーションの種類や状態、現在の端末の居場所情報などを示す。ネットワーク状態33は、モビリティ管理部3からの無線アクセスの種類に関する情報、セッション制御部5からのQoSの情報やセッションの状態情報やメディア変換部のメディア変換の状態情報や通信端末で実行中のアプリケーションの状態情報によって取得され、通信端末のネットワーク状態だけではなく、デバイスプロファイルに登録されている端末が現在接続中のネットワークの状態(伝送レートや無線方式やQoSなど)も管理する。尚、上記のうちで、必須構成は、ネットワーク状態33、加入者情報35－1、端末能力機能37－1である。

[0053] 図3は、ネットワーク状態、ユーザプロファイル、デバイスプロファイルのデータベースの例を示す図であり、データベースは例えばXML(eXtensible Markup Language)などの言語を利用して抽象的な記述により管理され、データベースの情報はサービス移動制御部21(図1、以下図番号を略して説明する。)に提供される。

[0054] 図3に示すように、例えば、ネットワーク状態41と、ユーザプロファイル43と、デバイスプロファイル45と、が関連付けされている。ネットワーク状態41は、端末(1)41－1と、端末(2)41－2と、端末(3)41－3と、から構成され、例えば、端末(1)41－1に関しては、アクセス方法としてW－CDMA、QoSクラスとしてマルチメディアが、セッション状態として音声通信、ファイル交換が、ビットレートとして10Mbpsが、ロケーションとして基地局1が、経路情報A－B－C…が、記載されている。ユーザプロファイ

ル43においては、例えば、端末(1)41－1の所有者であるユーザ(1)43－1に関する情報であって、加入者情報とプリファレンスと、居場所情報等とが記載されている。この場合には、端末(2)41－2の所有者もユーザ1であることを示している。デバイスプロファイル45は、端末(1)41－1の端末能力情報である、移動通信端末、画面サイズ、CPUクロック数、コーデック、アクセス方法、IPアドレスなどが記載されている。端末プレゼンス情報としては、経度・緯度情報、場所情報、移動速度、通信状態、起動中アプリケーションの有無と種類などが記載されている。端末(2)41－2の情報も、端末能力情報として、例えば固定端末である旨が、端末プレゼンス情報として通信可能であるか否かなどの情報が記載されている。そして、これらの情報41・43・45は、所有者、通信状況、位置などに基づいて関連付けされている。

[0055] あるユーザの情報をサービス移動制御部21から要求されると、ユーザの所有する端末、ユーザの居場所の近傍にある端末などが関連づけられ、関連付けが行なわれた情報群としてサービス移動制御部21に提供される。

[0056] また、メディア制御部7は、IMS101のMRF、MGCF／MGW107、を拡張したものに相当する。セッション制御部5からのメディア変換要求に応じてコンテンツのビットレートやコーデックや画像サイズやメディアフォーマットなどのメディア変換を制御、実行する。端末切替後にメディアを変換する場合には、セッションが再開された後に、メディアを変換できる単位までバッファリングして、メディア変換を行う。この際、再エンコードすることになるため、電子透かし等の認証機能をコンテンツに付加しても良い。

[0057] これらの通信ネットワーク制御システムの機能要素は、説明を簡単にするために、各図においては単一のモジュールとして示しているが、実際には、ローミングの場合や、通信相手が同一ネットワーク外の場合を考慮し、上記のような機能要素は各ネットワーク先、ローミング先にあり、1つのモジュールで実現しているわけではない。実施例における説明では、そのようなやり取りをまとめて一つの処理としてみなすことにより簡略化している。

[0058] また、通信端末は、図示しない画像表示装置および入力装置などから構成されるユーザインタフェースと、赤外線、ブルートゥース(登録商標)、あるいは将来実現が有望視されているUWBなどの無線通信方式またはUSB方式などの有線通信などを

用いた近距離通信部とを備えており、端末切替要求機能、端末ID通知機能、セッション状態再現機能、セッション管理機能、セッション状態送出機能、発呼要求・応答機能、および位置登録機能を発揮する。通信相手先は、アプリケーションサーバ装置でも良いし、通信端末でもよい。

[0059] 次に、図4を参照しつつ端末切替の手順について説明する。適宜図1を参照する。まず、通信端末23は端末切替要求信号を生成するが、その際にどの端末に切り替えるか指定する必要がある。近距離無線を利用して切替先端末25と通信して切替先通信端末25の端末情報を取得し、端末切替要求信号を作成する方法(C300)、通信端末25が切替可能な端末リストをユーザ関連情報収集提供部31から取得している状態で、ユーザが切替先通信端末25を選択して、端末切替要求信号の作成指示を出す方法を用いることができる(C301)。端末切替要求信号には、通信端末23のセッション状態や、アプリケーションの状態などが含まれていてもよい。もしくは、サービス移動制御部21がユーザ関連情報収集提供部31と定期的に情報のやり取りを行い、ユーザ環境が、端末切替を実行すべき状態になったか否かを判断するようにしても良い(C301')。

[0060] 端末切替を実行すべき状態の例としては、ネットワーク状態情報により、通信端末(#1)23のネットワークの状態よりも、切替先通信端末(#2)25のネットワークの状態のほうが安定している場合又は切替先通信端末(#2)25のネットワークの方が高速な場合に切替を行なう可能性が高い。或いは、ユーザプリファレンス情報とユーザ居場所情報と端末プレゼンス情報とを利用して、現在のユーザの居場所には、ユーザの利用できる端末が2台あり、ユーザがこの場所で優先して使用する(ユーザプリファレンス情報から判断)のは切替先端末(#2)25であると判断される場合に、切替を行なうようにすることもできる。

[0061] サービス移動制御部21は、ユーザ関連情報収集提供部31に対し、ユーザプロファイル35、デバイスプロファイル37、ネットワーク状態33に関する情報を要求し取得する。上記C301の端末切替要求信号に切替先の通信端末の端末情報が含まれている場合は、デバイスプロファイル37に端末情報を登録する作業も行う(C302)。サービス移動制御部21は、次に、ユーザ関連情報収集提供部31、端末切替要求信号か

ら取得したユーザプロファイル35、デバイスプロファイル37、ネットワーク状態33により、メディア変換の必要性を判断する。

[0062] ユーザの趣味指向や通信端末23と切替先通信端末25の能力の差などからメディア変換の必要があると判断されると、通信相手先17でメディア変換が可能か否かを問い合わせるようにセッション制御部5に要求する(C303)。但し、上記ユーザプロファイル35、デバイスプロファイル37、ネットワーク状態31の取得時に、通信相手先のメディア変換能力を取得している場合は、この手続きを省くことができる。

[0063] セッション制御部5は、メディア変換能力を通信相手先17に問い合わせ、メディア変換能力情報を取得し、メディア変換能力情報をサービス移動制御部21に通知する(C304, C305, C306)。

[0064] サービス移動制御部21は、メディア変換能力情報を受け取ると、これまで取得した情報からメディア変換先の選定、メディア変換処理の内容の選定、セッション状態の変更の必要性を判断し、それらを含んだセッション切替要求信号をセッション制御部5に対して送信し(C307)、セッション制御部5は、モビリティ管理部3に対して経路設定を指示する(C308)。経路設定が終了するとモビリティ管理部3から応答(ACK)が返る(C309)。この経路設定時には、切替先通信端末25がアクティブでない場合は発呼処理を行う。この時点で通信相手先17と通信端末23、通信相手先17と切替先通信端末25の2つの経路が設定されていることになり、マルチキャストなどの同時に2つの経路の設定が可能な場合は、そのままでいいが、2つの経路の設定が可能でない場合には、どちらかを保留するなどの処理が必要となる。

[0065] 次に、セッション制御部5は、通信端末23に対し、セッションの切替を行う準備が整ったことを示すセッション切替準備信号を送信し、通信端末23はセッションの切替を了承するか否かを返答する(C310、C311)。ネットワーク側から自動的に端末切替を行う際には、これが通信端末23に対して端末切替を行なってもよいかどうかを確認するメッセージとなる。セッション制御部5は、通信相手先17にセッションの中断を要求し、通信相手先17からACKがかえってくると、切替先通信端末25とのセッションの確立を行い、この間に切替先通信端末25はアプリケーションの起動を行う(C312～C315)。

[0066] セッション制御部5は、セッション切替要求信号に含まれていたメディア変換指示に従い、メディア制御部7又は通信相手先17に対しメディア変換を指示する(C316, C317, C316', C317')。続いて、セッションを再開し、通信端末とのセッションを切断する(C318, C319, C320)。この際、モビリティ管理部3による伝送経路の切断も行われる。最後に、サービス移動制御部21に対しセッション制御部5からセッション切替が終了したことを示す信号が送信される(C321)。これにより、通信相手先17と切り替え先端末25との通信を開始することができる。

[0067] 次に、本発明の第2の実施の形態による通信ネットワークの制御システムの一構成例を示す。図6に示すように、本実施の形態による通信ネットワークの制御システムBは、基本的には図1に示す構成と同様であるが、通信端末22が1つであり、アクセス方法(1)22－1とアクセス方法(2)22－2とを切り替えるものである。尚、図6に示すユーザ関連情報収集提供部31のうちの必須構成は、ネットワーク状態33、加入者情報35－1、ユーザ居場所管理機能35－3、端末能力管理機能37－1である。

[0068] 図5は、同一端末におけるアクセス方法の切替の手順を示す図である。これまでは、図1及び図4を参照して、通信端末(#1)23と切替先通信端末(＃2)25との間で切替を行なう手順について説明したが、図5ではアクセス方法1とアクセス方法2との間で経路およびセッションを切り替える手順について示す。通信端末22は、例えばW-CDMAの移動体通信手段に基づくアクセス方法1と、無線LANなどのホットスポットで高速の通信を行なうための無線通信手段に基づくアクセス方法2との2つのアクセス方法を具備しているものとする。異なるアクセス方法をアクセス方法1(22－1)とアクセス方法2(22－2)として示している。

[0069] 通信端末22がどのようなアクセス方法を具備しているかは、ユーザ関連情報収集提供部31の端末能力管理機能37－1において管理されている。ユーザ関連情報収集提供部31におけるネットワーク状態33は、アクセス方法1(22－1)の経路、アクセス方法2(22－2)の経路、それぞれのネットワークの状態を管理し、QoSや伝送レートや無線アクセス方式の種類などをサービス移動制御部21に提供する。

[0070] アクセス方法1(22－1)とアクセス方法2(22－2)とでは、マルチメディアサブシステムやモビリティ管理などの管理・制御の運営システムが異なる可能性がある。ユー

ザ関連情報収集提供部31は、ネットワークオペレータとは別のサードパーティの企業が運営し、ネットワークオペレータから情報を収集することにより、サービス移動制御部21に対し情報を提供する役割を担ってもよい。また、一つのネットワークオペレータがユーザ関連情報収集提供部31、サービス移動制御部21、異なるアクセス方法ともすべて管理を行ってもよい。そのため、ユーザ関連情報収集提供部31と各ネットワークノードとの間のインターフェイスは標準化されていることが望ましい。ユーザプロファイルのユーザ居場所管理機能35－3は、利用できるアクセス方法がユーザの居場所によって設定されている場合に使用される。例えば、ホットスポットの場所とユーザの位置を関連させて、ユーザがホットスポットのサービス範囲内にいることを示す情報を管理する。また、端末プレゼンス管理情報により、端末の位置を特定し、ホットスポットのサービス範囲内に端末があること管理してもよい。

[0071] 図4における手順の説明においては、端末切替について説明を行ったが、図6を参照しつつ同一端末における経路変更について説明する。基本的なフローは、同じものを利用可能である。但し、上記端末切替要求信号は経路切替要求信号に変更される。上記端末切替要求信号には、切替先通信端末の能力が含まれていたが、同一端末内での切替の場合はこの情報は必要とされない。経路切替要求信号は、切替先のアクセス方法や、切替先の電波状況、切替先のルーティングアドレス、切替先のドメイン名、切替先のビットレートなどを含んでいる(C401)。

[0072] また、図4で説明したようにネットワーク側から自動的に経路変更を行うことも可能であり、その場合には、ユーザ関連情報収集提供部31とサービス移動制御部21とによって切替の判断を行う(C401')。切替の判断は、主としてネットワーク状態と端末プレゼンス管理機能とから提供される情報で行なわれ、例えば、通信端末が2つのアクセス方法を利用でき、現在使用中のアクセス方法よりも、もう一方のアクセス方法のほうが高いビットレートで通信できることを検知した際に切替を命令する。ビットレートやQoSに応じてメディア変換が必要な場合には、メディア変換の手続きを行う。但し、同一端末であるため、図4の場合のように、端末の種別や属性の相違による変換の必要はない。またセッションの中断処理については、メディア変換が行われないときには省略も可能であり、アプリケーションの起動処理も必要ない。例えば、セッションに

関する情報をまったく変更する必要がない場合には、モビリティ管理部に対して経路変更を指示するだけでアクセス方法の切替が行われる場合もある。その指示は、サービス移動制御部で作成され、具体的な指示を含んだセッション切替要求信号が送信される。これにより、同じ端末においてアクセス方法をスムーズに変更することができる。

[0073] 本発明の実施の形態によれば、ユーザは、自己の状況の変化に応じて、切替要求時の簡単なボタン操作などだけで、使用する通信端末の切り替えを簡単にすることができ、従来より大幅に操作の手間と時間的なロスを軽減することができ、より高度なサービスを享受することができる。

[0074] また、配信側のサーバ装置においても、特別に新規の機能を実装せずに配信サービスが続けられるという利点がある。加えて、受信側の通信端末間の能力が異なっても、データ形式が個々の通信端末に応じて最適化されて伝送されるため、通信端末側にもサーバ装置側にも大きな負荷を与えることがないという利点がある。こうしたサービス提供基盤の共通化により、ユーザは従来型の有線・無線のネットワークやサービスの違い、通信端末の種別の違い等を意識することがなくなり、シームレスでユビキタスなサービス環境を享受が可能となる。

産業上の利用可能性

[0075] 本発明は端末自体又は端末の通信方式の切り替えに利用できる。

請求の範囲

[1] 第1の通信端末と該第1の通信端末と通信を行っている第2の通信端末との間の通信を中断させることなく、前記第2の通信端末を該第2の通信端末とは異なる第3の通信端末に切替えて第1の通信端末と第3の通信端末との通信を継続させる制御を行う通信ネットワーク制御システムであって、

通信端末間における物理的、論理的な伝送経路を設定し管理するモビリティ管理手段と、

前記伝送経路上において通信端末間のセッションを制御するセッション制御手段と、

セッションの切り替えを前記セッション制御手段に対して指示するサービス移動制御手段と、

セッションの切り替え時に用いられるユーザ関連情報であって、ネットワーク状態と、ユーザに関するユーザプロファイルと、デバイスに関するデバイスプロファイルと、のうちの少なくともいずれかを含むユーザ関連情報を収集し前記サービス移動制御手段に対して提供するユーザ関連情報収集提供手段と

を備える通信ネットワーク制御システム。

[2] 前記サービス移動制御手段は、前記第2の通信端末から端末切替要求信号を受信するかまたは前記ユーザ関連情報に基づいて端末切替を行うか判断することにより、セッション切替要求信号を生成し、

前記セッション制御手段は、前記セッション切替要求信号を受信して、セッションを中断する機能と、前記モビリティ管理手段に対して前記第3の通信端末との伝送経路を設定するよう指示する機能と、前記第3の通信端末との間でセッションを確立する機能と、前記セッション確立後、前記通信相手先との間でセッションを再開する機能と、を有することを特徴とする請求項1に記載の通信ネットワーク制御システム。

[3] 前記ユーザプロファイルは、ユーザの加入者情報とユーザの居場所情報とユーザの趣味趣向の少なくともいずれかを含み、前記デバイスプロファイルは、デバイスの種類や各デバイスの状態情報の少なくともいずれかを含むことを特徴とする請求項1又は2に記載の通信ネットワーク制御システム。

[4] 前記サービス移動制御手段は、前記ユーザ関連情報収集提供手段からの情報又は前記第2の通信端末からの端末切替要求に基づいて、セッション切替要求を前記セッション制御手段に指示することを特徴とする請求項1又は2に記載の通信ネットワーク制御システム。

[5] 前記ユーザ関連情報収集提供手段は、前記サービス移動制御手段からユーザに関する情報提供要求があった際に所有者情報と位置情報とに基づいて関連する情報を提供することを特徴とする請求項1又は2に記載の通信ネットワーク制御システム。

[6] ネットワーク主導の通信端末切替処理は、ユーザ関連情報収集提供手段から提供される前記第2の通信端末と前記第3の通信端末とのネットワーク状態と端末能力情報とに基づいて起動されることを特徴とする請求項5に記載の通信ネットワーク制御システム。

[7] さらにネットワーク上にメディア変換手段を有し、

前記サービス移動制御手段がメディアに関して指示する情報を生成し、セッション切替要求とともに前記セッション制御手段に送ることを特徴とする請求項1又は2に記載の通信ネットワーク制御システム。

[8] 前記メディアの変換処理を行うか否かを、前記第2の通信端末と前記第3の通信端末との端末能力とネットワーク状態とに基づいて判断することを特徴とする請求項7に記載の通信ネットワーク制御システム。

[9] 前記メディアの変換先と、前記メディアの変換処理の方法に関する指示を、ユーザプリファレンスに基づいて判断することを特徴とする請求項7に記載の通信ネットワーク制御システム。

[10] 前記メディアの変換先は、通信相手のメディア変換能力とネットワーク上のメディア変換手段の変換能力に基づいて判断されることを特徴とする請求項7に記載の通信ネットワーク制御システム。

[11] 前記サービス移動制御手段は、メディア変換能力を取得する要求を前記第1の通信端末に接続されるネットワークに要求するよう指示する情報を生成することを特徴とする請求項10に記載の通信ネットワーク制御システム。

[12] 前記第2の通信端末は切替先の通信端末を指定し、端末切替要求とともにネットワークに送ることを特徴とする請求項1又は2に記載の通信ネットワーク制御システム。

[13] 近距離通信により前記第3の通信端末との間で予め情報のやり取りを行なって取得した前記第3の通信端末の端末能力又は端末プレゼンス情報のうちの少なくともいずれか一方を前記端末切替要求に含めることを特徴とする請求項12に記載の通信ネットワーク制御システム。

[14] メディア変換先、メディア変換処理方法の指示情報を端末切替要求とともに行うことを特徴とする請求項12に記載の通信ネットワーク制御システム。

[15] 第1の通信端末と該第1の通信端末と通信を行っている第2の通信端末であって、複数のアクセス方法を有する第2の通信端末との間の通信を中断させることなく、当該通信を行っている少なくとも一つのアクセス方法を、前記通信を行っていない他のアクセス方法へ切替えて前記通信を継続させる制御を行う通信ネットワーク制御システムであって、

通信端末間における物理的、論理的な伝送経路を設定し管理するモビリティ管理手段と、

前記伝送経路上において通信端末間のセッションを制御するセッション制御手段と、

セッションの切替えを前記セッション制御手段に対して指示するサービス移動制御手段と、

ネットワーク状態と、ユーザに関するユーザプロファイルと、デバイスに関するデバイスプロファイルと、のうちの少なくともいずれかを含むユーザ関連情報を収集し提供するユーザ関連情報収集提供手段と、を有し、

前記サービス移動制御手段は、該ユーザ関連情報収集提供手段からの情報、または、通信端末からのアクセス方法切替要求信号に基づいて、セッション切替要求信号を生成し、前記セッション制御手段に命令することを特徴とする通信ネットワーク制御システム。

[16] 前記ユーザ関連情報収集提供手段は、前記サービス移動制御手段からユーザに関する情報の要求があった際に、所有者情報と位置情報とに基づいて関連する情報

を前記サービス移動制御手段へ提供することを特徴とする請求項15に記載の通信ネットワーク制御システム。

[17] ネットワーク主導によるアクセス方法の切替処理の起動を、前記通信端末のプレゼンス情報とネットワーク状態との少なくともいずれか一方に基づいて判断することを特徴とする請求項15に記載の通信ネットワーク制御システム。

[18] ネットワーク主導のアクセス方法の切替は、ユーザの居場所情報とユーザプリファレンスとに基づいて行われることを特徴とする請求項17に記載の通信ネットワーク制御システム。

[19] さらに、メディア変換手段をネットワーク内に有しており、該メディア変換手段において、前記サービス移動制御手段がメディア変換先とメディア変換処理方法について指示する情報を生成することを特徴とする請求項15に記載の通信ネットワーク制御システム。

[20] 前記メディア変換処理方法は、現在のアクセス方法と切替先のアクセス方法とのネットワーク状態に基づいて判断されることを特徴とする請求項19に記載の通信ネットワーク制御システム。

[21] 前記メディア変換先、前記メディア変換処理方法に関する指示を、前記ユーザプリファレンスに基づいて行うことを特徴とする請求項20に記載の通信ネットワーク制御システム。

[22] 前記メディア変換先は、通信相手のメディア変換能力とネットワークのメディア変換手段の変換能力との少なくともいずれか一方に基づいて判断されることを特徴とする請求項21に記載の通信ネットワーク制御システム。

[23] 前記サービス移動制御手段は、メディア変換能力取得する要求を通信相手のネットワークに要求するよう指示することを特徴とする請求項22に記載の通信ネットワーク制御システム。

[24] 前記第2の通信端末が切替先のアクセス方法を指定し、アクセス方法切替要求信号に含めてネットワークへ送信することを特徴とする請求項15に記載の通信ネットワーク制御システム。

[25] 前記メディア変換先、前記メディア変換処理方法の指示情報のうちの少なくともい

ずれか一方を、アクセス方法切替要求に含めることを特徴とする請求項24に記載の通信ネットワーク制御システム。

[26] 第1の通信端末と該第1の通信端末と通信を行っている第2の通信端末との間において物理的、論理的な伝送経路を設定された状態において、セッションの切り替え時に用いられるユーザ関連情報であって、ネットワーク状態と、ユーザに関するユーザプロファイルと、デバイスに関するデバイスプロファイルと、のうちの少なくともいずれかを含むユーザ関連情報を収集するステップと、

前記伝送経路上において通信端末間におけるセッションの切替えが指示された場合に、該セッションの切替え指示に応じて、収集された前記ユーザ関連情報に基づいて前記第1の通信端末と前記第2の通信端末との間の通信を中断させることなく、前記第2の通信端末を該第2の通信端末とは異なる第3の通信端末に切替えて第1の通信端末と第3の通信端末間において通信を継続させるためのセッションの切り替えを行うステップと

を備える通信ネットワーク制御方法。

[27] ユーザに関する情報の要求があった際に、所有者情報と位置情報とに基づいて関連する情報を提供するステップを有することを特徴とする請求項26に記載の通信ネットワーク制御方法。

[28] ネットワーク主導の端末切替の起動を、前記第2の通信端末と前記第3の通信端末との間のネットワーク状態と端末能力情報とのうちの少なくともいずれか一方に基づいて行なうことを特徴とする請求項26に記載の通信ネットワーク制御方法。

[29] メディア変換先とメディア変換処理方法について指示する情報を生成するステップと、 該情報に基づいてセッション切替に関するセッションの指示を行うことを特徴とする請求項26に記載の通信ネットワーク制御方法。

[30] 前記メディア変換先を、通信相手のメディア変換能力とネットワークのメディア変換手段との変換能力とに基づいて判断することを特徴とする請求項29に記載の通信ネットワーク制御方法。

[31] メディア変換能力を取得するための要求を通信相手のネットワークに要求するように指示する情報を生成するステップを有することを特徴とする請求項30に記載の通

信ネットワーク制御方法。

[32] 第1の通信端末と該第1の通信端末と通信を行っており複数のアクセス方法を有する第2の通信端末との間において物理的、論理的な伝送経路を設定された状態において、セッションの切り替え時に用いられるユーザ関連情報であって、ネットワーク状態と、ユーザに関するユーザプロファイルと、デバイスに関するデバイスプロファイルと、のうちの少なくともいずれかを含むユーザ関連情報を収集するステップと、

前記伝送経路上において通信端末間のおけるセッションの切替えが指示された場合に、該セッションの切替え指示に応じて、収集された前記ユーザ関連情報に基づいて前記第1の通信端末と前記第2の通信端末との間の通信を中断させることなく、前記第2の通信端末におけるアクセス方法を切替えて通信を継続させるためのセッションの切り替えを行うステップと

を備える通信ネットワーク制御方法。

[33] ユーザに関する情報の要求があった際に、前記通信端末の所有者情報と位置情報とに基づいて関連する情報を提供するステップを有することを特徴とする請求項32に記載の通信ネットワーク制御方法。

[34] ネットワーク主導によるアクセス方法の切替処理の起動を、前記通信端末のプレゼンス情報とネットワーク状態との少なくともいずれか一方に基づいて判断することを特徴とする請求項32に記載の通信ネットワーク制御システム。

[35] メディア変換先とメディア変換処理方法について指示する情報を生成するステップと、

該情報に基づいてセッション切替に関するセッションの指示を行うことを特徴とする請求項32に記載の通信ネットワーク制御方法。

[36] 前記メディア変換先を、通信相手のメディア変換能力とネットワークのメディア変換手段との変換能力とに基づいて判断することを特徴とする請求項35に記載の通信ネットワーク制御方法。

[37] メディア変換能力を取得するための要求を通信相手のネットワークに要求するように指示する情報を生成するステップを有することを特徴とする請求項36に記載の通信ネットワーク制御方法。

[38] 通信端末間における物理的、論理的な伝送経路を設定し管理するモビリティ管理手段と、前記伝送経路上において通信端末間のセッションを制御するセッション制御手段と、セッションの切替えを前記セッション制御手段に対して指示するサービス移動制御手段と、セッションの切り替え時に用いられるユーザ関連情報であって、ネットワーク状態と、ユーザに関するユーザプロファイルと、デバイスに関するデバイスプロファイルと、のうちの少なくともいずれかを含むユーザ関連情報を収集し前記サービス移動制御手段に対して提供するユーザ関連情報収集提供手段とを備える通信ネットワーク制御システムにおいて用いられる通信端末であって、

前記サービス移動制御手段への端末切り替え要求を行い、前記通信端末は、切替先の通信端末を指定し、端末切替要求に含めてネットワークへ送信することを特徴とする通信端末。

[39] 前記通信端末は、近距離通信により切替先の通信端末との間で予め情報のやり取りを行なって、切替先の端末能力や端末プレゼンス情報を端末切替要求に含めることを特徴とする請求項38に記載の通信端末。

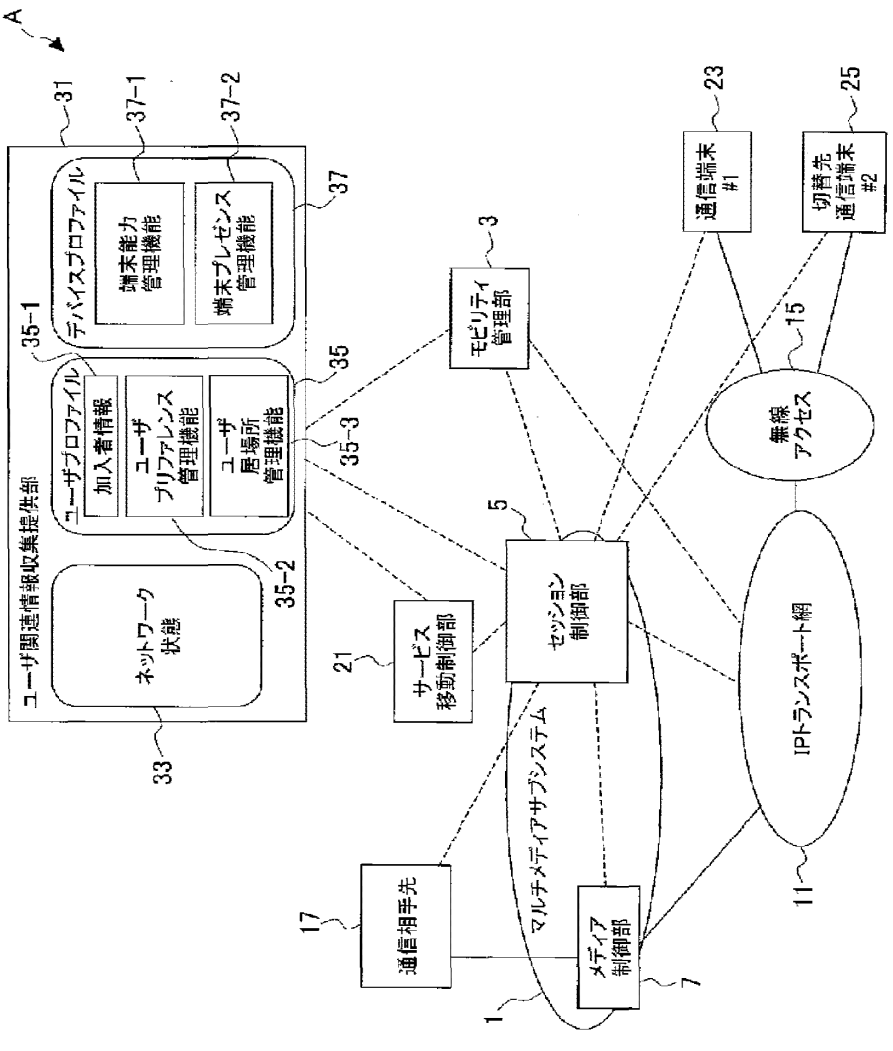
[40] メディア変換先、メディア変換処理方法の指示情報を前記端末切替要求に含めることを特徴とする請求項38に記載の通信端末。

[41] 通信端末間における物理的、論理的な伝送経路を設定し管理するモビリティ管理手段と、前記伝送経路上において通信端末間のセッションを制御するセッション制御手段と、セッションの切替えを前記セッション制御手段に対して指示するサービス移動制御手段と、セッションの切り替え時に用いられるユーザ関連情報であって、ネットワーク状態と、ユーザに関するユーザプロファイルと、デバイスに関するデバイスプロファイルと、のうちの少なくともいずれかを含むユーザ関連情報を収集し前記サービス移動制御手段に対して提供するユーザ関連情報収集提供手段とを備える通信ネットワーク制御システムにおいて、第1の通信端末と該第1の通信端末と通信を行っている第2の通信端末であって複数のアクセス方法を有する第2の通信端末との間の通信を中断させることなく、当該通信を行っている少なくとも一つのアクセス方法を、前記通信を行っていない他のアクセス方法へ切替えて前記通信を継続させる制御を行う第2の通信端末であって、 前記第2の通信端末が切替先のアクセス方法を指定

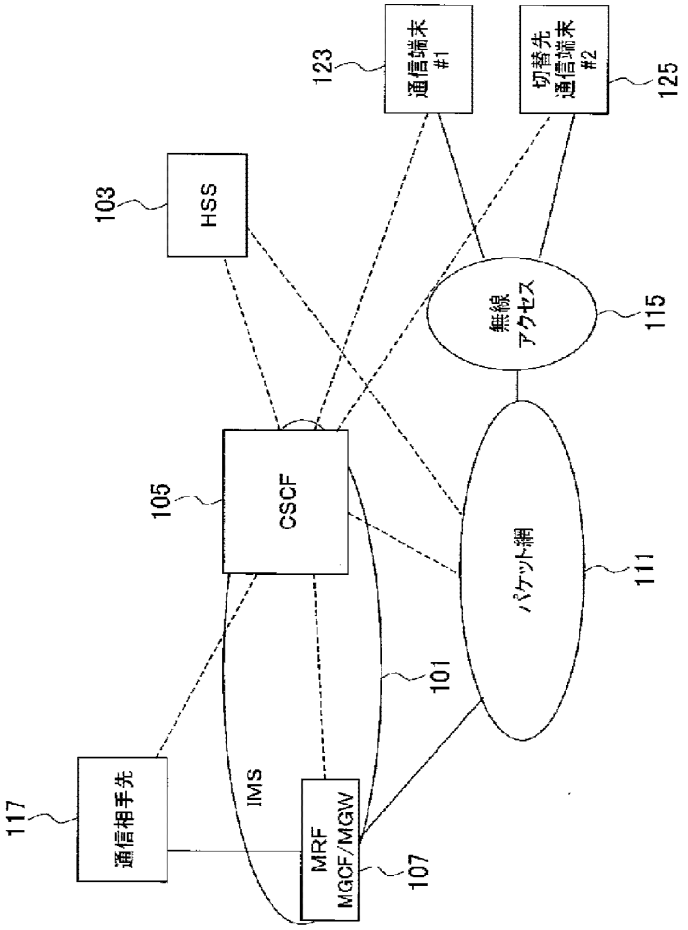
し、アクセス方法切替要求信号に含めてネットワークへ送信することを特徴とする第2の通信端末。

[42] メディア変換先、前記メディア変換処理方法の指示情報のうちの少なくともいずれか一方を、アクセス方法切替要求に含めることを特徴とする請求項41に記載の第2の通信端末。

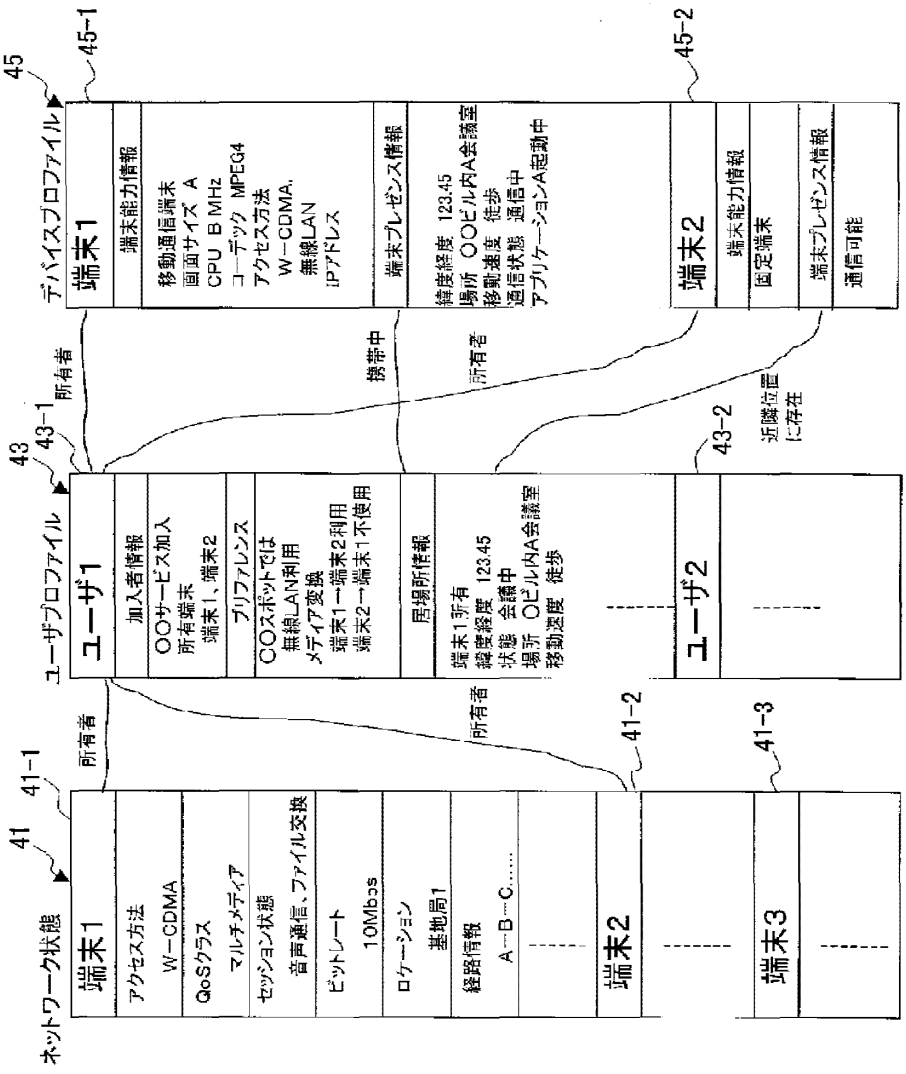
[図1]


A
31
37-1
37-2
37
35-1
35
35-3
35-2
33
ユーザ関連情報収集提供部
デバイスプロファイル
端末能力
管理機能
端末プレゼンス
管理機能
ユーザプロファイル
加入者情報
ユーザ
プリファレンス
管理機能
ユーザ
居場所
管理機能
ネットワーク
状態
3
モビリティ
管理部
5
セッション
制御部
21
サービス
移動制御部
17
通信相手先
1
マルチメディアサブシステム
7
メディア
制御部
23
通信端末
#1
25
切替先
通信端末
#2
15
無線
アクセス
11
IPトランスポート網

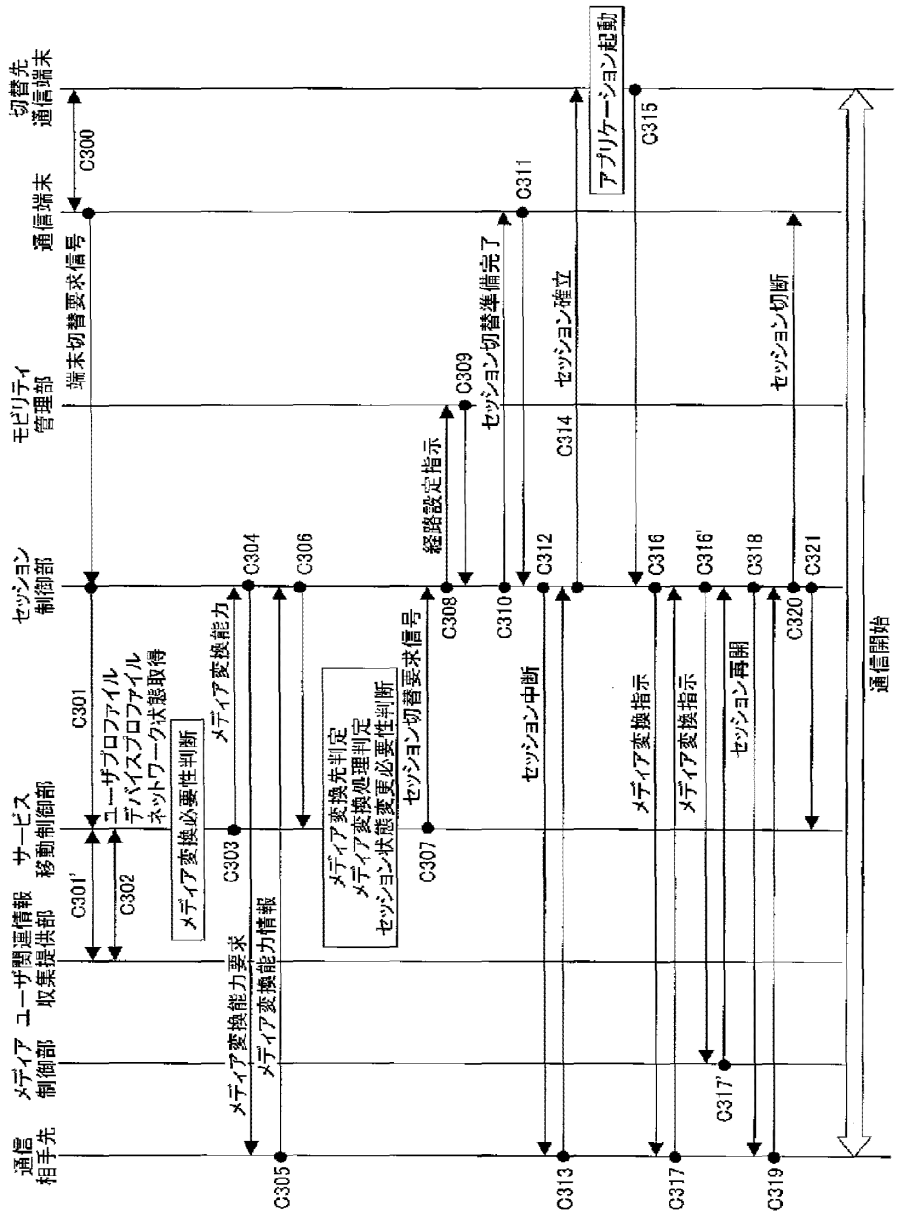
[図2]


通信端末
#1
123
切替先
通信端末
#2
125
HSS
103
無線
アクセス
115
CSCF
105
パケット網
111
101
IMS
MRF
MGCF/MGW
107
通信相手先
117

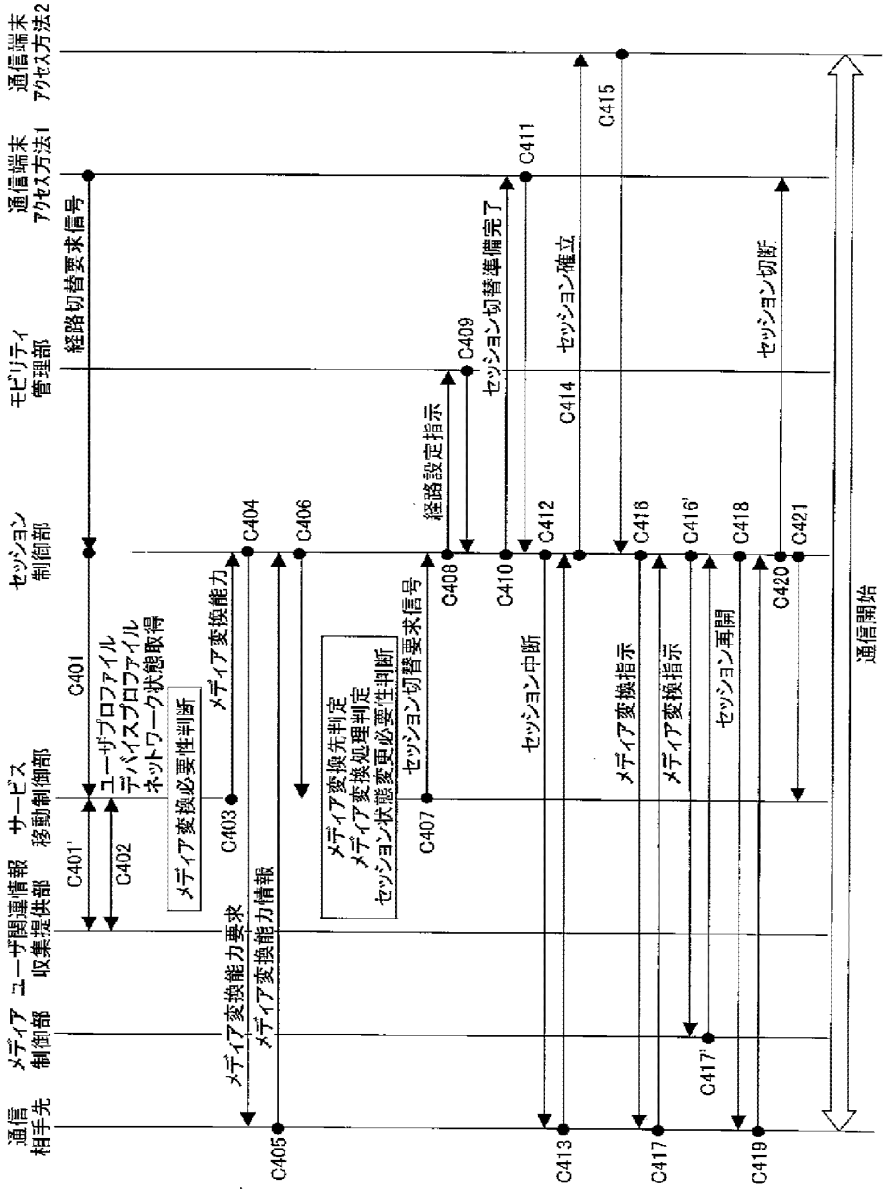
[図3]


ネットワーク状態
41
41-1
端末1
アクセス方法
W-CDMA
QoSクラス
マルチメディア
セッション状態
音声通信、ファイル交換
ビットレート
10Mbps
ロケーション
基地局1
経路情報
A-B-C……
端末2
端末3
所有者
ユーザプロファイル
43
43-1
ユーザ1
加入者情報
○○サービス加入
所有端末
端末1、端末2
プリファレンス
○○スポットでは
無線LAN利用
メディア変換
端末1ー端末2利用
端末2ー端末1不使用
居場所情報
端末1所有
緯度経度 123.45
状態 会議中
場所 ○○ビル内A会議室
移動速度 徒歩
ユーザ2
43-2
41-2
41-3
所有者
携帯中
所有者
近隣位置に存在
デバイスプロファイル
45
45-1
端末1
端末能力情報
移動通信端末
画面サイズ A
CPU B MHz
コーデック MPEG4
アクセス方法
W-CDMA,
無線LAN
IPアドレス
端末プレゼンス情報
緯度経度 123.45
場所 ○○ビル内A会議室
移動速度 徒歩
通信状態 通信中
アプリケーションA起動中
45-2
端末2
端末能力情報
固定端末
端末プレゼンス情報
通信可能

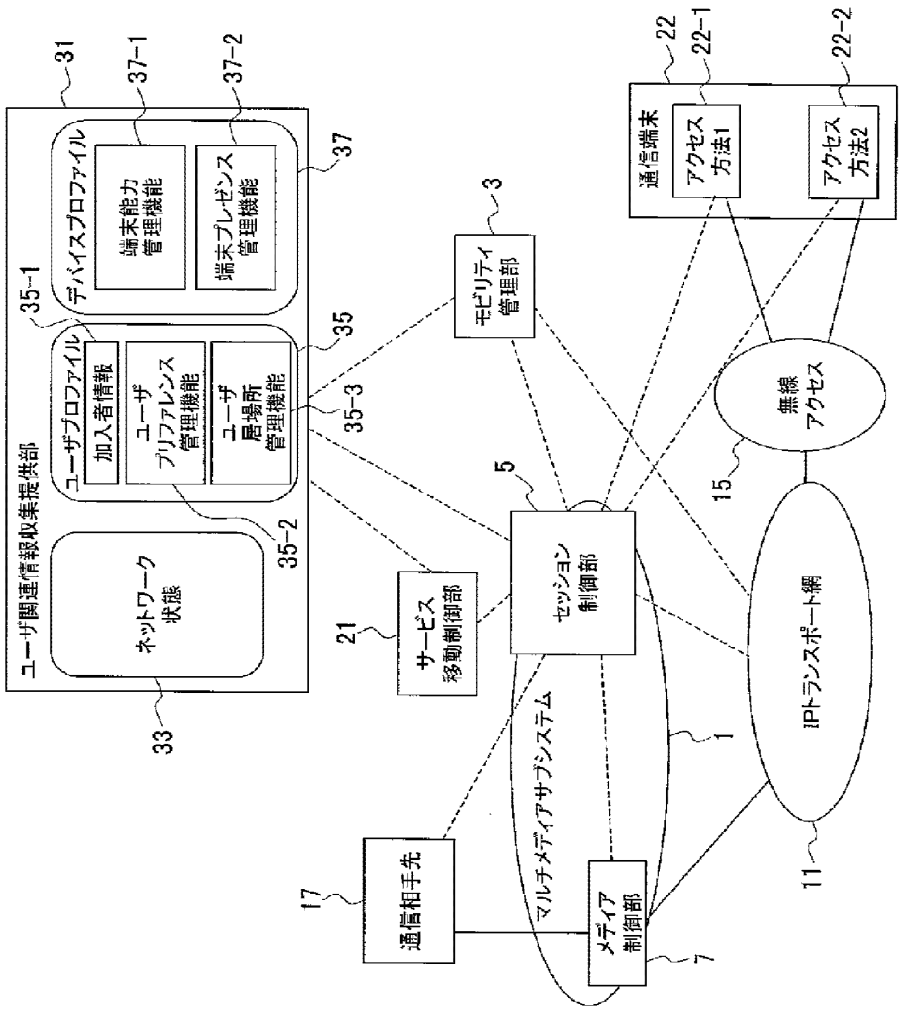
[図4]


通信相手先
メディア制御部
ユーザ関連情報収集提供部
サービス移動制御部
セッション制御部
モビリティ管理部
通信端末
切替先通信端末
C300
C301'
C301
C302
C303
C304
C305
C306
C307
C308
C309
C310
C311
C312
C313
C314
C315
C316
C316'
C317
C317'
C318
C319
C320
C321
端末切替要求信号
ユーザプロファイル
デバイスプロファイル
ネットワーク状態取得
メディア変換必要性判断
メディア変換能力
メディア変換能力要求
メディア変換能力情報
メディア変換先判定
メディア変換処理判定
セッション状態変更必要性判断
セッション切替要求信号
経路設定指示
セッション切替準備完了
セッション確立
アプリケーション起動
セッション中断
メディア変換指示
メディア変換指示
セッション再開
セッション切断
通信開始

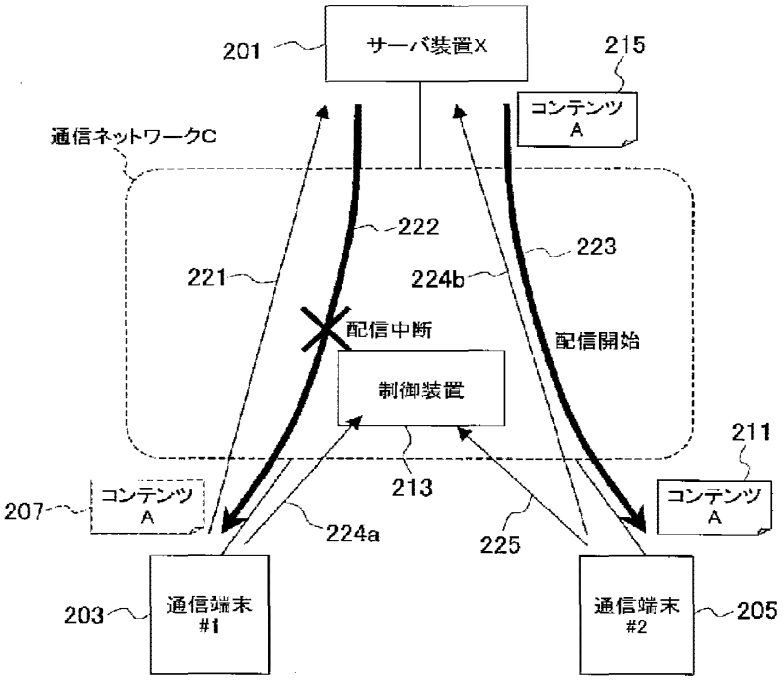
[図5]


通信相手先
メディア制御部
ユーザ関連情報収集提供部
サービス移動制御部
セッション制御部
モビリティ管理部
通信端末アクセス方法1
通信端末アクセス方法2
C401
C401'
C402
ユーザプロファイル
デバイスプロファイル
ネットワーク状態取得
メディア変換必要性判断
C403
メディア変換能力要求
メディア変換能力情報
C404
メディア変換能力
C405
C406
メディア変換先判定
メディア変換処理判定
セッション状態変更必要性判断
C407
セッション切替要求信号
C408
経路設定指示
C409
セッション切替準備完了
C410
C411
経路切替要求信号
C412
セッション中断
C413
C414
セッション確立
C415
メディア変換指示
C416
C416'
メディア変換指示
C417
C417'
セッション再開
C418
C419
C420
セッション切断
C421
通信開始

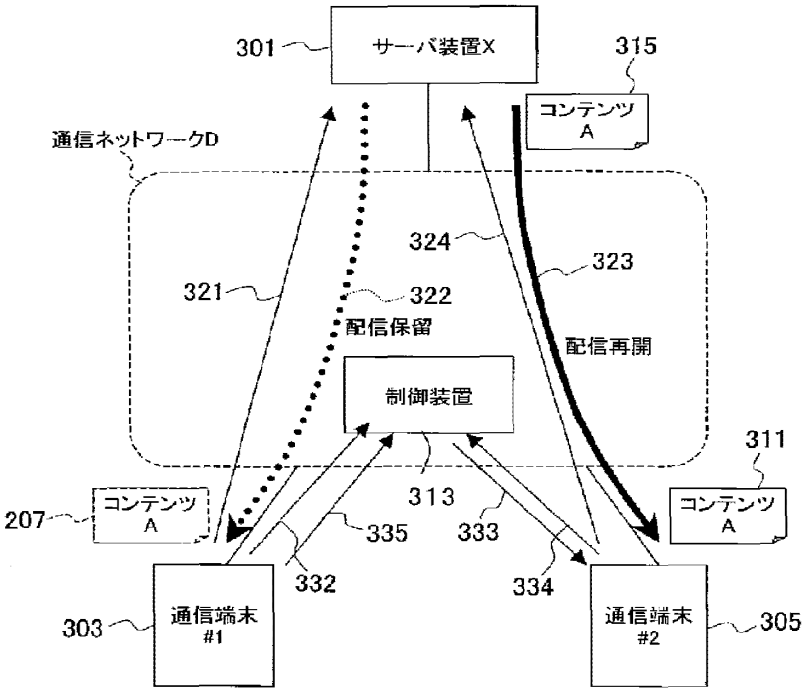
[図6]


ユーザ関連情報収集提供部
ネットワーク状態
ユーザプロファイル
加入者情報
ユーザプリファレンス管理機能
ユーザ居場所管理機能
デバイスプロファイル
端末能力管理機能
端末プレゼンス管理機能
31
33
35
35-1
35-2
35-3
37
37-1
37-2
サービス移動制御部
21
モビリティ管理部
3
セッション制御部
5
マルチメディアサブシステム
メディア制御部
7
通信相手先
17
IPトランスポート網
1
11
無線アクセス
15
通信端末
22
22-1
22-2
アクセス方法1
アクセス方法2

[図7]


201
サーバ装置X
215
コンテンツ
A
通信ネットワークC
222
223
221
224b
配信中断
配信開始
制御装置
211
213
207
コンテンツ
A
224a
225
コンテンツ
A
203
通信端末
#1
通信端末
#2
205

[図8]


301
サーバ装置X
315
コンテンツ
A
通信ネットワークD
324
323
321
322
配信保留
配信再開
制御装置
311
207
コンテンツ
A
313
335
333
コンテンツ
A
332
334
303
通信端末
#1
通信端末
#2
305

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2006/300324

A. CLASSIFICATION OF SUBJECT MATTER
H04L12/56(2006.01), ***H04Q7/38***(2006.01)

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)
H04L12/56(2006.01), ***H04Q7/38***(2006.01)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2006
Kokai Jitsuyo Shinan Koho 1971-2006 Toroku Jitsuyo Shinan Koho 1994-2006

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.
X Y	Takayuki WARABINO et al., "Tanmatsukan no Seamless na Kirikae o Jitsugen suru Device Hand-off Hoshiki no Teian", Information Processing Society of Japan Kenkyu Hokoku 2003-MBL-27-15, 14 November, 2003 (14.11.03), page 107, left column, line 22 to page 108, left column, line 23; page 109, left column, lines 8 to 18	1-14,26-31,38-40 15-25,32-37,41,42
X Y	Masatoshi KAWARAZAKI et al., "Meta Data o Riyo shita Contents Hand-over System -MetaPORT-, IEICE Technical Report IN2003-3, 09 May, 2003 (09.05.03), page 14, left column, line 9 to page 15, left column, line 8; page 15, right column, line 6 to page 17, left column, line 7	1-12,14,26-31,38,40 15-25,32-37,41,42

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
09 March, 2006 (09.03.06)	20 March, 2006 (20.03.06)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2006/300324

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	JP 2004-336310 A (Nippon Telegraph And Telephone Corp.), 25 November, 2004 (25.11.04), Par. Nos. [0009] to [0010], [0016], [0018], [0024] (Family: none)	1-6,12, 26-28,38 15-18,24, 32-34,41
Y	JP 2004-208001 A (Sharp Corp.), 22 July, 2004 (22.07.04), Abstract; Fig. 2 & WO 2004/062310 A1 & EP 1585354 A1	15-25,32-37, 41,42

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００６／３００３２４

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　*H04L12/56(2006.01), H04Q7/38(2006.01)*

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　*H04L12/56(2006.01), H04Q7/38(2006.01)*

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００６年
日本国実用新案登録公報	１９９６－２００６年
日本国登録実用新案公報	１９９４－２００６年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	蕨野貴之他，端末間のシームレスな切り換えを実現するデバイスハンドオフ方式の提案，情報処理学会研究報告 2003-MBL-27-15, 2003.11.14 第107頁左欄第22行－第108頁左欄第23行，第109頁左欄第8－18行	1-14, 26-31, 38-40
Y		15-25, 32-37, 41, 42

☑　Ｃ欄の続きにも文献が列挙されている。

☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日 ０９．０３．２００６	国際調査報告の発送日 ２０．０３．２００６
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　５Ｘ　２９４７ 高橋　真之 電話番号　０３－３５８１－１１０１　内線　３５９６

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（２００５年４月）

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X Y	川原崎雅敏他，メタデータを利用したコンテンツハンドオーバシステムーMetaPORTー，電子情報通信学会技術研究報告 IN2003-3，2003.05.09 第14頁左欄第9行ー第15頁左欄第8行， 第15頁右欄第6行ー第17頁左欄第7行	1-12,14, 26-31,38,40 15-25,32-37, 41,42
X Y	JP 2004-336310 A（日本電信電話株式会社）2004.11.25（ファミリーなし） 段落0009ー0010，段落0016，段落0018，段落0024	1-6,12, 26-28,38 15-18,24, 32-34,41
Y	JP 2004-208001 A（シャープ株式会社）2004.07.22，要約，図2 & WO 2004/062310 A1 & EP 1585354 A1	15-25,32-37, 41,42

(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2007-43598
(P2007-43598A)
(43)公開日　平成19年2月15日(2007.2.15)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/08	(2006.01)	H04L	9/00	601B	5J104
		H04L	9/00	601E	

審査請求 未請求　請求項の数 63　OL　（全 27 頁）

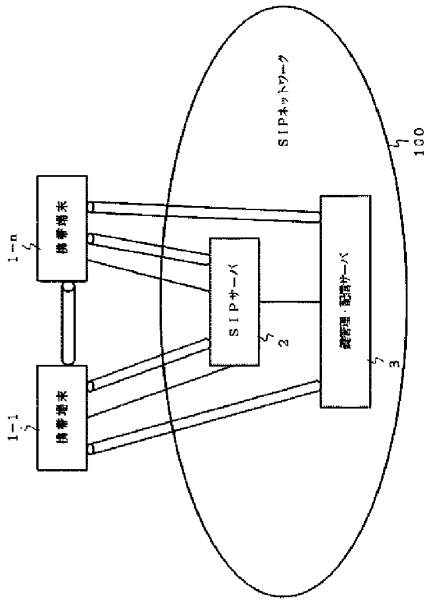
(21)出願番号　特願2005-227592 (P2005-227592)
(22)出願日　平成17年8月5日 (2005.8.5)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　100088812
弁理士　▲柳▼川　信
(72)発明者　坂口　泰彦
東京都港区芝五丁目７番１号　日本電気株式会社内
(72)発明者　三栖　利之
東京都港区芝五丁目７番１号　日本電気株式会社内
(72)発明者　冨山　卓二
東京都港区芝五丁目７番１号　日本電気株式会社内

最終頁に続く

(54)【発明の名称】通信システム、鍵管理・配信サーバ、端末装置及びそれらに用いるデータ通信方法並びにそのプログラム

Ex.1002 / Page 403 of 1173
Cisco Systems, Inc.



<1> 本発明は通信システム、鍵管理・配信サーバ、端末装置及びそれらに用いるデータ通信方法並びにそのプログラムに関し、特に動的生成された暗号鍵を安全に取得してデータ通信を行う方法に関する。

<2> 近年、携帯電話機等の携帯端末装置においては、その多機能化に伴って無線基地局を介した無線通信以外にも、携帯端末装置間を近距離無線通信等で直接接続してデータ通信を行う方法も提案されている（例えば、特許文献１参照）。

<3> その際、上記のように、携帯端末同士をＰ２Ｐ（Ｐｅｅｒ　ｔｏ　Ｐｅｅｒ：端末間の直接通信）通信（近距離無線通信等によるＰ２Ｐも含む）で接続する場合には、携帯端末装置が持っている秘密鍵を使って通信しようとすると、通信相手の携帯端末装置に対して自端末の秘密鍵を公開するか、公開鍵暗号化方式を使う必要がある。但し、近距離無線通信によるＰ２Ｐ通信は、端末装置同士が遠距離の場合、Ｐ２Ｐ通信を実現することはできない。

<4> 【特許文献 1】 特開２００３－０８７２６７号公報

<5> 上述した従来のデータ通信方法では、秘密鍵を公開する場合、自分の秘密鍵を複数人が持つことになるので、不正利用される恐れがあるという問題がある。また、公開鍵暗号化方式を使う場合には、複雑な暗号復号処理が必要となり、携帯端末装置のような小規模端末での処理には適さない。

<6> さらに、秘密鍵を通信相手毎に複数持つことは、それらの秘密鍵を記憶する携帯端末装置のメモリの記憶領域を圧迫し、通信相手のうちの誰か一人が携帯端末装置を紛失すると、そのメモリ内に記憶された複数の秘密鍵が漏洩することとなり、大きな問題となる。

<7> 一方、従来のデータ通信方法では、ＨＴＴＰ（ＨＴＴＰＳ）［Ｈｙｐｅｒ　Ｔｅｘｔ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ（Ｈｙｐｅｒ　Ｔｅｘｔ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ　ｏｖｅｒ　ｔｒａｎｓｐｏｒｔ　ｌａｙｅｒ　ｓｅｃｕｒｉｔｙ／ｓｅｃｕｒｅ　ｓｏｃｋｅｔｓ　ｌａｙｅｒ）］を使って鍵配送をする方法もあるが、リアルタイム性にかけることと、発信者が通信を開始したいという契機で通信相手に対しても同じ鍵を配送しなければならない。しかしながら、ＨＴＴＰ（ＨＴＴＰＳ）の性質上、鍵管理・配送サーバ側から端末装置（ＨＴＴＰクライアント）に対して鍵配送のトリガをかけることは困難である。

<8> そこで、本発明の目的は上記の問題点を解消し、暗号鍵の紛失による不正利用を防止することができ、暗号鍵を用いて端末間の直接通信を安全に行うことができる通信システム、鍵管理・配信サーバ、端末装置及びそれらに用いるデータ通信方法並びにそのプログラムを提供することにある。

Ex.1002 / Page 404 of 1173
Cisco Systems, Inc.

<9> 本発明による通信システムは、第１の端末装置及び第２の端末装置各々が共有する暗号鍵を基に前記第１の端末装置と前記第２の端末装置との間にピアツーピアのデータ通信を実現する通信システムであって、

前記第１の端末装置及び前記第２の端末装置のうちの一方が前記ピアツーピアのデータ通信開始のトリガを第１の通信方法による通信路にて前記第１の端末装置及び前記第２の端末装置のうちの他方に通知し、

前記第１の端末装置及び前記第２の端末装置各々が前記データ通信開始トリガの送受信に応答してそれぞれ前記暗号鍵を中継する中継サーバとの間に第２の通信方法による通信路を形成しかつ前記第１の通信方法による通信路から前記第２の通信方法による通信路に切替えて前記中継サーバを介して前記第１の端末装置と前記第２の端末装置との間で前記暗号鍵を共有している。

<10> 本発明による他の通信システムは、鍵管理・配信サーバから第１の端末装置及び第２の端末装置に配信される暗号鍵を基に前記第１の端末装置と前記第２の端末装置との間にピアツーピアのデータ通信を実現する通信システムであって、

前記第１の端末装置及び前記第２の端末装置のうちの一方が前記ピアツーピアのデータ通信開始のトリガを、前記鍵管理・配信サーバを経由してかつ第１の通信方法による通信路にて前記第１の端末装置及び前記第２の端末装置のうちの他方に通知し、

前記第１の端末装置及び前記第２の端末装置各々が前記データ通信開始トリガの送受信に応答してそれぞれ前記鍵管理・配信サーバとの間に第２の通信方法による通信路を形成しかつ前記第１の通信方法による通信路から当該第２の通信方法による通信路に切替えて前記鍵管理・配信サーバから前記第１の端末装置及び前記第２の端末装置各々に前記暗号鍵を配信している。

<11> 本発明による鍵管理・配信サーバは、第１の端末装置と第２の端末装置との間にピアツーピアのデータ通信を実現する通信システムにおいて前記第１の端末装置及び前記第２の端末装置各々に暗号鍵を配信する鍵管理・配信サーバであって、

前記第１の端末装置及び前記第２の端末装置のうちの一方が送信する前記ピアツーピアのデータ通信開始のトリガを、第１の通信方法による通信路にて受信した時に当該データ通信開始のトリガを前記第１の端末装置及び前記第２の端末装置のうちの他方に転送する手段と、前記第１の端末装置及び前記第２の端末装置各々が前記ピアツーピアのデータ通信開始のトリガの送受信に応答して切替えかつそれぞれ自装置との間に形成した第２の通信方法による通信路にて前記暗号鍵を配信する手段とを備えている。

<12> 本発明による端末装置は、自装置及び他の端末装置各々が共有する暗号鍵を基に自装置と前記他の端末装置との間にピアツーピアのデータ通信を行う端末装置であって、

前記ピアツーピアのデータ通信開始のトリガを、前記暗号鍵を中継する中継サーバを経由してかつ第１の通信方法による通信路にて前記他の端末装置に送信し、自装置からの前記ピアツーピアのデータ通信開始のトリガの送信及び前記他の端末装置からの前記ピアツーピアのデータ通信開始のトリガの受信のいずれかに応答して前記中継サーバとの間に第２の通信方法による通信路を形成しかつ前記第１の通信方法による通信路から前記第２の通信方法による通信路に切替えて前記中継サーバを介して前記暗号鍵の送信及び受信のいずれかを行っている。

<13> 本発明による他の端末装置は、鍵管理・配信サーバから自装置及び他の端末装置に配信される暗号鍵を基に自装置と前記他の端末装置との間でピアツーピアのデータ通信を行う端末装置であって、

前記ピアツーピアのデータ通信開始のトリガを、前記鍵管理・配信サーバを経由してかつ第１の通信方法による通信路にて前記他の端末装置に送信し、自装置からの前記ピアツーピアのデータ通信開始のトリガの送信及び前記他の端末装置からの前記ピアツーピアのデータ通信開始のトリガの受信のいずれかに応答して前記鍵管理・配信サーバとの間に第２の通信方法による通信路を形成しかつ前記第１の通信方法による通信路から当該第２の通信方法による通信路に切替えて前記鍵管理・配信サーバから前記暗号鍵を受信している。

<14> 本発明によるデータ通信方法は、自装置及び他の端末装置各々が共有する暗号鍵を基に自装置と前記他の端末装置との間にピアツーピアのデータ通信を行うシステムに用いられるデータ通信方法であって、

前記端末装置が、

前記ピアツーピアのデータ通信開始のトリガを、前記暗号鍵を中継する中継サーバを経由してかつ第１の通信方法による通信路にて前記他の端末装置に送信する処理と、自装置からの前記ピアツーピアのデータ通信開始のトリガの送信及び前記他の端末装置からの前記ピアツーピアのデータ通信開始のトリガの受信のいずれかに応答して前記中継サーバとの間に第２の通信方法による通信路を形成しかつ前記第１の通信方法による通信路から前記第２の

Ex.1002 / Page 405 of 1173
Cisco Systems, Inc.

通信方法による通信路に切替えて前記中継サーバを介して前記暗号鍵の送信及び受信のいずれかを行う処理とを実行している。

<15> 本発明による他のデータ通信方法は、鍵管理・配信サーバから端末装置及び他の端末装置に配信される暗号鍵を基に前記端末装置と前記他の端末装置との間でピアツーピアのデータ通信を行うシステムに用いられるデータ通信方法であって、

前記端末装置が、前記ピアツーピアのデータ通信開始のトリガを、前記鍵管理・配信サーバを経由してかつ第１の通信方法による通信路にて前記他の端末装置に送信する処理と、前記ピアツーピアのデータ通信開始のトリガの送受信に応答して前記鍵管理・配信サーバとの間に第２の通信方法による通信路を形成しかつ前記第１の通信方法による通信路から当該第２の通信方法による通信路に切替えて前記鍵管理・配信サーバから前記暗号鍵を受信する処理とを実行している。

<16> 本発明によるデータ通信方法のプログラムは、自装置及び他の端末装置各々が共有する暗号鍵を基に自装置と前記他の端末装置との間にピアツーピアのデータ通信を行うシステムに用いられるデータ通信方法のプログラムであって、

前記ピアツーピアのデータ通信開始のトリガを、前記暗号鍵を中継する中継サーバを経由してかつ第１の通信方法による通信路にて前記他の端末装置に送信する処理と、自装置からの前記ピアツーピアのデータ通信開始のトリガの送信及び前記他の端末装置からの前記ピアツーピアのデータ通信開始のトリガの受信のいずれかに応答して前記中継サーバとの間に第２の通信方法による通信路を形成しかつ前記第１の通信方法による通信路から前記第２の通信方法による通信路に切替えて前記中継サーバを介して前記暗号鍵の送信及び受信のいずれかを行う処理とを前記端末装置のコンピュータに実行させている。

<17> 本発明による他のデータ通信方法のプログラムは、鍵管理・配信サーバから端末装置及び他の端末装置に配信される暗号鍵を基に前記端末装置と前記他の端末装置との間でピアツーピアのデータ通信を行うシステムに用いられるデータ通信方法のプログラムであって、

前記ピアツーピアのデータ通信開始のトリガを、前記鍵管理・配信サーバを経由してかつ第１の通信方法による通信路にて前記他の端末装置に送信する処理と、前記ピアツーピアのデータ通信開始のトリガの送受信に応答して前記鍵管理・配信サーバとの間に第２の通信方法による通信路を形成しかつ前記第１の通信方法による通信路から当該第２の通信方法による通信路に切替えて前記鍵管理・配信サーバから前記暗号鍵を受信する処理とを前記端末装置のコンピュータに実行させている。

<18> すなわち、本発明の通信システムは、端末装置が常にＳＩＰ（Ｓｅｓｓｉｏｎ　Ｉｎｉｔｉａｔｉｏｎ　Ｐｒｏｔｏｃｏｌ）サーバにロケーション情報を登録することによって、端末装置が通信要求を発行時に、鍵管理・配信サーバがそれを受領して着信側の端末装置に対して通信要求をリアルタイムに送信することが可能となる。

<19> 本発明の通信システムでは、鍵管理・配信サーバが通信要求をトリガとして、端末間の通信毎にユニークな秘密鍵を、通信する両者の端末装置に配信することによって、毎回違う秘密鍵（暗号鍵）で通信を行うため、秘密鍵の安全性が高くなり、また端末装置側でも毎回違う秘密鍵を使うにも関わらず、それらの秘密鍵を記憶しておく必要がなくなる。よって、本発明の通信システムでは、端末装置同士、特に携帯電話端末同士で安全なＰ２Ｐ（Ｐｅｅｒ　ｔｏ　Ｐｅｅｒ：端末間の直接通信）のデータ通信を可能とする。

<20> 本発明による端末装置は、ＳＩＰ（Ｓｅｓｓｉｏｎ　Ｉｎｉｔｉａｔｉｏｎ　Ｐｒｏｔｏｃｏｌ）を使用して通信を行う端末であり、常にＳＩＰサーバに対して端末装置のロケーション情報を登録している。ある端末装置から別の端末装置へのＰ２Ｐ通信を要求する時には、その登録されたロケーション情報を用いるＳＩＰサーバが通信開始要求を発信側の端末装置から着信側の端末装置へプロキシすることで、これら両方の端末装置は、ＩＰｓｅｃ［ＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）　ｓｅｃｕｒｉｔｙ　ｐｒｏｔｏｃｏｌ］を使用したシグナリングセッションを再構築するロケーション情報登録処理を行う。この動作によって、本発明による端末装置は、端末装置とＳＩＰサーバとの間に安全な情報の送受信を行うためのトンネルを形成することが可能となる。

<21> 本発明による端末装置は、ＳＩＰサーバを経由して鍵管理・配送する鍵管理・配信サーバに対して、端末装置とＳＩＰサーバとの間にトンネル形成が完了したことを通知するメッセージを送信することによって、鍵管理・配信サーバからＳＩＰサーバを経由して発信側の端末装置及び着信側の端末装置に対して安全なデータセッションの確立を行う信号を送信し、鍵配送に使用するデータセッションの確立を可能とする。

<22> 本発明による端末装置は、鍵管理：配信サーバから安全なデータセッションを通して、その通信のみに適用可能な秘密鍵を受領するとともに受領完了を示すメッセージを送信することによって、鍵管理・配信サーバから発信側の端末装置と着信側の端末装置とをＰ２Ｐで接続するためのデータセッション切替え要求［Ｐ２Ｐのセッションへ

Ex.1002 / Page 406 of 1173
Cisco Systems, Inc.

の張替え要求（これはセッションの送り先アドレスの書換えを示し、Ｐ２Ｐのセッションの追加を含んでいる）］の受信が可能となる。

<23> 本発明による端末装置は、データセッション切替え要求を受信すると、配送済みの秘密鍵を使用して、相手端末との間の暗号化されたデータセッションを確立することが可能となる。

<24> 本発明による端末装置は、ＳＩＰサーバとの間の安全なシグナリングセッション確立及び鍵管理・配信サーバとの間の暗号化された安全なデータセッションの確立のために、事前に交換した暗号化鍵を持っていてもよいし、公開鍵を互いに持っていてもよい。

<25> これによって、本発明の通信システムでは、端末装置をＳＩＰモジュールを搭載した端末とすることによって、発信側の端末装置がＳＩＰサーバ、鍵管理・配信サーバを経由して着信側の端末装置に対してデータ通信開始のトリガを送信することで、着信側の端末装置がリアルタイムにこのトリガを受信することが可能となる。

<26> 発信側の端末装置及び着信側の端末装置とがともに、上記のデータ通信開始トリガを送受信した契機で、ＳＩＰサーバに対するロケーション情報登録処理をやり直すと同時に、端末装置とＳＩＰサーバとの間のシグナリングセッションをＩＰｓｅｃを使用して確立する。この動作によって、本発明の通信システムでは、ＳＩＰサーバと携帯端末装置との間のＩＰｓｅｃセッションの確立時間とＩＰｓｅｃセッションの確立端末装置の数とを減らすことが可能となり、ネットワーク負荷及びサーバ負荷を減らすことが可能となる。このＩＰｓｅｃセッション上でシグナリングを行うことで、ユーザ情報やシグナリングに必要なデータの暗号化を行い、安全に通信することが可能となる。

<27> 上記のＩＰｓｅｃ上のシグナリングセッションで、発信側の端末装置と着信側の端末装置との間のＰ２Ｐデータ通信に使用する秘密鍵を交換することも可能であるが、鍵管理・配信サーバと発信側の端末装置及び着信側の端末装置との間のデータセッションをＩＰｓｅｃ上で確立し、このセッション上で秘密鍵の交換を行うことで、ＳＩＰサーバをはじめとしたサーバ装置で秘密鍵の入ったデータをプロキシすることがなくなるため、秘密鍵を参照することが不可能となり、さらに安全に秘密鍵を配送管理することが可能となる。

<28> Ｐ２Ｐデータ通信で使用する秘密鍵は、鍵管理・配信サーバが一通信毎に生成する秘密鍵を発信側の端末装置及び着信側の端末装置に配送して使用するため、毎回使用する秘密鍵が違うものとなる。そのため、本発明の通信システムでは、一度使った秘密鍵をさらに不正に利用し続けたり、秘密鍵の紛失による不正利用を防止することが可能となる。

<29> 本発明は、以下に述べるような構成及び動作とすることで、暗号鍵の紛失による不正利用を防止することができ、暗号鍵を用いて端末間の直接通信を安全に行うことができるという効果が得られる。

<30> 次に、本発明の実施例について図面を参照して説明する。図１は本発明の一実施例による通信システムの構成を示すブロック図である。図１において、本発明の一実施例による通信システムは携帯端末装置１－１～１－ｎと、ＳＩＰ（Ｓｅｓｓｉｏｎ　Ｉｎｉｔｉａｔｉｏｎ　Ｐｒｏｔｏｃｏｌ）サーバ２と、鍵管理・配信サーバ３とから構成されている。ここで、ＳＩＰサーバ２と鍵管理・配信サーバ３とはＳＩＰネットワーク１００を構成し、携帯端末装置１－１～１－ｎとしては、携帯電話機やＰＤＡ（Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　Ａｓｓｉｓｔａｎｔ）、及びノート型のＰＣ（Ｐｅｒｓｏｎａｌ　Ｃｏｍｐｕｔｅｒ）端末等の携帯端末を指している。尚、図１においては、携帯端末装置１－１，１－ｎ間のＰ２Ｐ（Ｐｅｅｒ　ｔｏ　Ｐｅｅｒ：端末間の直接通信）通信を示しており、携帯端末装置１－１，１－ｎ間の無線通信のための無線基地局や無線通信網についてはそれらの図示を省略しており、またそれらの動作についても公知であるのでその説明を省略する。

<31> 図２は図１の携帯端末装置１の構成例を示すブロック図である。図２において、携帯端末装置１はＰ２Ｐ通信アプリケーション１１と、鍵管理モジュール１２と、ＳＩＰモジュール１３と、ＩＰｓｅｃ［ＩＰ（Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ）　ｓｅｃｕｒｉｔｙ　ｐｒｏｔｏｃｏｌ］モジュール１４とを備えている。尚、上記の購入者携帯端末１の各モジュールは図示せぬＣＰＵ（中央処理装置）がプログラム（コンピュータで動作可能なプログラム）を実行することでも実現可能である。また、上記の携帯端末装置１－１～１－ｎはこの携帯端末装置１と同様の構成で、同様の動作を行うものとする。

<32> 携帯端末装置１はＳＩＰモジュールを実装し、定期的に、ＳＩＰサーバ２に対して接続先ＩＰ（Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ）アドレスを登録する機能であるロケーション登録処理を行っている。また、携帯端末装置１はＳＩＰサーバ２との間で通信を行うためにロケーション登録処理時に既に秘密鍵を共有しており、新たに秘密鍵の交換を行うことなく、安全なシグナリングセッションを確立する。携帯端末装置１は他の携帯端末装置との間でデータのやりとり（授受）を行うためのデータセッションを確立する。携帯端末装置１が他の携帯端末装置との間にデータセッションを確立した時には、携帯端末装置１と他の携帯端末装置との間での秘密鍵の交換が必要となるが

Ex.1002 / Page 407 of 1173
Cisco Systems, Inc.

、この秘密鍵は鍵管理・配信サーバ３から安全なデータセッションを通して鍵配送されるので、それを使用する。尚、鍵配送の方法としては、例えば、ＤＨ（Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ）法等がある。

<33> 図３は図１のＳＩＰサーバ２の構成例を示すブロック図である。図３において、ＳＩＰサーバ２はプロキシサーバモジュール２１と、ロケーションサーバモジュール２２と、レジストレーションモジュール２３と、ＳＩＰモジュール２４と、ＩＰｓｅｃモジュール２５とを備えている。尚、上記のＳＩＰサーバ２の各モジュールは図示せぬＣＰＵがプログラムを実行することでも実現可能である。

<34> ＳＩＰサーバ２は携帯端末装置１－１，１－ｎのＩＰアドレス情報を保持し、携帯端末装置１－１，１－ｎから発信されたメッセージを鍵管理・配信サーバ３や別の携帯端末へと転送する機能を持つ。ＳＩＰサーバ２は携帯端末装置１－１，１－ｎ間がＰ２Ｐ通信に入っていない間、安全なシグナリングセッションを張ることなく、ＩＰアドレス情報のみを保持している。また、ＳＩＰサーバ２は、携帯端末装置１－１，１－ｎから安全なシグナリングセッションを張るための再レジストレーションを受信すると、携帯端末装置１－１，１－ｎとの間の安全なシグナリングセッションを確立する。

<35> その後、ＳＩＰサーバ２はこのセッションを使用し、携帯端末装置１－１，１－ｎ間、携帯端末装置１－１，１－ｎと鍵管理・配信サーバ３との間の暗号化された安全なデータセッションを確立するためのメッセージを送受信する。ＳＩＰサーバ２では携帯端末装置１－１，１－ｎと鍵管理・配信サーバ３との対地情報のみを管理するものとし、個人情報等が全てデータセッションを通してやりとりされ、ＳＩＰサーバ２で復号化されることはない。

<36> 図４は図１の鍵管理・配信サーバ３の構成例を示すブロック図である。図４において、鍵管理・配信サーバ３は鍵生成モジュール３１と、ＳＩＰモジュール３２と、ＩＰｓｅｃモジュール３３とを備えている。尚、上記の鍵管理・配信サーバ３の各モジュールは図示せぬＣＰＵがプログラムを実行することでも実現可能である。

<37> 鍵管理・配信サーバ３はＳＩＰモジュールを実装しており、常に、ＳＩＰサーバ２との間で安全なシグナリングセッションを張っている。鍵管理・配信サーバ３は携帯端末装置１－１からの通信開始要求を受信し、携帯端末装置１－１，１－ｎとＳＩＰサーバ２との間の安全なシグナリングセッションの確立を確認すると、携帯端末装置１－１，１－ｎの両方に対して安全なデータセッションを確立するためのメッセージを送信する。

<38> 鍵管理・配信サーバ３はそのセッションを使用し、携帯端末装置１－１，１－ｎの両携帯端末間のＰ２Ｐ通信で使用するための鍵配送を行う。その後、鍵管理・配信サーバ３は携帯端末装置１－１，１－ｎ間の安全なデータセッションを確立するためのシグナリングを行う。すなわち、鍵管理・配信サーバ３は携帯端末装置１－１，１－ｎ間のＰ２Ｐのセッションへの張替え（これはセッションの送り先アドレスの書換えを示し、Ｐ２Ｐのセッションの追加を含んでいる）、一通信毎にＰ２Ｐのセッション（ＩＰｓｅｃ）確立のための暗号鍵の配送制御を実施している。

<39> 図５及び図６は本発明の一実施例による通信システムの動作例を示すシーケンスチャートである。これら図１～図６を参照して本発明の一実施例による移動通信システムの動作について説明する。尚、図５及び図６における携帯端末装置（＃１）１－１，（＃ｎ）１－ｎ、鍵管理・配信サーバ３の動作は図示せぬＣＰＵがプログラムを実行することでも実現可能である。

<40> 携帯端末装置（＃１）１－１はＳＩＰモジュール１３からＳＩＰサーバ２のレジストレーションモジュール２３に対し、自端末のロケーション登録処理を行い（図５のａ１参照）、ＳＩＰサーバ２のロケーションサーバモジュール２２にそのロケーション情報を保持させる。携帯端末装置（＃ｎ）１－ｎも、上記の携帯端末装置（＃１）１－１と同様に、ロケーション登録処理を実施し（図５のａ２参照）、ＳＩＰサーバ２のロケーションサーバモジュール２２にそのロケーション情報を保持させる。

<41> 携帯端末装置（＃１）１－１がＰ２Ｐ通信のトリガとなるメッセージをＳＩＰサーバ２のプロキシサーバモジュール２１に送信すると（図５のａ３参照）、ＳＩＰサーバ２のプロキシサーバモジュール２１はそのメッセージを鍵管理・配信サーバ３へと転送する（図５のａ４参照）。鍵管理・配信サーバ３は携帯端末装置（＃１）１－１からのＰ２Ｐ通信のトリガとなるメッセージを折り返し、ＳＩＰサーバ２のプロキシサーバモジュール２１に送信する（図５のａ５参照）。ＳＩＰサーバ２はロケーションサーバモジュール２２で保持している携帯端末装置（＃ｎ）１－ｎのロケーション情報に基づき、そのメッセージを携帯端末装置（＃ｎ）１－ｎへと転送する（図５のａ６参照）。この場合、上記のＰ２Ｐ通信のトリガは個人情報を含まないため、ＩＰｓｅｃセッションを張る前の状態で送信可能となっている。

<42> 携帯端末装置（＃１）１－１，（＃ｎ）１－ｎは上記のメッセージ送信／受信をトリガとして、ＳＩＰモジュール１３によるロケーション登録処理を再度実施するが、その処理の中でＩＰｓｅｃモジュール１２を各々起動し、ＳＩＰサーバ２のＩＰｓｅｃモジュール２５との間のＩＰｓｅｃトンネルを形成する（図５のａ７～ａ１０参照

Ex.1002 / Page 408 of 1173
Cisco Systems, Inc.

）。このロケーション情報登録（図５のａ７，ａ９参照）時には、シグナリングセッションが確立する。

<43> 携帯端末装置（＃１）１－１，（＃ｎ）１－ｎはＳＩＰサーバ２との間のＩＰｓｅｃトンネル形成を完了すると、鍵管理・配信サーバ３宛てのメッセージを送信し、ＳＩＰサーバ２にＩＰｓｅｃトンネル形成が完了したことを通知する（図５のａ１１，ａ１３参照）。ＳＩＰサーバ２はこの通知を鍵管理・配信サーバ３へ転送する（図５のａ１２，ａ１４参照）。

<44> 鍵管理・配信サーバ３はＳＩＰサーバ２を介して携帯端末装置（＃１）１－１に対してＩＰｓｅｃデータセッションの確立を要求するメッセージを送信し（図５のａ１５，ａ１６参照）、鍵管理・配信サーバ３と携帯端末装置（＃１）１－１との間にＩＰｓｅｃデータセッションを確立し（図５のａ１７参照）、ＩＰｓｅｃデータセッションを利用して鍵生成モジュール３１で生成した秘密鍵Ａを携帯端末装置（＃１）１－１に配送する。

<45> 同様に、鍵管理・配信サーバ３はＳＩＰサーバ２を介して携帯端末装置（＃ｎ）１－ｎに対してＩＰｓｅｃデータセッションの確立を要求するメッセージを送信し（図５のａ１８，ａ１９参照）、鍵管理・配信サーバ３と携帯端末装置（＃ｎ）１－ｎとの間にＩＰｓｅｃデータセッションを確立し（図５のａ２０参照）、ＩＰｓｅｃデータセッションを利用して鍵生成モジュール３１で生成した秘密鍵Ａを携帯端末装置（＃ｎ）１－ｎに配送する。

<46> 携帯端末装置（＃１）１－１，（＃ｎ）１－ｎは同じ秘密鍵ＡをＳＩＰサーバ２を介して鍵管理・配信サーバ３から受信すると、鍵受信完了メッセージをＳＩＰサーバ２を介して鍵管理・配信サーバ３に送信する（図５のａ２１～ａ２４参照）。鍵管理・配信サーバ３は鍵受信完了メッセージを受取ると、携帯端末装置（＃１）１－１，（＃ｎ）１－ｎにＳＩＰサーバ２を介してＰ２Ｐ通信データセッション確立要求を送信する（図６のａ２５～ａ２８参照）。これによって、携帯端末装置（＃１）１－１，（＃ｎ）１－ｎ間にはＩＰｓｅｃデータセッションが確立される（図６のａ２９参照）。

<47> このように、本実施例では、携帯端末装置（＃１）１－１，（＃ｎ）１－ｎをＳＩＰモジュールを搭載した端末とすることによって、発信側の携帯端末装置（＃１）１－１がＳＩＰサーバ２、鍵管理・配信サーバ３を経由して着信側の携帯端末装置（＃ｎ）１－ｎに対してデータ通信開始のトリガを送信することで、着信側の携帯端末装置（＃ｎ）１－ｎがリアルタイムにこのトリガを受信することができる。

<48> 発信側の携帯端末装置（＃１）１－１及び着信側の携帯端末装置（＃ｎ）１－ｎがともに、上記のデータ通信開始トリガを送受信した契機で、ＳＩＰサーバ２に対するロケーション情報登録処理をやり直すと同時に、携帯端末装置（＃１）１－１，（＃ｎ）１－ｎとＳＩＰサーバ２との間のシグナリングセッションをＩＰｓｅｃを使用して確立する。この動作によって、本実施例では、ＳＩＰサーバ２と携帯端末装置（＃１）１－１，（＃ｎ）１－ｎとの間のＩＰｓｅｃセッションの確立時間とＩＰｓｅｃセッションの確立端末装置の数とを減らすことができ、ネットワーク負荷及びサーバ負荷を減らすことができる。このＩＰｓｅｃセッション上でシグナリングを行うことで、ユーザ情報やシグナリングに必要なデータの暗号化を行い、安全に通信することができる。

<49> 上記のＩＰｓｅｃ上のシグナリングセッションで、発信側の携帯端末装置（＃１）１－１と着信側の携帯端末装置（＃ｎ）１－ｎとの間のＰ２Ｐデータ通信に使用する秘密鍵を交換することも可能であるが、鍵管理・配信サーバ３と発信側の携帯端末装置（＃１）１－１及び着信側の携帯端末装置（＃ｎ）１－ｎとの間のデータセッションをＩＰｓｅｃ上で確立し、このセッション上で秘密鍵の交換を行うことで、ＳＩＰサーバ２をはじめとしたサーバ装置で秘密鍵の入ったデータをプロキシすることがなくなるため、秘密鍵を参照することができなくなり、さらに安全に秘密鍵を配送管理することができる。

<50> Ｐ２Ｐデータ通信で使用する秘密鍵は、鍵管理・配信サーバ３が一通信毎に生成する秘密鍵を発信側の携帯端末装置（＃１）１－１及び着信側の携帯端末装置（＃ｎ）１－ｎに配送して使用するため、毎回使用する秘密鍵が違うものとなる。そのため、本実施例では、一度使った秘密鍵をさらに不正に利用し続けたり、秘密鍵の紛失による不正利用を防止することができる。

<51> 図７は本発明の他の実施例による通信システムの構成を示すブロック図である。図７において、本発明の他の実施例による通信システムは、携帯端末装置１－１の代わりに、ゲートウェイサーバ４とＳＩＰ未対応端末［例えば、デスクトップ型のＰＣ（Ｐｅｒｓｏｎａｌ　Ｃｏｍｐｕｔｅｒ）端末等の固定端末や携帯端末を含む端末］５とを設けた以外は図１に示す本発明の一実施例による通信システムと同様の構成となっており、同一構成要素には同一符号を付してある。ここで、ＳＩＰサーバ２と鍵管理・配信サーバ３とゲートウェイサーバ４とはＳＩＰネットワーク１００を構成している。

<52> 図８は図７のＳＩＰ未対応端末５の構成例を示すブロック図である。図８において、ＳＩＰ未対応端末５はＰ２Ｐ通信アプリケーション５１と、ＨＴＴＰ／ＨＴＴＰＳ（Ｈｙｐｅｒ　Ｔｅｘｔ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ　ｏｖｅｒ　ｔｒａｎｓｐｏｒｔ　ｌａｙｅｒ　ｓｅｃｕｒｉｔｙ／ｓｅｃｕｒｅ　ｓｏｃｋｅｔｓ　ｌａｙｅ

Ex.1002 / Page 409 of 1173
Cisco Systems, Inc.

ｒ）モジュール５２とを備えている。尚、上記のＳＩＰ未対応端末５の各モジュールは図示せぬＣＰＵがプログラムを実行することでも実現可能である。

<53> 図９は図７のゲートウェイサーバ４の構成例を示すブロック図である。図９において、ゲートウェイサーバ４はＨＴＴＰ／ＨＴＴＰＳモジュール４１と、ＳＩＰモジュール４２と、ＩＰｓｅｃモジュール４３とを備えている。尚、上記のゲートウェイサーバ４の各モジュールは図示せぬＣＰＵがプログラムを実行することでも実現可能である。

<54> ゲートウェイサーバ４はＰ２Ｐ通信に使用されるＳＩＰ未対応端末５がＳＩＰモジュールを実装していない場合に、ＳＩＰモジュールを実装している端末（携帯端末装置１－ｎ）との間のＰ２Ｐ通信を可能とするためのプロトコル変換サーバである。ゲートウェイサーバ４はＨＴＴＰＳによって要求されたＳＩＰ未対応端末５からのＰ２Ｐ通信要求を受信し、ＳＩＰサーバ２に対して自ＩＰアドレスを接続先ＩＰアドレスとしてレジストレーション処理を行い、Ｐ２Ｐ通信要求のメッセージをＳＩＰサーバ２及び鍵管理・配信サーバ３経由で携帯端末装置１－ｎに送信する。

<55> ゲートウェイサーバ４は鍵管理・配信サーバ３からの要求を受けて、携帯端末装置１－ｎあるいは鍵管理・配信サーバ３との間のデータセッションを確立する。ゲートウェイサーバ４は携帯端末装置１－ｎとのデータセッション確立時に、ゲートウェイサーバ４と携帯端末装置１－ｎとの間での秘密鍵の交換が必要となるが、この秘密鍵は鍵管理・配信サーバ３を介して鍵配送されるので、それを使用する。

<56> ＳＩＰ未対応端末５はゲートウェイサーバ４を通して携帯端末装置１－ｎとの間のデータセッションの確立によるＰ２Ｐ通信を行う。その際、ゲートウェイサーバ４はＳＩＰ未対応端末５に対してＰ２Ｐ通信の内容をＨＴＴＰＳで通知する。

<57> 図１０及び図１１は本発明の他の実施例による通信システムの動作を示すシーケンスチャートである。これら図３と図４と図７～図１１とを参照して本発明の他の実施例による通信システムの動作について説明する。尚、図１０及び図１１における携帯端末装置１－ｎ、鍵管理・配信サーバ３、ゲートウェイサーバ４、ＳＩＰ未対応端末５の動作は図示せぬＣＰＵがプログラムを実行することでも実現可能である。

<58> ＳＩＰモジュールを持たないＳＩＰ未対応端末５は、ゲートウェイサーバ４のＨＴＴＰ／ＨＴＴＰＳモジュール４１に対してＨＴＴＰＳトンネルを形成し、ＳＩＰサーバ２に対してロケーション登録処理を行うためのトリガを送信し（図１０のｂ１参照）、ゲートウェイサーバ４がＳＩＰモジュール４２によってＳＩＰ未対応端末５の代理でＳＩＰサーバ２に対してロケーション登録処理を行い（図１０のｂ２参照）、ＳＩＰサーバ２のロケーションサーバモジュール２２にそのロケーション情報を保持させる。携帯端末装置（＃ｎ）１－ｎも、このゲートウェイサーバ４と同様に、ロケーション登録処理を実施し（図１０のｂ３参照）、ＳＩＰサーバ２のロケーションサーバモジュール２２にそのロケーション情報を保持させる。

<59> ＳＩＰ未対応端末５は決済要求のトリガとなるメッセージをＨＴＴＰ／ＨＴＴＰＳモジュール５２から送信し（図１１のｂ４参照）、それを受取ったゲートウェイサーバ４のＨＴＴＰ／ＨＴＴＰＳモジュール４１はそのメッセージをＳＩＰモジュール４２に渡す。ＳＩＰモジュール４２はメッセージをＳＩＰサーバ２のプロキシサーバモジュール２１に送信すると（図１０のｂ５参照）、ＳＩＰサーバ２のプロキシサーバモジュール２１はそのメッセージを鍵管理・配信サーバ３へと転送する（図１０のｂ６参照）。鍵管理・配信サーバ３４はＳＩＰ未対応端末５からのＰ２Ｐ通信の要求のトリガとなるメッセージを折り返し、ＳＩＰサーバ２のプロキシサーバモジュール２１に送信すると（図１０のｂ７参照）、ＳＩＰサーバ２はロケーションサーバモジュール２２で保持している携帯端末装置（＃ｎ）１－ｎのロケーション情報に基づき、そのメッセージを携帯端末装置（＃ｎ）１－ｎへと転送する（図１０のｂ８参照）。この場合、上記の決済要求のトリガは個人情報を含まないため、ＩＰｓｅｃセッションを張る前の状態で送信可能となっている。

<60> ゲートウェイサーバ４及び携帯端末装置（＃ｎ）１－ｎは上記のメッセージ送信／受信をトリガとして、ＳＩＰモジュール４２，１３によるロケーション登録処理を再度実施するが（図１０のｂ９，ｂ１１参照）、その処理の中でＩＰｓｅｃモジュール４３，１４を各々起動し、ＳＩＰサーバ２のＩＰｓｅｃモジュール２５との間にＩＰｓｅｃトンネルを形成する（図１０のｂ１０，ｂ１２参照）。このロケーション情報登録時には、シグナリングセッションが確立する。ゲートウェイサーバ４及び携帯端末装置（＃ｎ）１－ｎはＳＩＰサーバ２との間のＩＰｓｅｃトンネル形成を完了すると、鍵管理・配信サーバ３宛てのメッセージを送信し、ＳＩＰサーバ２にＩＰｓｅｃトンネル形成が完了したことを通知する（図１０のｂ１３，ｂ１５参照）。ＳＩＰサーバ２はこの通知を鍵管理・配信サーバ３へ転送する（図１０のｂ１４，ｂ１６参照）。

<61> 鍵管理・配信サーバ３はＳＩＰサーバ２を介してゲートウェイサーバ４に対してＩＰｓｅｃデータセッションの確立を要求するメッセージを送信し（図１１のｂ１７，ｂ１８参照）、鍵管理・配信サーバ３とゲートウェイサ

Ex.1002 / Page 410 of 1173
Cisco Systems, Inc.

ーバ４との間にＩＰｓｅｃデータセッションを確立し（図１１のｂ２１参照）、ＩＰｓｅｃデータセッションを利用して鍵生成モジュール３１で生成した秘密鍵Ａをゲートウェイサーバ４に配送する。同様に、鍵管理・配信サーバ３と携帯端末装置（＃ｎ）１－ｎとの間にもＩＰｓｅｃデータセッションが確立され（図１１のｂ１９，ｂ２０，ｂ２２参照）、ＩＰｓｅｃデータセッションを利用して鍵生成モジュール３１で生成した秘密鍵Ａが携帯端末装置（＃ｎ）１－ｎに配送される。尚、鍵管理・配信サーバ３とゲートウェイサーバ４との間にはＩＰｓｅｃを用いないデータセッションの確立も可能である。

<62> ゲートウェイサーバ４及び携帯端末装置（＃ｎ）１－ｎは同じ秘密鍵ＡをＳＩＰサーバ２を介して鍵管理・配信サーバ３から受信すると、鍵受信完了メッセージをＳＩＰサーバ２を介して鍵管理・配信サーバ３に送信する（図１１のｂ２３～ｂ２６参照）。鍵管理・配信サーバ３は鍵受信完了メッセージを受取ると、ゲートウェイサーバ４及び携帯端末装置（＃ｎ）１－ｎにＳＩＰサーバ２を介してＰ２Ｐ通信データセッション確立要求を送信する（図１１のｂ２７～ｂ３０参照）。これによって、ゲートウェイサーバ４と携帯端末装置（＃ｎ）１－ｎとの間にはＩＰｓｅｃデータセッションが確立される（図１１のｂ３１参照）。

<63> この場合、ＳＩＰ未対応端末５とゲートウェイサーバ４との間にはＨＴＴＰＳトンネルが形成されているので、携帯端末装置（＃ｎ）１－ｎとゲートウェイサーバ４との間のＩＰｓｅｃデータセッションの確立によるＰ２Ｐ通信が行われると、ゲートウェイサーバ４がその情報をＨＴＴＰＳに載せ換えてＳＩＰ未対応端末５へ送信する（図１１のｂ３２参照）。

<64> このように、本実施例では、ＳＩＰモジュールを未搭載のＳＩＰ未対応端末５をＳＩＰモジュールを搭載するゲートウェイサーバ４を介して着信側の携帯端末装置（＃ｎ）１－ｎとの間にＩＰｓｅｃトンネルを形成することで、ＳＩＰモジュールを未搭載のＳＩＰ未対応端末５においても、上記の本発明の一実施例と同様に、暗号鍵の紛失による不正利用を防止することができ、その暗号鍵を用いて端末間の直接通信を安全に行うことができる。

<65> 図１２は本発明の別の実施例による通信システムの構成を示すブロック図である。図１２において、本発明の別の実施例による決済システムは、携帯端末装置１－ｎの代わりに、ゲートウェイサーバ６とＳＩＰ未対応端末７とを設けた以外は図８に示す本発明の他の実施例による通信システムと同様の構成となっており、同一構成要素には同一符号を付してある。ここで、ＳＩＰサーバ２と鍵管理・配信サーバ３とゲートウェイサーバ４，６とはＳＩＰネットワーク１００を構成している。尚、上記のＳＩＰ未対応端末５，７は図８に示すＳＩＰ未対応端末５と同様の構成となっており、ゲートウェイサーバ４，６は図９に示すゲートウェイサーバ４と同様の構成となっており、それらの動作は上記と同様である。

<66> 図１３及び図１４は本発明の別の実施例によるモバイル決済システムの動作を示すシーケンスチャートである。これら図３と図４と図８と図９と図１２～図１４とを参照して本発明の別の実施例による通信システムの動作について説明する。尚、図１３及び図１４における鍵管理・配信サーバ３、ゲートウェイサーバ４，６、ＳＩＰ未対応端末５，７の動作は図示せぬＣＰＵがプログラムを実行することでも実現可能である。

<67> ＳＩＰモジュールを持たないＳＩＰ未対応端末５は、ゲートウェイサーバ４のＨＴＴＰ／ＨＴＴＰＳモジュール４１に対してＨＴＴＰＳトンネルを形成し、ＳＩＰサーバ２に対してロケーション登録処理を行うためのトリガを送信し（図１３のｃ１参照）、ゲートウェイサーバ４がＳＩＰモジュール４２によってＳＩＰ未対応端末５の代理でＳＩＰサーバ２に対してロケーション登録処理を行い（図１３のｃ２参照）、ＳＩＰサーバ２のロケーションサーバモジュール２２にそのロケーション情報を保持させる。同様に、ＳＩＰモジュールを持たないＳＩＰ未対応端末７は、ゲートウェイサーバ６のＨＴＴＰ／ＨＴＴＰＳモジュール４１に対してＨＴＴＰＳトンネルを形成し、ＳＩＰサーバ２に対してロケーション登録処理を行うためのトリガを送信し（図１３のｃ３参照）、ゲートウェイサーバ６がＳＩＰモジュール４３によってＳＩＰ未対応端末７の代理でＳＩＰサーバ２に対してロケーション登録処理を行い（図１３のｃ４参照）、ＳＩＰサーバ２のロケーションサーバモジュール２２にそのロケーション情報を保持させる。

<68> ＳＩＰ未対応端末５は決済要求のトリガとなるメッセージをＨＴＴＰ／ＨＴＴＰＳモジュール５２から送信し（図１３のｃ５参照）、それを受取ったゲートウェイサーバ４のＨＴＴＰ／ＨＴＴＰＳモジュール４１はそのメッセージをＳＩＰモジュール４２に渡す。ＳＩＰモジュール４２はメッセージをＳＩＰサーバ２のプロキシサーバモジュール２１に送信すると（図１３のｃ６参照）、ＳＩＰサーバ２のプロキシサーバモジュール２１はそのメッセージを鍵管理・配信サーバ３へと転送する（図１３のｃ７参照）。

<69> 鍵管理・配信サーバ３はＳＩＰ未対応端末５からの決済要求のトリガとなるメッセージを折り返し、ＳＩＰサーバ２のプロキシサーバモジュール２１に送信すると（図１３のｃ８参照）、ＳＩＰサーバ２はロケーションサーバモジュール２２で保持しているゲートウェイサーバ６のロケーション情報に基づき、そのメッセージをゲートウェイサーバ６へと転送する（図１３のｃ９参照）。ゲートウェイサーバ６はそのメッセージをＨＴＴＰＳトンネルにてＳＩＰ未対応端末７に送信する（図１３のｃ１０参照）。この場合、上記の決済要求のトリガは個人情報を

Ex.1002 / Page 411 of 1173
Cisco Systems, Inc.

含まないため、ＩＰｓｅｃセッションを張る前の状態で送信可能となっている。

<70> ゲートウェイサーバ４，６は上記のメッセージ送信／受信をトリガとして、ＳＩＰモジュール４２によるロケーション登録処理を再度実施するが（図１３のｃ１１，ｃ１３参照）、その処理の中でＩＰｓｅｃモジュール４３を各々起動し、ＳＩＰサーバ２のＩＰｓｅｃモジュール２５との間のＩＰｓｅｃトンネルを形成する（図１３のｃ１２，ｃ１４参照）。このロケーション情報登録時には、シグナリングセッションが確立する。ゲートウェイサーバ４，６はＳＩＰサーバ２との間にＩＰｓｅｃトンネル形成を完了すると、ＳＩＰサーバ２に鍵管理・配信サーバ３宛てのメッセージを送信し、ＩＰｓｅｃトンネル形成が完了したことを通知する（図１３のｃ１５，ｃ１７参照）。ＳＩＰサーバ２はこの通知を鍵管理・配信サーバ３へ転送する（図１３のｃ１６，ｃ１８参照）。

<71> 鍵管理・配信サーバ３はＳＩＰサーバ２を介してゲートウェイサーバ４に対してＩＰｓｅｃデータセッションの確立を要求するメッセージを送信し（図１４のｃ１９，ｃ２０参照）、鍵管理・配信サーバ３とゲートウェイサーバ５との間にＩＰｓｅｃデータセッションを確立し（図１４のｃ２３参照）、ＩＰｓｅｃデータセッションを利用して鍵生成モジュール３１で生成した秘密鍵Ａをゲートウェイサーバ４に配送する。同様に、鍵管理・配信サーバ３とゲートウェイサーバ６との間にもＩＰｓｅｃデータセッションが確立され（図１４のｃ２１，ｃ２２，ｃ２４参照）、ＩＰｓｅｃデータセッションを利用して鍵生成モジュール３１で生成した秘密鍵Ａがゲートウェイサーバ６に配送される。尚、鍵管理・配信サーバ３とゲートウェイサーバ４，６との間にはＩＰｓｅｃを用いないデータセッションの確立も可能である。

<72> ゲートウェイサーバ４，６は同じ秘密鍵ＡをＳＩＰサーバ２を介して鍵管理・配信サーバ３から受信すると、鍵受信完了メッセージをＳＩＰサーバ２を介して鍵管理・配信サーバ３に送信する（図１４のｃ２５～ｃ２８参照）。鍵管理・配信サーバ３は鍵受信完了メッセージを受取ると、ゲートウェイサーバ４，６にＳＩＰサーバ２を介してＰ２Ｐ通信データセッション確立要求を送信する（図１４のｃ２９～ｃ３２参照）。これによって、ゲートウェイサーバ４，６間にはＩＰｓｅｃデータセッションが確立される（図１４のｃ３３参照）。

<73> この場合、ＳＩＰ未対応端末５とゲートウェイサーバ４との間、ＳＩＰ未対応端末７とゲートウェイサーバ６との間にはそれぞれＨＴＴＰＳトンネルが形成されているので、ゲートウェイサーバ４，６間のＩＰｓｅｃデータセッションの確立によるＰ２Ｐ通信の内容が、ゲートウェイサーバ４，６にてその情報をＨＴＴＰＳに載せ換えられてＳＩＰ未対応端末５，７へと送信される（図１４のｃ３４，ｃ３５参照）。

<74> このように、本実施例では、ＳＩＰモジュールを未搭載のＳＩＰ未対応端末５，７の間にＳＩＰモジュールを搭載するゲートウェイサーバ４，６を介してＩＰｓｅｃトンネルを形成することで、ＳＩＰモジュールを未搭載のＳＩＰ未対応端末５，７の間においても、上記の本発明の一実施例と同様に、暗号鍵の紛失による不正利用を防止することができ、その暗号鍵を用いて端末間の直接通信を安全に行うことができる。

<75> 本発明では、各実施例において、鍵管理・配信サーバ３を設け、Ｐ２Ｐ通信を行う端末各々に鍵管理・配信サーバ３で生成した秘密鍵（暗号鍵）を配信しているが、Ｐ２Ｐ通信を行う端末の一方が秘密鍵を生成し、その秘密鍵を中継する中継サーバを介してＰ２Ｐ通信を行う端末の他方に渡すことも可能であり、実施例に限定されるものではない。この場合、中継サーバは秘密鍵を中継するだけで、暗号化には関与しない。また、秘密鍵は定期的に使い捨てにすることで、より安全な通信路を確保することができる。

<76> また、本発明では、上記の各実施例において、ＳＩＰモジュールを実装していない端末とゲートウェイサーバとの間の通信方法としてＨＴＴＰについて述べているが、近距離無線通信［例えば、Ｂｌｕｅｔｏｏｔｈ（登録商標）、ＺｉｇＢｅｅ（国際登録商標）等］、UWB（Ｕｌｔｒａ　ＷｉｄｅＢａｎｄ）、赤外線通信［ＩｒＤＡ（Ｉｎｆｒａｒｅｄ　Ｄａｔａ　Ａｓｓｏｃｉａｔｉｏｎ）］等の通信方法にも適用可能である。

<78> １，１－１～１－ｎ　携帯端末装置
２　ＳＩＰサーバ
３　鍵管理・配信サーバ
４，６　ゲートウェイサーバ
５，７　ＰＣ端末
１１，５１　Ｐ２Ｐ通信アプリケーション
１２　鍵管理モジュール

Ex.1002 / Page 412 of 1173
Cisco Systems, Inc.

１３，２４，３２，４２　ＳＩＰモジュール

１４，２５，３３，４３　ＩＰｓｅｃモジュール

２１　プロキシサーバモジュール

２２　ロケーションサーバモジュール

２３　レジストレーションモジュール

３１　鍵生成モジュール

４１，５２　ＨＴＴＰ／ＨＴＴＰＳモジュール

１００　ＳＩＰネットワーク

【請求項 1】

第１の端末装置及び第２の端末装置各々が共有する暗号鍵を基に前記第１の端末装置と前記第２の端末装置との間にピアツーピアのデータ通信を実現する通信システムであって、

前記第１の端末装置及び前記第２の端末装置のうちの一方が前記ピアツーピアのデータ通信開始のトリガを第１の通信方法による通信路にて前記第１の端末装置及び前記第２の端末装置のうちの他方に通知し、

前記第１の端末装置及び前記第２の端末装置各々が前記データ通信開始トリガの送受信に応答してそれぞれ前記暗号鍵を中継する中継サーバとの間に第２の通信方法による通信路を形成しかつ前記第１の通信方法による通信路から前記第２の通信方法による通信路に切替えて前記中継サーバを介して前記第１の端末装置と前記第２の端末装置との間で前記暗号鍵を共有することを特徴とする通信システム。

【請求項 2】

前記第１の端末装置及び前記第２の端末装置各々は、それぞれ自装置の所在を示すロケーション情報を予め登録しておき、

前記第２の通信方法は、前記ロケーション情報を用いて装置間の通信路を形成する通信方法にて前記暗号鍵を用いた暗号通信路を前記第１の端末装置及び前記第２の端末装置各々と前記中継サーバとの間にそれぞれ形成する通信方法であることを特徴とする請求項１記載の通信システム。

【請求項 3】

前記第１の端末装置及び前記第２の端末装置各々がその所在を示すロケーション情報を予め登録するサーバ装置を含み、

前記サーバ装置は、前記第１の端末装置及び前記第２の端末装置各々と前記中継サーバとの間に前記第２の通信方法にて、前記ロケーション情報を用いて装置間の通信路を形成する通信方法にて前記暗号鍵を用いた暗号通信路をそれぞれ形成することを特徴とする請求項１記載の通信システム。

【請求項 4】

前記第１の端末装置及び前記第２の端末装置のうちの少なくとも一方が移動自在な携帯端末であることを特徴とする請求項１から請求項３のいずれか記載の通信システム。

【請求項 5】

前記第１の通信方法は、少なくともＳＩＰ（Ｓｅｓｓｉｏｎ　Ｉｎｉｔｉａｔｉｏｎ　Ｐｒｏｔｏｃｏｌ）を含む通信方法であり、

前記第２の通信方法は、少なくともＳＩＰとＩＰｓｅｃ［ＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）　ｓｅｃｕｒｉｔｙ　ｐｒｏｔｏｃｏｌ］との組合せを含む通信方法であることを特徴とする請求項１から請求項４のいずれか記載の通信システム。

Ex.1002 / Page 413 of 1173
Cisco Systems, Inc.

【請求項 6】

前記第１の端末装置及び前記第２の端末装置のうちの少なくとも一方が前記第２の通信方法に未対応な端末であり、

前記第２の通信方法と前記未対応な端末で使用可能な第３の通信方法との変換を行うゲートウェイを含み、

前記ゲートウェイは、前記未対応な端末の代わりに前記第２の通信方法による通信路を他端末との間に形成することを特徴とする請求項１から請求項５のいずれか記載の通信システム。

【請求項 7】

前記第３の通信方法は、少なくともＨＴＴＰ（Ｈｙｐｅｒ　Ｔｅｘｔ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ）、近距離無線通信、ＵＷＢ（Ｕｌｔｒａ　ＷｉｄｅＢａｎｄ）、赤外線通信のいずれかを使用する通信方法であることを特徴とする請求項６記載の決済システム。

【請求項 8】

鍵管理・配信サーバから第１の端末装置及び第２の端末装置に配信される暗号鍵を基に前記第１の端末装置と前記第２の端末装置との間にピアツーピアのデータ通信を実現する通信システムであって、

前記第１の端末装置及び前記第２の端末装置のうちの一方が前記ピアツーピアのデータ通信開始のトリガを、前記鍵管理・配信サーバを経由してかつ第１の通信方法による通信路にて前記第１の端末装置及び前記第２の端末装置のうちの他方に通知し、

前記第１の端末装置及び前記第２の端末装置各々が前記データ通信開始トリガの送受信に応答してそれぞれ前記鍵管理・配信サーバとの間に第２の通信方法による通信路を形成しかつ前記第１の通信方法による通信路から前記第２の通信方法による通信路に切替えて前記鍵管理・配信サーバから前記第１の端末装置及び前記第２の端末装置各々に前記暗号鍵を配信することを特徴とする通信システム。

【請求項 9】

前記第１の端末装置及び前記第２の端末装置各々は、それぞれ自装置の所在を示すロケーション情報を予め登録しておき、

前記第２の通信方法は、前記ロケーション情報を用いて装置間の通信路を形成する通信方法にて前記暗号鍵を用いた暗号通信路を前記第１の端末装置及び前記第２の端末装置各々と前記鍵管理・配信サーバとの間にそれぞれ形成する通信方法であることを特徴とする請求項８記載の通信システム。

【請求項 10】

前記第１の端末装置及び前記第２の端末装置各々がその所在を示すロケーション情報を予め登録するサーバ装置を含み、

前記サーバ装置は、前記第１の端末装置及び前記第２の端末装置各々と前記鍵管理・配信サーバとの間に前記第２の通信方法にて、前記ロケーション情報を用いて装置間の通信路を形成する通信方法にて前記暗号鍵を用いた暗号通信路をそれぞれ形成することを特徴とする請求項８記載の通信システム。

【請求項 11】

前記鍵管理・配信サーバは、前記第１の端末装置と前記第２の端末装置との間に前記第２の通信方法による通信路を形成させるために前記第１の端末装置及び前記第２の端末装置に対して前記第２の通信方法による通信路のセッションの送り先アドレスの書換えを指示する手段と、前記セッションの送り先アドレスの書換えのための暗号鍵の配送を前記ピアツーピアのデータ通信毎に行う手段とを含むことを特徴とする請求項８から請求項１０のいずれか記載の通信システム。

Ex.1002 / Page 414 of 1173
Cisco Systems, Inc.

【請求項 12】

前記第１の端末装置及び前記第２の端末装置は、前記鍵管理・配信サーバからの前記セッションの送り先アドレスの書換えの指示に応答しかつ前記鍵管理・配信サーバから配送される暗号鍵を用いて相互の間に前記第２の通信方法による通信路を形成することを特徴とする請求項１１記載の通信システム。

【請求項 13】

前記鍵管理・配信サーバは、前記第１の端末装置と前記第２の端末装置との間に前記第２の通信方法による通信路を形成させるために前記第１の端末装置及び前記第２の端末装置に対して前記第１の端末装置と前記第２の端末装置との間の前記第２の通信方法による通信路のセッションの追加を指示する手段と、前記セッションの追加のための暗号鍵の配送を前記ピアツーピアのデータ通信毎に行う手段とを含むことを特徴とする請求項８から請求項１０のいずれか記載の通信システム。

【請求項 14】

前記第１の端末装置及び前記第２の端末装置は、前記鍵管理・配信サーバからの前記セッションの追加の指示に応答しかつ前記鍵管理・配信サーバから配送される暗号鍵を用いて相互の間に前記第２の通信方法による通信路を形成することを特徴とする請求項１３記載の通信システム。

【請求項 15】

前記第１の端末装置及び前記第２の端末装置のうちの少なくとも一方が移動自在な携帯端末であることを特徴とする請求項８から請求項１４のいずれか記載の通信システム。

【請求項 16】

前記第１の通信方法は、少なくともＳＩＰ（Ｓｅｓｓｉｏｎ　Ｉｎｉｔｉａｔｉｏｎ　Ｐｒｏｔｏｃｏｌ）を含む通信方法であり、

前記第２の通信方法は、少なくともＳＩＰとＩＰｓｅｃ［ＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）　ｓｅｃｕｒｉｔｙ　ｐｒｏｔｏｃｏｌ］との組合せを含む通信方法であることを特徴とする請求項８から請求項１５のいずれか記載の通信システム。

【請求項 17】

前記第１の端末装置及び前記第２の端末装置のうちの少なくとも一方が前記第２の通信方法に未対応な端末であり、

前記第２の通信方法と前記未対応な端末で使用可能な第３の通信方法との変換を行うゲートウェイを含み、

前記ゲートウェイは、前記未対応な端末の代わりに前記第２の通信方法による通信路を他端末との間に形成することを特徴とする請求項８から請求項１６のいずれか記載の通信システム。

【請求項 18】

前記第３の通信方法は、少なくともＨＴＴＰ（Ｈｙｐｅｒ　Ｔｅｘｔ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ）、近距離無線通信、ＵＷＢ（Ｕｌｔｒａ　ＷｉｄｅＢａｎｄ）、赤外線通信のいずれかを使用する通信方法であることを特徴とする請求項１７記載の決済システム。

【請求項 19】

第１の端末装置と第２の端末装置との間にピアツーピアのデータ通信を実現する通信システムにおいて前記第１の端末装置及び前記第２の端末装置各々に暗号鍵を配信する鍵管理・配信サーバであって、

前記第１の端末装置及び前記第２の端末装置のうちの一方が送信する前記ピアツーピアのデータ通信開始のトリガを、第１の通信方法による通信路にて受信した時に前記データ通信開始のトリガを前記第１の端末装置及び前記第２の端末装置のうちの他方に転送する手段と、前記第１の端末装置及び前記第２の端末装置各々が前記ピアツ

Ex.1002 / Page 415 of 1173
Cisco Systems, Inc.

ーピアのデータ通信開始のトリガの送受信に応答して切替えかつそれぞれ自装置との間に形成した第２の通信方法による通信路にて前記暗号鍵を配信する手段とを有することを特徴とする鍵管理・配信サーバ。

【請求項 20】

前記第２の通信方法による通信路は、前記第１の端末装置及び前記第２の端末装置各々がそれぞれ登録している前記第１の端末装置及び前記第２の端末装置各々の所在を示すロケーション情報を用いて装置間の通信路を形成する通信方法にて暗号鍵を用いた暗号通信路として前記第１の端末装置及び前記第２の端末装置各々と自装置との間にそれぞれ形成されることを特徴とする請求項１９記載の鍵管理・配信サーバ。

【請求項 21】

前記第２の通信方法による通信路は、前記第１の端末装置及び前記第２の端末装置各々がその所在を示すロケーション情報を予め登録するサーバ装置が、前記第１の端末装置及び前記第２の端末装置各々と自装置との間に、前記ロケーション情報を用いて装置間の通信路を形成する通信方法にて暗号鍵を用いた暗号通信路としてそれぞれ形成されることを特徴とする請求項１９記載の鍵管理・配信サーバ。

【請求項 22】

前記第１の端末装置と前記第２の端末装置との間に前記第２の通信方法による通信路を形成させるために前記第１の端末装置及び前記第２の端末装置に対して前記第２の通信方法による通信路のセッションの送り先アドレスの書換えを指示する手段と、前記セッションの送り先アドレスの書換えのための暗号鍵の配送を前記ピアツーピアのデータ通信毎に行う手段とを含むことを特徴とする請求項１９から請求項２１のいずれか記載の鍵管理・配信サーバ。

【請求項 23】

前記第１の端末装置と前記第２の端末装置との間に前記第２の通信方法による通信路を形成させるために前記第１の端末装置及び前記第２の端末装置に対して前記第２の通信方法による通信路のセッションの追加を指示する手段と、前記セッションの追加のための暗号鍵の配送を前記ピアツーピアのデータ通信毎に行う手段とを含むことを特徴とする請求項１９から請求項２１のいずれか記載の鍵管理・配信サーバ。

【請求項 24】

前記第１の端末装置及び前記第２の端末装置のうちの少なくとも一方が移動自在な携帯端末であることを特徴とする請求項１９から請求項２３のいずれか記載の鍵管理・配信サーバ。

【請求項 25】

前記第１の通信方法は、少なくともＳＩＰ（Ｓｅｓｓｉｏｎ　Ｉｎｉｔｉａｔｉｏｎ　Ｐｒｏｔｏｃｏｌ）を含む通信方法であり、

前記第２の通信方法は、少なくともＳＩＰとＩＰｓｅｃ［ＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）　ｓｅｃｕｒｉｔｙ　ｐｒｏｔｏｃｏｌ］との組合せを含む通信方法であることを特徴とする請求項１９から請求項２４のいずれか記載の鍵管理・配信サーバ。

【請求項 26】

前記第１の端末装置及び前記第２の端末装置のうちの少なくとも一方が前記第２の通信方法に未対応な端末であり、

前記第２の通信方法と前記未対応な端末で使用可能な第３の通信方法との変換を行うゲートウェイが、前記未対応な端末の代わりに前記第２の通信方法による通信路を他端末との間に形成することを特徴とする請求項１９から請求項２５のいずれか記載の鍵管理・配信サーバ。

Ex.1002 / Page 416 of 1173
Cisco Systems, Inc.

【請求項 27】

前記第３の通信方法が、少なくともＨＴＴＰ（Ｈｙｐｅｒ　Ｔｅｘｔ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ）、近距離無線通信、ＵＷＢ（Ｕｌｔｒａ　ＷｉｄｅＢａｎｄ）、赤外線通信のいずれかを使用する通信方法であることを特徴とする請求項２６記載の鍵管理・配信サーバ。

【請求項 28】

自装置及び他の端末装置各々が共有する暗号鍵を基に自装置と前記他の端末装置との間にピアツーピアのデータ通信を行う端末装置であって、

前記ピアツーピアのデータ通信開始のトリガを、前記暗号鍵を中継する中継サーバを経由してかつ第１の通信方法による通信路にて前記他の端末装置に送信し、自装置からの前記ピアツーピアのデータ通信開始のトリガの送信及び前記他の端末装置からの前記ピアツーピアのデータ通信開始のトリガの受信のいずれかに応答して前記中継サーバとの間に第２の通信方法による通信路を形成しかつ前記第１の通信方法による通信路から前記第２の通信方法による通信路に切替えて前記中継サーバを介して前記暗号鍵の送信及び受信のいずれかを行うことを特徴とする端末装置。

【請求項 29】

自装置の所在を示すロケーション情報を予め登録しておき、

前記第２の通信方法が、前記ロケーション情報を用いて装置間の通信路を形成する通信方法にて暗号鍵を用いた暗号通信路を前記中継サーバとの間に形成する通信方法であることを特徴とする請求項２８記載の端末装置。

【請求項 30】

自装置の所在を示すロケーション情報を予め登録するサーバ装置が、自装置と前記中継サーバとの間に前記第２の通信方法を用いて、前記ロケーション情報を用いて装置間の通信路を形成する通信方法にて暗号鍵を用いた暗号通信路を形成することを特徴とする請求項２８記載の端末装置。

【請求項 31】

自装置及び前記他の端末装置のうちの少なくとも一方が移動自在な携帯端末であることを特徴とする請求項２８から請求項３０のいずれか記載の端末装置。

【請求項 32】

前記第１の通信方法は、少なくともＳＩＰ（Ｓｅｓｓｉｏｎ　Ｉｎｉｔｉａｔｉｏｎ　Ｐｒｏｔｏｃｏｌ）を含む通信方法であり、

前記第２の通信方法は、少なくともＳＩＰとＩＰｓｅｃ［ＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）　ｓｅｃｕｒｉｔｙ　ｐｒｏｔｏｃｏｌ］との組合せを含む通信方法であることを特徴とする請求項２８から請求項３１のいずれか記載の端末装置。

【請求項 33】

自装置及び前記他の端末装置のうちの少なくとも一方が前記第２の通信方法に未対応な端末であり、

前記第２の通信方法と前記未対応な端末で使用可能な第３の通信方法との変換を行うゲートウェイが、前記未対応な端末の代わりに前記第２の通信方法による通信路を他端末との間に形成することを特徴とする請求項２８から請求項３２のいずれか記載の端末装置。

【請求項 34】

前記第３の通信方法は、少なくともＨＴＴＰ（Ｈｙｐｅｒ　Ｔｅｘｔ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ）、近距離無線通信、ＵＷＢ（Ｕｌｔｒａ　ＷｉｄｅＢａｎｄ）、赤外線通信のいずれかを使用する通信方法であることを特徴とする請求項３３記載の端末装置。

Ex.1002 / Page 417 of 1173
Cisco Systems, Inc.

【請求項 35】

鍵管理・配信サーバから自装置及び他の端末装置に配信される暗号鍵を基に自装置と前記他の端末装置との間でピアツーピアのデータ通信を行う端末装置であって、

前記ピアツーピアのデータ通信開始のトリガを、前記鍵管理・配信サーバを経由してかつ第１の通信方法による通信路にて前記他の端末装置に送信し、自装置からの前記ピアツーピアのデータ通信開始のトリガの送信及び前記他の端末装置からの前記ピアツーピアのデータ通信開始のトリガの受信のいずれかに応答して前記鍵管理・配信サーバとの間に第２の通信方法による通信路を形成しかつ前記第１の通信方法による通信路から前記第２の通信方法による通信路に切替えて前記鍵管理・配信サーバから前記暗号鍵を受信することを特徴とする端末装置。

【請求項 36】

自装置の所在を示すロケーション情報を予め登録しておき、

前記第２の通信方法が、前記ロケーション情報を用いて装置間の通信路を形成する通信方法にて暗号鍵を用いた暗号通信路を前記鍵管理・配信サーバとの間に形成する通信方法であることを特徴とする請求項３５記載の端末装置。

【請求項 37】

自装置の所在を示すロケーション情報を予め登録するサーバ装置が、自装置と前記鍵管理・配信サーバとの間に前記第２の通信方法を用いて、前記ロケーション情報を用いて装置間の通信路を形成する通信方法にて暗号鍵を用いた暗号通信路を形成することを特徴とする請求項３５記載の端末装置。

【請求項 38】

前記鍵管理・配信サーバからの指示によって前記他の端末装置との間に前記第２の通信方法による通信路のセッションの送り先アドレスの書換えを行い、前記セッションの送り先アドレスの書換えを前記鍵管理・配信サーバから前記ピアツーピアのデータ通信毎に配送される暗号鍵を用いて行うことを特徴とする請求項３５から請求項３７のいずれか記載の端末装置。

【請求項 39】

前記鍵管理・配信サーバからの指示によって前記他の端末装置との間に前記第２の通信方法による通信路のセッションの追加を行い、前記セッションの追加を前記鍵管理・配信サーバから前記ピアツーピアのデータ通信毎に配送される暗号鍵を用いて行うことを特徴とする請求項３５から請求項３７のいずれか記載の端末装置。

【請求項 40】

自装置及び前記他の端末装置のうちの少なくとも一方が移動自在な携帯端末であることを特徴とする請求項３５から請求項３９のいずれか記載の端末装置。

【請求項 41】

前記第１の通信方法は、少なくともＳＩＰ（Ｓｅｓｓｉｏｎ　Ｉｎｉｔｉａｔｉｏｎ　Ｐｒｏｔｏｃｏｌ）を含む通信方法であり、

前記第２の通信方法は、少なくともＳＩＰとＩＰｓｅｃ［ＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）　ｓｅｃｕｒｉｔｙ　ｐｒｏｔｏｃｏｌ］との組合せを含む通信方法であることを特徴とする請求項３５から請求項４０のいずれか記載の端末装置。

【請求項 42】

自装置及び前記他の端末装置のうちの少なくとも一方が前記第２の通信方法に未対応な端末であり、

前記第２の通信方法と前記未対応な端末で使用可能な第３の通信方法との変換を行うゲートウェイが、前記未対

Ex.1002 / Page 418 of 1173
Cisco Systems, Inc.

応な端末の代わりに前記第２の通信方法による通信路を他端末との間に形成することを特徴とする請求項３５から請求項４１のいずれか記載の端末装置。

【請求項 43】

前記第３の通信方法は、少なくともＨＴＴＰ（Ｈｙｐｅｒ　Ｔｅｘｔ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ）、近距離無線通信、ＵＷＢ（Ｕｌｔｒａ　ＷｉｄｅＢａｎｄ）、赤外線通信のいずれかを使用する通信方法であることを特徴とする請求項４２記載の端末装置。

【請求項 44】

自装置及び他の端末装置各々が共有する暗号鍵を基に自装置と前記他の端末装置との間にピアツーピアのデータ通信を行うシステムに用いられるデータ通信方法であって、

前記端末装置が、

前記ピアツーピアのデータ通信開始のトリガを、前記暗号鍵を中継する中継サーバを経由してかつ第１の通信方法による通信路にて前記他の端末装置に送信する処理と、自装置からの前記ピアツーピアのデータ通信開始のトリガの送信及び前記他の端末装置からの前記ピアツーピアのデータ通信開始のトリガの受信のいずれかに応答して前記中継サーバとの間に第２の通信方法による通信路を形成しかつ前記第１の通信方法による通信路から前記第２の通信方法による通信路に切替えて前記中継サーバを介して前記暗号鍵の送信及び受信のいずれかを行う処理とを実行することを特徴とするデータ通信方法。

【請求項 45】

前記端末装置及び前記他の端末装置各々が、それぞれ自装置の所在を示すロケーション情報を予め登録しておき、

前記第２の通信方法が、前記ロケーション情報を用いて装置間の通信路を形成する通信方法にて前記暗号鍵を用いた暗号通信路を前記端末装置及び前記他の端末装置各々と前記中継サーバとの間にそれぞれ形成する通信方法であることを特徴とする請求項４４記載のデータ通信方法。

【請求項 46】

前記第１の端末装置及び前記第２の端末装置各々がその所在を示すロケーション情報を予め登録するサーバ装置を含み、

前記サーバ装置は、前記第１の端末装置及び前記第２の端末装置各々と前記中継サーバとの間に前記第２の通信方法にて、前記ロケーション情報を用いて装置間の通信路を形成する通信方法にて前記暗号鍵を用いた暗号通信路をそれぞれ形成することを特徴とする請求項４４記載のデータ通信方法。

【請求項 47】

前記第１の端末装置及び前記第２の端末装置のうちの少なくとも一方が移動自在な携帯端末であることを特徴とする請求項４４から請求項４６のいずれか記載のデータ通信方法。

【請求項 48】

前記第１の通信方法は、少なくともＳＩＰ（Ｓｅｓｓｉｏｎ　Ｉｎｉｔｉａｔｉｏｎ　Ｐｒｏｔｏｃｏｌ）を含む通信方法であり、

前記第２の通信方法は、少なくともＳＩＰとＩＰｓｅｃ［ＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）　ｓｅｃｕｒｉｔｙ　ｐｒｏｔｏｃｏｌ］との組合せを含む通信方法であることを特徴とする請求項４４から請求項４７のいずれか記載のデータ通信方法。

【請求項 49】

前記第１の端末装置及び前記第２の端末装置のうちの少なくとも一方が前記第２の通信方法に未対応な端末であり、

前記第２の通信方法と前記未対応な端末で使用可能な第３の通信方法との変換を行うゲートウェイを含み、

前記ゲートウェイが、前記未対応な端末の代わりに前記第２の通信方法による通信路を他端末との間に形成することを特徴とする請求項４４から請求項４８のいずれか記載のデータ通信方法。

【請求項 50】

前記第３の通信方法は、少なくともＨＴＴＰ（Ｈｙｐｅｒ　Ｔｅｘｔ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ）、近距離無線通信、ＵＷＢ（Ｕｌｔｒａ　ＷｉｄｅＢａｎｄ）、赤外線通信のいずれかを使用する通信方法であることを特徴とする請求項４９記載のデータ通信方法。

【請求項 51】

鍵管理・配信サーバから端末装置及び他の端末装置に配信される暗号鍵を基に前記端末装置と前記他の端末装置との間でピアツーピアのデータ通信を行うシステムに用いられるデータ通信方法であって、

前記端末装置が、前記ピアツーピアのデータ通信開始のトリガを、前記鍵管理・配信サーバを経由してかつ第１の通信方法による通信路にて前記他の端末装置に送信する処理と、前記ピアツーピアのデータ通信開始のトリガの送受信に応答して前記鍵管理・配信サーバとの間に第２の通信方法による通信路を形成しかつ前記第１の通信方法による通信路から前記第２の通信方法による通信路に切替えて前記鍵管理・配信サーバから前記暗号鍵を受信する処理とを実行することを特徴とするデータ通信方法。

【請求項 52】

前記端末装置及び前記他の端末装置各々が、それぞれ自装置の所在を示すロケーション情報を予め登録しておき、

前記第２の通信方法が、前記ロケーション情報を用いて装置間の通信路を形成する通信方法にて前記暗号鍵を用いた暗号通信路を前記端末装置及び前記他の端末装置各々と前記鍵管理・配信サーバとの間にそれぞれ形成する通信方法であることを特徴とする請求項５１記載のデータ通信方法。

【請求項 53】

前記端末装置及び前記他の端末装置各々がその所在を示すロケーション情報を予め登録するサーバ装置を含み、

前記サーバ装置が、前記端末装置及び前記他の端末装置各々と前記鍵管理・配信サーバとの間に前記第２の通信方法にて、前記ロケーション情報を用いて装置間の通信路を形成する通信方法にて前記暗号鍵を用いた暗号通信路をそれぞれ形成することを特徴とする請求項５１記載のデータ通信方法。

【請求項 54】

前記鍵管理・配信サーバが、前記第１の端末装置と前記第２の端末装置との間に前記第２の通信方法による通信路を形成させるために前記第１の端末装置及び前記第２の端末装置に対して前記第２の通信方法による通信路のセッションの送り先アドレスの書換えを指示する処理と、前記セッションの送り先アドレスの書換えのための暗号鍵の配送を前記ピアツーピアのデータ通信毎に行う処理とを実行することを特徴とする請求項５１から請求項５３のいずれか記載のデータ通信方法。

【請求項 55】

前記端末装置及び前記他の端末装置は、前記鍵管理・配信サーバからの前記セッションの送り先アドレスの書換えの指示に応答しかつ前記鍵管理・配信サーバから配送される暗号鍵を用いて相互の間に前記第２の通信方法による通信路を形成することを特徴とする請求項５４記載のデータ通信方法。

【請求項 56】

前記鍵管理・配信サーバが、前記第１の端末装置と前記第２の端末装置との間に前記第２の通信方法による通信路を形成させるために前記第１の端末装置及び前記第２の端末装置に対して前記第１の端末装置と前記第２の端末装置との間の前記第２の通信方法による通信路のセッションの追加を指示する処理と、前記セッションの追加のた

Ex.1002 / Page 420 of 1173
Cisco Systems, Inc.

めの暗号鍵の配送を前記ピアツーピアのデータ通信毎に行う処理とを実行することを特徴とする請求項５１から請求項５３のいずれか記載のデータ通信方法。

【請求項 57】

前記端末装置及び前記他の端末装置は、前記鍵管理・配信サーバからの前記セッションの追加の指示に応答しかつ前記鍵管理・配信サーバから配送される暗号鍵を用いて相互の間に前記第２の通信方法による通信路を形成することを特徴とする請求項５６記載のデータ通信方法。

【請求項 58】

前記端末装置及び前記他の端末装置のうちの少なくとも一方が移動自在な携帯端末であることを特徴とする請求項５１から請求項５７のいずれか記載のデータ通信方法。

【請求項 59】

前記第１の通信方法は、少なくともＳＩＰ（Ｓｅｓｓｉｏｎ　Ｉｎｉｔｉａｔｉｏｎ　Ｐｒｏｔｏｃｏｌ）を含む通信方法であり、

前記第２の通信方法は、少なくともＳＩＰとＩＰｓｅｃ［ＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）　ｓｅｃｕｒｉｔｙ　ｐｒｏｔｏｃｏｌ］との組合せを含む通信方法であることを特徴とする請求項５１から請求項５８のいずれか記載のデータ通信方法。

【請求項 60】

前記端末装置及び前記他の端末装置のうちの少なくとも一方が前記第２の通信方法に未対応な端末であり、

前記第２の通信方法と前記未対応な端末で使用可能な第３の通信方法との変換を行うゲートウェイを含み、

前記ゲートウェイが、前記未対応な端末の代わりに前記第２の通信方法による通信路を他端末との間に形成することを特徴とする請求項５１から請求項５９のいずれか記載のデータ通信方法。

【請求項 61】

前記第３の通信方法は、少なくともＨＴＴＰ（Ｈｙｐｅｒ　Ｔｅｘｔ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ）、近距離無線通信、ＵＷＢ（Ｕｌｔｒａ　ＷｉｄｅＢａｎｄ）、赤外線通信のいずれかを使用する通信方法であることを特徴とする請求項６０記載のデータ通信方法。

【請求項 62】

自装置及び他の端末装置各々が共有する暗号鍵を基に自装置と前記他の端末装置との間にピアツーピアのデータ通信を行うシステムに用いられるデータ通信方法のプログラムであって、

前記ピアツーピアのデータ通信開始のトリガを、前記暗号鍵を中継する中継サーバを経由してかつ第１の通信方法による通信路にて前記他の端末装置に送信する処理と、自装置からの前記ピアツーピアのデータ通信開始のトリガの送信及び前記他の端末装置からの前記ピアツーピアのデータ通信開始のトリガの受信のいずれかに応答して前記中継サーバとの間に第２の通信方法による通信路を形成しかつ前記第１の通信方法による通信路から前記第２の通信方法による通信路に切替えて前記中継サーバを介して前記暗号鍵の送信及び受信のいずれかを行う処理とを前記端末装置のコンピュータに実行させるためのプログラム。

【請求項 63】

鍵管理・配信サーバから端末装置及び他の端末装置に配信される暗号鍵を基に前記端末装置と前記他の端末装置との間でピアツーピアのデータ通信を行うシステムに用いられるデータ通信方法のプログラムであって、

前記ピアツーピアのデータ通信開始のトリガを、前記鍵管理・配信サーバを経由してかつ第１の通信方法による通信路にて前記他の端末装置に送信する処理と、前記ピアツーピアのデータ通信開始のトリガの送受信に応答して前記鍵管理・配信サーバとの間に第２の通信方法による通信路を形成しかつ前記第１の通信方法による通信路から

前記第２の通信方法による通信路に切替えて前記鍵管理・配信サーバから前記暗号鍵を受信する処理とを前記端末装置のコンピュータに実行させるためのプログラム。

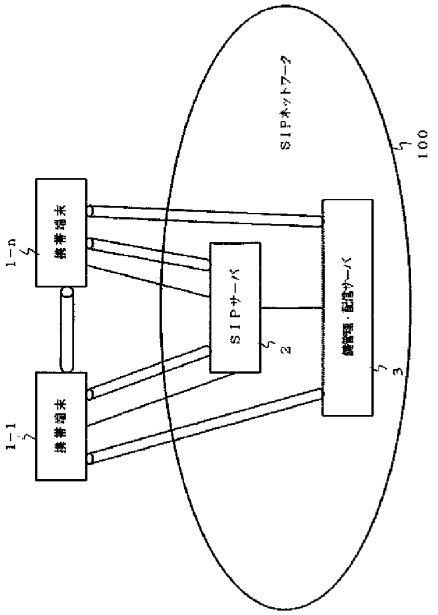
(57)【要約】

【課題】　暗号鍵の紛失による不正利用を防止し、その暗号鍵を用いて端末間の直接通信を安全に行うことが可能な移動通信システムを提供する。

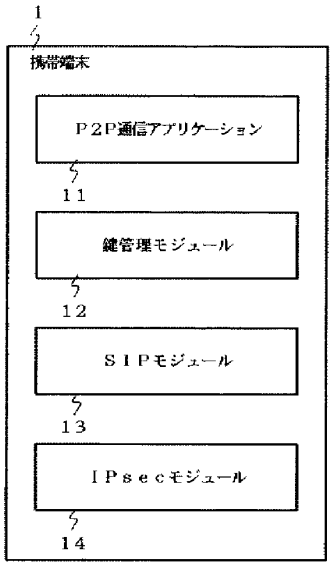
【解決手段】　携帯端末装置１－１は鍵管理・配信サーバ３を通して携帯端末装置１－ｎにＰ２Ｐ通信のトリガを送る。このトリガの送受信に応答して携帯端末装置１－１，１－ｎはＳＩＰサーバ２を通して鍵管理・配信サーバ３との間にＩＰｓｅｃデータセッションを確立して鍵管理・配信サーバ３から携帯端末装置１－１，１－ｎに一通信毎の秘密鍵を配信する。携帯端末装置１－１，１－ｎはその秘密鍵を用いて互いの間にＩＰｓｅｃデータセッションを確立してＰ２Ｐ通信を行う。鍵管理・配信サーバ３は携帯端末装置１－１，１－ｎに対してセッションへの張替え、セッション確立のための鍵配送制御を実施する。

【選択図】　　図１

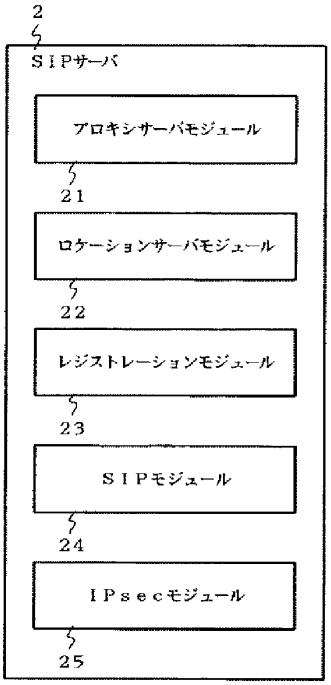
【圖 1】



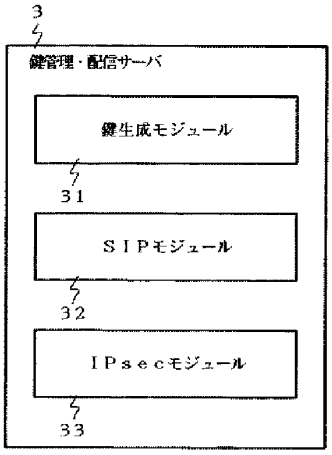
【圖 2】


1
携帯端末
P2P通信アプリケーション
11
鍵管理モジュール
12
ＳＩＰモジュール
13
ＩＰｓｅｃモジュール
14

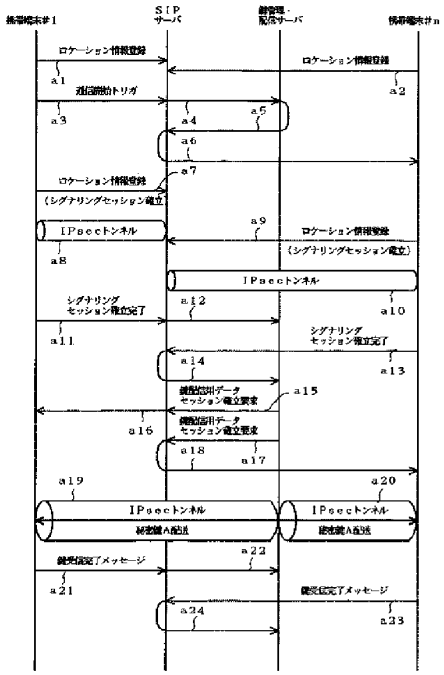
【圖 3】


2
ＳＩＰサーバ
プロキシサーバモジュール
21
ロケーションサーバモジュール
22
レジストレーションモジュール
23
ＳＩＰモジュール
24
ＩＰｓｅｃモジュール
25

【圖 4】

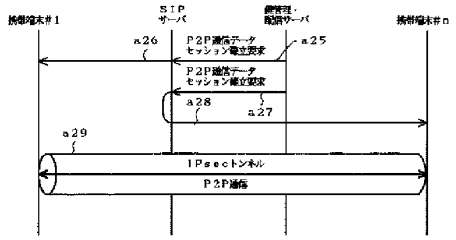


【圖 5】

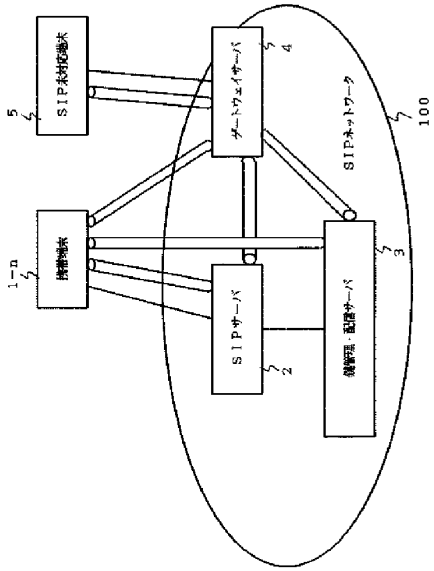


Ex.1002 / Page 424 of 1173
Cisco Systems, Inc.

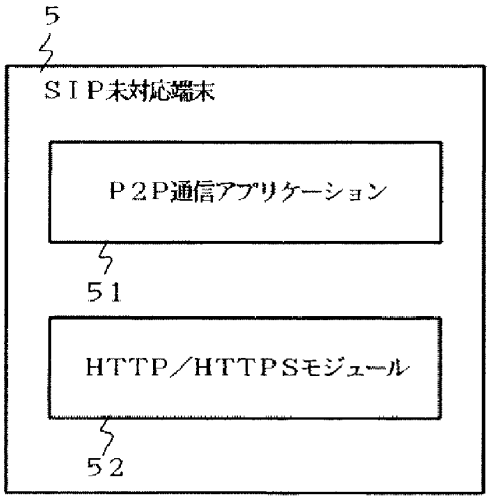
【圖 6】


SIP
サーバ
携帯端末#1
携帯端末#n
a26
a25
P2P通信データ
セッション確立要求
P2P通信データ
セッション確立要求
a28
a27
a29
IPsecトンネル
P2P通信

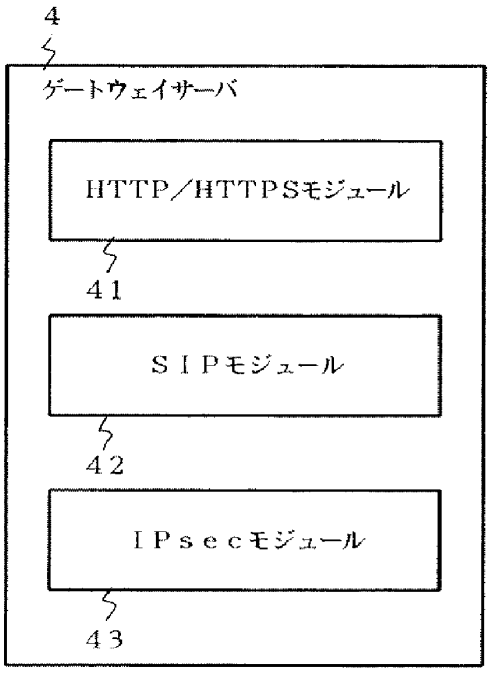
【圖 7】


SIP未対応端末
5
ゲートウェイサーバ
4
SIPネットワーク
100
携帯端末
1-n
SIPサーバ
2
3

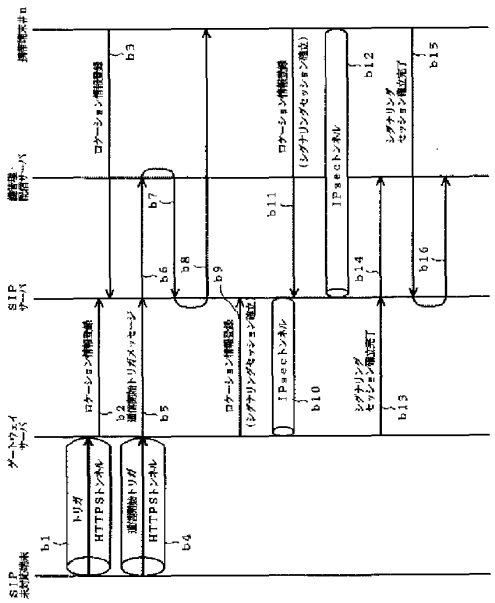
【圖 8】


5
ＳＩＰ未対応端末
Ｐ２Ｐ通信アプリケーション
51
HTTP／HTTPSモジュール
52

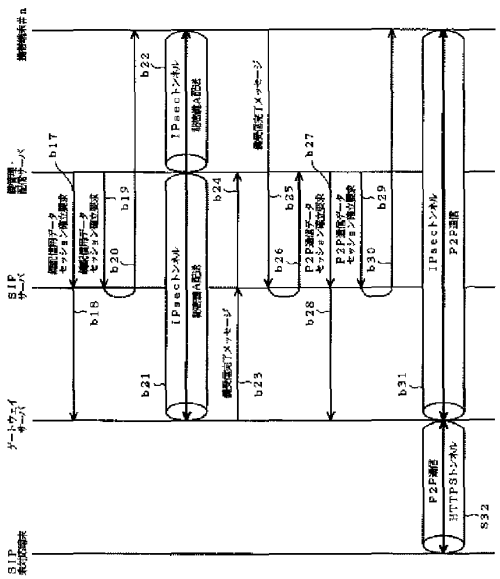
【圖 9】


4
ゲートウェイサーバ
HTTP／HTTPSモジュール
41
ＳＩＰモジュール
42
ＩＰｓｅｃモジュール
43

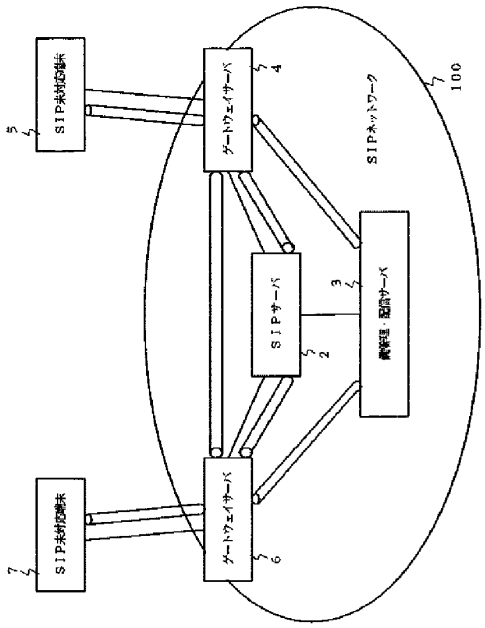
【圖 10】



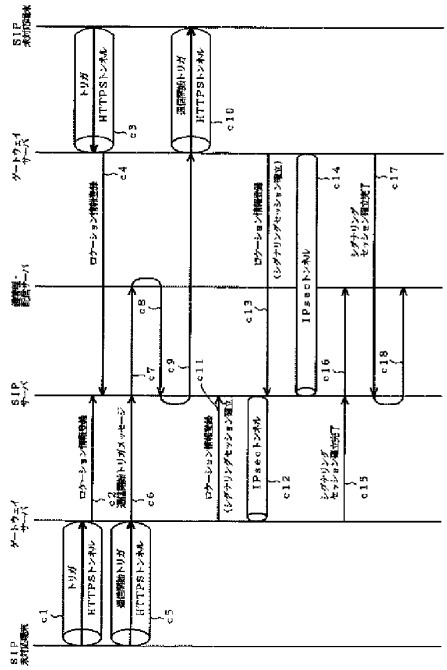
【圖 11】



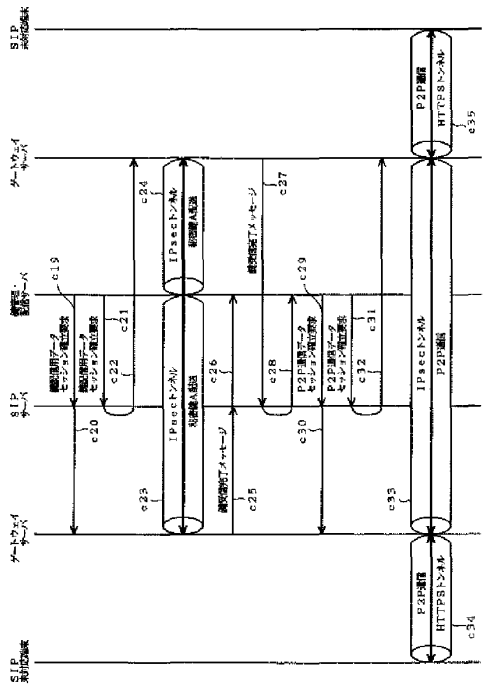
【図 12】



【図 13】



【図 14】



(72)発明者　藤田　直毅

東京都港区芝五丁目７番１号　日本電気株式会社内

Ｆターム(参考) 5J104 AA01　AA16　EA04　EA15　EA16　EA17　EA18　JA03　MA05　NA02

NA37

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.[7]
G06F 15/00

(11) 공개번호 10-2005-0030548
(43) 공개일자 2005년03월30일

(21) 출원번호	10-2004-0074456
(22) 출원일자	2004년09월17일
(30) 우선권주장	10/671,397 2003년09월25일 미국(US)
(71) 출원인	마이크로소프트 코포레이션 미국 워싱턴주 (우편번호 : 98052) 레드몬드 원 마이크로소프트 웨이
(72) 발명자	다니엘리데이먼브이. 미국 98004 워싱턴주 클라이드 힐 84번 플레이스 노쓰이스트 2685
(74) 대리인	주성민, 백만기, 이중희

심사청구 : 없음

(54) 피어-투-피어 통신의 서버 제어

요약

서버는 클라이언트들 간의 피어-투-피어 통신을 확립하기 위한 보안 환경을 제공한냐. 서버의 2개의 클라이언트가 피어-투-피어 통신을 확립하기를 원할 때, 이들은 우선 서버에 접속한다. 서버는 각각의 클라이언트를 인증하고, 인증된 클라이언트에 정보를 제공하여 피어-투-피어 통신을 확립할 수 있게 한다. 피어-투-피어 통신의 특권을 악용하는 모든 클라이언트는 인증된 권리를 상실할 수 있다. 실시예에서, 서버는 게임 서버이며, 클라이언트는 바람직하게는 음성 기반의 피어-투-피어 통신을 사용하여 게임 플레이에 참여한다. 상이한 허가 레벨이 상이한 클라이언트에 허가되어 클라이언트들 간의 인터랙션을 제한할 수 있다.

대표도

도5

색인어

피어-투-피어 통신, 서버 제어, 보안 환경, 액세스 허가

명세서

도면의 간단한 설명

도 1은 게임 콘솔, 및 4개까지의 사용자 입력 디바이스를 위한 지원을 포함하는 예시적인 전자 게임 시스템을 도시한 도면.

도 2는 게임 시스템의 구성요소들을 더 상세하게 나타낸 기능 블럭도.

도 3은 네트워크를 통하여 다수의 게임 시스템을 상호 접속하는 예시적인 네트워크 게임 환경을 도시한 도면.

도 4는 온라인 서비스를 위한 예시적인 시스템에서 사용되는 종래의 서버 컴퓨터 형태의 범용 컴퓨팅 디바이스의 기능 블럭도.

도 5는 서버의 클라이언트들 간의 피어-투-피어 접속의 확립을 용이하게 하는 신뢰되는 환경을 제공하는 서버를 개략적으로 도시한 도면.

도 6은 서버가 자신의 클라이언트들 간의 피어-투-피어 접속의 확립을 용이하게 하는 신뢰되는 환경을 제공할 수 있게 하기 위하여 본 발명에서 사용되는 논리를 나타낸 흐름도.

도 7은 도 5에 기초하는 것으로서, 서버가 게임 서버이고 각각의 클라이언트가 플레이어인 본 발명의 바람직한 실시예를 나타낸 도면.

도 8은 도 3의 예시적인 네트워크 게임 환경의 구성요소들을 더 상세하게 나타낸 기능 블럭도.

Ex.1002 / Page 430 of 1173
Cisco Systems, Inc.

도 9는 게임 플레이 동안 플레이어들 간의 피어-투-피어 접속을 용이하게 하기 위하여 게임 서버에 의해 사용되는 논리를 나타낸 흐름도.

도 10은 게임 플레이 동안 플레이어들 간의 피어-투-피어 접속을 용이하게 하기 위하여 게임 서버에 의해 사용되는 논리에 관한 추가의 세부 사항을 나타낸 흐름도.

도 11은 핵심 기능이 클라이언트들 간의 피어-투-피어 접속의 확립을 용이하게 하는 것인 호스팅 서버를 포함하며, 클라이언트 클래스에 따라 호스팅 서버에 대한 액세스 권한이 상이한 경우의 예시적인 네트워크의 개략도.

<도면의 주요 부분에 대한 부호의 설명>

510 : 네트워크

512 : 서버

514, 516, 518 : 클라이언트

발명의 상세한 설명

발명의 목적

발명이 속하는 기술분야 및 그 분야의 종래기술

본 발명은 일반적으로 피어-투-피어 통신에 관한 것으로, 더 상세하게는 서버를 사용하여 허가된 클라이언트를 인증하고, 인증된 클라이언트들 간에서 피어-투-피어 통신이 확립될 수 있게 하는 것에 관한 것이다.

현재, 전자 디바이스의 사용자들에게 있어서, 다른 사용자와 전자적으로 인터랙션하고, 또한 채팅 세션, 인스턴스 메시징, 합동 작업 프로젝트 및 멀티플레이어 게임을 비롯한 그룹 활동에 참여하는 것은 흔한 일이다. 특히, 게임 및 기타 전자 활동을 위한 음성 통신은 인터넷 또는 기타 네트워크를 통해 접속된 개인들에게 점점 더 인기를 얻어가고 있다. 멀티플레이어 게임에 참여하는 개인들에게 있어서, 음성 통신은 즐거움의 깊이 및 게임 플레이어들 간의 사회적인 인터랙션을 크게 확장시키고 있다.

이와 같은 많은 응용 분야에서, 사용자는 그룹에 참여하는 동안 익명으로 남아있음으로써, 민감한 그룹 토론에 참여하거나, 관습에 어긋나는 견해를 표현하거나, 또는 자신의 신분이 그룹 내의 다른 사람들에게 알려져 있었다면 하지 않았을 사회적으로 위험한 다른 행동들을 하는 것에 관한 걱정을 덜 수 있다. 따라서, 이와 같은 전자 통신 및 그룹 세션을 통한 다른 사용자와의 인터랙션은 종종 개별 사용자 및 그룹 양자 모두의 생산성, 교육적 경험 및 엔터테인먼트를 강화한다.

불행하게도, 공개 포럼의 악용은, 선택된 일부를 제외한 모두에 대하여 이러한 공공 포럼의 유용성 및 즐거움을 파괴시킨다. 예를 들어, 공용 인터넷 통신 디렉토리의 채용은 "성인 자료"에 의하여 방해받아 왔다 (파괴되지 않은 경우). 경험에 의하여, 그룹 내 회원들의 디렉토리가 공용으로 이용가능한 경우, "성인" 회사들이 이러한 디렉토리를 이용하여 성적으로 노골적인 자료를 광고하거나 전송한다는 것을 알고 있다. 이러한 디렉토리를 유지하는 그룹의 호스트들은, 이와 같은 광고의 내용이 일부 사용자들을 몰아내는 것은 물론, 그룹 내 회원들을 대상으로 하는 이러한 성인 광고의 양이 지나치게 많아서, 다른 주제에 관한 대화를 설정하고자 하는 사용자들이 실제로 성적으로 노골적이지 않은 주제에 관심이 있는 합법적인 회원을 식별하는 데에 어려움을 겪는다는 것을 경험해왔다. 마이크로소프트사는 마이크로소프트 회사 서버 상에서의 피어-투-피어 통신을 위한 공용 ILS(Internet Lookup Service)를 유지했었다. 최초 공개 후, 성인 자료는 점점 더 대량으로 나타나기 시작했고, 결국에는 디렉토리 내의 컨텐츠의 대부분이 원래의 관심있는 주제가 아니라, 성적으로 노골적인 자료에 관한 것이 되었다. 이러한 원하지 않는 자료가 원래의 의도된 개인 또는 사업 통신 사용에 대한 디렉토리의 유용성에 심각한 부정적인 영향을 미쳤기 때문에, 마이크로소프트사는 디렉토리 서비스를 중단했다.

온라인 커뮤니티의 대두사구 규정되거나 암묵적인 행동 규약을 따르는 경우에서도, 참가자들 간의 행동 규범을 스스로 구현하고 강제할 수 있는 사용자들의 커뮤니티는 거의 존재하지 않는다. 물론, 전자 그룹의 통신이 제3자 호스트의 총괄적인 제어 하에 있다면, 그 호스트는 커뮤니티 규범을 제정하여 필요에 따라 개입할 수 있다. 개별 회원들 각각의 서버의 클라이언트이고, 클라이언트의 환경 사용을 제어할 수 있는 충분한 권한을 갖는 서버 및 호스트에 의하여 클라이언트들 간의 통신이 관리되는 종래의 클라이언트/서버 환경에서는, 이러한 방식이 효과가 있다. 온라인 게임에서는 각각의 게이머가 게임 서버의 클라이언트이므로, 온라인 게임 플레이는 이러한 패러다임의 대표적인 예이다. 게임 서버(들)가 상이한 플레이어들 간에 택스트 및/또는 음성 통신 서비스를 제공하는 한, 호스트는 서버에 대한 클라이언트 액세스를 통제함으로써 제어를 행할 수 있다. 마찬가지로, 개별 사용자들 간의 피어-투-피어 통신의 확립을 용이하게 하는 신뢰할 수 있는 환경을 형성하는 방법 및 시스템을 제공하는 것이 바람직할 것이다.

특히, 서버의 주된 역할이 클라이언트들 간의 통신을 관리하는 것 이외의 것인 경우, 클라이언트들 간의 통신의 총량은 서버에 바람직하지 못한 부담을 줄 정도로 크게 증가할 수 있다. 서버가 온라인 게임 플레이를 호스트하는 예에서, 플레이어들 간의 음성 통신을 관리하는 데에 요구되는 서버 오버헤드의 양은 상당히 많을 수 있다.

예를 들어, 대규모 멀티플레이어 게임은 중앙화된 대형 서버(또는 서버 그룹)에 의해 호스트되며, 여기에는 수천의 클라이언트가 접속될 수 있다. 중앙화된 서버는 "세계 상태(world state)"를 담당하고, 클라이언트(즉, 플레이어의 컴퓨터 또는 게임 콘솔)는 플레이어의 관점에서 본 세계(일반적으로 전체 세계의 일부분일 뿐임)를 디스플레이하는 것을 담당한다. 클라이언트는 플레이어의 입력과 상태를 계속적으로 서버에 송신한다. 서버는 세계를 업데이트하고, 새로운 세계의 정보를 클라이언트에 계속적으로 리턴시킨다.

현재, 알려져 있는 모든 대규모 멀티플레이어 게임 네트워크는 모든 통신을 중앙 서버를 통하여 라우팅한

다. 즉, 플레이어 A가 플레이어 B에 텍스트 메시지를 보내고자 하는 경우, 플레이어 A는 메시지를 서버에 보내고, 서버는 그 메시지를 플레이어 B에 중계한다. 이와 같은 방식을 택하는 데에는 다음과 같은 좋은 이유가 있다.

· 텍스트 채팅에서, 추가의 대역폭은 상당량의 서버 오버헤드를 부과하지 않는다.

· 피어-투-피어 접속을 확립하는 데에는 시간이 소요된다.

· 피어-투-피어 접속은 서버에 의한 추가의 도움없이는 작동하지 않을 수도 있다.

· 다수의 플레이어에게 메시지를 "패닝(panning)"하는 것은 서버 상에서 효율적으로 행해질 수 있다.

· 송신측 플레이어의 IP 어드레스는 수신측 플레이어에게 "히든" 상태로 된다.

그러나, 음성 채팅은 텍스트 채팅보다 훨씬 큰 대역폭을 필요로 하기 때문에, 대규모 멀티플레이어 게임 네트워크에서 음성 채팅 기능을 추가하는 것은 게임을 호스트하는 중앙 서버에 막대한 부담이 될 수 있다. 그러므로, 게임 서버가 플레이어들 간의 피어-투-피어 통신을 용이하게 하여, 이러한 피어-투-피어 통신이 시작될 수 있는 보안 환경을 제공하면서, 서버 자원에 대한 요구를 감소시킬 수 있게 하는 시스템 및 방법을 제공하는 것이 바람직하다.

발명이 이루고자 하는 기술적 과제

본 발명은, 그에 대한 액세스를 갖는 사용자들 간에서의 피어-투-피어 통신의 확립을 용이하게 하는 신뢰되는 환경을 제공하는 방법 및 시스템에 관한 것이다. 특히, 서버는 각각의 사용자가 그에 대한 액세스를 허가받기 전에 소정의 규범에 따를 것을 확실하게 함으로써, 사용자를 위한 신뢰되는 세션 환경을 제공한다. 서버는 한 세션을 호스트하고, 그 세션에 액세스하려고 시도하는 각각의 사용자의 자격을 검사하여, 서버에 의해 자격을 승인받은 사용자만이 세션에 들어오게 한다. 세션동안, 사용자들은 현재 서버에 의해 승인받은 한명 이상의 다른 사용자를 식별하는 리스트에 대한 액세스를 허가받는다. 리스트는 현재 세션에 액세스하고 있는 사용자를 포함하는 것이 바람직하다. 제1 사용자는 이러한 리스트로부터 제2 사용자를 선택하고, 제1 사용자와 제2 사용자 간에 형성될 피어-투-피어 접속을 용이하게 하기 위한 정보를 제공할 것을 서버에 요청한다. 서버는 제1 사용자에게 필요한 정보를 전송하고, 제1 사용자는 제2 사용자와의 피어-투-피어 통신 링크를 확립하려고 시도한다. 시도가 실패하는 경우, 제1 사용자는 서버에 실패를 알리고, 서버는 제2 사용자에게 정보를 전송하여, 제2 사용자가 피어-투-피어 통신의 확립을 시도할 수 있게 한다.

서버는 상이한 세션들을 동시에 호스트할 수 있고, 사용자는 개별 사용자에게 허가된 액세스 레벨에 따라 이러한 세션들 전부보다 적은 수의 세션에 액세스할 수 있다. 예를 들어, 서버는 복수의 상이한 게임 세션을 호스트할 수 있고, 각각의 사용자는 동일한 게임 세션에 액세스하는 다른 사용자하고만 통신하도록 제한될 수 있다.

피어-투-피어 통신의 확립을 용이하게 하기 위하여 서버에 의해 제공되는 정보는 사용자의 외부 IP 어드레스, 사용자와 연관된 임의의 내부 IP 어드레스, 및 사용자와 연관된 임의의 포트 어드레스를 포함한다. 각각의 사용자가 서버에 액세스할 때, 서버에 의해 해당 사용자에게 고유 사용자 키가 할당되는 것이 바람직하다. 그런 경우, 사용자 키는 서버에 의해 제공되는 정보에 추가되어, 피어-투-피어 통신을 수락하도록 하는 요청을 수신한 사용자가, 그 요청이 신뢰되는 소스로부터 온 것임을 확인할 수 있게 한다.

일 실시예에서, 보안 세션을 호스트하는 서버는 사용자들 간의 피어-투-피어 통신을 용이하게 하는 것과는 다른 핵심 기능을 갖는다. 본 실시예에 대한 바람직한 구현은, 서버가 멀티플레이어 게임을 호스트하는 네트워크 게임 환경이다. 서버의 주된 기능은 게임을 호스트하는 것이며, 피어-투-피어 통신을 용이하게 하는 것은 게임 환경에 대한 향상이다.

다른 실시예에서, 서버의 핵심 기능은 사용자들 간의 피어-투-피어 통신을 사용자가 확립할 수 있게 하는 보안 환경을 제공하는 것이다. 이러한 제2 실시예의 구현에서, 서버는 사용자의 자격 또는 관심에 기초하여 서비스의 상이한 세션들 또는 서브세트들에 대한 개별 액세스를 허가한다. 개별 사용자의 행동에 대한 불만이 다른 사용자들로부터 수신되면, 서버는 그 사용자가 이후의 세션에 참가하는 것을 금지할 수 있다.

본 발명의 다른 양태는, 이하에 더 상세하게 설명되는 본 발명에 따라 전술한 단계들을 수행하기 위한 기계 명령들을 저장하는 메모리 매체에 관한 것이다.

발명의 구성 및 작용

상기와 같은 본 발명의 양태 및 다수의 부수적인 이점은 첨부 도면과 함께 이하의 상세한 설명을 참조함으로써 더 쉽게 이해될 수 있을 것이다.

본 발명의 바람직한 실시예는, 서버를 사용하여 일반 클라이언트들 간의 피어-투-피어 통신에 대한 어느 정도의 제어를 용이하게 하고 수행한다. 서버는 피어-투-피어 통신의 컨텐트를 실시간으로 모니터링하고 제어하는 데에는 관여하지 않지만, 참가자들을 인증 및 허가하며, 이에 의하여 참가자들은 서버에 의하여 유사하게 인증 및 허가된 다른 참가자들에 대한 액세스를 허용받는다. 서버는 인증된 사용자들 간의 피어-투-피어 통신 링크의 확립을 용이하게 하는 데에 사용될 수 있다.

본 발명의 제1 실시예에서, 서버의 핵심 기능을 소정의 다른 기능을 클라이언트에게 제공하는 것이고, 피어-투-피어 통신을 용이하게 하는 것은 2차적인 기능이다. 제1 실시예에서, 서버의 주요 기능을 온라인 게임 플레이를 호스트하는 것이고, 게임 서버에 의해 가능하게 되는 피어-투-피어 통신은 게임 플레이어의 경험을 향상시키기 위해 제공된다.

본 발명의 제2 실시예에서, 서버의 핵심 기능을 신뢰되는 클라이언트들 간의 피어-투-피어 통신을 용이하게 하는 신뢰되는 환경을 제공하는 것이다. 제2 실시예에서, 관심사를 공유하는 회원들 간의 피어-투-피

어 통신을 용이하게 하기 위하여, 공용 인터넷 디렉토리가 만들어진다. 이러한 공용 인터넷 디렉토리는 종래에도 존재했지만, 기존의 디렉토리는 신뢰되는 환경에서 만들어진 것이 아니었으며, 곧바로 성적으로 노골적인 컨텐트를 공급하는 사람들에 의해 악용되었고, 이들로 인해 해당 디렉토리의 본래 목적에 관심이 있던 다른 클라이언트들이 급속하게 떠나게 되었다. 본 실시예의 한 양태에서, 서버는 상이한 "등급"의 엔티티(익명 사용자, 인증된 사용자, 사업자, 대학 등)이 보안 방식으로 강요될 수 있는 상이한 액세스 권한을 할당받게 함으로써, 보안 환경을 제공한다.

네트워크화된 게임 환경에서 피어-투-피어 통신을 용이하게 하는 것은 본 발명의 바람직한 기능을 대표하므로, 이하의 상세한 설명은 예시적인 게임 시스템을 설명한다. 게임 서버 실시예가 바람직한 응용이긴 하지만, 본 발명은 여기에 상세하게 설명된 게임 서버 실시예, 또는 서버의 주요 기능이 피어-투-피어 통신을 용이하게 하는 것 이외의 것인 실시예로만 한정되는 것이 아님에 주의해야 한다. 이하의 상세한 설명 및 그 이후의 특허 청구 범위에 기술된 핵심 개념은 각각의 실시예에 적용되며, 게임 서버 실시예는 본 발명을 한정하기 위한 것이 아니라 예시적인 것으로만 고려되어야 한다. 본 기술 분야의 숙련된 자라면, 본 발명이 네트워크화된 게임 시스템을 비롯한 다양한 컴퓨팅 디바이스를 사용하여 구현될 수 있음을 알 것이다. 따라서, 본 발명은 셋탑 박스를 사용하여, 아케이드 게임에서, 핸드헬드형 디바이스를 사용하여, 퍼스널 컴퓨터(PC) 상에서 실행되는 어플리케이션과 관련하여, 그리고 공통 서버를 공유하는 신뢰되는 클라이언트들 간에서 피어-투-피어 통신을 용이하게 하고자 하는 요구가 있는 기타 네트워크화된 환경에서 구현될 수 있다.

예시적인 게임 시스템

도 1에 도시된 바와 같이, 본 발명을 구현하는 데에 적합한 예시적인 전자 게임 시스템(100)은 게임 콘솔(102), 및 4개까지의 사용자 입력 디바이스를 위한 컨트롤러(104a 및 104b) 등의 지원을 포함한다. 게임 콘솔(102)에는 내부 하드 디스크 드라이브(도면에는 도시되지 않음), 및 광 저장 디스크(108)로 표시된 것과 같은 다양한 형태의 휴대형 광 저장 매체를 판독하는 광 매체 드라이브(106)를 포함한다. 적합한 휴대형 저장 매체의 예는 DVD(digital versatile disc) 및 CD-ROM(compact disk-read only memory disc)를 포함한다. 이러한 게임 시스템에서, 게임 프로그램은 게임 콘솔을 갖는 사용자에게 DVD 디스크 형태로 배포되는 것이 바람직하지만, 여기에 개시된 것과 그 이외의 본 발명을 채용하는 시스템의 유형에서 다른 저장 매체가 대신하여 사용될 수 있을 것으로 예상된다.

게임 콘솔(102)의 전면(前面)에는, 지원되는 컨트롤러와의 접속을 위한 4개의 슬롯(110)이 배치되지만, 슬롯의 개수 및 배열은 보다 많은 수 또는 보다 적은 수의 컨트롤러를 지원하기 위하여 필요에 따라 수정될 수 있다. 전원 버튼(112) 및 인출 버튼(114)도 게임 콘솔(102)의 전면에 배치된다. 전원 버튼(112)은 게임 콘솔로의 전력 인가를 제어하며, 인출 버튼(114)은 광 매체 드라이브(106)의 트레이(도시되지 않음)를 교대로 열고 닫음으로써 저장 디스크(108)를 삽입 및 인출할 수 있게 하여, 사용자가 디스크 상의 디지탈 데이터를 게임 콘솔에 의해 판독할 수 있게 한다.

게임 콘솔(102)은 A/V(audio/visual) 인터페이스 케이블(120)을 통하여 텔레비젼(121)이나 기타 디스플레이 모니터 또는 스크린에 접속된다. 파워 케이블 플러그(122)는 종래의 교류선 소스(도시되지 않음)에 접속될 때, 게임 콘솔에 전력을 공급한다. 게임 콘솔(102)은, 예를 들어 허브 또는 스위치(도시되지 않음)로의 접속을 통하는 네트워크 상에서, 또는 예를 들어 xDSL 인터페이스, 케이블 모뎀 또는 기타 광대역 인터페이스(도시되지 않음)에의 접속을 통한 인터넷 상에서 데이터를 송수신하기 위한 이더넷 데이터 커넥터(124)를 포함한다. 본 발명을 구현하는 다른 유형의 게임 콘솔들은, 종래의 전화 모뎀을 이용하여 통신함으로써, 서로 연결될 수도 있고 원격 서버에 연결될 수도 있다.

각각의 컨트롤러(104a 및 104b)는 리드를 통해 (또는 무선 인터페이스를 통해) 게임 콘솔(102)에 연결된다. 도시된 구현예에서는, 컨트롤러가 USB 호환가능하며, USB 케이블(130)을 통해 게임 콘솔(102)에 접속되어 있지만, 다른 유형의 데이터 인터페이스가 그를 대신하여 채용될 수 있음을 예상할 수 있다. 게임 콘솔9102)에는 게임 소프트웨어와 인터랙션하고 게임 소프트웨어를 제어하는 매우 다양한 사용자 디바이스 중 어느 것이라도 장착될 수 있다. 도 1에 도시된 바와 같이, 각각의 컨트롤러(104a 및 104b)에는 2개의 썸스틱(thumbstick)(132a 및 132b), D 패드(134), 버튼(136) 및 2개의 트리거(138)가 장착된다. 이러한 컨트롤러들은 단지 예시적인 것일 뿐이며, 다른 게임 입력 및 제어 디바이스가 도 1에 도시된 디바이스를 대체하거나 그에 추가되어 게임 콘솔(102)에서 사용될 수 있다.

추가의 특징 및 기능을 제공하기 위하여, 분리가능한 기능 유닛(140)이 각각의 컨트롤러(104a 및 104b)에 선택적으로 삽입될 수 있다. 예를 들어, 휴대형 메모리 유닛(MU)은, 사용자가 게임 파라미터를 저장할 수 있게 하고, 또한 다른 게임 콘솔에 접속된 컨트롤러에 휴대형 MU를 삽입하여 그 다른 게임 콘솔에서 플레이할 수 있도록 게임 파라미터를 운반할 수 있게 한다. 다른 분리가능한 기능 유닛은, 사용자가 다른 사용자들과 국부적으로 및/또는 네트워크 상으로 구두로 통신할 수 있게 하는 음성 통신 유닛을 포함한다. 음성 통신 유닛에는, 붐 마이크로폰(boom microphone)(144)을 포함하는 헤드셋(142)이 접속된다. 이와 달리, 음성 통신 유닛의 회로가 컨트롤러에 일체화될 수 있으며, 붐 마이크로폰을 갖는 헤드셋은 컨트롤러에 분리가능하게 접속될 수도 있고 영구적으로 접속될 수도 있다. 각각의 컨트롤러는 2개의 분리가능한 기능 유닛을 수용하도록 구성되는 것이 바람직하지만, 더 많은 수 또는 더 적은 수의 분리가능한 기능 유닛 또는 모듈이 대신 채용될 수도 있다.

게임 시스템(100)은 예를 들어 게임, 음악 및 비디오를 플레이할 수 있다. 하드 디스크 드라이브 상에 저장되어 있거나 드라이브(106) 내의 광 저장 디스크(108)로부터 판독된 디지탈 데이터를 사용하여, 또는 온라인 소스나 MU로부터 획득된 디지탈 데이터를 사용하여, 다른 기능들이 구현될 수 있는 것으로 예상된다. 예를 들어, 게임 시스템(100)은 잠재적으로 다음과 같은 것들을 재생할 수 있다.

· 광 매체 드라이브에 의해 판독되는 CD 및 DVD 상에 저장되거나, 하드 디스크 드라이브 상에 저장되거나, 또는 온라인 소스로부터 다운로드된 게임 타이틀;

· 광 매체 드라이브(106)에 의해 판독되는 CD 상에 저장되어 있거나, 또는 하드 디스크 드라이브 상의 파일[예를 들어, WINDOWS MEDIA AUDIO™(WMA) 포맷]에 저장되어 있거나, 인터넷 또는 다른 네트워크 상의 온

라인 스트리밍 소스로부터 유도된 디지탈 음악;

·광 매체 드라이브(106)에 의해 판독되는 DVD 디스크 상에 저장되어 있거나, 또는 하드 디스크 드라이브 상의 파일(예를 들어, 액티브 스트리밍 포맷)에 저장되어 있거나, 인터넷 또는 다른 네트워크 상의 온라인 스트리밍 소스로부터 액세스된 디지탈 A/V 데이터.

도 2는 게임 시스템(100)의 기능적 구성요소들을 더 상세하게 도시하고 있다. 게임 콘솔(102)은 CPU(200), ROM(204)에 대한 CPU 액세스를 용이하게 하는 메모리 컨트롤러(202), RAM(206), 하드 디스크 드라이브(208), 휴대형 광 매체 드라이브(106)를 포함한다. CPU(200)에는, 요구되는 메모리 액세스 사이클의 수를 감소시키도록 일시적으로 데이터를 저장하여 게임 시스템의 처리 속도 및 처리량을 증가시키기 위한 레벨 1 캐시(210) 및 레벨 2 캐시(212)가 장착된다. CPU(200), 메모리 컨트롤러(202) 및 다양한 메모리 디바이스는, 다양한 버스 아키텍쳐 중 임의의 것을 사용하는 프로세서 또는 로컬 버스, 주변 버스, 메모리 버스, 직렬/병렬 버스를 비롯한 하나 이상의 버스를 통하여 상호 접속된다. 예를 들어, 이러한 아키텍쳐는 ISA(Industry Standard Architecture) 버스, MCA(micro channel architecture) 버스, EISA(enhanced ISA) 버스, VESA(Video Electronics Standards Association) 로컬 버스, 및 PCI(peripheral component interconnect) 버스를 포함할 수 있다.

적절한 구현의 일례로서, CPU(200), 메모리 컨트롤러(202), ROM(204) 및 RAM(206)은 공통 모듈(214) 상에 일체화된다. 이러한 구현예에서, ROM(204)은 PCI 버스 및 ROM 버스(양자 모두 도시되지 않음)를 통해 메모리 컨트롤러(202)에 접속되는 플래시 ROM으로서 구성된다. RAM(206)은 별도의 버스(도시되지 않음)를 통해 메모리 컨트롤러(202)에 의하여 독립적으로 제어되는 다수의 DDR SDRAM(double data rate synchronous dynamic RAM) 모듈로서 구현된다. 하드 디스크 드라이브(208) 및 광 매체 드라이브(106)는 PCI 버스 및 ATA(advanced technology attachment) 버스(216)를 통해 메모리 컨트롤러에 접속된다.

3D 그래픽 프로세스 유닛(GPU)(220) 및 비디오 인코더(222)는 고속 고해상도 그래픽 프로세스를 위한 비디오 프로세스 파이프라인을 형성한다. 데이터는 디지탈 비디오 버스(도시되지 않음)를 통해 GPU(220)로부터 비디오 인코더(222)로 전달된다. 오디오 프로세스 유닛(224) 및 오디오 인코더/디코더(CODEC)(226)는 하이파이 스테레오 오디오 데이터 프로세스를 위한 대응 오디오 프로세스 파이프라인을 형성한다. 오디오 데이터는 오디오 프로세스 유닛(224)과 CODEC(226) 간에서 통신 링크(도시되지 않음)를 통해 전달된다. 비디오 및 오디오 프로세스 파이프라인은 텔레비전 또는 다른 디스플레이 모니터로의 전송을 위하여 데이터를 A/V 포트(228)에 출력한다. 도시된 구현에에서, 비디오 및 오디오 프로세스 구성요소(220-228)는 모듈(214) 상에 실장된다.

모듈(214) 상에는, USB 호스트 컨트롤러(230) 및 네트워크 인터페이스(232)도 구현된다. USB 호스트 컨트롤러(230)는 버스(예를 들어, PCI 버스)를 통해 CPU(200) 및 메모리 컨트롤러(202)에 연결되고, 주변 게임 컨트롤러(104a-104d)를 위한 호스트로서 기능한다. 네트워크 인터페이스(232)는 네트워크(인터넷, 홈 네트워크 등)에 대한 액세스를 제공하며, 이더넷 카드, 전화 모뎀 인터페이스, 블루투스 모듈, 케이블 모뎀 인터페이스, xDSL 인터페이스 등을 비롯하여 다양한 유선 또는 무선 인터페이스 구성요소 중 임의의 것을 포함할 수 있다.

게임 콘솔(102)은 2개의 듀얼 컨트롤러 지원 서브어셈블리(240a 및 240b)를 포함하고, 각각의 서브어셈블리는 게임 컨트롤러들(104a-104d) 중 2개를 지원한다. 프론트 패널 입출력(I/O) 서브어셈블리(242)는 전원 버튼(112) 및 인출 버튼(114)의 기능성은 물론, 게임 콘솔의 외측 표면에 노출된 임의의 발광 다이오드(LED) 또는 기타 표시기를 지원한다. 서브어셈블리(240a, 240b, 242)는 하나 이상의 케이블 어셈블리(244)를 통하여 모듈(214)에 연결된다.

8개의 기능 유닛(140a-140h)이 4개의 컨트롤러(104a-104d)에 접속가능한 것으로 도시되어 있다. 즉, 각각의 컨트롤러에 2개의 기능 유닛이 접속가능하다. 각각의 기능 유닛은 게임, 게임 파라미터 및 기타 데이터를 위한 추가의 기능 또는 저장공간을 제공한다. MU가 컨트롤러에 삽입되면, MU는 메모리 컨트롤러(202)에 의하여 액세스될 수 있다.

시스템 전력 공급 모듈(250)은 게임 시스템(100)의 구성요소들에 전력을 제공한다. 팬(252)은 게임 콘솔(102) 내의 구성요소들 및 회로를 냉각시킨다.

본 발명을 구현하기 위하여, DVD 또는 기타 저장 매체 상에 저장되어 있는 (또는 네트워크를 통해 다운로드된) 기계 명령들을 포함하는 게임 소프트웨어 어플리케이션(260)이 CPU(200)에 의해 실행되기 위하여 RAM(206) 및/또는 캐시(210 및/또는 212)에 로드된다. 소프트웨어 어플리케이션(260)의 부분들이 필요한 때에만 RAM에 로드될 수도 있고, 소프트웨어 어플리케이션 전체가 (그 크기에 따라) RAM(206)에 로드될 수도 있다. 소프트웨어 어플리케이션(260), 및 그 소프트웨어 어플리케이션이 본 발명을 구현하기 위하여 수행하는 관련 기능들이 이하에 더 상세하게 설명된다.

게임 시스템(100)을 텔레비전 또는 다른 디스플레이 모니터에 단순히 접속하는 것에 의하여, 게임 시스템(100)은 독립형 시스템으로서 동작할 수 있다. 이러한 독립형 모드에서, 게임 시스템(100)은 한명 이상의 사용자가 게임을 플레이하거나 영화를 보거나 음악을 들을 수 있게 한다. 그러나, 네트워크 인터페이스(232)를 통하여 이용가능하게 되는 인터넷 또는 기타 네트워크로의 접속에 의하여, 게임 시스템(100)은 보다 큰 네트워크 게임 커뮤니티의 구성요소로서 동작하여, 인터넷 또는 기타 네트워크를 통하여 플레이되는 게임에서 다른 게임 시스템을 사용하는 플레이어들과의 온라인 멀티플레이어 인터액션이 가능하게 할 수 있다. 게임 시스템(100)은 네트워크 인터페이스 및 적합한 케이블(도시되지 않음)을 사용하여 다른 게임 시스템과 피어-투-피어 통신으로 연결될 수 있다.

제1 실시예를 위한 예시적인 게임 네트워크

도 3은 네트워크(302)를 통하여 다수의 게임 시스템(100a, ...100n)을 상호접속한 예시적인 네트워크 게임 환경(300)을 도시하고 있다. 바람직하게는, 각각의 게임 시스템은, 플레이어들 간에서의 음성 통신을 위하여, 적어도 하나의 대응 헤드셋(142a, ...142n) 및 대응 마이크로폰(144a, ...144n)을 포함한다. 네트워크(302)는 다양한 데이터 통신 네트워크 중 임의의 것을 나타내며, 공용 부분(예를 들어, 인터넷)은 물

론 전용 부분(예를 들어, 주거용 또는 상업용 LAN)을 포함할 수 있다. 네트워크(302)는 유선 타입 및 무선 타입 양자 모두를 비롯하여 다양한 종래의 통신 구성 중 임의의 하나 또는 그 이상을 사용하여 구현될 수 있다. 공용 및 전용 프로토콜을 비롯하여, 다양한 통신 프로토콜 중 어느 것이라도 네트워크(302)를 통하여 데이터를 통신하는 데에 사용될 수 있다. 이러한 프로토콜의 예는 TCP/IP, IPX/SPX, NetBEUI 등을 포함한다.

게임 시스템(100a, ...100n)에 더하여, 온라인 게임을 서비스 및/또는 호스트하는 것, 다운로드가능한 음악 또는 비디오 파일을 서비스하는 것, 게임 경쟁을 호스트하는 것, 스트리밍 A/V 파일을 서비스하는 것, 이메일 또는 기타 메체 통신의 교환을 가능하게 하는 것과 같은 다양한 서비스를 참가자들에게 제공하기 위하여, 하나 이상의 온라인 서비스(304a,...304s)가 네트워크(302)를 통하여 액세스 될 수 있다. 네트워크 게임 환경(300)은, 개별 플레이어 및/또는 게임 시스템(100a,...100n)이 온라인 서비스(304a,...304s)에는 물론 다른 플레이어 및/또는 게임 시스템에 상호접속할 수 있게 하는 인증에 있어서 중요한 역할을 하는 키 분배 센터(306)를 더 포함할 수 있다. 분배 센터(306)는 키 및 서비스 티켓을 정당한 참가자들에게 분배하고, 이러한 키 및 서비스 티켓은 다수의 플레이어를 포함하는 게임 플레이 그룹을 형성하거나 온라인 서비스(304a,...304s)로부터 서비스를 구입하는 데에 사용될 수 있다.

네트워크 게임 환경(300)은 개별 게임 시스템(100a, ...100n)에 이용가능한 다른 메모리 소스, 즉 온라인 저장소를 도입한다. 광 저장 디스크(108), 하드 디스크 드라이브(208) 및 기능 유닛(140) 상의 데이터에 액세스하는 것에 더하여, 게임 시스템(100a, ...100n)은, 온라인 서비스(304s)의 원격 저장소(308)에 의해 예시된 바와 같이, 네트워크(302)를 통하여 원격 저장 위치에서 이용가능한 데이터 파일에도 액세스할 수 있다.

네트워크 게임 환경은, 강화된 보안을 제공하고 다른 컴퓨팅 디바이스에 의한 액세스를 제한하기 위하여, 예를 들어 가상 전용 네트워크 터널을 통한 통신을 이용하여, 다른 게임 시스템 및 게임 환경으로의 액세스만을 제공하는 폐쇄된 네트워크일 수 있음에 유의해야 한다.

<u>온라인 서비스 및 서버 컴퓨터를 위한 예시적인 시스템</u>

도 4를 참조하면, 본 발명에 따른 온라인 서비스(304a, ...304s)를 위한 예시적인 시스템은, 프로세싱 유닛(421), 시스템 메모리(422) 및 시스템 버스(423)를구비하는 종래의 서버 컴퓨터(SC)(420) 형태의 범용 컴퓨팅 디바이스를 포함한다. 시스템 버스는 시스템 메모리를 비롯한 다양한 시스템 컴포넌트들을 프로세싱 유닛(421)에 연결하며, 다양한 버스 아키텍처 중 임의의 것을 사용하는 로컬 버스, 주변 버스, 및 메모리 버스 또는 메모리 컨트롤러를 포함하는 여러 유형의 버스 아키텍쳐 중 임의의 것일 수 있다. 시스템 메모리는 ROM(424) 및 RAM(425)을 포함한다. 기동시에 SC(420) 내의 소자들 간의 정보 전송을 돕는 기본 루틴을 포함하는 기본 입출력 시스템(BIOS)(426)은 ROM(424) 내에 저장된다. SC(420)는 하드 디스크(도시되지 않음)에 대한 판독 및 기입을 위한 하나 이상의 하드 디스크 드라이브(427), 분리가능한 자기 디스크(429)에 대한 판독 및 기입을 위한 자기 디스크 드라이브(428), 및 CD-ROM 또는 기타 광 매체와 같은 분리가능한 광 디스크(431)에 대한 판독 및 기입을 위한 광 디스크 드라이브(430)를 더 포함할 수 있다. 하드 디스크 드라이브(427), 자기 디스크 드라이브(428) 및 광 디스크 드라이브(430)는 하드 디스크 드라이브 인터페이스(432), 자기 디스크 드라이브 인터페이스(433) 및 광 디스크 드라이브 인터페이스(434)를 통하여 각각 시스템 버스(423)에 접속된다. 드라이브 및 그 관련 컴퓨터 판독가능 매체는 컴퓨터 판독가능한 기계 명령, 데이터 구조, 프로그램 모듈 및 SC(420)를 위한 기타 데이터에 대한 비휘발성 저장소를 제공한다. 여기에 개시된 예시적인 환경에서는 하드 디스크, 분리가능한 자기 디스크(429) 및 분리가능한 광 디스크(431)를 이용하지만, 본 기술 분야의 숙련된 기술자라면, 자기 카세트, 플래시 메모리 카드, DVD(digital video disc), 베르누이 카트리지, RAM, ROM 등과 같이, 컴퓨터에 의해 액세스가능한 데이터 및 기계 명령을 저장할 수 있는 다른 유형의 컴퓨터 판독가능 매체도 예시적인 오퍼레이팅 환경에서 이용될 수 있음을 알 것이다.

오퍼레이팅 시스템(435), 하나 이상의 어플리케이션 프로그램(436), 기타 프로그램 모듈(437) 및 프로그램 데이터(438)를 비롯한 다수의 프로그램 모듈이 하드 디스크, 자기 디스크(429), 광 디스크(431), ROM(424) 또는 RAM(425) 상에 저장될 수 있다. 사용자는 SC(420)에 명령 및 정보를 입력할 수 있고, 키보드(440) 및 포인팅 디바이스(442)와 같은 입력 디바이스를 통하여 제어 입력을 제공할 수 있다. 포인팅 디바이스(442)는 마우스, 스타일러스, 무선 리모콘 또는 기타 커서 컨트롤을 포함할 수 있다. 이하에서, "마우스"라는 용어는 스크린 상에서 커서의 위치를 제어하는 데에 유용한 임의의 포인팅 디바이스를 모두 포괄하도록 의도된 것이다. 다른 입력 디바이스(도시되지 않음)로는, 마이크로폰, 조이스틱, 햅틱 조이스틱, 요크(yoke), 풋 페달, 게임 패드, 위성 접시, 스캐너 등이 있을 수 있다. 여기에 개시된 것과 그 이외의 I/O 디바이스는, 시스템 버스에 연결된 I/O 인터페이스(446)를 통해 프로세싱 유닛(421)에 접속된다. I/O 인터페이스라는 용어는, 직렬 포트, 병렬 포트, 게임 포트, 키보드 포트 및/또는 USB 포트에 전용으로 사용되는 각각의 인터페이스를 포괄하도록 의도된 것이다. 모니터(447) 또는 다른 유형의 디스플레이 디바이스도, 비디오 어댑터(448)와 같은 적합한 인터페이스를 통하여 시스템 버스(423)에 접속되며, 어플리케이션 프로그램, 그래픽 이미지, 웹 페이지 및/또는 다른 정보를 디스플레이하는 데에 사용될 수 있다. 모니터에 더하여, SC는 스피커(사운드 카드 또는 기타 오디오 인터페이스를 통함, 도시되지 않음) 및 프린터와 같은 다른 주변 출력 디바이스(도시되지 않음)에 연결될 수 있다.

SC(420)는 원격 컴퓨터(449) 또는 전술한 게임 시스템과 같은 하나 이상의 원격 컴퓨팅 디바이스로의 논리적 접속을 이용하여 네트워크화된 환경에서 동작하는 것이 바람직하다. 따라서, 원격 컴퓨터(449)는 다른 SC, 게임 콘솔, 퍼스널 컴퓨터[일반적으로 SC(420)와 거의 유사하게 구성됨], 라우터, 네트워크 PC, 피어 디바이스, 또는 위성 또는 기타 통신 네트워크 노드일 수 있으며, 도 4에는 외부 메모리 저장 디바이스(450)만이 도시되어 있지만, 전형적으로 SC(420)과 관련하여 기술된 요소의 다수 또는 전부를 포함한다. 도 3의 네트워크(302)와 관련하여 전술한 바와 같이, 도 4에 도시된 논리적 접속은 근거리 네트워크(LAN)(451) 및 광역 네트워크(WAN)(452)를 포함한다. 이러한 네트워크 환경은 현재 가정에서 비교적 일반적으로 사용되며, 사무실, 기업내 컴퓨터 네트워크, 인트라넷 및 인터넷에서는 매우 흔하다.

LAN 네트워크 환경에서 이용하기 위하여, SC(420)는 네트워크 인터페이스 또는 어댑터(453)를 통하여 LAN(451)에 접속된다. WAN 네트워크 환경에서 이용될 때, SC(420)는 전형적으로 인터넷 등의 WAN(452)을

통한 통신을 확립하기 위하여, 모뎀(454), 케이블 모뎀과 같은 다른 수단, DSL 인터페이스 또는 ISDN(Integrated Service Digital Network)를 포함한다. 내장형 또는 외장형일 수 있는 모뎀(454)은, I/O 디바이스 인터페이스(446)를 통해, 즉 직렬 포트를 통해 시스템 버스(423)에 접속되거나 버스에 연결된다. 네트워크화된 환경에서, SC(420)와 관련하여 나타난 프로그램 모듈 또는 그 일부는 원격 메모리 저장 디바이스에 저장될 수 있다. 여기에 도시된 네트워크 접속은 예시적인 것이며, 무선 통신 및 광대역 네트워크 링크와 같이, 컴퓨터/컴퓨팅 디바이스들 간의 통신 링크를 확립하기 위한 다른 수단들도 사용될 수 있음을 알 것이다.

제1 및 제2 실시예에 적용될 수 있는 핵심 개념

도 5에 도시된 바와 같이, 네트워크(510)는 서버(512) 및 클라이언트(514, 516 및 518)를 포함한다. 서버(512)는 서버에 의해 호스트되는 세션에 대한 액세스를 허가받은 클라이언트들을 제어함으로써 신뢰되는 환경을 제공한다. 서버(512)는 각각의 클라이언트가 서버에 의해 호스트되는 세션으로의 액세스에 대한 요금을 지불하는 가입 서비스로서 동작할 수 있다. 다르게는, 세션으로의 액세스를 위한 요금이 클라이언트에게 부과되지는 않지만, 서버가 자신이 호스트하는 각각의 세션에 어떤 클라이언트들이 액세스하는지를 제어하도록, 클라이언트가 각각의 세션에 등록할 것이 요구된다. 예를 들어, 등록 프로세스에서, 클라이언트는 피어-투-피어 컨텍스트에서 다른 클라이언트와의 성적인 주제에 관한 통신을 금지하는 것과 같은 커뮤니티 정책에 동의해야 한다. 다른 클라이언트가 이러한 정책의 악용을 보고하면, 위반을 행한 클라이언트는 이후로는 서버로부터 추방될 수 있다. 서버는 복수의 세션을 조작할 수 있으며, 일부 세션에 대해서만 클라이언트의 액세스를 제한할 수 있다. 예를 들어, 서버(512)는 십대용 세션, 모델 트레이닝을 강조하는 취미 세션, 및 클라이언트들간의 성적으로 노골적인 통신의 허용도가 큰 성인용 세션을 동시에 호스트할 수 있다. 18세 미만의 등록 클라이언트들은 십대용 세션 및 취미 세션에 대한 액세스는 허가받지만, 성인용 세션에 대한 액세스는 허가받지 못한다. 성인 클라이언트 등록자는 원하는 경우에 성인 세션에서 나올 것을 선택할 수 있다. 서버(512)가 게임 서버인 경우, 상이한 게임 및 상이한 난이도에서의 게임 플레이에 대응하는 복수의 상이한 세션이 이용가능할 수 있다.

본 발명의 하나의 핵심적인 개념은, 서버에 의해 호스트되는 세션에 대한 액세스를 제어함으로써, 서버가 정한 행동 지침을 위반한 클라이언트가 이후의 세션에서 추방될 수 있다는 것이다. 위반은 여러 컨텍스트에서 발생할 수 있다. 클라이언트는 서버에 의해 지원되지 않는 주제(예를 들어, 성 관련 주제 또는 정치 관련 주제)에 관한 피어-투-피어 통신에 참여하도록 하는 요청을 서버 상에 발송할 수 있다. 서버는 발송된 것을 삭제하고, 그 클라이언트가 이후에 서버에 액세스하는 것을 금지할 수 있다. 다른 컨텍스트에서, 클라이언트는 피어-투-피어 컨텍스트에서 다른 클라이언트와 무례하거나 귀찮은 통신에 참가할 수 있다. 서버는 이러한 행위에 관하여 다른 클라이언트들로부터의 피드백을 수집하고, 요구에 따라 위반을 행한 클라이언트를 추방한다. 공동 양도된 미국 특허 출원 10/151,793호 "자동 피드백 및 플레이어 거부"는 온라인 게임 환경에서 플레이어의 행위에 관한 피드백을 수집하는 시스템 및 방법을 개시하고 있다. 여기에 개시된 시스템 및 방법은 서버(512)의 클라이언트에 관한 피드백을 수집하고 필요에 따라 클라이언트를 추방하는 데에 사용될 수 있다.

서버(512)에 의해 호스트되는 세션은 광범위하게 변화할 수 있다. 전술한 바와 같이, 제1 실시예에서, 서버의 가장 중요한 기능은 피어-투-피어 통신을 용이하게 하는 것이 아니라, 온라인 게임을 호스트하는 등의 다른 기능을 수행하는 것이다. 이러한 실시예에서, 클라이언트(플레이어)들 간의 피어-투-피어 통신을 확립하는 것은 게임 경험을 강화한다. 제2 실시예에서, 서버의 핵심 기능은 클라이언트가 피어-투-피어 통신을 확립하고자 하는 다른 클라이언트를 찾을 수 있게 하는 것이다. 어떤 실시예가 구현되는지와 무관하게, 서버(512)는, 자신에 의하여 인에이블된 세션으로의 액세스를 허가받은 클라이언트에 대한 제어를 서버 자신이 행하는 신뢰되는 환경을 제공한다.

서버(512)는 다수의 상이한 하드웨어 구성을 이용하여 구현될 수 있음을 알아야 한다. 서버(512)는 단일 컴퓨팅 플랫폼으로서 구현될 수도 있고, 서로 협력적으로 기능하는 복수의 컴퓨팅 플랫폼으로서 구현될 수도 있다. "서버"라는 용어는 단일 컴퓨팅 디바이스로만 한정하기 위한 것이 아니라, "서버"의 기능을 수행하는 복수의 컴퓨팅 디바이스를 포괄하도록 더 넓은 의미를 갖는다는 점에 유의해야 한다.

다시 도 5를 참조하면, 클라이언트(514, 516, 518)는 각각 서버(512)와 서버/클라이언트 접속(520)을 확립하고 있다. 서버(512)에 의해 제공되는 정보에 기초하여, 클라이언트(514)는 클라이언트(516)과 피어-투-피어 접속(522)을 확립한다. 마찬가지로, 클라이언트(518)는 클라이언트(516)과 피어-투-피어 접속(522)을 확립한다.

도 6은 서버를 이용하여, 클라이언트들 간의 피어-투-피어 통신이 서버에 의하여 용이하게 되는 보안 환경을 제공하는 논리를 개괄적으로 나타낸 흐름도(610)이다. 논리는 블럭(612)에서 시작하고, 블럭(614)에서 서버는 자신이 호스트하는 세션에 액세스하려고 시도하는 각각의 클라이언트를 인증 및 허가하여 해당 세션에 참가시킨다. 블럭(616)에서, 서버는 세션에 현재 액세스하고 있는 다른 허가된 클라이언트들을 포함하는 리스트를 클라이언트에게 제공한다. 일부 상황에서는, 피어-투-피어 통신을 원하지만 현재는 세션에 포함되어 있지 않은 클라이언트들을 포함하는 것이 바람직하다. 그러나, 대부분의 상황에서, 이러한 리스트 내의 각각의 클라이언트는 서버에 로그인하여 온라인 상태이며, 피어-투-피어 통신을 확립할 수 있을 것이다. 리스트는 단일 클라이언트만을 포함할 수도 있지만, 일반적으로는 복수의 클라이언트를 포함할 것이다.

리스트가 클라이언트들에게 제공되는 방식은 광범위하게 달라질 수 있다. 리스트의 컨텐트도 다양한 방식으로 구성될 수 있다. 예를 들어, 서버가 게임 서버인 경우, 리스트는 제1 클라이언트의 "팀"의 회원인 클라이언트들로만 한정될 수 있고, 그 결과 리스트는 세션에 참가하고 있는 모든 클라이언트를 포함하지는 않을 것이다. 클라이언트들 간의 피어-투-피어 통신을 용이하게 하는 것을 주된 기능으로 하는 서버와 관련하여, 리스트는 특정 클라이언트에 연관된 인증에 기초할 수 있다. 성인용 세션, 십대용 세션 및 취미 세션을 호스트하는 서버의 경우를 고찰하기로 한다. 제1 클라이언트의 연령에 기초하여, 리스트는 성인용 세션으로부터의 임의의 클라이언트를 포함하지 않을 수 있다. 특히, 피어-투-피어 통신을 용이하게 하기 위한 전용 서버와 관련하여, 클라이언트들이 특정 관심사를 공유하는 다른 클라이언트들을 식별하도록 리스트를 좁게 정의할 수 있게 하는 것이 바람직하다. 예를 들어, 제1 클라이언트는 성인용 세션에 참여하

는 데에 충분한 연령이지만, 실제로 자신이 거주하는 동일 지역 내의 취미 생활자들과만 통신하기를 원할 수 있다. 이 경우, 서버에 의해 제공되는 리스트는 주제 및 지역에 의해 한정될 것이다. 본 기술 분야의 통상적인 지식을 가진 자라면, 많은 다른 변경이 가능함을 알 것이다.

다시 도 6의 흐름도(610)를 참조하면, 블럭(618)에서, 제1 클라이언트는 리스트로부터 제2 클라이언트를 선택할 수 있게 된다. 그러면, 서버는 블럭(620)에 나타난 바와 같이 제2 클라이언트에 대한 접속 정보를 제1 클라이언트에게 송신한다. 이러한 접속 정보는 적어도 제2 클라이언트와의 피어-투-피어 통신을 확립하기 위하여 제1 클라이언트에게 필요한 정보를 포함한다. 예를 들어, 제2 클라이언트의 외부 IP 어드레스가 포함될 것이다. 제2 클라이언트가 내부 IP 어드레스와 연관되고/되거나(예를 들어 공유 인터넷 접속 네트워크 상에 있음) 특정 포트 어드레스와 연관되는 경우에는, 그 정보도 포함될 것이다. 정보는 서버에 의해 제공되는 사용자 키를 포함하여, 제2 클라이언트가 제1 클라이언트와의 피어-투-피어 통신을 확립하기 위한 요청을 수신한 때에, 제1 클라이언트가 서버에 의해 제2 클라이언트에 할당된 사용자 키를 갖는다는 사실이 제1 클라이언트가 서버에 의해 신뢰된다는 것을 나타내도록 하는 것이 바람직하다.

블럭(622)에서, 제1 클라이언트는 서버로부터 수신된 제2 클라이언트에 관한 접속 정보를 사용하여, 제2 클라이언트와의 피어-투-피어 통신의 확립을 시도한다. 결정 블럭(624)은 그 시도가 성공적이었는지를 결정한다. 성공적이었던 경우에는, 블럭(626)에 나타난 바와 같이, 참가자들 중 한 명에 의하여 (또는 네트워크 실패에 의하여) 해제될 때까지 접속이 유지된다. 시도가 성공적이지 않았던 경우에는, 블럭(628)에 나타난 바와 같이, 서버는 제1 클라이언트의 접속 정보를 제2 클라이언트에 전송한다. 블럭(630)에서, 제2 클라이언트는 제1 클라이언트의 접속 정보를 사용하여, 제1 클라이언트와의 피어-투-피어 통신의 확립을 시도한다. 결정 블럭(632)은 시도가 성공적이었는지를 결정한다. 마찬가지로, 블럭(626)에 나타나 있는 바와 같이, 접속은 참가자들 중 한 명에 의하여 (또는 네트워크 실패에 의하여) 해제될 때까지 유지된다. 논리는 블럭(636)에서 종료한다. 피어-투-피어 통신을 확립하기 위한 제2의 시도가 성공적이지 않은 경우, 논리는 블럭(618)로 되돌아가서, 서버가 제2 클라이언트의 접속 정보를 제1 클라이언트에게 다시 송신하게 하거나[블럭(632)을 블럭(618)에 연결시키는 점선에 의해 나타나 있는 바와 같이], 서버가 선택 블럭(634)에 나타나 있는 바와 같이 서버를 통한 음성 트래픽(또는 클라이언트들 간의 다른 통신)을 선택적으로 라우팅할 수 있게 한다. 블럭(630)에서 피어-투-피어 접속이 확립되지 않은 경우의 또다른 선택안은, 단순하게 시도된 통신이 성공적이지 않았음을 표시하고 블럭(636)에서 논리를 종료하는 것이다.

제1 실시예의 게임 서버 구현에 관한 세부 사항

도 7은 도 5에 기초하는 것으로서, 본 발명의 개념이 온라인 게임 환경과 관련하여 어떻게 적용되는지를 나타내고 있다. 네트워크(710)는 대규모 멀티플레이어(massively multi player) 게임 서버(712) 및 플레이어(714, 716, 718, 719)를 포함한다. 도 7에 나타난 바와 같이, 바람직한 구현에서, 각각의 클라이언트는 도 1 및 도 2와 관련하여 설명된 것과 같은 게임 콘솔을 사용하는 플레이어이다. 본 기술 분야의 통상의 지식을 가진 자라면, 도 7의 각각의 플레이어가 상이한 유형의 게임 디바이스 또는 퍼스널/랩탑 컴퓨터를 사용하여 게임 서버에 액세스할 수 있음을 알 것이다.

각각의 플레이어는 서버/클라이언트 접속(720)을 사용하여 게임 서버(712)에 의해 호스트되는 게임 세션에 액세스한다. 서버(712)에 의해 제공되는 정보에 기초하여, 플레이어(714)는 플레이어(716)와의 피어-투-피어 접속(722)을 확립한다. 마찬가지로, 플레이어(714)는 플레이어(718)와의 피어-투-피어 접속(722)을 확립한다.

게임 네트워크(300)와 관련하여, 각각의 플레이어(714-719)는 전술한 것과 같이 4명까지의 플레이어를 지원할 수 있는 게임 콘솔(102)을 사용하는 것이 바람직하다. 따라서, 도 7에 도시된 각각의 클라이언트/플레이어는 실질적으로 4명까지의 개별 플레이어를 포함할 수 있고, 이들 각각이 다른 게임 콘솔을 사용하여 선택된 개별 플레이어들과의 피어-투-피어 통신을 확립할 수 있기 때문에, 도 7은 다소 단순화된 것이다. 하나의 접속은 각각의 네트워크 엔티티(즉, 각각의 게임 콘솔 또는 각각의 컴퓨터)로 이루어지는 것이 바람직하고, 해당 엔티티 상의 모든 플레이어는 동일한 피어-투-피어 접속을 사용할 것이다. 도 8은 게임 콘솔(102)이 세션 내의 11명의 플레이어 간의 통신을 어떻게 지원하는지를 설명하는 추가의 세부 사항을 제공한다. 도 8을 참조할 때, 도시된 게임 콘솔(832)(즉, 게임 콘솔 2)이 2명의 플레이어를 지원하고 있고, 게임 콘솔(836)(즉, 게임 콘솔 3)이 1명의 플레이어를 지원하고 있지만, 도 8의 각각의 게임 콘솔은 4명까지의 플레이어를 지원할 수 있음에 유의해야 한다. 따라서, 도 8에 도시된 세션에서는 11명의 플레이어만이 통신하고 있지만, 이러한 구성에서는 16명의 플레이어[게임 콘솔(832)에 2명의 플레이어를 추가하고 게임 콘솔(836)에 3명의 플레이어를 추가]까지의 통신이 지원될 수 있다.

도시된 예에서는, 게임 콘솔(102)을 사용하는 플레이어들은 메시지를 타이핑할 키보드를 갖지 않기 때문에, 음성 채팅을 포함하는 기능은 중요하다. 게임 콘솔(102)에서 사용될 게임 타이틀을 개발하는 게임 설계자들이 음성 채팅을 지원하는 것과 관련한 많은 다른 기능을 제공할 수 있지만, 게임 콘솔(102)을 사용하는 음성 채팅은 다음과 같은 기능들을 포함하는 것이 바람직하다.

· 플레이어는 자신의 음성을 다른 플레이어들에게 전혀 들리지 않도록 뮤트시키는 기능을 가져야 한다.

· 플레이어는 게임 동안 다른 플레이어들이 자신에게 말하는 것을 뮤트시킬 수 있어야 한다.

· 플레이어는 다른 플레이어가 미래의 임의의 게임에서 자신에게 말하는 것을 뮤트시키는 기능을 가져야 한다. 이에 의하여, 한 플레이어를 영구적으로 뮤트시키면, 그 사람과는 절대로 다시 대화하지 않게 된다.

· 사람의 음성은, 성별 및 연령과 같은 특성을 식별하는 것을 비롯하여, 통상적으로 텍스트 채팅에 의해서는 드러나지 않는 개인의 상세한 정보를 드러낸다. 따라서, 플레이어는 자신의 음성을 마스크할 수 있어야 한다. 사용자가 음성 마스크가 적용된 자신의 음성을 들을 수 있게 하는 기능이 추천된다. 음성 마스크는 디폴트로 턴온되고, 사용자에 의하여 언제라도 온/오프될 수 있는 것이 바람직하다.

· 게임 콘솔(102) 상에서 플레이되는 게임에서, 플레이어가 판타지에 기초를 둔 롤 플레잉 게임에서의 드래곤 또는 엘프와 같은 자신의 온스크린 캐릭터에 일치하도록, 자신의 음성을 변경하는 것이 선택적으로

허용될 수 있다.

도 8은 게임 콘솔(810)이 음성 채팅을 어떻게 지원하는지를 나타내는 세부도이다. 음성 채팅의 품질을 유지하기 위하여, 음성 채팅 세션은 게임 타이틀에 의하여 일정한 비율로 업데이트되어야 한다. 게임이 규칙적인 비디오 프레임 레이트를 유지해야만 하는 것과 마찬가지로, 규칙적인 프레임 레이트도 유지되어야만 한다. 그렇지 않은 경우, 음성 품질이 저하될 것이고, 그에 따라 사용자의 경험도 저하될 것이다. 게임 콘솔(810)은 통상적으로 만날 수 있는 다양한 시나리오에서 양호하게 음성 채팅을 수행하도록 최적화된다. 주된 제한 요인은 음성 프레임 당 행해질 수 있는 인코드 및 디코드의 수이다. 게임 콘솔(810)은 게임 콘솔(102)과 대체적으로 동일하다는 것을 알아야 한다. 전술한 바와 같이, 게임 콘솔(102)은 오디오 프로세스 유닛(224) 및 오디오 CODEC(226)을 포함한다. 게임 콘솔(810)에서는, 구현되는 오디오 프로세스를 보다 더 명확하게 설명하기 위하여, 오디오 프로세스 유닛(224)과 오디오 CODEC(226)은 추가의 기능 블럭으로 분리되어 있다. 예를 들어, 게임 콘솔(102)과 관련하여 기술된 오디오 CODEC(226)은 인코더와 디코더 양자 모두를 포함하지만, 음성 채팅 동안 발생하는 오디오 신호 프로세스를 보다 더 명확하게 설명하기 위하여, 게임 콘솔(810) 내에서는 인코더와 디코더가 별개의 기능 블럭으로 도시된다. [게임 콘솔(102)와 관련하여 설명된] 오디오 프로세스 유닛(224)은 복수의 네트워크 큐(816a, 816b, 816c)를 포함하며, 임의의 네트워크 레이턴시는 엔티티들 사이에 존재하므로, 상이한 네트워크 엔티티와의 각각의 접속마다 하나의 큐를 갖는 것이 바람직하다. 필요한 구성요소이지만, 게임 콘솔(102)에 관련해서는 특별히 논의되지 않은 입력 라우터(826) 및 출력 라우터(820)가 도 8에 도시되어 있다. 게임 콘솔(810)은 16명까지의 화자(talker)(즉, 네트워크를 통해 4개까지의 게임 콘솔이 링크되고, 게임 콘솔마다 4명까지의 통화자를 가짐)를 동시에 신뢰할 수 있게 지원하도록 설계되어 있다. 게임 콘솔(810)은 평활한 게임 프레임 레이트를 지원하기 위하여 음성 프레임당 소정량의 데이터를 인코딩 및 디코딩할 수 있는 것이 바람직하다.

게임 콘솔(810)은 각각의 플레이어(828a-828d)의 헤드셋 상의 마이크로폰으로부터 각각의 플레이어에 대한 가정 음성 스트림을 수신하도록 구성된 입력부(824a-824d)를 포함한다. 입력부(824a-824d)는 어떤 플레이어가 말할 수 있는지를 결정하여 그러한 말할 수 있는 플레이어에 대응하는 음성 스트림만을 포워드하도록 구성된 입력 라우터(826)에 연결된다. 포워드된 음성 스트림은 입력 라우터(826)에 논리적으로 연결된 인코더(814)에 의해 수신된다. 인코더(814)는 가청 스피치를 네트워크(83)를 통해 수신측 게임 콘솔(832, 836 또는 840)에 요구되는 대로 송신할 수 있는 음성 데이터로 압축한다. 또한, 인코더(814)는, 네트워크(830)를 통해 게임 및 음성 트래픽을 송신하는 것을 담당하는 네트워크 계층(812)에 논리적으로 연결된다.

게임 콘솔(810)은 네트워크(830)를 통해 게임 콘솔(810)에 링크된 각각의 다른 게임 콘솔에 대한 네트워크 큐를 포함한다. 바람직하게는, 게임 콘솔(810)은 3개까지의 다른 게임 콘솔[즉, 콘솔(832, 836 및 840)]과 통신할 수 있다. 따라서, 게임 콘솔(810)은 3개의 네트워크 큐(816a, 816b 및 816c)를 확립하기 위한 충분한 메모리 및 처리 자원을 할당할 수 있다. 데이터를 송신하는 각각의 네트워크 엔티티에 대하여, 수신 엔티티에 대한 단일의 큐가 존재하는 것이 바람직하다. 게임 콘솔(836)은 단 한명의 플레이어(838)만을 지원하며, 네트워크 큐(816b)는 플레이어(838)로부터의 데이터만을 큐잉할 것이다. 네트워크 큐(816c)는 4명의 플레이어(842a-842d)를 지원하는 게임 콘솔(840)로부터의 데이터를 수신하기 때문에, 보다 많은 자원을 필요로 한다. 네트워크 큐는 인터넷 또는 기타 상호접속 네트워크를 통해 송신되는 패킷의 도달 시간 차이에 의해 유발되는 "지터" 효과를 제거한다. 네트워크 큐는 음성 데이터를 그대로 저장하고 음성 데이터의 플레이백을 평활화하기 때문에, 청취자는 네트워크를 통해 전파되는 음성 패킷의 임의의 지연에 의하여 유발되는 "팝(pops)"을 듣지 않는다.

각각의 네트워크 큐는 디코더(818)에 논리적으로 연결된다. 인코더(814)를 제어하는 알고리즘과 디코더(818)를 제어하는 알고리즘은 상보적이다. 디코더(818)는 디코딩된 가청 스트림을 수신하여 그것을 플레이어마다의 정확한 출력 오브젝트에 송신하는 출력 라우터(820)에 논리적으로 연결된다. 따라서, 출력 라우터(820)는 플레이어(828a-828d) 중 적절한 사람들에게 오디오 스트림을 제공하는 출력부(822a-822d)에 논리적으로 연결된다. 각각의 출력부는 모든 적합한 스트림을 혼합하여 그들을 적합한 플레이어의 헤드셋에 송신하는 것을 담당한다.

게임 콘솔(810)과의 음성 채팅을 지원하기 위해 요구되는 것을 분석할 때에, 게임 기반의 음성 채팅을 3개의 주요 시나리오로 분할하는 것이 도움이 된다. 포인트-투-포인트 시나리오에서는, 게임 콘솔당 한 사람씩 채팅하고, 2개의 게임 콘솔이 존재한다. 멀티포인트 시나리오에서는, 게임 콘솔당 한 사람씩 채팅하고, 16개까지의 게임 콘솔이 존재한다. 최종적으로, 멀티플레이어-온-멀티게임 콘솔 시나리오에서는, 게임 콘솔당 4명까지의 화자가 있고, 4개까지의 게임 콘솔이 존재한다. 대부분의 게임은 이러한 시나리오 중 하나에 해당할 것이다.

포인트-투-포인트는, 하나의 게임 콘솔 상의 단일 플레이어가 다른 게임 콘솔 상의 다른 단일 플레이어와 대화하는 것에 해당한다. 일반적인 예는, 단 2명의 플레이어만이 존재하며 플레이어들이 게임 진행 동안 통신하기를 원하는 체스 등의 게임이다. 이러한 경우에서, 각각의 게임 콘솔은 하나의 인코더와 하나의 디코더를 인스턴스화한다. 음성 프레임 업데이트 동안, 각각의 게임 콘솔은 임의의 인코딩과 임의의 디코딩을 필요에 따라 업데이트한다. 이러한 경우에서, 뮤트는, 뮤트된 플레이어의 음성 스트림을 디코딩하지 않는 것에 의해 간단하게 행해진다.

멀티포인트 시나리오에서는, 각각의 게임 콘솔 상에 한명의 플레이어가 존재하지만, 세션 내에 복수의 게임 콘솔이 존재한다. 예를 들면, 콘솔당 단일 플레이어만을 허용하는 4 플레이어용 브리지 게임이 있다. 게임은, 모든 플레이어가 모두에게 말하는지 또는 팀이 존재하는지를 결정할 수 있고, 플레이어의 서브세트가 서로 말할 수 있는지를 결정할 수 있다. 이러한 경우에서, 각각의 게임 콘솔은 하나의 인코더와 하나의 4-인-1(4 in 1) 디코더를 인스턴스화한다. 음성 프레임 업데이트 동안, 각각의 게임 콘솔은 (게임 콘솔 상의 단일 사용자에 대한) 임의의 인코딩과 (다른 게임 콘솔들로부터의 3명까지의 사용자에 대한) 임의의 디코딩을 업데이트한다. 4 in 1 디코더는, 복수의 입력 스트림을 취하고, 그들을 주파수 영역에서 조합하고, 그 조합에 단일 동작을 수행하여 하나의 단일 출력 스트림으로 변환하는 멀티스트림 병렬 디코더로서 구현된다. 이러한 최적화에 의하여, 각각의 단일 스트림에 대한 개별 동작들은, 스트림들을 결합한 후에 모든 스트림에 적용되는 단일 동작으로 보다 더 효율적으로 조합될 수 있다.

멀티플레이어-온-멀티게임 콘솔 시나리오에 대하여, 각각의 게임 콘솔은 복수의 플레이어와 복수의 게임 콘솔이 접속되는 것을 허용한다. 예를 들어, 각 콘솔 상의 4명까지의 플레이어와 4개까지의 콘솔을 허용하는 16 플레이어용 게임이 있다.

게임 설계자는 모든 플레이어가 서로 대화할 수 있는지, 또는 팀이 존재하여 플레이어들의 서브세트만이 서로 말할 수 있는지를 결정할 수 있다. 16명의 플레이어에 있어서, 대화가 알기 어려워지지 않도록, 동시에 말할 수 있는 사람의 수(예를 들어, 단 4명)를 제한하는 것이 바람직하다.

각 게임 콘솔 내에서 음성 프레임당 플레이어당 하나의 인코더 및 4개의 4-인-1 디코더를 인스턴스화하고 처리하는 것은, 각각의 게임 콘솔 내의 프로세서를 압도할 가능성이 있다. 그러나, 이러한 상황을 관리하기 위하여, 다음과 같은 가정이 이루어진다.

· 4명 이상의 말을 한꺼번에 듣는 것은 다루기 어렵고 바람직하지 않은 것으로 가정한다. 이러한 가정은 한꺼번에 디코딩되는 음성의 수를 제한하는 데에 사용된다. 바람직한 알고리즘은 게임 콘솔 상의 청취자당 4개의 "가장 큰" 음성을 선택한다. 따라서, 최악의 시나리오는 게임 콘솔 당 2명의 청취자가 있고, 각각 4명(가능하면 그 청취자에 고유함)의 상이한 화자를 한꺼번에 듣는 것이다.

· 인코딩시에, 실제로 음성을 인코딩할 시간이 존재하지 않는 경우, 음성 프레임이 복제될 수 있는 것으로 가정한다. 이러한 가정에 기초하면, 2개의 인코더와 "라운드-로빈" 시스템(나중에 설명됨)을 사용하여, 모든 4개의 음성이 각각의 음성 프레임 내에서 처리될 수 있다.

· 음성 채널은 양방향 라디오 상의 채널과 같이 간단하게 사용된다. 즉, (개별적인 뮤트가 고려되기 전에는) 채널 상의 모든 화자가 서로 말하는 것을 들을 수 있다. 채팅할 플레이어가 세션에 들어오면, 그 플레이어는 그들이 이용하고 있는 채널을 명시적으로 설정해야만 한다. 일반적으로, 채널은 "팀" 내의 모든 회원이 서로 말할 수 있게 하는 데에 사용된다 (디폴트로서, 게임 내의 모든 플레이어에 대하여 하나의 채널이 사용될 수 있다). 채널은 음성을 위한 네트워크 트래픽을 최적화하는 데에 사용될 수 있다.

· 추가의 프로세서 전력을 사용할 것을 선택하는 타이틀은 추가의 디코더를 사용가능하게 하는 옵션을 가질 것이며, 이는 하나의 음성 프레임동안 추가의 음성을 동시에 들을 수 있게 할 것이다.

따라서, 멀티플레이어-온-멀티게임 콘솔 시나리오에서, 각각의 게임 콘솔은 하나의 4-대-4 디코더를 인스턴스화한다. 음성 프레임 업데이트 동안, 각각의 게임 콘솔은 (게임 콘솔 상의 4명까지의 사용자에 대한) 임의의 인코딩 및 (다른 게임 콘솔 상의 4명까지의 사용자에 대한) 임의의 디코딩을 업데이트한다. 이러한 음성 프레임 동안 4개 이상의 상이한 음성 스트림이 이용가능한 경우, 4개의 가장 큰 음성 스트림이 디코딩용으로 선택된다. 게임 설계자가 보다 더 많은 프로세스 전력이 채팅이 사용되는 것을 허용한 경우, 프레임당 디코딩되는 다중 음성 스트림의 수를 증가시키기 위하여, 추가의 디코더가 인스턴스화될 수 있다.

단 2개의 인코더만을 이용하는 인코딩은 다음과 같이 행해진다 (즉, 4개의 인코더 인스턴스가 있지만, 한 음성 간격에서 2개만이 작동함). 플레이어 1, 2, 3, 4 모두가 동시에 말하고, 최근에 인코딩되었던 2개의 음성에 관한 이력이 유지되는 것으로 가정한다. 현재의 마이크로폰 패킷은 플레이어 1의 음성에 대하여 분석되고, 플레이어 1의 음성이 존재하는 경우에는 그것이 인코딩된다. 다음으로, 현재의 마이크로폰 패킷은 플레이어 2의 음성에 대하여 다음에 분석되며, 플레이어 2의 음성이 존재하는 경우에는 그것이 인코딩된다. 프로세스가 중단되고, 이력은 {3, 4, 1, 2}로 업데이트된다. 후속 마이크로폰 간격(통상적으로 40 마이크로초) 동안, 마이크로폰 패킷은 플레이어 3 및 4(즉, 선행 마이크로폰 패킷 동안 처리되지 않았던 2명의 플레이어)에 대하여 분석된다. 마이크로폰 패킷이 분석되고, 플레이어 3의 음성이 발견되지 않은 경우, 인코딩은 수행되지 않는다. 플레이어 4의 음성이 발견되는 경우, 인코딩이 수행되며, 이력은 {3, 1, 2, 4}로 업데이트된다. 동일한 마이크로폰 패킷 동안, 플레이어 1의 음성이 존재하는 경우에 그것이 인코딩되고, 이력은 {3, 2, 4, 1}로 된다. 마이크로폰 패킷 간격 동안, 분석은 플레이어 3 및 2로부터의 음성을 찾는다. 플레이어 3이 여전히 음성을 갖지 않는 경우, 인코딩은 플레이어 2 및 플레이어 4에 대하여 행해지며, 이력은 {3, 1, 2, 4}로 업데이트된다.

라운드 로빈 인코딩 방식은 한번에 2 프레임의 스피치에 대해서만 행해지고, 현재 인코딩되고 있지 않은 스트림의 다른 프레임들에 대해 반복한다. 최종 결과는 4명의 플레이어 모두가 말할 때의 음향 저하이지만, 그 때 추가의 프로세스 전력은 사용되지 않는다.

제1 실시예를 위한 예시적인 방법

도 9는 본 발명의 본 실시예의 바람직한 구현에 따라, 게임 플레이 동안 플레이어들 간의 피어-투-피어 통신을 용이하게 하기 위하여, 게임 서버에 의해 사용되는 논리를 나타낸 흐름도(910)이다. 논리는 블럭(912)에서 시작하고, 블럭(914)에서는, 이용되는 게임 콘솔[예를 들어, 게임 콘솔(102)]을 위해 개발된 표준에 따라, 특정 게임을 위한 통신 컨트롤이 설정된다. 블럭(916)에 나타난 바와 같이, 표준에 기초하여, 특정 게임에 의해 지원될 통신의 타입(예를 들어, 텍스트 전용, 텍스트 및 음성, 메뉴에 의해 선택할 수 있는 녹음된 음성 응답, 또는 실시간 음성)이 지원된다. 블럭(914) 및 블럭(916)을 둘러싸고 있는 점선(913)에 의해 나타나는 바와 같이, 블럭(914 및 916)과 관련된 단계들은 게임 설계자에 의하여 구현된다.

그리고나서, 블럭(918)에 나타나 있는 바와 같이, 게임 서버는 이와 같이 설정된 게임 파라미터에 기초하여 게임 세션을 호스트할 수 있다. 블럭(920)에서, 게임 서버에 의해 호스트되는 게임 세션에 액세스하는 각각의 플레이어는, 게임 서버에 의하여 인증 및 허가된다. 블럭(922)에 나타난 바와 같이, 게임 서버는 자신에 액세스하는 각각의 게임 콘솔을 식별하는 것은 물론, 특정 게임 콘솔에 의해 서비스되는 각각의 개별 플레이어도 식별해야 한다. 바람직하게, 게임 서버는 각각의 개별 플레이어에게 로그온 시에 사용자 키를 제공하며, 그 사용자 키는 게임 서버에 의해 신뢰되는 플레이어들 간의 피어-투-피어 통신의 확립을 용이하게 하는 데에 사용된다.

블럭(924)에서, 서버는 플레이어들이 다른 플레이어와 원하는 대로 피어-투-피어 통신을 확립할 수 있게 한다. 블럭(924)와 관련된 특정 세부사항들은 이하에 설명되는 도 10에 제공된다. 블럭(926)에 나타난

바와 같이, 플레이어들 간의 피어-투-피어 통신을 허용하는 게임 플레이는 원하는 기간 동안 계속된다. 플레이어가 게임 환경에서 나가면, 논리는 종료 블럭(928)에서 종료된다.

도 10의 흐름도(1010)에서, 게임 서버는 블럭(1012)에 나타난 바와 같이 각각의 플레이어에게 다른 플레이어들의 리스트를 제공함으로써, 플레이어들 간의 피어-투-피어 통신의 확립을 용이하게 한다. 전형적으로, 게임 환경 내에서 플레이어들 간의 통신이 바람직하고 실현가능하도록 하기 위하여, 이러한 리스트는 동일 팀에 속하는 플레이어들, 또는 게임 세계 내에서 서로 충분히 인접한 플레이어들로 한정될 것이다. 블럭(1014)에서, 서버는 CONSOLE1-P1으로 식별되는 플레이어(즉, 제1 게임 콘솔을 사용하여 게임 서버에 액세스하는 제1 플레이어)가 음성 통신을 위하여 CONSOLE2-P4로 식별되는 플레이어(즉, 제2 게임 콘솔을 사용하여 게임 서버에 액세스하는 제4 플레이어)를 선택할 수 있게 한다. 이러한 선택은, 다른 플레이어들에 관한 스크롤가능한 리스트를 디스플레이하여, CONSOLE1-P1이 리스트를 스크롤하여 CONSOLE2-P4를 선택할 수 있게 함으로써 용이하게 행해질 수 있다.

그 다음, 서버는 블럭(1016)에 나타난 바와 같이 CONSOLE1-P1에 CONSOLE2-P4에 관한 정보를 제공한다. 정보는 CONSOLE2의 외부 IP 어드레스, CONSOLE2의 내부 IP 어드레스(내부 어드레스를 갖는 경우에만), 및 CONSOLE2의 제4 플레이어가 접속한 포트 번호를 포함한다. 바람직하게는, 서버는 CONSOLE2-P4가 게임 서버에 로그온할 때 CONSOLE2-P4에 할당되었던 사용자 키를 CONSOLE1-P1에 송신하여, CONSOLE2-P4가 CONSOLE1-P1으로부터 피어-투-피어 통신을 확립하기 위한 요청을 수신한 때에, CONSOLE2-P4가 CONSOLE1-P1이 서버에 의해 신뢰되는 것으로 인식할 수 있게 한다. CONSOLE1-P1이 신뢰되지 않았다면, 게임 서버는 CONSOLE1-P1이 CONSOLE2-P4의 사용자 키에 액세스하는 것을 허용하지 않았을 것이다. 블럭(1018)에서, CONSOLE1-P1은 CONSOLE2-P4와의 피어-투-피어 통신 링크를 확립하려고 시도한다. 이 단계는 게임 콘솔 CONSOLE1에 의해 자동적으로 수행된다.

판정 블럭(1020)은 시도가 성공적이었는지를 판정한다. CONSOLE1-P1과 CONSOLE2-P4 간의 피어-투-피어 통신이 확립된 경우에는, 블럭(1024)에 나타난 바와 같이, 플레이어 중 한명에 의해 (또는 네트워크 실패에 의해) 해제될 때까지 접속이 유지된다. 시도가 성공적이지 않았던 경우에는, 블럭(1022)에 나타난 바와 같이, 게임 서버는 제1 플레이어(즉, CONSOLE1-P1)의 접속 정보를 제2 플레이어(즉, CONSOLE2-P4)에 전송한다. 도 6과 관련하여 설명한 바와 같이, 피어-투-피어 통신 링크를 확립하기 위한 제2의 시도가 성공적이지 않은 경우, 논리는 블럭(1016)으로 진행하여 게임 서버가 제2 플레이어의 접속 정보를 제1 플레이어에게 다시 송신하게 하거나, 또는 게임 서버가 플레이어들 간의 모든 통신을 자신을 통해 라우팅할 수 있게 하거나, 또는 게임 서버가 피어-투-피어 관계 접속의 실패를 표시할 수 있게 한다.

제2 실시예에 관한 세부사항

도 11은, 클라이언트들 간의 피어-투-피어 통신의 확립을 용이하게 하는 것을 주요 기능으로 하는 서버(1114a-1114s)를 포함하는 예시적인 네트워크(1110)를 나타내고 있다. 본 발명의 본 실시예의 바람직한 구현에서, 서버는 호스트 서버에 대한 액세스 권한이 다를 수 있는 상이한 클라이언트 등급을 인식하도록 구성된다.

도 11에 도시된 실시예는, 보안 방식으로 강제될 수 있는 상이한 액세스 정책을 상이한 엔티티 "등급"(익명 사용자, 인증된 사용자, 사업, 대학 등)에 제공함으로써, 피어-투-피어 통신을 확립하고자 하는 클라이언트들의 공용 인터넷 디렉토리의 관리를 용이하게 한다. 예를 들어, 서버는 익명 사용자(1116)가 서버에 접속할 때, 익명 사용자(1116)가 서버에 의해 호스트되고 있는 세션 1에 액세스하는 것만을 허용하도록 구성된다. 세션 1은 다수의 상이한 방식으로 구성될 수 있다. 세션 1에 액세스하는 각각의 클라이언트는, 자신의 사이트로 트래픽을 유도하기를 원하는 웹사이트 운영 홍보자를 나타낼 수 있다. 따라서, 익명 사용자(1116)는 피어-투-피어 통신을 원하는 개인들에 관한 접속 정보를 얻을 수 있는 것과는 달리, 이러한 웹사이트에 액세스하기 위해서만 네트워크(1110)를 사용할 수 있다. 대안적으로, 세션 1은 거의 또는 전혀 제한없이 피어-투-피어 통신을 확립하는 것에 대한 선호를 표명한 클라이언트들을 포함할 수 있다.

네트워크(1110) 내의 서버는 제한적으로 인증된 사용자를 인식하여, 제한적으로 인증된 사용자(1118)가 서버에 액세스할 때 세션 1 및 세션 2에 대한 액세스가 제공되게 할 수 있도록 구성된다. 따라서, 제한적으로 인증된 사용자(1118)는 익명 사용자(1116)가 액세스할 수 없는 클라이언트들(즉, 세션 2에 액세스하는 클라이언트들)에 액세스할 수 있다. 또한, 서버는 또 다른 액세스 권한을 허가받은 인증된 사용자를 인식하도록 구성된다. 인증된 사용자(1120)는 세션 1, 세션 2 또는 세션 3에 대한 액세스를 허가받을 수 있으며, 세션 3은 또 다른 옵션을 제공한다. 또한, 네트워크(1110)는, 다른 클라이언트에 대한 자신의 접속을 광고하는 것을 서버에 의해 허가받은 리스트 엔티티(list entity)(1122a 및 1122b)를 더 포함한다.

바람직하게, 통신 네트워크에 접속하기를 원하는 각각의 클라이언트는 인증 및 허가되어야 한다. 인증 및 허가(A&A)는, 마이크로소프트사의 Passport, 신뢰 계층을 이용한 증명을 채용하는 공용 키 암호화, 또는 TA(Trusted Authoruty)를 사용하여 "티켓"을 허여하는 Kerberos[RFC(1510)] 등의 보안 프로토콜에서와 같이, 웹 사이트 사인-인(sign-in)에 기초할 수 있다. 이러한 메커니즘들 중 임의의 것, 또는 이러한 메커니즘들의 조합이 본 발명의 본 양태와 관련하여 사용될 수 있다.

인증은 서버에 대한 액세스를 시도하는 클라이언트의 신분을 확인하는 프로세스이다. 인증은 사용자명/패스워드 조합과 같은 보안 증명서, 또는 클라이언트에 연관된 스마트 카드 및/또는 패스워드의 소유를 제공함으로써 달성될 수 있다. 또한, 인증은 클라이언트를 "보증(vouch)"할 수 있는 소정의 엔티티에도 의존할 수 있다. 예를 들어, 새로운 클라이언트가 다른 클라이언트들에 대한 액세스를 획득하기 위하여 서버에 등록할 때, 인증은 신용카드, 루트 인증기관(root certificate authority), 또는 기타 제3의 신뢰되는 인증기관을 사용하여 달성될 수 있다.

인증은 클라이언트에게 서비스(또는 서비스의 서브세트) 사용에 대한 허가를 제공한다. 도 11에서, 익명 사용자(1116), 제한적으로 인증된 사용자(1118) 및 인증된 사용자(1120)는 각각 상이한 허가를 할당받은 상태이다. 클라이언트가 인증되고 나면, 그 클라이언트의 인증 데이터는 서비스 및 서비스의 상이한 서브세트(들)(즉, 세션 1, 세션 2 및/또는 세션 3)로의 액세스에 대한 허가를 포함한다. 인증은 액세스를 허용하며, 정책을 강요한다. 디렉토리의 정책은 서비스의 설계자에 의해 결정될 수 있으며, 폭넓게 달라질 수 있다. 예를 들어, 네트워크(1110)에서, 바람직하게, 익명 사용자는 인증을 필요로 하지 않으며, 세션

1은 서비스의 매우 제한적인 서브세트일 뿐이다. 일반적으로, 익명 사용자는 (옐로우 페이지에 액세스하는 것과 같이) 익명 접속을 허락하는 제한된 공개용 리스트 엔티티(즉, 광고자, 회사 및/또는 대학)를 브라우징하는 것을 허가받을 것이다. 익명 접속의 접속 타입은 리스트 엔티티에 의해 결정되며, 온라인 컨텐트를 듣고 보고 읽는 것과 같은 단방향 통신으로만 제한될 수 있다.

도 11의 사용자(1118)와 같이 제한적으로 인증된 사용자는 보안 증명서를 제시함으로써 자신의 신분을 증명한 사용자이다. 제한적으로 인증된 사용자는 제한된 공개용 리스트 엔티티를 보고 그에 접속할 수 있으며, 그러한 엔티티와 양방향으로 통신하는 것도 허용된다. 또한, 이들은 부적절한 컨텐트를 리스트화한 엔티티의 위반을 보고하는 것도 할 수 있다.

인증된 사용자[즉, 도 11의 사용자(1120)]는 보안 증명서를 제시함으로써 자신의 신분을 증명하고, 또한 기업 인증기관과 사업 관계를 가지며, 따라서 제한적으로 인증된 사용자보다 더 많은 액세스를 허가하는 인증의 수퍼세트를 허여받은 사용자이다. 인증된 사용자는 제한적으로 인증된 사용자의 허가를 전부 갖지만, 보다 안전한 통신을 원하는 클라이언트들을 포함하는 것과 같은 추가 세션에 대해서도 액세스할 수 있다 (예를 들어, 회사의 인트라넷 디렉토리에 대한 액세스).

바람직하게, 리스트 엔티티는 자신의 접속을 익명 사용자, 제한적으로 인증된 사용자 및 인증된 사용자 중 누구에게라도 광고할 수 있는 엔티티이다. 리스트 엔티티는 개인, 기업, 교회, 대학 및 기타 기관일 수 있다. 리스트 엔티티는 사용자 세트에 기초하여 자신의 액세스를 설정할 수 있다. 예를 들어, 고객 지원을 제공하는 리스트 엔티티는 익명 사용자가 컴퓨터로부터의 자동화된 도움을 얻을 수 있게 하고, 제한적으로 인증된 사용자에 대해 제한된 고객 지원을 허용하며, 그들과 지원 계약을 맺은 인증된 사용자에 대해 프리미어 지원을 허용한다.

본 발명이 바람직한 실시 형태 및 그에 대한 수정과 관련하여 설명되었지만, 본 기술 분야의 숙련된 기술자라면, 이하의 특허청구범위 내에서 많은 다른 수정이 본 발명에 행해질 수 있음을 알 것이다. 예를 들어, 네트워크화된 게임 서비스에 독립적인 게임 시스템의 로컬 네트워크 내에서, 화자는 시각적으로 식별될 수 있다. 또한, 논리 흐름 내에서 구현되고 상기에 설명된 결정 단계들은 다른 구성으로 배열될 수 있다. 따라서, 상기의 설명은 본 발명의 범위를 어떤 방식으로든 제한하기 위한 것이 아니며, 본 발명의 범위는 이하의 특허청구범위를 참조하여 전체적으로 결정되어야 한다.

발명의 효과

본 발명에 따르면, 개별 사용자들 간의 피어-투-피어 통신의 확립을 용이하게 하는 신뢰할 수 있는 환경을 형성하는 방법 및 시스템이 제공된다.

청구의 범위

청구항 1

서버를 사용하여, 클라이언트들이 서로 피어-투-피어 통신을 확립할 수 있게 되는 신뢰되는 세션 환경을 확립하는 방법에 있어서,

(a) 상기 서버를 사용하여, 상기 클라이언트들이 피어-투-피어 통신을 확립하기 전에 처음에 액세스하는 세션을 호스트하는 단계,

(b) 상기 서버에 의해 호스트되는 세션에 액세스하려고 시도하는 각각의 클라이언트의 자격을 검사하여, 상기 서버에 의해 승인받은 자격을 갖는 클라이언트들만이 상기 세션에 대한 액세스를 허가받도록 하는 단계,

(c) 상기 세션에 대한 액세스를 허가받은 제1 클라이언트에게, 현재 상기 세션에 대한 액세스를 허가받은 하나 이상의 다른 클라이언트를 식별하는 리스트를 제공하는 단계,

(d) 상기 제1 클라이언트가 상기 리스트로부터 제2 클라이언트를 선택할 수 있게 하는 단계 - 상기 제1 클라이언트에 의해 선택된 제2 클라이언트는 상기 서버에 알려짐 -, 및

(e) 상기 제2 클라이언트에 관한 정보를 상기 서버로부터 상기 제1 클라이언트로 전송하는 단계 - 상기 정보는 상기 제1 클라이언트와 상기 제2 클라이언트 간에서 피어-투-피어 통신이 확립될 수 있게 하는 상기 제2 클라이언트에 대한 어드레스를 포함함 -

를 포함하는 방법.

청구항 2

제1항에 있어서,

(a) 상기 세션에 액세스하려고 시도하는 각 클라이언트의 자격을 검사하는 단계는,

각각의 클라이언트를 인증하는 단계, 및

각각의 인증된 클라이언트가 상기 세션의 특정 부분에 액세스하는 것을 허가하는 단계

를 포함하고,

(b) 상기 제1 클라이언트에게 제공된 리스트는, 상기 제1 클라이언트와 동일한 세션 부분에 액세스하는 것을 허가받은 클라이언트만을 식별하는 방법.

청구항 3

제2항에 있어서,

Ex.1002 / Page 441 of 1173
Cisco Systems, Inc.

한 클라이언트의 상기 서버의 다른 클라이언트들과의 피어-투-피어 통신에서의 상기 클라이언트의 행동에 관하여 상기 서버에 의해 수신된 피드백에 응답하여, 상기 한 클라이언트의 상기 세션의 특정 부분에 대한 액세스 허가를 변경하는 단계를 더 포함하는 방법.

청구항 4

제1항에 있어서,

상기 서버는, 클라이언트들이 피어-투-피어 통신을 확립할 수 있게 되는 신뢰되는 세션 환경을 확립하는 것 이외의 기능을 클라이언트에게 제공하는 방법.

청구항 5

제4항에 있어서,

상기 서버는 게임 서버를 포함하고, 각각의 클라이언트는 네트워크화된 게임 플레이용 컴퓨팅 디바이스를 사용하여 상기 서버에 액세스하는 방법.

청구항 6

제5항에 있어서,

상기 제1 클라이언트에게 제공된 하나 이상의 클라이언트의 리스트는, 상기 게임 서버에 의해 제어되는 게임 환경에서 인터랙션하는 클라이언트들만을 포함하는 방법.

청구항 7

제5항에 있어서,

하나의 게임 플레이용 컴퓨팅 디바이스가 복수의 상이한 클라이언트를 지원할 수 있는 방법.

청구항 8

제1항에 있어서,

상기 제2 클라이언트에 관한 정보를 상기 서버로부터 상기 제1 클라이언트로 전송하는 단계는, 상기 제2 클라이언트의 외부 IP 어드레스, 상기 제2 클라이언트와 연관된 임의의 내부 IP 어드레스, 및 상기 제2 클라이언트와 피어-투-피어 통신을 하는 데에 요구되는 임의의 포트 어드레스를 전송하는 단계를 포함하는 방법.

청구항 9

제8항에 있어서,

상기 각각의 클라이언트의 자격을 검사하는 단계는, 각각의 클라이언트에게 고유한 사용자 키를 할당하는 단계를 포함하고,

상기 서버로부터 상기 제1 클라이언트에게 전송된 상기 제2 클라이언트에 관한 정보는 제2 클라이언트의 사용자 키를 포함하여, 상기 제1 클라이언트와의 피어-투-피어 통신을 열게 하는 요청이 신뢰되는 소스로부터 온 것임을 상기 제2 클라이언트에게 확신시키는 방법.

청구항 10

제1항에 있어서,

상기 제2 클라이언트에 관한 정보를 수신한 후에, 상기 제1 클라이언트가 상기 제2 클라이언트와의 피어-투-피어 통신을 확립할 수 없는 경우,

(a) 상기 피어-투-피어 통신을 확립하기 위한 상기 제1 클라이언트의 시도가 실패했음을 상기 서버에 통지하는 단계,

(b) 상기 제1 클라이언트에 관한 정보를 상기 서버로부터 상기 제2 클라이언트로 전송하는 단계 - 상기 정보는, 상기 제1 클라이언트와 상기 제2 클라이언트 간에서 피어-투-피어 통신이 확립될 수 있게 하는 상기 제1 클라이언트에 대한 어드레스를 포함함 -, 및

(c) 상기 제2 클라이언트에게 상기 제1 클라이언트와의 피어-투-피어 통신을 확립할 것을 요청하는 단계

를 더 포함하는 방법.

청구항 11

제10항에 있어서,

상기 제1 클라이언트에 관한 정보를 수신한 후, 상기 제2 클라이언트가 상기 제1 클라이언트와의 피어-투-피어 통신을 확립할 수 없는 경우, 상기 제1 클라이언트와 상기 제2 클라이언트 간의 모든 통신을 상기 서버를 통해 라우팅하는 단계를 더 포함하는 방법.

청구항 12

제1항에 따른 단계들을 실행하기 위한 기계 명령들이 저장되어 있는 메모리 매체.

청구항 13

Ex.1002 / Page 442 of 1173
Cisco Systems, Inc.

사용자들이 서로 피어-투-피어 통신을 확립할 수 있는 신뢰되는 세션 환경을제공하는 시스템에 있어서,

(a) 프로세서, 및

(b) 상기 프로세서와 통신하며, 상기 프로세서가 복수의 기능을 수행하게 하는 기계 명령들을 저장하는 메모리

를 포함하고,

상기 복수의 기능은,

(ⅰ) 사용자의 자격을 검사함으로써, 상기 시스템에 의해 호스트되는 세션에 액세스하려고 시도하는 각각의 사용자를 스크리닝(screening)하여, 스크리닝된 사용자들만이 상기 세션에 대한 액세스를 허가받게 하는 기능,

(ⅱ) 제1 스크리닝된 사용자에게, 현재 상기 세션에 대한 액세스를 허가받은 적어도 한명의 다른 스크리닝된 사용자를 포함하는 리스트를 제공하는 기능, 및

(ⅲ) 상기 제1 스크리닝된 사용자로부터의 요청에 응답하여, 상기 리스트 내에 포함된 제2 스크리닝된 사용자에 관한 정보를 상기 제1 스크리닝된 사용자에게 제공하는 기능 - 상기 정보는 상기 제2 스크리닝된 사용자와의 피어-투-피어 통신을 확립하는 데에 요구되는 임의의 어드레스를 포함함 -

을 포함하는 시스템.

청구항 14

제13항에 있어서,

상기 기계 명령들은, 상기 프로세서가,

(a) 상기 제2 스크리닝된 사용자와의 피어-투-피어 통신을 확립하기 위한 상기 제1 스크리닝된 사용자의 시도가 실패했음을 통지받은 경우, 상기 제1 스크리닝된 사용자에 관한 정보를 상기 제2 스크리닝된 사용자에게 제공하는 기능 - 상기 정보는 상기 제1 스크리닝된 사용자와의 피어-투-피어 통신을 확립하는 데에 요구되는 임의의 어드레스를 포함함 -, 및

(b) 상기 제2 스크리닝된 사용자에게 상기 제1 스크리닝된 사용자와의 피어-투-피어 통신을 확립할 것을 요청하는 기능

을 더 수행하게 하는 시스템.

청구항 15

제14항에 있어서,

상기 기계 명령들은, 상기 프로세서가,

상기 제1 스크리닝된 사용자와의 피어-투-피어 통신을 확립하기 위한 상기 제2 스크리닝된 사용자의 시도가 실패했음을 통지받은 경우, 상기 제1 스크리닝된 사용자와 상기 제2 스크리닝된 사용자 간의 모든 통신을 상기 시스템을 통해 라우팅하게 하는 기능

을 더 수행하게 하는 시스템.

청구항 16

서버를 사용하여, 상기 서버의 클라이언트들 간의 피어-투-피어 통신을 용이하게 하는 보안 환경을 제공하는 방법에 있어서,

(a) 상기 서버를 사용하여, 클라이언트가 상기 보안 환경에 액세스하는 것을 허가하기 전에 각각의 클라이언트를 인증 및 허가하는 단계,

(b) 상기 서버를 사용하여, 상기 보안 환경에 대한 액세스를 허가받은 제1 클라이언트에게, 상기 보안 환경에 대한 액세스를 허가받은 제2 클라이언트에 연관된 식별자를 제공하는 단계, 및

(c) 상기 제1 클라이언트에 의한 요청에 응답하여, 상기 서버를 사용하여, 상기 서버에 의한 또다른 인터랙션을 요구하지 않고서 상기 제1 클라이언트와 상기 제2 클라이언트 간의 피어-투-피어 통신이 확립될 수 있게 하기 위한 정보를, 상기 제1 클라이언트에게 제공하는 단계

를 포함하는 방법.

청구항 17

제16항에 있어서,

상기 서버에 의하여, 각각의 상이한 클라이언트 등급마다 상이한 액세스 정책이 적용되도록, 각각의 클라이언트에게 등급을 할당하는 단계를 더 포함하고,

상기 서버를 사용하여 각각의 클라이언트를 인증 및 허가하는 단계는, 클라이언트가 속하는 등급을 결정하는 단계를 포함하는 방법.

청구항 18

제17항에 있어서,

Ex.1002 / Page 443 of 1173
Cisco Systems, Inc.

상기 각각의 클라이언트에게 등급을 할당하는 단계는,

클라이언트가 익명 사용자인지를 결정하는 단계, 및

익명 사용자인 경우, 상기 보안 환경에 액세스하기 위한 상기 클라이언트의 허가를 정의하는 소정의 허가를 상기 클라이언트에게 할당하는 단계

를 포함하고,

상기 각각의 익명 사용자의 허가를 정의하는 허가는, 익명 사용자인 하나의 클라이언트가 익명이 아닌 다른 클라이언트와의 제한적인 피어-투-피어 통신을 확립하여, 상기 다른 클라이언트가 상기 하나의 클라이언트에게 데이터에 대한 단방향 액세스를 제공하는 서버의 역할을 할 수 있게 하는 방법.

청구항 19

제17항에 있어서,

상기 각각의 클라이언트에게 등급을 할당하는 단계는,

클라이언트가 제한적으로 인증된 사용자인지를 결정하는 단계, 및

제한적으로 인증된 사용자인 경우, 상기 보안 환경에 액세스하기 위한 상기 클라이언트의 허가를 정의하는 소정의 허가를 상기 클라이언트에게 할당하는 단계

를 포함하고,

상기 소정의 허가는, 제한적으로 인증된 사용자인 클라이언트가, 제한적으로 인증된 사용자와의 피어-투-피어 통신을 허가하는 데에 동의한 다른 클라이언트와의 피어-투-피어 통신을 확립할 수 있도록, 각각의 제한적으로 인증된 사용자의 허가를 정의하는 방법.

청구항 20

제17항에 있어서,

상기 각각의 클라이언트에게 등급을 할당하는 단계는,

클라이언트가 인증된 사용자인지를 결정하는 단계, 및

인증된 사용자인 경우, 상기 보안 환경에 액세스하기 위한 상기 클라이언트의 허가를 정의하는 소정의 허가를 상기 클라이언트에게 할당하는 단계

를 포함하고,

상기 각각의 인증된 사용자의 허가를 정의하는 허가는, 인증된 사용자인 클라이언트가, 인증된 사용자와의 피어-투-피어 통신을 허가하는 데에 동의한 다른 클라이언트와의 피어-투-피어 통신을 확립할 수 있게 하는 방법.

청구항 21

제17항에 있어서,

상기 각각의 클라이언트에게 등급을 할당하는 단계는,

클라이언트가 리스트 엔티티(listing entity)인지를 결정하는 단계, 및

리스트 엔티티인 경우, 상기 보안 환경에 액세스하기 위한 상기 클라이언트의 허가를 정의하는 소정의 허가를 상기 클라이언트에 할당하는 단계

를 포함하고,

상기 각각의 리스트 엔티티의 허가를 정의하는 허가는, 리스트 엔티티인 클라이언트가, 다른 클라이언트와의 통신을 상기 다른 클라이언트에 등급에 기초하여 지향시킬 수 있게 하는 방법.

청구항 22

제17항에 있어서,

상기 서버를 사용하여, 상기 제2 클라이언트에 연관된 식별자를 상기 제1 클라이언트에게 제공하는 단계는, 상기 제1 클라이언트와 동일한 등급에 속하는 클라이언트들에 연관된 식별자만을 상기 제1 클라이언트에게 제공하는 단계를 포함하는 방법.

청구항 23

제16항에 있어서,

(a) 상기 서버는, 클라이언트가 관여하기를 원하는 피어-투-피어 통신의 주제에 기초하여, 복수의 상이한 클라이언트 그룹을 설정하고,

(b) 상기 서버를 사용하여 상기 서버에 액세스하는 각각의 클라이언트를 인증하는 단계는, 특정 클라이언트가 어느 그룹에 연관되는지를 결정하는 단계를 포함하고,

(c) 상기 서버를 사용하여, 상기 제2 클라이언트에 연관된 식별자를 상기 제1 클라이언트에게 제공하는 단계는, 상기 제1 클라이언트와 적어도 하나의 그룹을 공유하는 클라이언트들에 연관된 식별자만을 상기 제1 클라이언트에게 제공하는 단계를 포함하는 방법.

청구항 24

제16항에 있어서,

상기 서버를 사용하여, 상기 서버에 액세스하는 각각의 클라이언트를 인증 및 허가하는 단계는,

(a) 웹 사이트의 사인-인(sign-in)을 사용하여 각각의 클라이언트를 인증 및 허가하는 단계,

(b) 공용 키 암호를 사용하여 각각의 클라이언트를 인증 및 허가하는 단계, 및

(c) 신뢰되는 인증기관을 사용하여, 인증을 위해 클라이언트에 의해 사용되는 티켓을 제공하는 단계

중 적어도 하나를 포함하는 방법.

청구항 25

제16항에 있어서,

상기 서버는, 피어-투-피어 통신이 확립될 수 있게 하는 것 이외의 기능을 클라이언트에게 제공하는 방법.

청구항 26

제25항에 있어서,

상기 서버는 게임 서버를 포함하는 방법.

청구항 27

제26항에 있어서,

상기 서버를 사용하여, 상기 제2 클라이언트와 연관된 식별자를 상기 제1 클라이언트에게 제공하는 단계는, 상기 게임 서버에 의해 제어되는 게임 환경 내에서 상기 제1 클라이언트와 인터랙션하는 클라이언트들에 대한 식별자를 상기 제1 클라이언트에게 제공하여, 상기 클라이언트들과 상기 제1 클라이언트 간의 피어-투-피어 통신을 가능하게 하는 단계를 포함하는 방법.

청구항 28

제16항에 있어서,

상기 정보는 상기 제2 클라이언트의 외부 IP 어드레스, 상기 제2 클라이언트에 연관된 임의의 내부 IP 어드레스, 및 상기 제2 클라이언트와의 피어-투-피어 통신에 요구되는 임의의 포트 어드레스를 포함하는 방법.

청구항 29

제28항에 있어서,

상기 서버를 사용하여, 상기 서버에 액세스하는 각각의 클라이언트를 인증 및 허가하는 단계는, 각각의 클라이언트에게 고유한 사용자 키를 할당하는 단계를 포함하고,

상기 정보는 상기 제2 클라이언트의 사용자 키를 포함하여, 피어-투-피어 통신을 열도록 하는 요청이 신뢰되는 소스로부터 온 것임을 상기 제2 클라이언트에게 확신시키는 방법.

청구항 30

제28항에 있어서,

상기 제2 클라이언트에 대한 정보를 수신한 후, 상기 제1 클라이언트가 상기 제2 클라이언트와의 피어-투-피어 통신을 확립할 수 없는 경우,

(a) 상기 제2 클라이언트와의 피어-투-피어 통신을 확립하기 위한 상기 제1 클라이언트의 시도가 실패했음을 상기 서버에 통지하는 단계,

(b) 상기 서버를 사용하여, 상기 제2 클라이언트가 상기 제1 클라이언트와의 피어-투-피어 통신을 확립할 수 있게 하는 데에 요구되는 상기 제1 클라이언트에 관한 정보를 상기 제2 클라이언트에게 제공하는 단계, 및

(c) 상기 제2 클라이언트에게 상기 제1 클라이언트와의 피어-투-피어 통신을 확립할 것을 요청하는 단계

를 더 포함하는 방법.

청구항 31

제30항에 있어서,

상기 제1 클라이언트에 관한 정보를 수신한 후, 상기 제2 클라이언트가 상기 제1 클라이언트와의 피어-투-피어 통신을 확립할 수 없는 경우, 상기 제1 클라이언트와 상기 제2 클라이언트 간의 각각의 통신을 상기 서버를 통해 라우팅하는 단계를 더 포함하는 방법.

청구항 32

제16항의 단계들을 수행하기 위한 기계 명령들이 저장되어 있는 메모리 매체.

청구항 33

Ex.1002 / Page 445 of 1173
Cisco Systems, Inc.

대규모 멀티플레이어(massively multiplayer) 게임을 호스트하는 게임 서버의 작업 부하를 실질적으로 감소시키기 위하여, 상기 대규모 멀티플레이어 게임 내의 플레이어들이 피어-투-피어 관계로 서로 통신할 수 있게 하는 방법에 있어서,

(a) 상기 대규모 멀티플레이어 게임의 플레이에 플레이어로서 참여하기를 원하는 사람 각각에게, 우선 상기 게임 서버를 운영하는 게임 서비스에 등록할 것을 요구하는 단계,

(b) 플레이어가 상기 게임 서비스에 등록했는지를 결정함으로써 상기 게임 서버에 액세스하려고 시도하는 각각의 플레이어를 인증하여, 등록한 사람만이 상기 게임 서버에 플레이어로서 액세스할 수 있게 하는 단계,

(c) 제1 플레이어에게, 상기 게임 서버에 의해 호스트되는 대규모 멀티플레이어 게임 내에서 상기 제1 플레이어와 인터랙션할 수 있는 적어도 한명의 다른 플레이어를 식별하는 리스트를 제공하는 단계,

(d) 상기 제1 플레이어가 상기 리스트로부터 제2 플레이어를 선택할 수 있게 하는 단계 - 선택된 상기 제2 플레이어는 상기 게임 서버에게 알려짐 -, 및

(e) 상기 제2 플레이어에 관한 정보를 상기 게임 서버로부터 상기 제1 플레이어로 전송하는 단계 - 상기 정보는 상기 제1 플레이어와 상기 제2 플레이어 간에서 피어-투-피어 통신이 확립될 수 있게 하는 데에 요구됨 -

를 포함하는 방법.

청구항 34

제33항에 있어서,

상기 게임 서버에 액세스하려고 시도하는 각각의 플레이어를 인증하는 단계는, 각각의 플레이어에게 고유한 사용자 키를 할당하는 단계를 포함하고,

상기 제2 플레이어에 관한 정보를 상기 서버로부터 상기 제1 플레이어로 전송하는 단계는, 상기 제2 플레이어의 사용자 키를 전송하여, 상기 피어-투-피어 통신을 열게 하는 요청이 상기 게임 서버에 의해 호스트되는 대규모 멀티플레이어 게임에 참여하고 있는 신뢰되는 플레이어로부터 온 것임을, 상기 제2 플레이어에게 확신시키는 단계를 포함하는 방법.

청구항 35

제33항에 있어서,

상기 제2 플레이어에 대한 정보를 수신한 후, 상기 제1 플레이어가 상기 제2 플레이어와의 피어-투-피어 통신을 확립할 수 없는 경우,

(a) 피어-투-피어 통신을 확립하기 위한 상기 제1 플레이어의 시도가 실패했음을 상기 게임 서버에 통지하는 단계,

(b) 상기 제1 플레이어에 관한 정보를 상기 서버로부터 상기 제2 플레이어로 전송하는 단계 - 상기 정보는 상기 제1 플레이어와 상기 제2 플레이어 간의 피어-투-피어 통신이을 확립될 수 있게 하는 데에 요구됨 -, 및

(c) 상기 제2 플레이어에게 상기 제1 플레이어와의 피어-투-피어 통신을 확립할 것을 요청하는 단계

를 더 포함하는 방법.

청구항 36

제35항에 있어서,

상기 제1 플레이어에 관한 정보를 수신한 후, 상기 제2 플레이어가 상기 제1 플레이어와의 피어-투-피어 통신을 확립할 수 없는 경우, 상기 제1 플레이어와 상기 제2 플레이어 간의 각각의 통신을 상기 게임 서버를 통해 라우팅하는 단계를 더 포함하는 방법.

청구항 37

제33항의 단계들을 수행하기 위한 기계 명령들이 저장되어 있는 메모리 매체.

청구항 38

게임 플레이 동안, 허가된 플레이어들만이 다른 허가된 플레이어와의 피어-투-피어 통신을 확립하도록 허용되는 게임 환경을 제공하여, 진행중인 플레이어들 간의 통신을 관리하기 위해 네트워크화된 게임 시스템으로부터의 자원을 요구하지 않으면서 게임 플레이를 향상시키는 네트워크화된 게임 시스템에 있어서,

(a) 프로세서, 및

(b) 상기 프로세서와 통신하며, 상기 프로세서가 복수의 기능을 수행하게 하는 기계 명령들을 저장하는 메모리

를 포함하고,

상기 복수의 기능은,

(ⅰ) 상기 게임 시스템에 의해 호스트되는 게임 환경에 액세스하려고 시도하는 각각의 플레이어를 스크리닝하여, 허가된 플레이어들만이 상기 게임 시스템에 의해 호스트되는 게임 환경에 액세스할 수 있는 기능,

Ex.1002 / Page 446 of 1173
Cisco Systems, Inc.

(ii) 제1 허가된 플레이어에게, 상기 게임 환경에 참여하고 있는 적어도 한명의 다른 허가된 플레이어를 포함하는 리스트를 제공하는 기능,

(iii) 상기 제1 허가된 플레이어가 상기 리스트로부터 제2 허가된 플레이어를 식별할 수 있게 하는 기능, 및

(iv) 상기 제2 허가된 플레이어에 관한 정보를 상기 게임 시스템으로부터 상기 제1 허가된 플레이어로 전송하는 기능 - 상기 정보는 상기 제1 허가된 플레이어와 상기 제2 허가된 플레이어 간에 피어-투-피어 통신이 확립될 수 있게 하는 데에 요구되는 임의의 어드레스를 포함함 -

를 포함하는 네트워크화된 게임 시스템.

청구항 39

제38항에 있어서,

상기 정보는 상기 게임 시스템에 의해 상기 제2 허가된 플레이어에 할당된 사용자 키를 포함하여, 상기 피어-투-피어 통신을 열게 하는 요청이 신뢰되는 플레이어로부터 온 것임을 상기 제2 허가된 플레이어에게 확신시키는 네트워크화된 게임 시스템.

청구항 40

제38항에 있어서,

상기 기계 명령들은, 상기 프로세서가,

(a) 상기 제2 허가된 플레이어와의 피어-투-피어 통신을 확립하기 위한 상기 제1 허가된 플레이어의 시도가 실패했음을 통지받은 경우, 상기 제2 허가된 플레이어에게 상기 제1 허가된 플레이어에 관한 정보를 제공하는 기능 - 상기 정보는 상기 제1 허가된 플레이어와 상기 제2 허가된 플레이어 간에 피어-투-피어 통신이 확립될 수 있게 하는 데에 요구되는 임의의 어드레스를 포함함 -, 및

(b) 상기 제2 허가된 플레이어에게 상기 제1 허가된 플레이어와의 피어-투-피어 통신을 확립할 것을 요청하는 기능

을 더 수행하게 하는 네트워크화된 게임 시스템.

청구항 41

서버를 사용하여, 클라이언트들이 서로 피어-투-피어 통신을 확립할 수 있게 하는 신뢰되는 세션 환경을 확립하는 방법에 있어서,

(a) 서버를 사용하여, 상기 클라이언트들이 피어-투-피어 통신을 확립하기 전에 처음에 액세스하는 세션을 호스트하는 단계,

(b) 상기 서버에 의해 호스트되는 상기 세션에 액세스하려고 시도하는 각 클라이언트의 자격을 검사하여, 상기 서버에 의해 승인받은 자격을 갖는 클라이언트들만이 상기 세션에 대한 액세스를 허가받도록 하는 단계,

(c) 상기 세션에 대한 액세스를 허가받은 제1 클라이언트에게, 상기 서버에 의해 승인받은 자격을 갖는 하나 이상의 다른 클라이언트를 식별하는 리스트를 제공하는 단계,

(d) 상기 제1 클라이언트가 상기 리스트로부터 제2 클라이언트를 선택할 수 있게 하는 단계 - 상기 제1 클라이언트에 의해 선택된 제2 클라이언트는 상기 서버에 알려짐 -, 및

(e) 상기 제2 클라이언트에 관한 접속 정보를 상기 서버로부터 상기 제1 클라이언트로 전송하는 단계 - 상기 접속 정보는 상기 제1 클라이언트와 상기 제2 클라이언트 간에서 피어-투-피어 통신이 확립될 수 있게 함 -

를 포함하는 방법.

청구항 42

제41항에 있어서,

상기 제2 클라이언트에 관한 정보를 수신한 후에, 상기 제1 클라이언트가 상기 제2 클라이언트와의 피어-투-피어 통신을 확립할 수 없는 경우,

(a) 피어-투-피어 통신을 확립하기 위한 상기 제1 클라이언트의 시도가 실패했음을 상기 서버에 통지하는 단계,

(b) 상기 제1 클라이언트에 관한 정보를 상기 서버로부터 상기 제2 클라이언트로 전송하는 단계 - 상기 정보는 상기 제1 클라이언트와 상기 제2 클라이언트 간에 피어-투-피어 통신이 확립될 수 있게 하는 데에 요구됨 -, 및

(c) 상기 제2 클라이언트에게 상기 제1 클라이언트와의 피어-투-피어 통신을 확립할 것을 요청하는 단계

를 더 포함하는 방법.

청구항 43

제41항에 있어서,

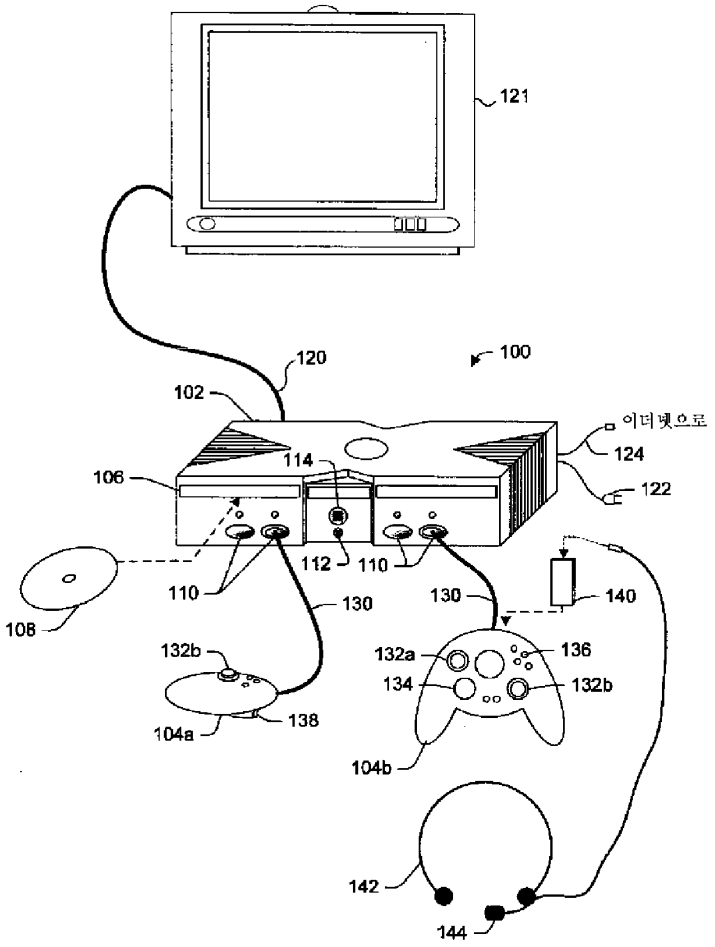
상기 제1 클라이언트에 관한 정보를 수신한 후, 상기 제2 클라이언트가 상기 제1 클라이언트와의 피어-투-

Ex.1002 / Page 447 of 1173
Cisco Systems, Inc.

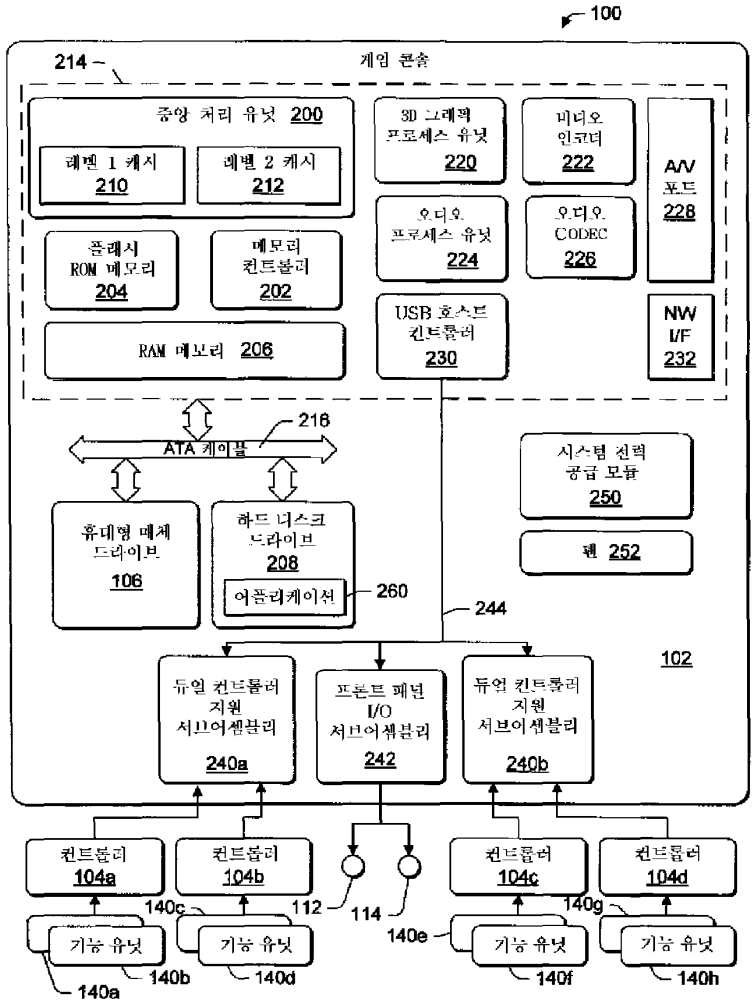
피어 통신을 확립할 수 없는 경우, 상기 제1 클라이언트와 상기 제2 클라이언트 간의 모든 통신을 상기 서버를 통해 라우팅하는 단계를 더 포함하는 방법.

도면

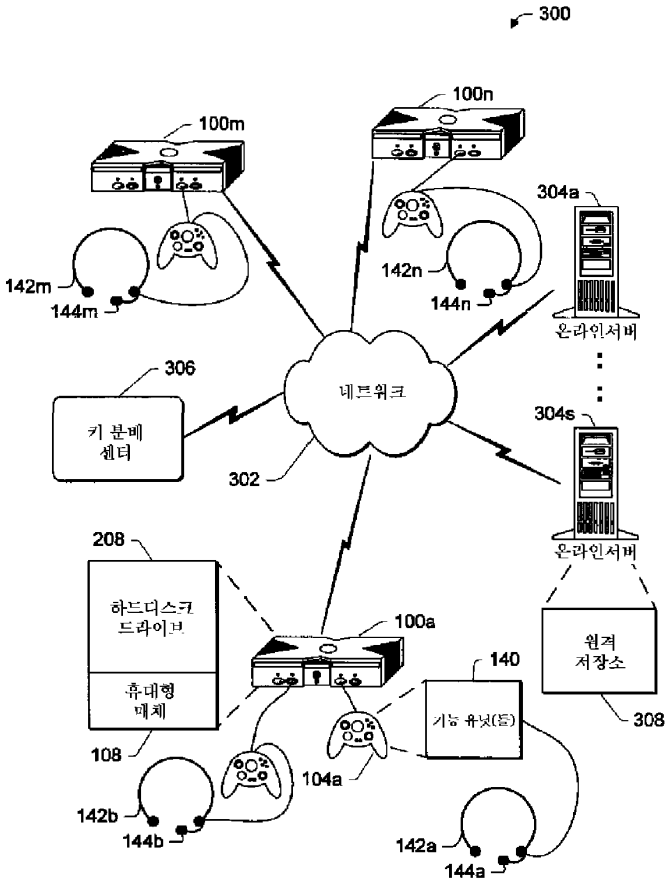
도면1



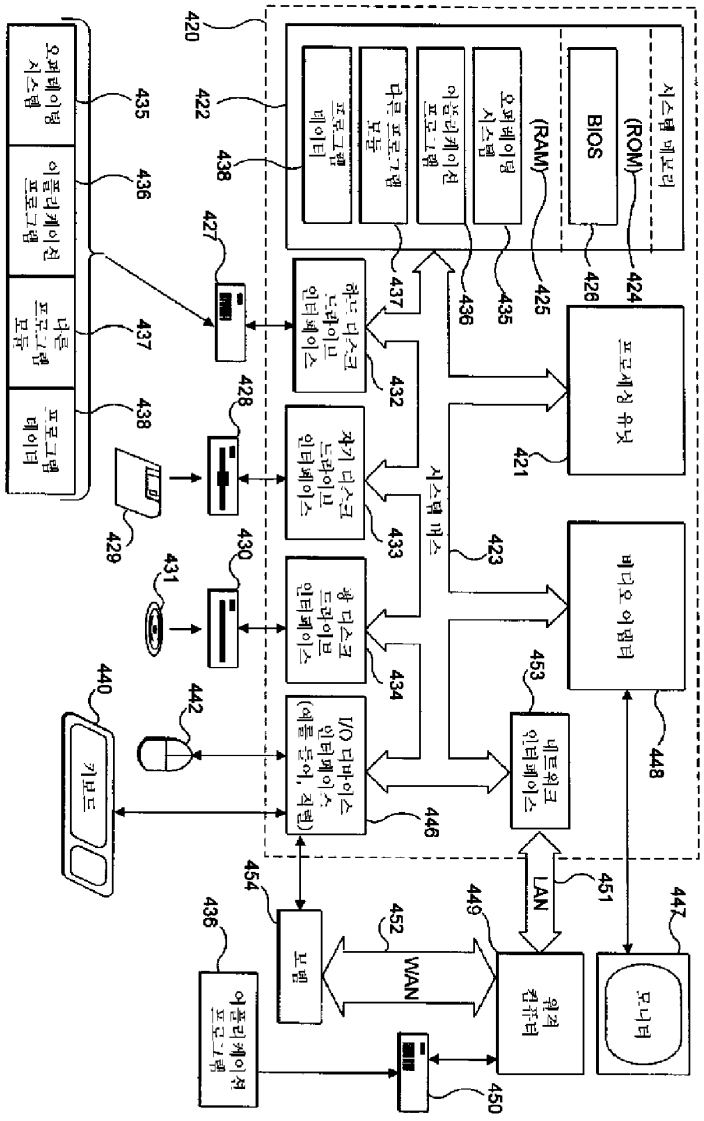
도면2


100
214
게임 콘솔
중앙 처리 유닛 200
레벨 1 캐시 210
레벨 2 캐시 212
3D 그래픽 프로세스 유닛 220
비디오 인코더 222
A/V 포트 228
오디오 프로세스 유닛 224
오디오 CODEC 226
플래시 ROM 메모리 204
메모리 컨트롤러 202
USB 호스트 컨트롤러 230
NW I/F 232
RAM 메모리 206
216
ATA 케이블
시스템 전력 공급 모듈 250
휴대형 매체 드라이브 106
하드 디스크 드라이브 208
팬 252
어플리케이션
260
244
102
듀얼 컨트롤러 지원 서브어셈블리 240a
프론트 패널 I/O 서브어셈블리 242
듀얼 컨트롤러 지원 서브어셈블리 240b
컨트롤러 104a
컨트롤러 104b
컨트롤러 104c
컨트롤러 104d
112
114
140c
140e
140g
기능 유닛
140a
140b
140d
140f
140h

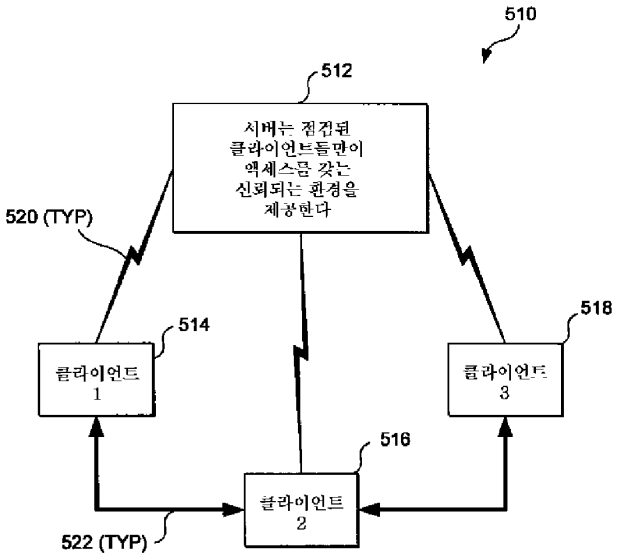
도면3


300
100m
100n
304a
142m
144m
142n
144n
온라인서버
306
키 분배
센터
네트워크
302
304s
온라인서버
208
하드디스크
드라이브
휴대형
매체
108
100a
140
기능 유닛(들)
원격
저장소
308
104a
142b
144b
142a
144a

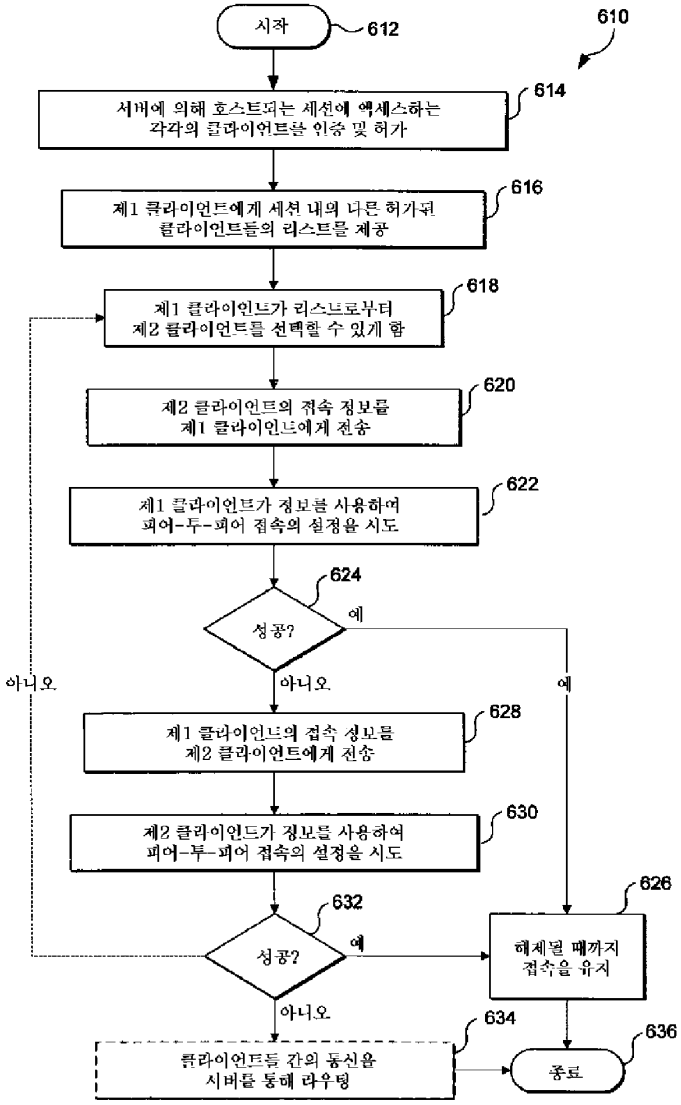
도면4


420
422
438
427
428
429
430
431
440
442
435
436
437
438
시스템 메모리
(ROM)
BIOS
(RAM)
오퍼레이팅 시스템
어플리케이션 프로그램
다른 프로그램 모듈
프로그램 데이터
424
426
425
435
436
437
432
433
434
421
423
453
448
446
454
452
449
451
447
450
하드 디스크 드라이브 인터페이스
자기 디스크 드라이브 인터페이스
광 디스크 드라이브 인터페이스
I/O 디바이스 인터페이스 (에를 들어, 직렬)
시스템 버스
프로세싱 유닛
비디오 어댑터
네트워크 인터페이스
LAN
WAN
모뎀
원격 컴퓨터
모니터
어플리케이션 프로그램
키보드

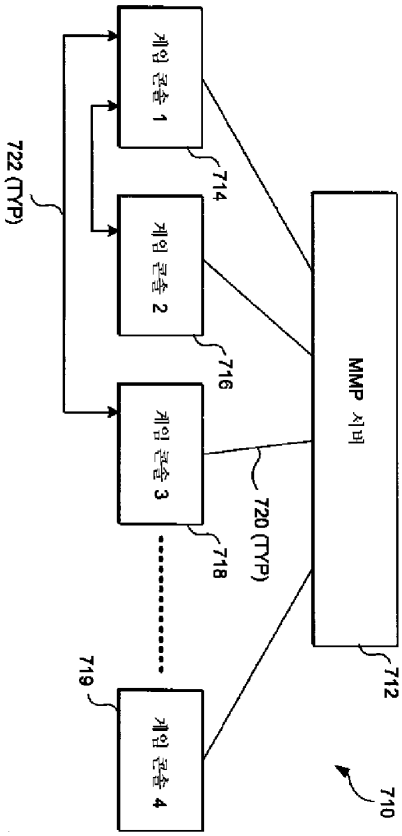
도면5


510
512
서버는 접근된
클라이언트들만이
액세스를 갖는
신뢰되는 환경을
제공한다
520 (TYP)
514
518
클라이언트
1
클라이언트
3
516
클라이언트
2
522 (TYP)

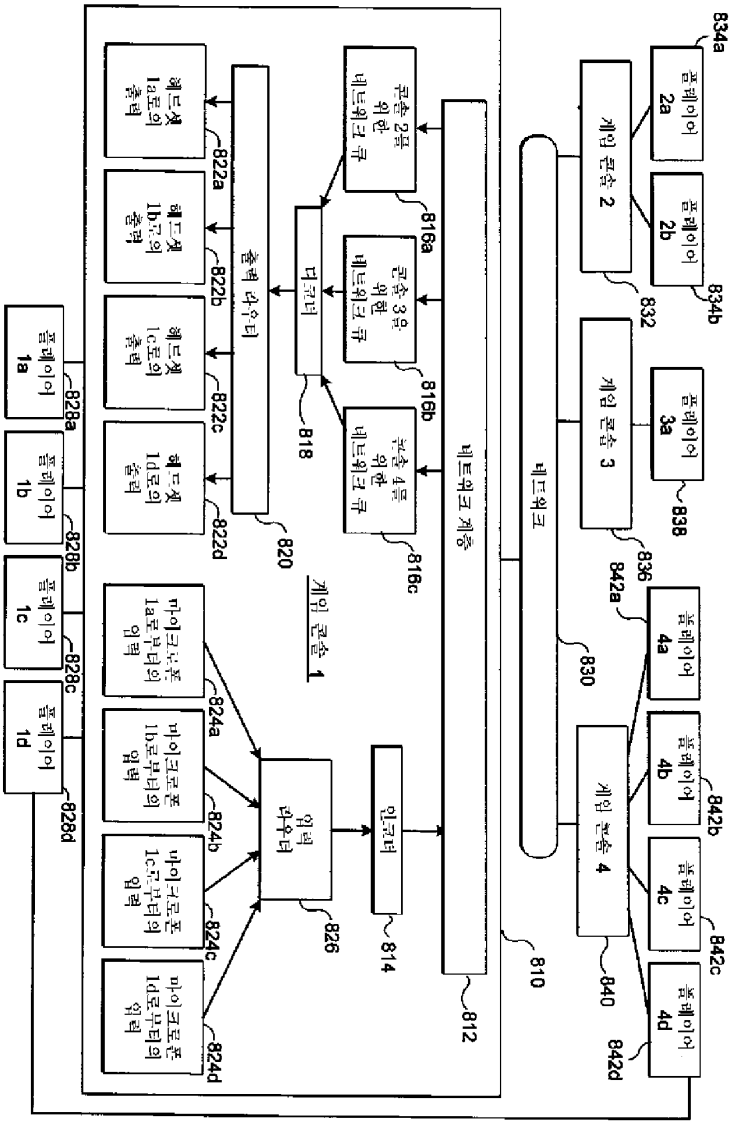
도면6


610
시작
612
서버에 의해 호스트되는 세션에 액세스하는 각각의 클라이언트를 인증 및 허가
614
제1 클라이언트에게 세션 내의 다른 허가된 클라이언트들의 리스트를 제공
616
제1 클라이언트가 리스트로부터 제2 클라이언트를 선택할 수 있게 함
618
제2 클라이언트의 접속 정보를 제1 클라이언트에게 전송
620
제1 클라이언트가 정보를 사용하여 피어-투-피어 접속의 설정을 시도
622
성공?
624
예
아니오
아니오
예
제1 클라이언트의 접속 정보를 제2 클라이언트에게 전송
628
제2 클라이언트가 정보를 사용하여 피어-투-피어 접속의 설정을 시도
630
성공?
632
예
해제될 때까지 접속을 유지
626
아니오
클라이언트들 간의 통신을 서버를 통해 라우팅
634
종료
636

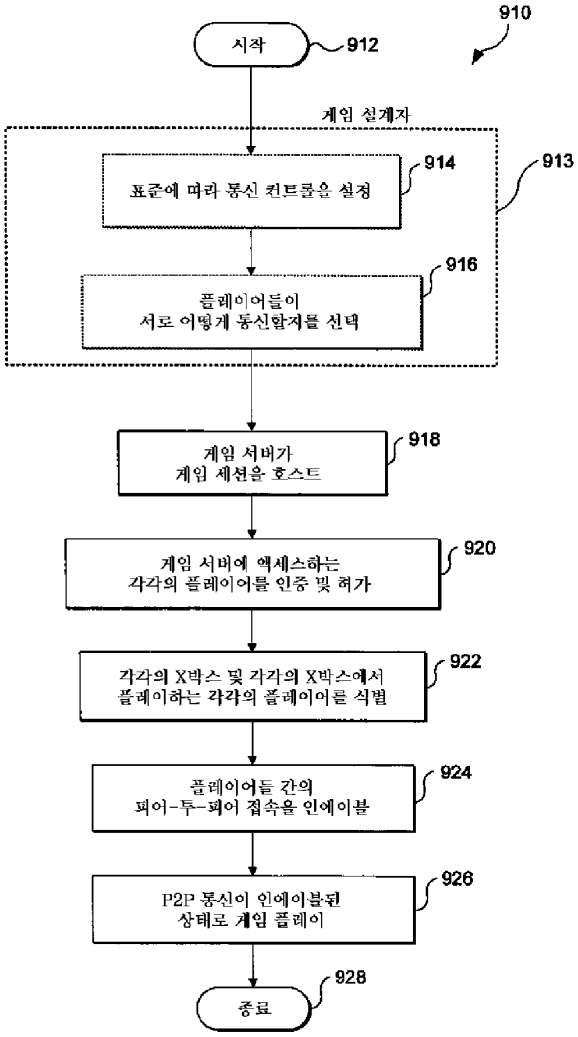
도면7


게임 콘솔 1
게임 콘솔 2
게임 콘솔 3
게임 콘솔 4
MMP 서버
710
712
714
716
718
719
720 (TYP)
722 (TYP)

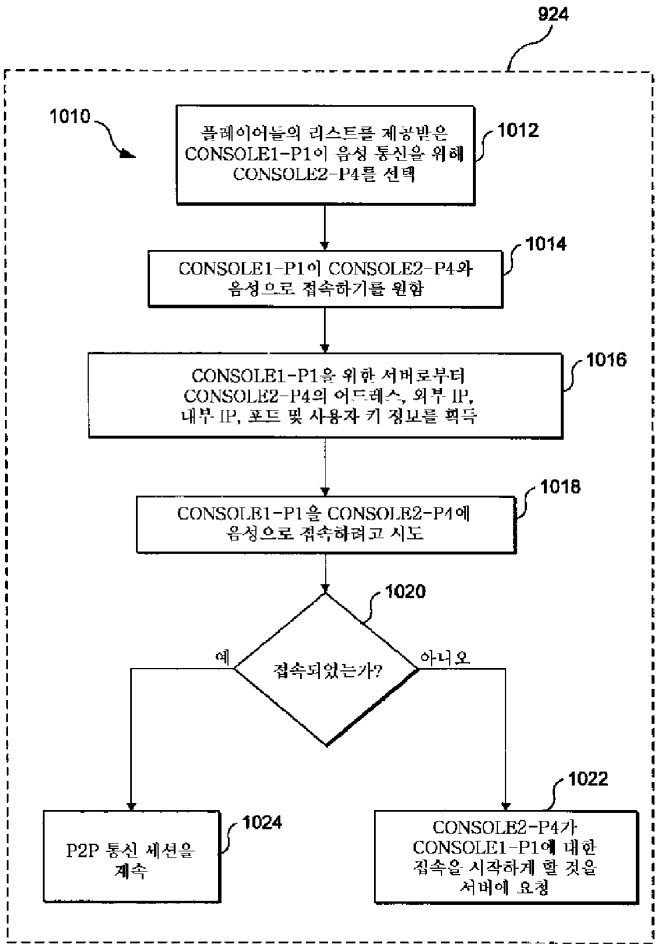
도면8


834a
플레이어 2a
플레이어 2b
834b
게임 콘솔 2
832
플레이어 3a
838
게임 콘솔 3
836
842a
플레이어 4a
842b
플레이어 4b
842c
플레이어 4c
842d
플레이어 4d
게임 콘솔 4
840
830
네트워크
810
812
네트워크 계층
816a
콘솔 2을 위한 네트워크 큐
816b
콘솔 3을 위한 네트워크 큐
816c
콘솔 4을 위한 네트워크 큐
818
디큐어
820
출력 라우터
822a
헤드셋 1a로의 출력
822b
헤드셋 1b로의 출력
822c
헤드셋 1c로의 출력
822d
헤드셋 1d로의 출력
게임 콘솔 1
824a
마이크로폰 1a로부터의 입력
824b
마이크로폰 1b로부터의 입력
824c
마이크로폰 1c로부터의 입력
824d
마이크로폰 1d로부터의 입력
826
입력 라우터
814
인큐어
828a
플레이어 1a
828b
플레이어 1b
828c
플레이어 1c
828d
플레이어 1d

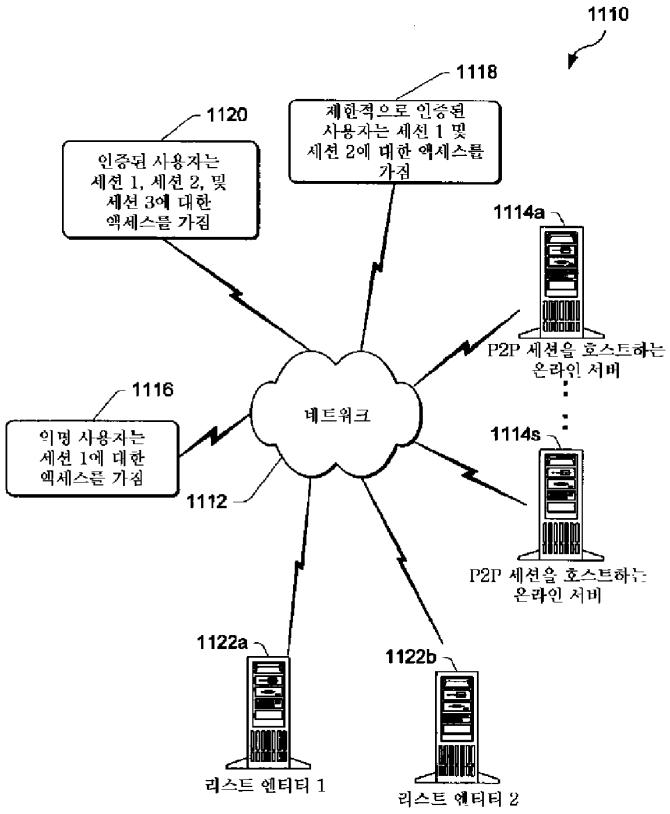
도면9


910
시작
912
게임 설계자
914
913
표준에 따라 통신 컨트롤을 설정
916
플레이어들이
서로 어떻게 통신할지를 선택
918
게임 서버가
게임 세션을 호스트
920
게임 서버에 액세스하는
각각의 플레이어를 인증 및 허가
922
각각의 X박스 및 각각의 X박스에서
플레이하는 각각의 플레이어를 식별
924
플레이어들 간의
피어-투-피어 접속을 인에이블
926
P2P 통신이 인에이블된
상태로 게임 플레이
928
종료

도면10


924
1010
플레이어들의 리스트를 제공받은 CONSOLE1-P1이 음성 통신을 위해 CONSOLE2-P4를 선택
1012
CONSOLE1-P1이 CONSOLE2-P4와 음성으로 접속하기를 원함
1014
CONSOLE1-P1을 위한 서버로부터 CONSOLE2-P4의 어드레스, 외부 IP, 내부 IP, 포트 및 사용자 키 정보를 획득
1016
CONSOLE1-P1을 CONSOLE2-P4에 음성으로 접속하려고 시도
1018
1020
접속되었는가?
예
아니오
P2P 통신 세션을 계속
1024
CONSOLE2-P4가 CONSOLE1-P1에 대한 접속을 시작하게 할 것을 서버에 요청
1022

도면11


1110
1118
제한적으로 인증된 사용자는 세션 1 및 세션 2에 대한 액세스를 가짐
1120
인증된 사용자는 세션 1, 세션 2, 및 세션 3에 대한 액세스를 가짐
1114a
P2P 세션을 호스트하는 온라인 서비
1116
익명 사용자는 세션 1에 대한 액세스를 가짐
네트워크
1112
1114s
P2P 세션을 호스트하는 온라인 서비
1122a
1122b
리스트 엔티티 1
리스트 엔티티 2

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 848 163 A1

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

(43) Date of publication:
24.10.2007 Bulletin 2007/43

(21) Application number: **06702680.7**

(22) Date of filing: **13.01.2006**

(51) Int Cl.:
H04L 12/56 *(2006.01)* ***H04Q 7/38*** *(2006.01)*

(86) International application number:
PCT/JP2006/300324

(87) International publication number:
WO 2006/075677 (20.07.2006 Gazette 2006/29)

(84) Designated Contracting States:
DE FR GB

(30) Priority: **17.01.2005 JP 2005009301**

(71) Applicant: **Sharp Kabushiki Kaisha**
Osaka-shi, Osaka 545-8522 (JP)

(72) Inventors:
- **YAMADA, Shohei**
  Chiba, 2610004 (JP)
- **MORIWAKI, Tetsuro**
  Saitama, 3300071 (JP)
- **HIBI, Keiichi**
  Chiba 2700034 (JP)

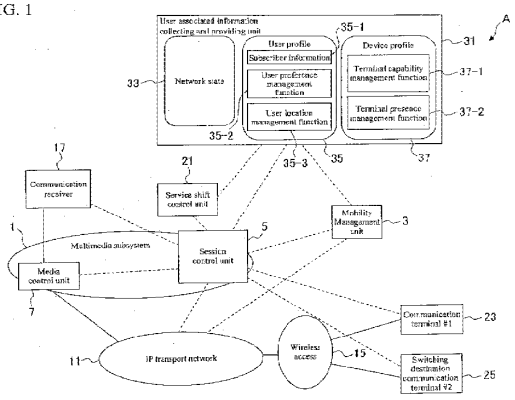
(74) Representative: **Müller, Frithjof E.**
Müller Hoffmann & Partner
Patentanwälte
Innere Wiener Strasse 17
81667 München (DE)

(54) COMMUNICATION NETWORK CONTROL SYSTEM

(57) Smooth and seamless terminal switching which guarantees continuity of communication at the level of application is realized.

A communication network control system includes a mobility management unit 3 for setting up and managing a physical and logical transmission path between a communication terminal 23 and a communication receiver 17 by controlling the path for transmitting data packets, a session control unit 5 for controlling a session between the communication terminal 23 and the communication receiver 17 along the transmission path, a service shift control unit 21 for transmitting to the session control unit 5 a session switching request signal which instructs the session to be switched from communication terminal 23 to a communication terminal 25 to which the connection is to be switched, and a user associated information collecting and providing unit 31 for collecting a user profile which includes information on the user's location, the state of the network of the user and the preferences and interests of the user, and a device profile which includes the type of the device and the state of connection of each device to the network from each function element of the network, the user, the user terminal and a device in the vicinity of the user, and providing user associated information.

FIG. 1



EP 1 848 163 A1

Description

Technical Field

[0001] The present invention relates to a technology for switching terminals in a communication network which provides mobile communication service, and in particular, to a technology for switching terminals where communication can be continued seamlessly and without interruption when a user switches the terminal he or she is using to a different terminal during communication.

Background Art

[0002] In recent years, communication service at a higher degree has been expected to be realized as network services represented by the internet, and cellular phones have quickly spread and expanded. Though a so-called handover function or a mobility management function where communication continues even when a user moves while holding a terminal have been provided to cellular phones, this function is desired to be further developed to a higher level so that a function which allows communication to continue even if the terminal is changed during communication can be realized.

[0003] When it becomes possible to connect various terminals to a communication network as a result of expansion and development of the network, users can own various types of communication terminals which can be connected to a communication network. These communication terminals are not limited to portable terminals, such as cellular phones, but it is considered that information apparatuses, such as stationary home electronics which are installed within a house, for example, a television receiver (hereinafter, referred to as information apparatus), can also be used as a communication terminal.

[0004] Meanwhile, on the communication network side, it becomes easy to provide a common service to various types of communication terminals without recognizing a difference between wireless and wired access means in the network operator or in the service provider, by providing a common IP (internet protocol) backbone where IP communication technology that has been constructed through the development of the internet is used.

[0005] As a result, users can selectively use communication terminals they own, such as information apparatuses, for example, mobile communication terminals, PDA's and personal computers, depending on the current situation or the preference of the user, and then the same service is required to be used through a terminal the user owns or selects at a point in time. Furthermore, a situation where a terminal is desired to be switched to another terminal during communication can be assumed. In this case, it is necessary to realize the demand of the user in which the terminal can be switched to another terminal seamlessly, that is, without interruption, while maintaining the state of communication instead of the communication being cut off and connected again through another terminal.

[0006] There is a concrete example where video contents are distributed through streaming and viewed on a personal computer at home, and the receiving terminal is switched to a mobile communication terminal or a PDA when the user goes out so that the same contents can be continuously viewed on the terminal which is taken out with the user. In addition, there is another possible example where the user communicates with someone on a television phone while going out, and then comes home, and therefore, the television phone is switched to a television at home so that the communication with the other person can be continued.

[0007] In the case where a multicasting type distribution is received when the seamless switching of terminals is realized as described above, the data of the same contents is simultaneously distributed to a number (unspecified large number) of communication terminals from the terminal on the transmission side. Therefore, the receiving terminal may be connected to this terminal on the transmission side such that this data is received by the switching destination terminal, and thus, switching of the terminals can be realized relatively easily.

[0008] In the case of a unicasting type distribution where the communication is distributed to only a certain terminal or one-on-one communication, a procedure becomes necessary where an interruption of communication is instructed to the terminal on the transmission side, the switching destination terminal is connected to this terminal on the transmission side, and then, it is notified that the terminal on the receiving side has been switched, and after that, the communication is resumed.

[0009] Fig 7 shows an example where terminals are switched in a control system of a conventional communication network as described above. Fig 7 shows an example in the case where a user switches a communication terminal (#1) 203, which is being used for the communication, to a communication terminal (#2) 205. First, the user transmits control information, as shown by arrow 221, from the communication terminal (#1) 203, which is receiving data, to a server apparatus 201 on the distribution side, and thus, instructs interruption of distribution. Next, the control information requesting an interruption of the communication connected to the server apparatus 201, as shown by arrow 224a, is sent out to a control apparatus 213 within the communication network, and thus, the communication is cut off.

[0010] Next, when the user sends out a request for connection to the server apparatus 201, as shown by arrow 225, to the control apparatus 213 in the communication network from the communication terminal (#2) 205, to which the connection is to be switched, the control apparatus 213 sets up a communication path between the communication terminal (#2) 205 and the server apparatus 201 within the communication network, and sets up the communication between these apparatuses. Subsequently, when the control information for instructing resumption of distribution, as shown by arrow 224b, is

Ex.1002 / Page 460 of 1173
Cisco Systems, Inc.

sent out from the communication terminal (#2) 213 to the server apparatus 201, the server apparatus 201 sends out data from the point in time when the distribution is interrupted so that the user can receive the following data using the communication terminal (#2) 205, that is, switching of the terminals can be realized.

[0011] Here, address information on the server apparatus 201 for the communication terminal (#2) 205, to which the connection is to be switched, to be connected to the server apparatus 201 is designated by means of the communication terminal (#2) 205, which is operated by the user so that the address information is inputted in the form of a telephone number, a URL or the like. In this example, the control apparatus 213 in the communication network only makes and cuts off the connection between the communication terminal (#1) 203 or the communication terminal (#2) 205 and the server apparatus 201 and does not have the control function for switching terminals. Thus, the switching of terminals can be realized by using only the communication terminals and the functions of interrupting and resuming communication in the server apparatus.

[0012] Fig 8 shows a conventional example of another method for switching terminals. A communication terminal (#1) 303 on the receiving side sends out the control information for instructing a server apparatus 301 on the distribution side to interrupt the distribution, as shown by arrow 321, when terminals are switched. When the user carries out a transfer operation after the communication with the server apparatus 301 has been suspended, the communication terminal (#1) 303 sends out the control information for requesting the transfer of the connection with the server apparatus 301 to a communication terminal (#2) 305 to a control apparatus 313 in the communication network, as shown by arrow 332.

[0013] The control apparatus 313 which has received the control information sends out the control information for instructing the communication terminal (#2) 305 to connect with the server apparatus 301, as shown by arrow 333, and thus, calls the communication terminal (#2) 305 and sets up a communication path between the communication terminal (#2) 305 and the server apparatus 301 so that a connection is established when the communication terminal (#2) 305 responds to this call, as shown by arrow 334.

[0014] Thereafter, as shown by arrow 335, upon the transmission and reception of the control information between the communication terminal (#1) 303, which is the transfer source and the control apparatus 313, the connection between the communication terminal (#1) 303 and the server apparatus 301 is cut off. At the same time, the communication terminal (#2) 305 sends out the control information for requesting resumption of the suspended communication, as shown by arrow 324, to the server apparatus 301, and thus, the communication terminal (#2) 305 receives the following data. In this example, though the control apparatus 313 within the communication network has a control function for transferring a call to another terminal, this control apparatus 313 does not have a function of controlling the interruption and resumption of data transmission and reception between the communication terminal and the server apparatus, and thus, does not guarantee the continuity of communication, that is, seamless switching (Non-Patent Document 1).

[0015] In addition, Fig 2 shows an example of a configuration of a third generation mobile communication of which the standard is defined by 3GPP as the configuration of a conventional communication network. IMS (IP Multimedia CN Subsystem) has a purpose of providing an IP multimedia service through a packet exchanging system, and to do so, a session control function is arranged within the network 101. SIP (Session Initiation Protocol) is adopted as the session control protocol. CSCF 105 is a call state control function and communicates with HSS (Home Subscriber Server) 103 as a registered server of the SIP so as to carry out a user registering process, transfer session information and control the call connection. It also has an interface for communicating with an application server in order to provide a service. In addition, the HSS 103 manages the subscriber and location information of users. MRF (Media Resource Function) 107 controls the resource of media streaming and carries out media synthesis and the conversion of media streams in a multimedia conference and the like. In addition, MGCF (MediaGateway Control Function) and MGW (MediaGateway) carry out media conversion at the time of the connection with PSTN (Public Switched Telephone Network). However, there are no mechanisms where a service is continuously provided to a terminal 123 or 125 for wireless access 115 to a receiver of communication 117 via a network 101 and a packet network 111 even after change (see Non-Patent Document 2).

Non-Patent Document 1: Yabusaki et al. "All-IP Conversion in Mobile Network, Special Issue," NTT DoCoMo Technical Journal, Vol. 10, No. 4, January 2003, pp. 6-34

Non-Patent Document 2: 3GPP TS22. 228, V5. 6. 0

Disclosure of the Invention

Problems to be Solved by the Invention

[0016] In any of the conventional examples, however, the continuity is secured by the suspension and resumption of the communication between the communication terminal and the server apparatus, that is, between both ends, when terminals are switched, and thus, a technology for guaranteeing seamless switching without interruption is not used. That is, in any of the conventional examples, a function of suspending communication, that is, data transmission, is provided in a server apparatus, and after the suspension, the resumption of data transmission is required from another communication terminal, so that the switching of terminals is realized only in appearance. In the case where contents stored in a serv-

Ex.1002 / Page 461 of 1173
Cisco Systems, Inc.

er apparatus are distributed in one direction towards a communication terminal, or in the case of two directional, one-on-one real time communication, such as a television phone, the function to a certain degree can be realized.

[0017] In the case where the communication application in an upper level has a state corresponding to the transmission data, for example, in the case where a communication type game is continued on another terminal or group work where the same document is edited through communication is done, however, there is a problem that it is difficult to inform the switching destination terminal of the state of the communication application.

[0018] More specifically, in the case where a number of communications (connections) are set up between the applications on the ends even in a service, such as communication between television phones or contents distribution, for example, in the case of an application where a large number of media are simultaneously used or an application where various types of contents or information are used in cooperation, there is a problem that a process or procedure for switching to another terminal becomes complicated.

[0019] In addition, there are problems as follows.

[0020] 1) Since contents are received in an optimal communication form (bit rate, resolution and the like) corresponding to the capability of a terminal as the terminal is switched, it is difficult to provide a service which works in cooperation with the control of the communication network so that the quality of the service (bit rate, delay and the like) in the network can be appropriately controlled.

[0021] 2) It is also difficult to determine whether the quality of the service is appropriately switched as described above on the network control side or on the receiver of communication side, or to decide that the quality of the service is switched according to the preference of the user.

[0022] 3) In addition, there is a problem that it is difficult to provide a service for finding what type of terminal exists in the periphery and controlling the switching to a terminal after it has been determined which terminal the connection should be switched to.

[0023] An object of the present invention is to provide a seamless and ubiquitous service environment where it is not necessary for a user to be aware of the difference in wireless and wire networks and service or the difference in the type of communication terminal, unlike in the prior art.

Means for Solving the Problem

[0024] A communication network control system according to the present invention has user associated information collecting and providing means for collecting a user profile which includes the state of the network, information on the user's location, and the preference and interests of the user, and a device profile which includes the type of device and the state of the connection of each device to the network from each functional element of the network, the user, the user terminal and the peripheral device of the user, and providing user associated information in a communication network system including mobility management means for setting up and managing a physical and logical transmission path between the communication terminal and the receiver of communication by controlling the path for data packet transfer, session control means for controlling a session between the communication terminal and the receiver of communication along the transmission path, and service shift control means for transmitting a session switching request signal, which instructs the session to be switched to a switching destination communication terminal from the communication terminal, to the session control means.

[0025] The service shift control means determines whether a terminal switching request signal is received from the communication terminal or the terminal is switched on the basis of the user associated information, and thus, generates a session switching requesting signal. The session control means performs a function of receiving the session switching requesting signal to interrupt the session, a function of instructing the mobility management means to set up a transmission path with the switching destination communication terminal, a function of establishing a session with the switching destination communication terminal, and a function of resuming the session with the receiver of communication after the establishment of the session. As a result, the communication can be controlled so as to be continued by switching at least one communication terminal which is being used for this communication to another communication terminal which is not being used for the communication without interrupting the communication between the communication terminals. Thus, a function of managing and controlling a session between the ends, that is, a logical transmission path between the applications using the transmitted data, and a function of transferring the session are achieved in addition to a function of setting up and managing a transmission path for data in a communication network. Therefore, it becomes possible to realize a smooth and seamless switching of a communication terminal, including the management of the session state and the application.

[0026] In addition, it becomes possible to determine whether or not a terminal is switched corresponding to the environment of the user, and it becomes possible to provide service control on the network side in accordance with the user's location and the network state. In addition, since means for instructing switching of the terminal while maintaining the provision of the user associated information concerning the service and the service and means for establishing a session between terminals are separated, a more efficient network control becomes possible. Furthermore, this can be realized by adding service shift control means to the CSCF which controls a session in the existing 3GPP system.

Ex.1002 / Page 462 of 1173
Cisco Systems, Inc.

[0027] In addition, the communication network control system according to the present invention is characterized in that the service shift control means has a function of determining media to which the media is to be converted, which acquires the device profile of the communication terminal and the switching destination terminal from the user associated information, as well as media switching capability information from the receiver of communication, and instructs conversion of the media at the media control means or change of the session to the receiver of communication, and a media conversion process determining function for determining which media conversion is carried out, wherein the service shift control means generates information on an instruction to change the session and an instruction to change media on the basis of the determination of media to which the media is to be converted and the media conversion process determination.

[0028] As a result, it becomes possible to automatically determine whether the media should be converted on the network side or in the receiver of communication, in order for the state of service to be maintained, in terms of the media switching capability of the receiver of communication and the terminal capability in the communication terminal and the switching destination communication terminal.

[0029] In addition, the communication network control system according to the present invention is characterized in that the user associated information collecting and providing means manages the determination standard for media to which the media is to be converted of the user and the media conversion process as user preference and the service shift control means generates information on media conversion instruction on the basis of the user preference.

[0030] As a result, the user can set his or her own preference in advance and set which service provider is desired to convert the media and which media conversion process is desired, and thus, service which has expandability and flexibility can be provided to the user and to the service provider.

[0031] In addition, the communication network control system according to the present invention is characterized in that the communication terminal has means for communicating with the switching destination communication terminal, and acquires information on terminal presence indicating the state and the address of the switching destination communication terminal and information on terminal capability, which includes information on of what type the switching destination communication terminal is, the attributes, the process, the available bit rate, the type of media and the type of codec from the switching destination communication terminal, the terminal switching request signal includes information on the terminal presence and information on the terminal capability of the switching destination communication terminal, and the service shift control means generates a session switching request signal on the basis of the terminal switching request signal and registers the information on the terminal presence and the information on the terminal capability in the device profile.

[0032] As a result, session control becomes possible even in the case where the communication network side does not have information on the switching destination communication terminal, and a new device can be registered at the same time.

[0033] In addition, the communication network control system according to the present invention is characterized in that the communication terminal operates as the switching destination communication terminal, an instruction requesting only change in the connection path instead of switching of the terminal is transmitted as a terminal switching request signal, or it is determined whether or not the path is switched on the basis of the user associated information, and as a result, the service shift control means generates a session switching signal which instructs switching of the session within the communication terminal and transmits the session switching signal to the session control unit.

[0034] As a result, it becomes possible to maintain the service when the connection is switched to a network having a different access method and a different operator using a communication terminal.

Effect of the Invention

[0035] According to the present invention, the user can switch the communication terminal used through a simple button operation or the like at the time when switching is requested in accordance with the change in his/her situation with the effort required for operation and loss of time greatly reduced in comparison with in the prior art, and thus, can enjoy service at a higher level. There is also an advantage such that distribution service can be continued in the server apparatus on the distribution side without mounting any special new functions. Furthermore, since the data format is optimized for individual communication terminals before being transmitted even when the capability is different between the communication terminals on the receiver side, there is an advantage such that there is no load on the communication terminal side and the server apparatus side. In this manner, the basis for providing service is shared, so that the user is not aware of the difference in the wire and wireless networks and service, or the difference in the type of communication terminal, unlike in the prior art. This makes it possible to enjoy a seamless and ubiquitous service environment.

Brief Description of the Drawings

[0036] Fig 1 is a diagram schematically showing the configuration of a communication network control system according to a first embodiment of the present invention;

Fig 2 is a schematic diagram showing an example

Ex.1002 / Page 463 of 1173
Cisco Systems, Inc.

of the configuration of a conventional communication network control system;

Fig 3 is a diagram showing an example of the configuration of a database in a user associated information collecting and providing unit;

Fig 4 is a diagram showing a procedure for switching terminals in the communication network control system according to the present embodiment;

Fig 5 is a schematic diagram showing a communication network control system in terms of switching of an access method according to a second embodiment of the present invention;

Fig 6 is a diagram showing a procedure for switching a path in the communication network control system in terms of switching of the access method according to the present embodiment;

Fig 7 is a diagram showing an example of terminal switching in the communication network control system; and

Fig 8 is a diagram showing an example of terminal switching in the communication network control system.

Explanation of Symbols

[0037] A ... communication network control system, 3 ... mobility management unit, 5 ... session control unit, 11 ... IP transport network, 21 ... service shift control unit, 31 ... user associated information collecting and providing unit, 33 ... network state, 35 ... user profile, 37 ... device profile

Best Mode for Carrying Out the Invention

[0038] A communication network control system according to the present invention has a function of managing and controlling a session at the ends, that is, a logical transmission path between applications using transmitted data, and a function of transferring the session, in addition to a function of setting up and managing a transmission path for data in a control apparatus within a communication network. These functions allow communication terminals to be switched smoothly and seamlessly, including management of the session state and the application.

[0039] In addition, the communication terminal according to the present invention has a function of making notification of the session state and the application in order to switch terminals and a function of setting the session and the application to the state of which notification has been made as described above, and then, resuming this state. These functions allow terminals to be switched smoothly and seamlessly while maintaining the session in an appropriate state.

[0040] Furthermore, handover and mobility management functions for switching to an appropriate transmission path following the changes in the location of the communication terminal and address information, which are provided through a mobile communication network or the like, are used in cooperation with the session control function, and thus, a function of setting a transmission path when the communication terminal is switched is realized with minimal change from the prior art. Thus, a session control function having high flexibility and expandability is realized.

[0041] In the next generation mobile communication networks, it is assumed that all IP based platforms where all data is transmitted and exchanged in the form of IP packets will be formed for use. In addition, provision of a so-called call and control separating type architecture where the function of transmitting data and the control function of call setting, routing management and the like are clearly separated has been examined. In such an architecture, a transport layer, which is a lower layer, is specialized in the function of transmitting data, that is, IP packets, efficiently and at high speed and the function of controlling the path (routing) and controlling traffic are allocated in the connection control layer, and this connection control layer instructs the transport layer to allocate routing and resources of the IP packets in the configuration, which enables to achieve increase in the speed and increase in the efficiency in the system as a whole. In all-IP based platforms, it is assumed that control signals, such as call control and signaling are transferred in the form of IP packets.

[0042] Furthermore, in the above-described all-IP based architecture, provision of a function for supporting service in order to increase the level of the network and add more value such that various communication services can be flexibly and freely provided has been examined. This means that a call control function for setting up a physical and logical transmission path at the ends is the main function in previous networks, which mainly handle speech sound telephone calls, while in next generation networks, a function of controlling a session, which is logical connection between communication applications at ends, will be provided within the network.

[0043] Here, call and call connection indicate (setting up of) a physical and logical path for transmitting data to a receiver between terminals at the ends, and session indicates that a communication application at a terminal is in such a state as to be able to receive and process (has processed) data from the application in the terminal of the receiver of communication. More specifically, a state where data can be transmitted to or received from a receiver terminal but it is not determined which application should be used or no application is prepared is a state in which call connection can be achieved but no session is connected. Conversely, a state where the application is prepared to transmit or receive data while the data transmission path is lost (for example when a cellular phone is moved out of range) is a state where a session is connected but no call connection is achieved.

[0044] So far, call connection has mainly been described. In conventional speech sound telephone calls, call connection and sessions are not particularly distin-

Ex.1002 / Page 464 of 1173
Cisco Systems, Inc.

guished, but in the case of multimedia communication or data communication, a session is set up between applications of communication terminals along the transmission path established at the ends after setting up of the call connection. For the next generation mobile communication networks, inclusion of a session control function within the network has been examined. This is because it has become necessary for the network to have such functions as connection control and communication control in accordance with various forms of communication, modes and media, due to diversification and increase in the level of communication. In the case where, for example, the difference between calls of only speech sound and television phone calls, the quality and the terminal capability, such as resolution and bit rate, in the television phones are designated for a receiver when a call is made, it is necessary for the capability of the network to include functions of address solution for designated terminals which satisfy these requirements and setting up of a transmission path having appropriate quality (call control, path control) and the like, which cannot sufficiently be provided through negotiation between the ends.

[0045] Therefore, a session control unit for session control is provided, so that a session, that is, a state of communication or the mode between the applications at the ends, is managed and controlled, and this session control function instructs and controls the call control function and the path control function in the mobility management unit to set up a transmission path in an appropriate band having appropriate quality in the configuration. At this time, connection request (session setup request) from the application at the communication terminal is sent to the session control function so as to be processed.

[0046] Fig 1 shows an example of the configuration of a communication network control system according to a first embodiment of the present invention. As shown in Fig 1, a communication network control system A according to the present embodiment includes an IP transport network 11 for transferring IP packets, a mobility management unit 3 for controlling the IP transport network 11 and managing the physical location of the communication terminals, controlling calls and controlling handover (controls paths), as described above, a session control unit 5 for establishing and managing sessions, and a service shift control unit 21 which is charged with dealing with higher level requirements by the user so that communication terminals are switched while maintaining the session.

[0047] The mobility management unit 3 corresponds to the HSS 103 of the IMS in Fig 2, and is a functional element which is specialized particularly to control the IP transport network. The session control unit 5 corresponds to the CSCF 105 of the IMS in Fig 2, and the service shift control unit 21 is a new functional element for the IMS in Fig 2. However, it is construable that the service shift control unit 21 is realized as a result of function expansion of the CSCF 105 in Fig 2. In order to switch terminals while maintaining the service, the service shift control unit 21 allows a terminal to request the session control unit to instruct switching of terminals, a terminal switching request to be received by the session control unit, a session switching request signal to be transmitted to the session control unit, and a user associated information collecting and providing unit 31 to be informed of the state of the user, so that a session switching request signal can be automatically transmitted in accordance with the state of the user.

[0048] The user associated information collecting and providing unit 31 manages a network state 33, a user profile 35 concerning the user, and a device profile 37 concerning the device, collects information from functional elements of various networks, and provides information to function elements of various services and networks. This is a function further expanded from the HSS 103 of the IMS 101 shown in Fig 2, and may be realized by being integrated with the mobility management unit 3 and expanding the function of the HSS 103 shown in Fig 2. The user profile 35 is made up of subscriber information 35-1, a user preference management function 35-2, and a user location management function 35-3. Information on the user's location can be acquired from information on access points from the mobility management unit 3, information on the speed of movement and information from GPS's mounted on RFID's in the periphery and the communication terminal.

[0049] The preference and interests of the user are managed in accordance with such a method that the user sets the user location, the speed of movement, the type of wireless access corresponding to the type of device used, the type of service, a method for roaming, a terminal to which media conversion is to be carried out, and a method for converting media in advance, or the history of use as described above on the network side is managed and the preference and interests of the user are guessed on the basis of the history and set.

[0050] The device profile 37 has terminal capability information 37-1 which includes the form of the terminal, the data conversion system, compatibility with animation, the size of the screen and the like, and terminal presence information 37-2 which includes the situation (location) of the terminal at the time. The device profile 37 is acquired when information is transmitted from the terminal so as to be automatically managed on the network side at the time registered by the user in advance, or when the terminal is connected to the network. In addition, in the case where the switching destination communication terminal is not registered, short distance communication is used, so that the terminal capability information on the switching destination communication terminal can be acquired so as to be included a terminal switching request signal and transmitted from the communication terminal, and thus registered in the device profile 37.

[0051] The device profile 37 and the user profile 35 are associated with information on the user's location and information on the owner of the device. Accordingly, in

Ex.1002 / Page 465 of 1173
Cisco Systems, Inc.

some cases, the user is associated with a public device which is not the user's own device, or a shared device.

[0052] Terminal capability information on terminal capability managed by the terminal capability management function 37-1 is information indicating the type, the attributes, the process, the IP address and the available bit rate of the terminal, the type of media and the type of codec, the size of the screen, the capability of the CPU, the connectable networks and the like. Terminal presence information managed by the terminal presence management function 37-2 indicates the type and state of the application currently running, information on the current terminal's location and the like. The network state 33 is acquired from information on the type of wireless access from the mobility management unit 3, information on QoS from the session control unit 5, information on the session state, information on the state of media conversion in the media converting unit and information on the state of the application currently running in the communication terminal. The terminal registered in the device profile manages not only the state of the network in the communication terminal but also the state of the network currently connected (transmission rate, wireless system, QoS and the like). Here, in the above description, indispensable configuration features are the network state 33, the subscriber information 35-1 and the terminal capability function 37-1.

[0053] Fig 3 is a diagram showing an example of a database for a network state, user profile and device profile. The database is managed through abstract descriptions using such a language as XML (extensible Markup Language), and information on the database is provided to the service shift control unit 21 (Fig 1; in the following, the figure number is omitted for description).

[0054] As shown in Fig 3, a network state 41, a user profile 43 and a device profile 45, for example, are associated with one another. The network state 41 is formed of a terminal (1) 41-1, a terminal (2) 41-2 and a terminal (3) 41-3. For the terminal (1) 41-1, for example, W-CDMA is described as the access method, multimedia is described as the QoS class, speech sound communication is described as the session state, file exchange is described, 10 Mbps is described as the bit rate, a base station 1 is described as the location and path information A-B-C... is described. In the user profile 43, subscriber information, preference, location information and the like are described, in terms of information on a user (1) 43-1 who is the owner of the terminal (1) 41-1, for example. In this case, it is also indicated that the owner of the terminal (2) 41-2 is also the user 1. In the device profile 45, the mobile communication terminal, the size of the screen, the clock number of the CPU, the codec, the access method, the IP address and the like, which are terminal capability information on the terminal (1) 41-1, are described. As the terminal presence information, information on longitude and latitude, information on the location, the speed of movement, the state of communication, the existence and type of application that has been started up and the like are described. As the information on the terminal (2) 41-2, it is described, as the terminal capability information, that the terminal is stationary, for example, and information on whether or not communication is possible is described as the terminal presence information. Thus, these pieces of information 41, 43 and 45 are associated with one another on the basis of the owner, the situation of communication, the location and the like.

[0055] When information on a certain user is requested from the service shift control unit 21, the terminal owned by the user and terminals in the vicinity of the user's location are associated with each other and provided in the service shift control unit 21 as a group of associated information.

[0056] In addition, the media control unit 7 corresponds to expanded MRF and MGCF/MGW 107 in the IMS 101. Media conversion of the bit rate, the codec, the size of the image, the media format and the like of the contents is controlled and carried out in response to the media conversion request from the session control unit 5. In the case where the media are converted after switching of the terminal, buffering is carried out in the unit, which allows for media conversion until the media are converted after resumption of the session. At this time, encoding is carried out again, and therefore, authentication function, for example, using an electronic watermark, may be added to the contents.

[0057] For the purpose of simplifying the description, these function elements of the communication network control system are shown as a single module in the respective figures. In reality, however, function elements as those described above are placed in the respective networks or the area in which the user roams by taking a case of roaming and a case where the receiver of communication is outside the same network into consideration, and thus, are not realized in one module. The description of the embodiment is simplified by regarding such use collectively as one process.

[0058] The communication terminals are also provided with a user interface formed of an image display apparatus, an input apparatus and the like (not shown), and a short distance communication unit using infrared rays, Bluetooth (registered trademark), a wireless communication system, such as UWB, which is expected to become prominent in the future, or wired communication, such as USB systems. The communication terminals have a function of requesting terminal switching, a function of making notification of a terminal ID, a function of reproducing the state of a session, a function of managing a session, a function of sending out the state of a session, a function of requesting and responding to calls, and a function of registering locations. The receiver of the communication may be an application server apparatus or a communication terminal.

[0059] Next, the procedure of switching terminals will be described with reference to Fig 4. Fig 1 is also referred to whenever necessary. First, the communication termi-

Ex.1002 / Page 466 of 1173
Cisco Systems, Inc.

nal 23 generates a terminal switching request signal, and at this time, it is necessary to designate to which terminal the connection is to be switched. Available methods include a method for communicating with a switching destination communication terminal 25 using short distance wireless communication to acquire terminal information on the switching destination communication terminal 25, and thus preparing a terminal switching request signal (C300), and a method according to which a user selects a switching destination communication terminal 25 in a state where the communication terminal 25 has acquired a switchable terminal list from the user associated information collecting and providing unit 31 so as to instruct preparation of a terminal switching request signal (C301). The terminal switching request signal may include the session state of the communication terminal 23, the state of the application and the like. Alternatively, the service shift control unit 21 may periodically exchange information with the user associated information collecting and providing unit 31 so as to determine whether or not the user environment is in such a state that the terminal should be switched (C301').

[0060] As an example of the state where the terminal should be switched, in cases where the state of the network in the communication terminal (#2) 25 is more stable than the state of the network in the communication terminal (#1) 23 according to information on the state of the network or in cases where the network in the communication terminal (#2) 25 is faster, the possibility that the terminal will be switched is high. Alternatively, the terminal can be switched in cases where it is determined that there are two terminals which can be used by the user in the current user's location using user preference information, information on the user's location and the terminal presence information, and what the user will use with priority in this location (determination from user preference information) is determined to be the switching destination terminal (#2) 25.

[0061] The service shift control unit 21 requests information on the user profile 35, the device profile 37 and the network state 33 from the user associated information collecting and providing unit 31, and acquires this. In the case where the terminal switching request signal in the C301 includes terminal information on the switching destination communication terminal, a task of registering the terminal information in the device profile 37 is also carried out (C302). Next, the service shift control unit 21 determines whether or not media conversion is necessary from the user profile 35, the device profile 37 and the network state 33 acquired from the user associated information collecting and providing unit 31 and the terminal switching request signal.

[0062] In the case where it is determined from the preference and tendencies of the user and the difference in capability between the communication terminal 23 and the switching destination communication terminal 25 that media conversion is necessary, the session control unit 5 is requested to ask whether or not media conversion is possible in the communication receiver 17 (C303). However, this procedure can be omitted in the case where the media conversion capability in the communication receiver is acquired when the user profile 35, device profile 37 and network state 31 are acquired.

[0063] The session control unit 5 makes inquiry about the media conversion capability to the communication receiver 17, acquires information on the media conversion capability, and makes notification of the information on the media conversion capability to the service shift control unit 21 (C304, C305, C306).

[0064] Upon receiving the information on the media conversion capability, the service shift control unit 21 selects media to which the media is to be converted and the content of the media conversion process and determines whether or not change in the session state is necessary from the information that has been acquired up to that point, and transmits a session switching request signal including these to the session control unit 5 (C307). The session control unit 5 instructs the mobility management unit 3 to set up a path (C308). When setting up of the path is completed, a response (ACK) is returned from the mobility management unit 3 (C309). When this path is set up, a call process is carried out in the case where the switching destination communication terminal 25 is not active. At this point in time, two paths between the communication receiver 17 and the communication terminal 23 and between the communication receiver 17 and the switching destination communication terminal 25 are set up. Thus, the settings are fine as they are in the case where it is possible to set up two paths simultaneously, for example in multicasting, while a process for suspending one of the two paths becomes necessary in the case where it is not possible to set up two paths.

[0065] Next, the session control unit 5 transmits a session switching preparation signal indicating that the preparations for switching the session are ready to the communication terminal 23, and the communication terminal 23 returns whether or not switching of the session is accepted (C310, C311). When the terminal is automatically switched from the network side, this becomes a message to confirm whether or not the connection may be switched to the communication terminal 23. The session control unit 5 requests interruption of the session to the communication receiver 17. When ACK is returned from the communication receiver 17, the session with the switching destination communication terminal 25 is established, and during this time, the switching destination communication terminal 25 starts up an application (C312 to C315).

[0066] The session control unit 5 follows the instruction to convert media included in the session switching request signal, and instructs the media control unit 7 or the communication receiver 17 to convert the media (C316, C317, C316', C317'). Subsequently, the session is resumed, and the session with the communication terminal is cut off (C318, C319, C320). At this time, the transmission path is also cut off by the mobility management unit

Ex.1002 / Page 467 of 1173
Cisco Systems, Inc.

3. Finally, a signal indicating the completion of switching of the session is transmitted from the session control unit 5 to the service shift control unit 21 (C321). As a result, communication between the communication receiver 17 and the switching destination terminal 25 can be started.

[0067] Next, one example of the configuration of a communication network control system according to a second embodiment of the present invention will be described. As shown in Fig 6, a communication network control system B according to the present embodiment basically has the same configuration as that shown in Fig 1, except that there is only one communication terminal 22 and an access method (1) 22-1 and an access method (2) 22-2 are switched. Here, essential constituent features in a user associated information collecting and providing unit 31 shown in Fig 6 are a network state 33, subscriber information 35-1, user location management function 35-3 and terminal capability management function 37-1.

[0068] Fig 5 is a diagram showing the procedure for switching in the access method in the same terminal. Though so far, the procedure for switching between the communication terminal (#1) 23 and the switching destination communication terminal (#2) 25 has been described with reference to Figs 1 and 4, Fig 5 shows the procedure for switching paths and sessions between an access method 1 and an access method 2. Assume that the communication terminal 22 is provided with two access methods: the access method 1 based on mobile communication means of, for example, W-CDMA, and an access method 2 based on wireless communication means for high speed communication in hot spots, such as wireless LAN. Different access methods are shown for the access method 1 (22-1) and the access method 2 (22-2).

[0069] What type of access method the communication terminal 22 has is managed by the terminal capability management function 37-1 in the user associated information collecting and providing unit 31. The network state 33 in the user associated information collecting and providing unit 31 manages the path for the access method 1 (22-1), the path for the access method 2 (22-2) and the state of the respective networks, and provides QoS, the transmission rate and the type of the wireless access system to the service shift control unit 21.

[0070] There is a possibility that the operation system for management and control, for example, a multimedia subsystem or mobility management, may be different between the access method 1 (22-1) and the access method 2 (22-2). The user associated information collecting and providing unit 31 is operated by a third party company which is different from the network operator, and may play a role of providing information to the service shift control unit 21 by collecting information from the network operator. In addition, one network operator may manage all of the user associated information collecting and providing unit 31, the service shift control unit 21 and the different access methods. Therefore, it is desirable for the interface between the user associated information collecting and providing unit 31 and the respective nodes in the network to be standardized. The user location management function 35-3 in the user profile is used in the case where the available access method is set up on the basis of the user's location. For example, the location of a hot spot and the user's location are associated with each other, so that information showing that the user is within the service range of the hot spot is managed. Also, the location of a terminal may be specified using terminal presence management information to manage the terminal so as to be located in the service range of the hot spot.

[0071] Switching of terminals has been described in the description of the procedure in Fig 4, and change in the path in the same terminal is described with reference to Fig 6. It is possible to use the same basic flow. However, the above-described terminal switching request signal is changed to a path switching request signal. Though the terminal switching request signal includes the capability of the switching destination communication terminal, this information is not required in the case where the connection is switched within the same terminal. The path switching request signal includes the access method in a switching destination path, the situation of radio waves in the switching destination path, the routing address in the switching destination path, the domain name in the switching destination path, the bit rate of the switching destination path and the like (C401).

[0072] In addition, as shown in Fig 4, it is possible to automatically change the path from the network side, and in this case, the user associated in formation collecting and providing unit 31 and the service shift control unit 21 determine switching (C401'). The determination on the switching is made on the basis of the information provided mainly from the state of the network and the terminal presence management function. Switching is instructed when, for example, the communication terminal can use the two access methods and a higher bit rate than in the access method currently used is detected in the communication using the other access method. In the case where media conversion is necessary in accordance with the bit rate and QoS, the procedure for media conversion is carried out. However, the media are converted in the same terminal, and therefore, conversion due to the difference in the type of terminal and the attributes is not necessary, unlike in the case of Fig 4. It is possible to omit the process for interrupting the session when the media are not converted, and a process for starting up an application is also not necessary. For example, in the case where it is not necessary to change information on the session at all, the access method is sometimes switched only by instructing the mobility management unit to change the path. This instruction is prepared in the service shift control unit, and a session switching request signal including concrete instructions is transmitted. As a result, the access method can be smoothly changed in the same terminal.

[0073] According to the embodiment of the present in-

Ex.1002 / Page 468 of 1173
Cisco Systems, Inc.

vention, the user can easily switch the communication terminal used through a simple button operation or the like when switching is required in accordance with the change in his or her own situation. Thus, the effort required for operation and loss of time can be greatly reduced in comparison with the prior art, and service can be enjoyed at a higher level.

[0074] There is also an advantage in the server apparatus on the distribution side, such that distribution service can be continued without providing any new particular function. Additionally, the data format is optimized in accordance with individual communication terminals before transmission, even when the capability is different between the communication terminals on the receiver side. For this reason, there is an advantage, such that a large burden is not imposed on the communication side and the server apparatus side. In this manner, the basis for providing a service is shared, and thus, the user is not aware of the difference in wireless and wire networks and service or the difference in the type of communication terminal, unlike in the prior art, and it becomes possible to enjoy a seamless and ubiquitous service environment.

Industrial Applicability

[0075] The present invention can be used in switching of terminals themselves or communication systems in terminals.

Claims

1. A communication network control system for controlling continuous communication between a first communication terminal and a third communication terminal in such a manner that a second communication terminal is switched to the third communication terminal which is different from the second communication terminal without interrupting communication between the first communication terminal and the second communication terminal which is communicating with the first communication terminal, comprising:

   mobility management means for setting up and managing a physical and logical transmission path between communication terminals;
   session control means for controlling a session between communication terminals along the transmission path;
   service shift control means for instructing the session control means to switch the session; and
   user associated information collecting and providing means for collecting user associated information which is used when the session is switched and includes at least one of a network state, a user profile concerning a user and a device profile concerning a device, and providing the user associated information to the service shift control means.

2. The communication network control system according to Claim 1, **characterized in that**
   the service shift control means receives a terminal switching request signal from the second communication terminal or determines whether or not the terminal is switched on the basis of the user associated information, to thereby generate a session switching request signal; and
   the session control means has a function of receiving the session switching request signal to interrupt the session, a function of instructing the mobility management means to set up a transmission path with the third communication terminal, a function of establishing a session with the third communication path, and a function of resuming the session with a communication receiver after establishing the session.

3. The communication network control system according to Claim 1 or 2, **characterized in that** the user profile includes at least one of subscriber information of the user, user location information and taste and tendencies of the user, and the device profile includes at least one of the type of the device and information on the state of each device.

4. The communication network system according to Claim 1 or 2, **characterized in that** the service shift control means instructs the session control means to request switching of the session on the basis of information from the user associated information collecting and providing means or the terminal switching request from the second communication terminal.

5. The communication network control system according to Claim 1 of 2, **characterized in that** the user associated information collecting and providing means provides associated information on the basis of owner information and location information when the service shift control means requests provision of information on the user.

6. The communication network control system according to Claim 5, **characterized in that** a communication terminal switching process which is carried out mainly by the network is started up on the basis of information on the network state between the second communication terminal and the third communication terminal, and on the terminal capability provided from the user associated information collecting and providing means.

7. The communication network control system according to Claim 1 or 2, **characterized by** further com-

Ex.1002 / Page 469 of 1173
Cisco Systems, Inc.

prising media conversion means on the network, wherein
the service shift control means generates information in terms of an instruction concerning media, and sends the information to the session control means together with a session switching request.

8. The communication network control system according to Claim 7, **characterized in that** whether or not a process for converting the media is carried out is determined on the basis of the terminal capability between the second communication terminal and aid third communication terminal and the network state.

9. The communication network control system according to Claim 7, **characterized in that** instructions in terms of media to which the media is to be converted and a method for the media conversion process determined on the basis of user preference.

10. The communication network control system according to Claim 7, **characterized in that** the media to which the media is to be converted are determined on the basis of the media conversion capability of the communication receiver and the conversion capability of the media conversion means on the network.

11. The communication network control system according to Claim 10, **characterized in that** the service shift control means generates information for instructing the network which is connected to the first communication terminal to request acquirement of the media conversion capability.

12. The communication network control system according to Claim 1 or 2, **characterized in that** the second communication terminal designates a switching destination communication terminal and sends the information to the network together with a terminal switching request.

13. The communication network control system according to Claim 12, **characterized in that** at least one of the terminal capability of the third communication terminal and terminal presence information which are acquired in advance through the exchange of information with the third communication terminal through short distance communication is included in the terminal switching request.

14. The communication network control system according to Claim 12, **characterized in that** information for instructing media to which the media is to be converted and the method for the media conversion process is provided together with a terminal switching request.

15. A communication network control system for controlling continuous communication by switching at least one access method according to which a second communication terminal having a number of access methods communicates with a first communication terminal to another access method according to which there is no communication between the first communication terminal and the second communication terminal without interrupting the communication, comprising:

mobility management means for setting up and managing a physical and logical transmission path between communication terminals;
session control means for controlling a session between communication terminals along the transmission path;
service shift control means for instructing the session control means to switch the session; and
user associated information collecting and providing means for collecting and providing user associated information which includes at least one of a network state, a user profile concerning a user and a device profile concerning a device, wherein
the service shift control means generates a session switching request signal and instructs the session control means on the basis of information from the user related information collecting and providing means or an access method switching request signal from a communication terminal.

16. The communication network control system according to Claim 15, **characterized in that** the user associated information collecting and providing means provides associated information to the service shift control means on the basis of owner information and location information when the service shift control means requests provision of information on the user.

17. The communication network control system according to Claim 15, **characterized in that** starting up of a process for switching the access method carried out mainly by the network is determined on the basis of at least one of the presence information on the communication terminal and the network state.

18. The communication network control system according to Claim 17, **characterized in that** the access method which is mainly carried out by the network is switched on the basis of user location information and user preference.

19. The communication network control system according to Claim 15, **characterized by** further comprising media conversion means within the network, where-

Ex.1002 / Page 470 of 1173
Cisco Systems, Inc.

in information instructed by the service shift control means in terms of media to which the media is to be converted and the method for the media conversion process is generated in the media conversion means.

20. The communication network control system according to Claim 19, **characterized in that** the method for the media conversion process is determined on the basis of the state of the network according to a current access method and an access method to which the access method is to be switched.

21. The communication network control system according to Claim 20, **characterized in that** instruction in terms of media to which the media is to be converted and the method for the media conversion process is made on the basis of the user preference.

22. The communication network control system according to Claim 21, **characterized in that** the media to which the media is to be converted is determined on the basis of at least one of the media conversion capability of a communication receiver and the conversion capability of the media conversion means of the network.

23. The communication network control system according to Claim 22, **characterized in that** the service shift control means instructs the network of the communication receiver to request the acquisition of the media conversion capability.

24. The communication network control system according to Claim 15, **characterized in that** the second communication terminal designates the access method to which the access method is to be switched and includes the information in the access method switching request signal to be transmitted to the network.

25. The communication network control system according to Claim 24, **characterized by** including at least one of the media to which the media is to be converted and instruction information of the method for the media conversion process in the access method switching request.

26. A communication network control method, comprising the steps of:

collecting user associated information which includes at least one of a network state, a user profile concerning a user and a device profile concerning a device, the user associated information being used when a session is switched in a state where a physical and logical transmission path is set up between a first communication terminal and a second communication terminal which is communicating with the first communication terminal; and

in the case where a session is instructed to be switched between communication terminals along the transmission path, switching the session for continuous communication between the first communication terminal and a third communication terminal by switching the second communication terminal to the third communication terminal which is different from the second communication terminal without interrupting communication between the first communication terminal and the second communication terminal on the basis of the collected user associated information in accordance with an instruction to switch the session.

27. The communication network control method according to Claim 26, **characterized by** comprising the step of providing associated information on the basis of owner information and location information when information concerning the user is requested.

28. The communication network control method according to Claim 26, **characterized in that** switching of the terminal carried out mainly by the network is started up on the basis of at least one of the network state between the second communication terminal and the third communication terminal and the terminal capability information.

29. The communication network control method according to Claim 26, **characterized by** the step of generating information which indicates the media to which the media is to be converted and the method for the media conversion process, as well as in that the session concerning the switching of the session is indicated on the basis of the infonnation.

30. The communication network control method according to Claim 29, **characterized in that** the media to which the media is to be converted is determined on the basis of the media conversion capability of a communication receiver and the conversion capability of media conversion means of the network.

31. The communication network control method according to Claim 30, **characterized by** comprising the step of generating information for instructing the network of the communication receiver to request acquisition of the media conversion capability.

32. A communication network control method, comprising the steps of:

collecting user associated information which includes at least one of a network state, a user

Ex.1002 / Page 471 of 1173
Cisco Systems, Inc.

profile concerning a user and a device profile concerning a device, the user associated information being used when a session is switched in a state where a physical and logical transmission path is set up between a first communication terminal and a second communication terminal having a number of access methods, which communicates with the first communication terminal; and

in the case where a session is instructed to be switched between the communication terminals along the transmission path, switching the session for continuous communication by switching an access method in the second communication terminal without interrupting the communication between the first.

communication terminal and the second communication terminal on the basis of the collected user associated information in accordance with an instruction to switch the session.

33. The communication network control method according to Claim 32, **characterized by** comprising the step of providing associated information on the basis of owner information and location information of the communication terminals when information concerning the user is requested.

34. The communication network control method according to Claim 32, **characterized in that** starting up of a process for switching the access method which is carried out mainly by the network is determined on the basis of at least one of the presence information of the communication terminals and the network state.

35. The communication network control method according to Claim 32, **characterized by** the step of generating information which indicates the media to which the media is to be converted and the method for the media conversion process, as well as in that the session concerning the switching of the session is indicated on the basis of the information.

36. The communication network control method according to Claim 35, **characterized in that** the media to which the media is to be converted is determined on the basis of the media conversion capability of a communication receiver and the conversion capability of media conversion means of the network.

37. The communication network control method according to Claim 36, **characterized by** comprising the step of generating information for instructing the network of the communication receiver to request acquisition of the media conversion capability.

38. A communication terminal for use in a communication network control system comprising: mobility management means for setting up and managing a physical and logical transmission path between communication terminals; session control means for controlling a session between communication terminals along the transmission path; service shift control means for instructing the session control means to switch the session; and user associated information collecting and providing means for collecting user associated information which is used when the session is switched and includes at least one of a network state, a user profile concerning a user and a device profile concerning a device, and providing the user associated information to the service shift control means, **characterized in that**
the service shift control means is requested to switch the terminal, and the communication terminal designates a switching destination communication terminal and includes the information in the terminal switching request to be transmitted to the network.

39. The communication terminal according to Claim 38, **characterized in that** the communication terminal exchanges information with the switching destination communication terminal in advance through short distance communication, and the terminal capability of a switching destination and the terminal presence information are included in the terminal switching request.

40. The communication terminal according to claim 38, **characterized in that** the media to which the media is to be converted and the instruction information of a method for a media conversion process are included in the terminal switching request.

41. A second communication terminal having a number of access methods, which communicates with a first communication terminal and controls continuous communication between the first communication terminal and the second communication terminal by switching at least one access method according to which the second communication terminal communicates with the first communication terminal to another access method according to which there is no communication without interrupting the communication in a communication network control system comprising: mobility management means for setting up and managing a physical and logical transmission path between communication terminals; session control means for controlling a session between communication terminals along the transmission path; service shift control means for instructing the session control means to switch the session; and user associated information collecting and providing means for collecting user associated information which is used when the session is switched and in-

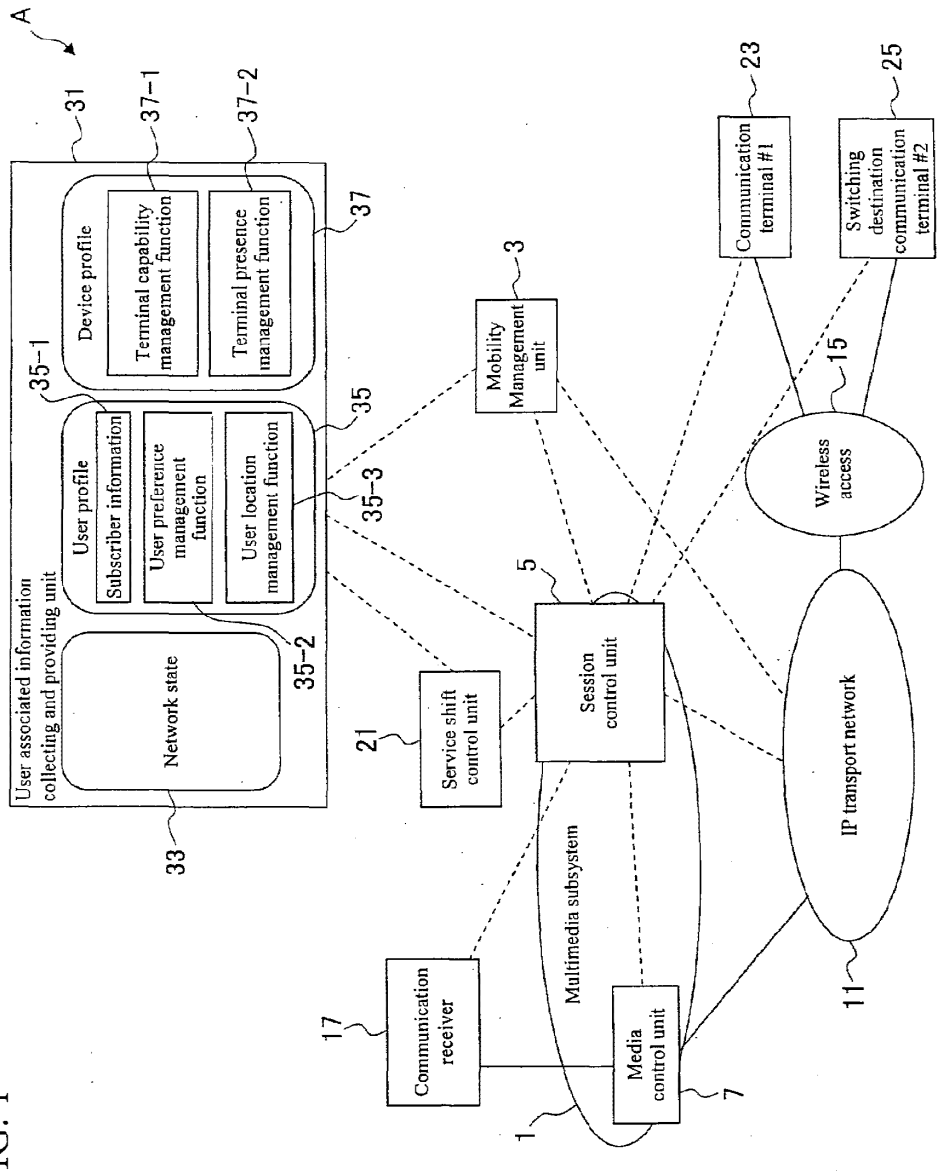
Ex.1002 / Page 472 of 1173
Cisco Systems, Inc.

cludes at least one of a network state, a user profile concerning a user and a device profile concerning a device, and providing the user associated information to the service shift control means, **characterized in that** the second communication terminal designates the access method to which the access method is to be switched and includes the information in an access method switching request signal to be transmitted to the network.

42. The second communication terminal according to Claim 41, **characterized in that** at least one of the media to which media is to be converted and the instruction information of the method for the media conversion process is included in the access method switching request.

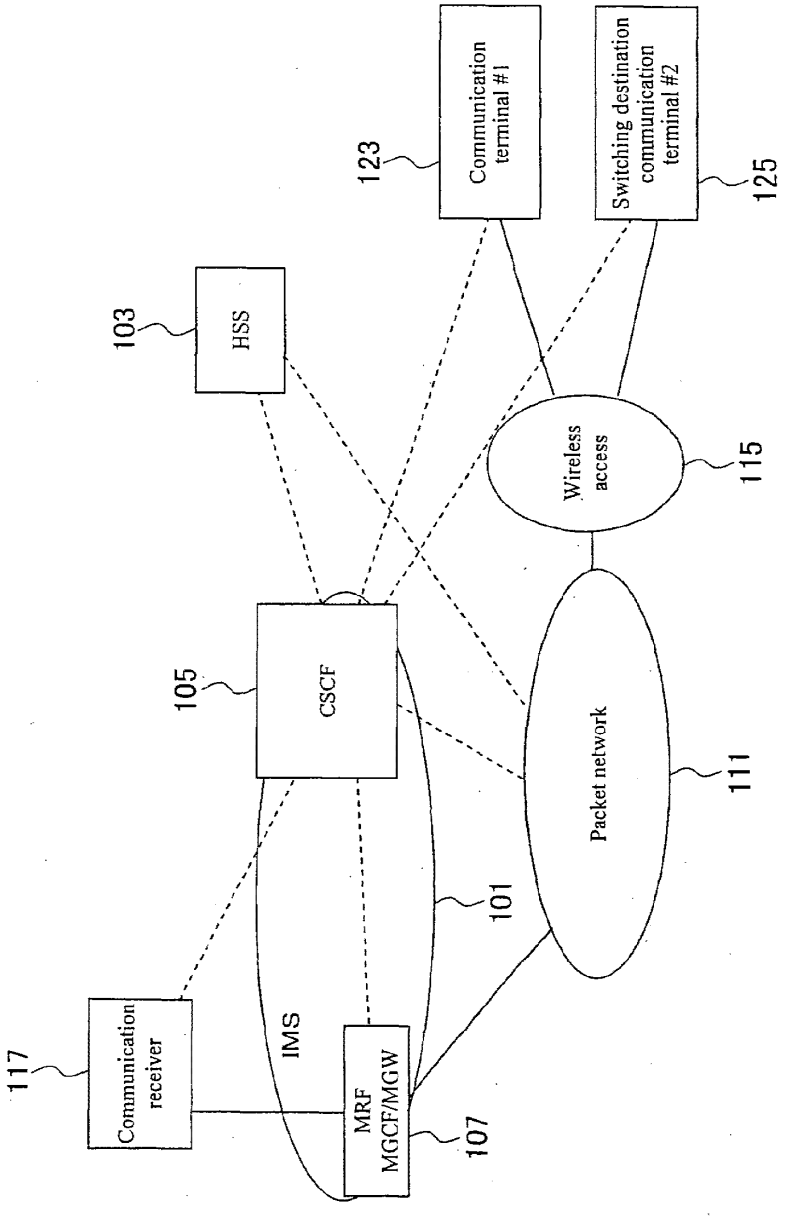
Ex.1002 / Page 473 of 1173
Cisco Systems, Inc.

FIG. 1



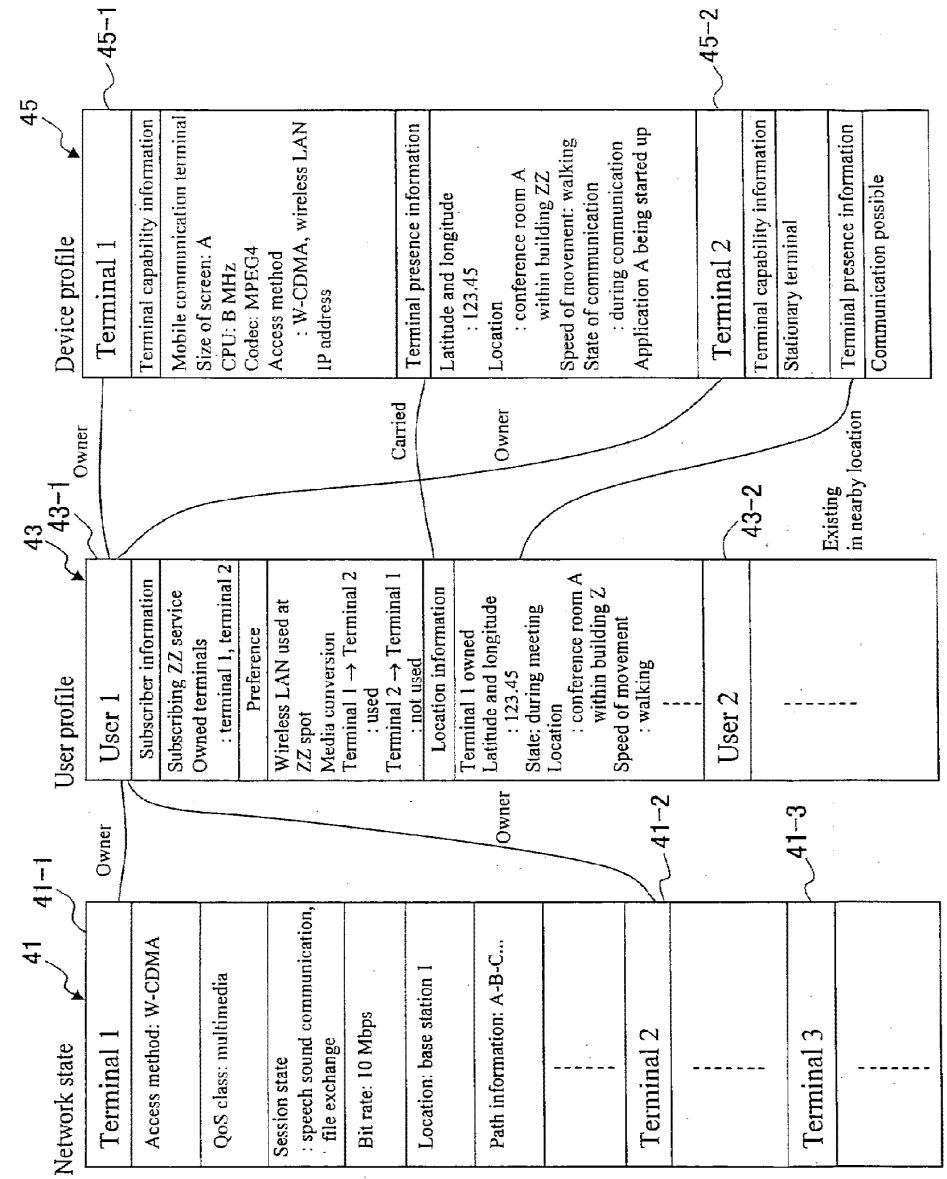
Ex.1002 / Page 474 of 1173
Cisco Systems, Inc.

FIG. 2



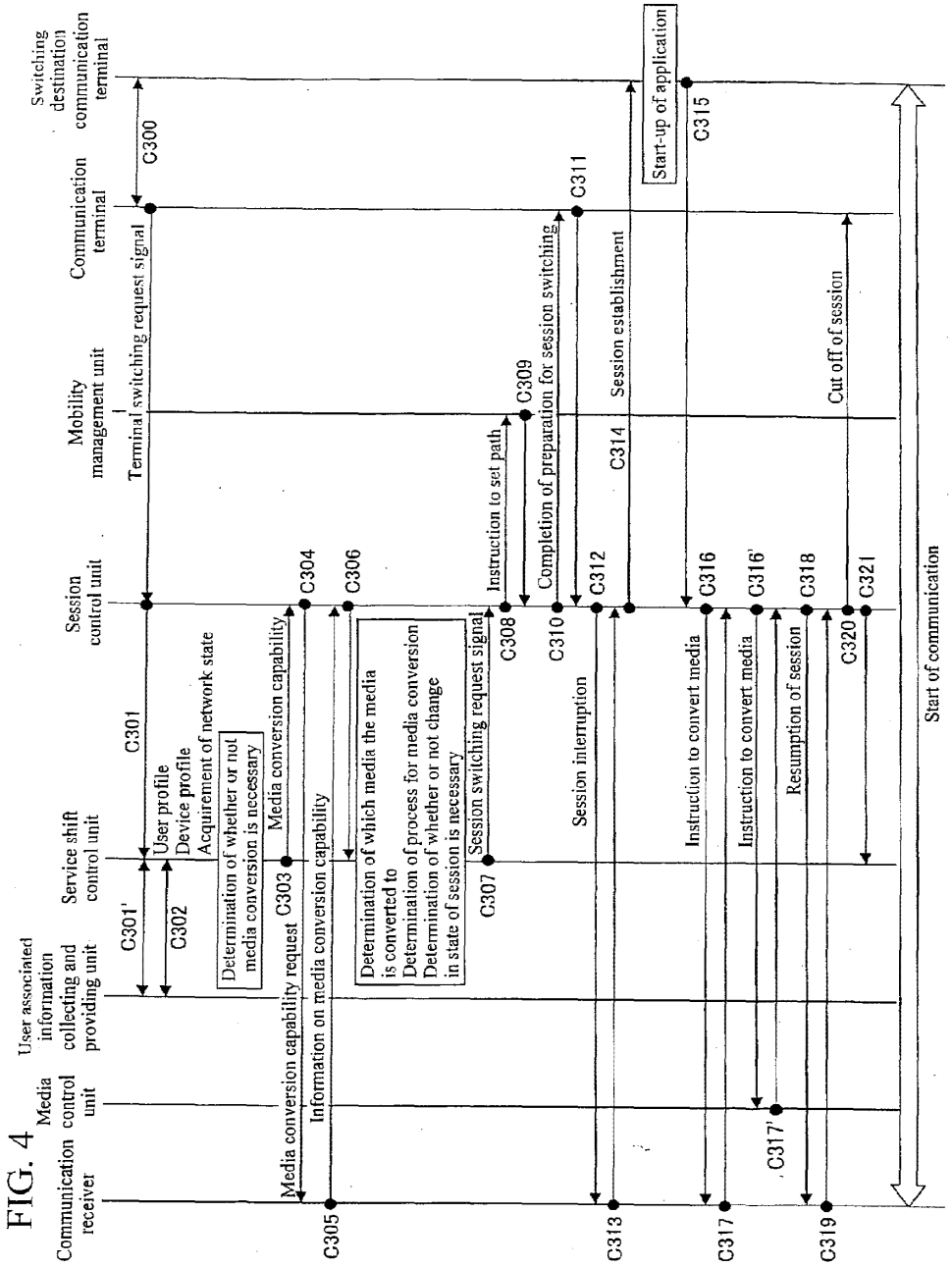
Ex.1002 / Page 475 of 1173
Cisco Systems, Inc.

FIG. 3



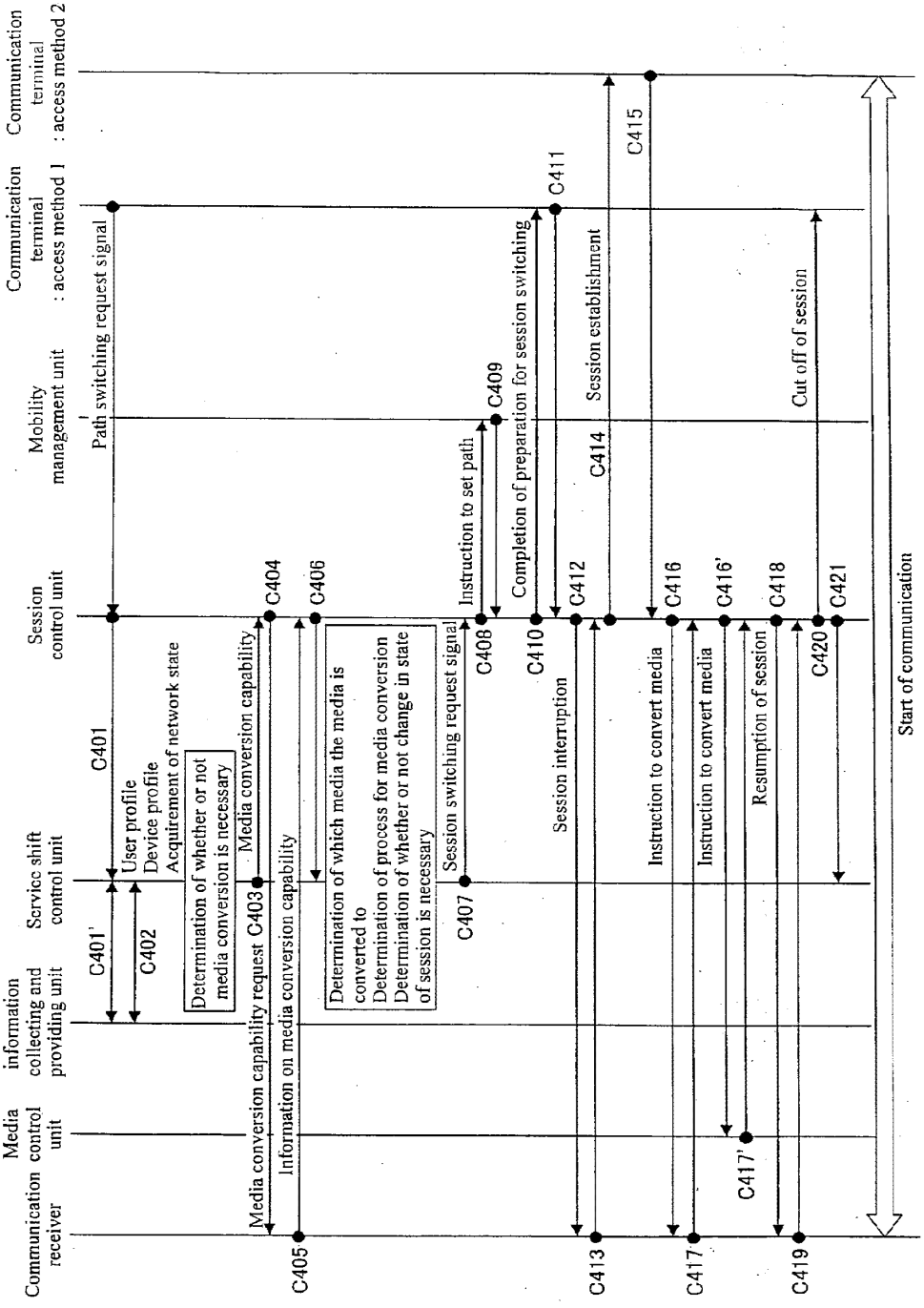
Ex.1002 / Page 476 of 1173
Cisco Systems, Inc.

FIG. 4



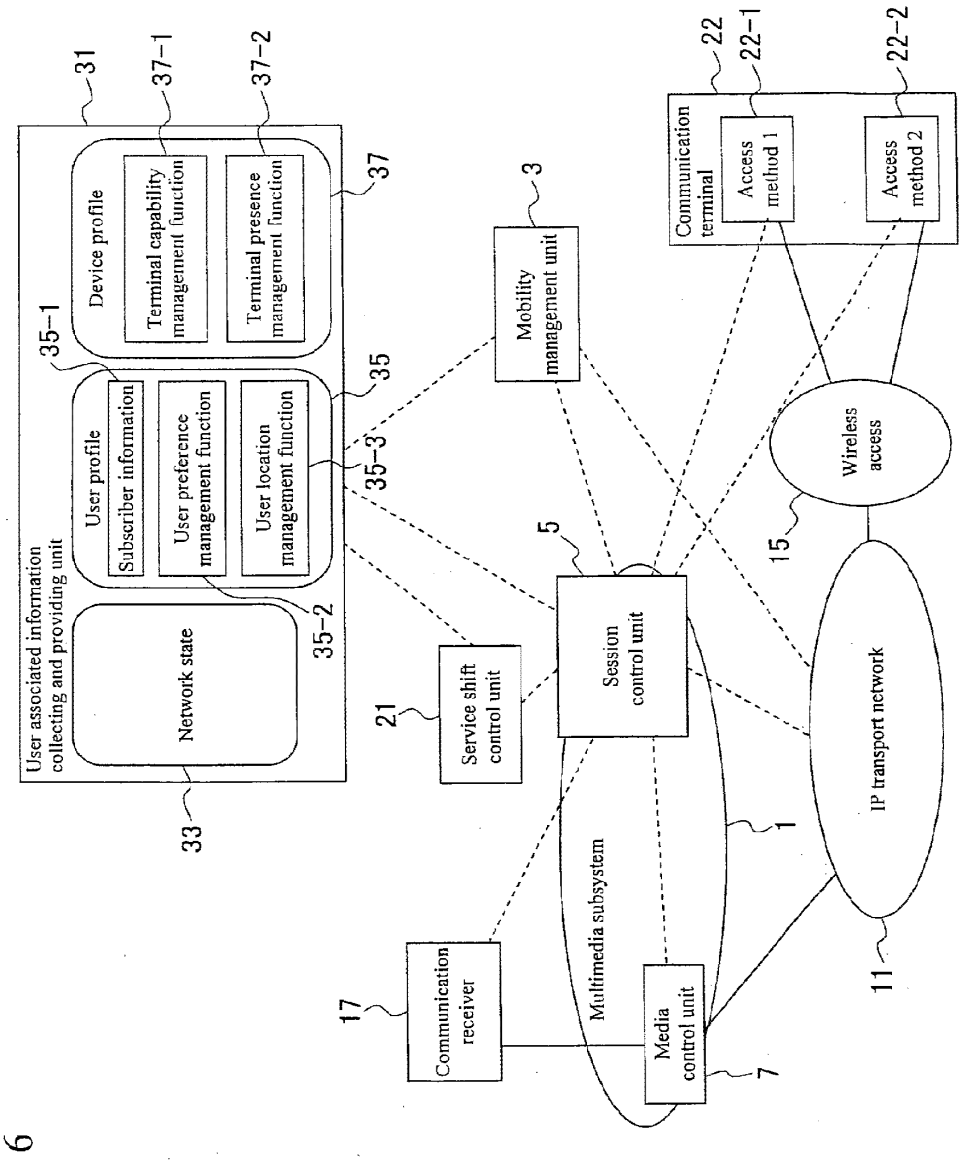
Ex.1002 / Page 477 of 1173
Cisco Systems, Inc.

FIG. 5



Ex.1002 / Page 478 of 1173
Cisco Systems, Inc.

FIG. 6



Ex.1002 / Page 479 of 1173
Cisco Systems, Inc.

FIG. 7

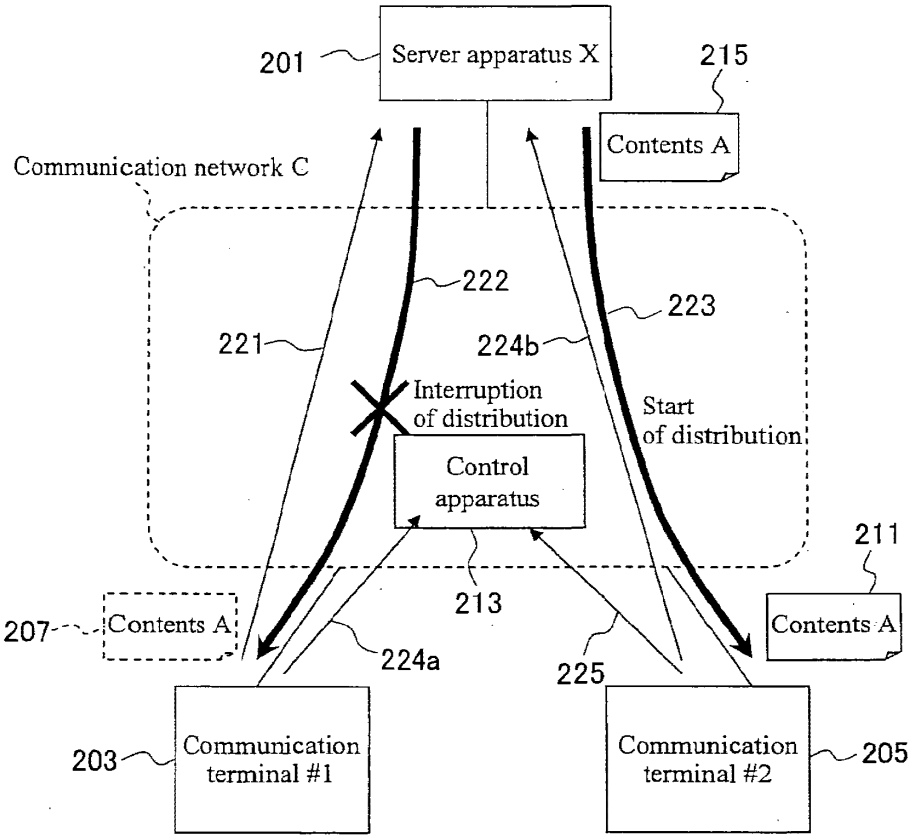
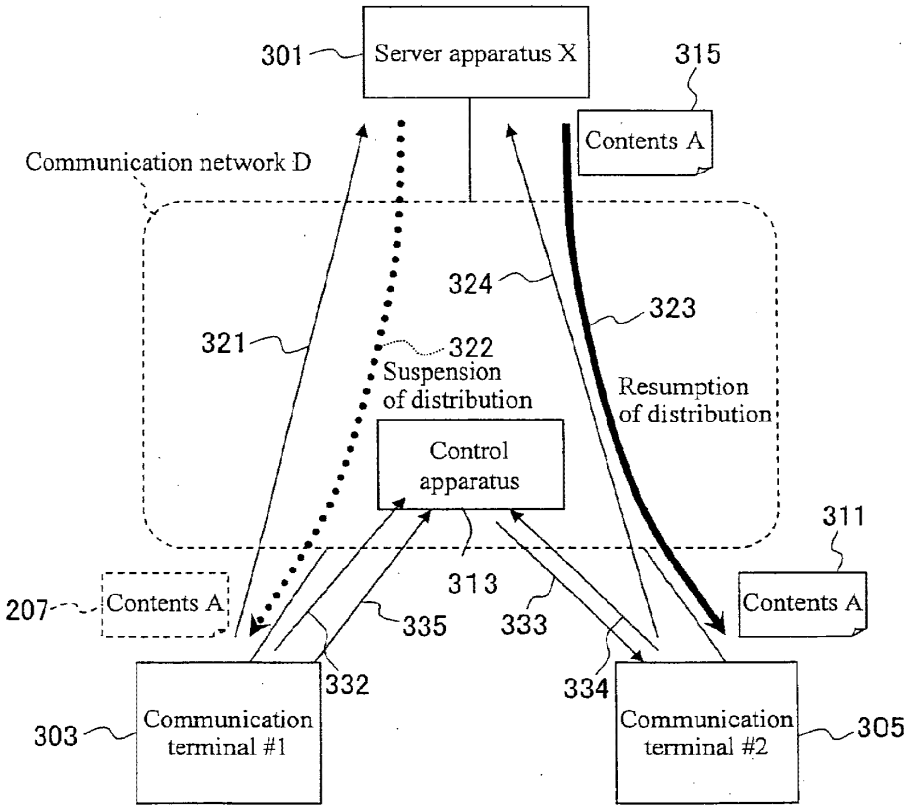

201
Server apparatus X
215
Contents A
Communication network C
222
223
221
224b
Interruption of distribution
Start of distribution
Control apparatus
211
213
207
Contents A
224a
225
Contents A
203
Communication terminal #1
Communication terminal #2
205

FIG. 8


301
Server apparatus X
315
Contents A
Communication network D
324
323
321
322
Suspension of distribution
Resumption of distribution
Control apparatus
311
313
207
Contents A
335
333
Contents A
332
334
303
Communication terminal #1
Communication terminal #2
305

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2006/300324

A. CLASSIFICATION OF SUBJECT MATTER
H04L12/56(2006.01), ***H04Q7/38***(2006.01)

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)
H04L12/56(2006.01), ***H04Q7/38***(2006.01)

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

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2006
Kokai Jitsuyo Shinan Koho	1971-2006	Toroku Jitsuyo Shinan Koho	1994-2006

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.
X Y	Takayuki WARABINO et al., "Tanmatsukan no Seamless na Kirikae o Jitsugen suru Device Hand-off Hoshiki no Teian", Information Processing Society of Japan Kenkyu Hokoku 2003-MBL-27-15, 14 November, 2003 (14.11.03), page 107, left column, line 22 to page 108, left column, line 23; page 109, left column, lines 8 to 18	1-14,26-31, 38-40 15-25,32-37, 41,42
X Y	Masatoshi KAWARAZAKI et al., "Meta Data o Riyo shita Contents Hand-over System -MetaPORT-, IEICE Technical Report IN2003-3, 09 May, 2003 (09.05.03), page 14, left column, line 9 to page 15, left column, line 8; page 15, right column, line 6 to page 17, left column, line 7	1-12,14, 26-31,38,40 15-25,32-37, 41,42

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
09 March, 2006 (09.03.06)	20 March, 2006 (20.03.06)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (April 2005)

Ex.1002 / Page 482 of 1173
Cisco Systems, Inc.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2006/300324

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	JP 2004-336310 A (Nippon Telegraph And Telephone Corp.), 25 November, 2004 (25.11.04), Par. Nos. [0009] to [0010], [0016], [0018], [0024] (Family: none)	1-6,12, 26-28,38 15-18,24, 32-34,41
Y	JP 2004-208001 A (Sharp Corp.), 22 July, 2004 (22.07.04), Abstract; Fig. 2 & WO 2004/062310 A1 & EP 1585354 A1	15-25,32-37, 41,42

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

REFERENCES CITED IN THE DESCRIPTION

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

Non-patent literature cited in the description

- **YABUSAKI et al.** All-IP Conversion in Mobile Network, Special Issue. *NTT DoCoMo Technical Journal,* January 2003, vol. 10 (4), 6-34 **[0015]**

Ex.1002 / Page 484 of 1173
Cisco Systems, Inc.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 988 698 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
05.11.2008 Bulletin 2008/45

(21) Application number: **07107248.2**

(22) Date of filing: **30.04.2007**

(51) Int Cl.:
H04M 7/12 *(2006.01)* ***H04L 29/06*** *(2006.01)*
H04M 1/253 *(2006.01)* ***H04M 1/725*** *(2006.01)*

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC MT NL PL PT RO SE SI SK TR
Designated Extension States:
AL BA HR MK RS

(71) Applicant: **Research In Motion Limited**
Waterloo, Ontario N2L 3W8 (CA)

(72) Inventors:
- **Buckley, Adrian**
  Tracy, CA 95376 (US)
- **Luu, Lap**
  Markham, Ontario L6C 2X7 (CA)
- **Allen, Andrew**
  Mundelein, IL 60060 (US)
- **George, Richard**
  Waterloo, Ontario N2T 2S3 (CA)
- **Oliver, Brian**
  Ontario N1M 1C8 (CA)
- **Lee, Dalsu**
  Thornhill, Ontario L4J 7Y8 (CA)

(74) Representative: **Roberts, Gwilym Vaughan et al**
Kilburn & Strode
20 Red Lion Street
London WC1R 4PJ (GB)

Remarks:
Amended claims in accordance with Rule 137(2) EPC.

(54) Hybrid IMS-GSM system and method for establishing an outgoing GSM call as an enterprise call

(57) The application relates to systems based upon Voice-over-IP and Session Initiation Protocol-based signaling systems that utilize the existing enterprise IP infrastructure. Mobile communication devices are being enhanced to provide SIP-based communications (including VoIP) over WLAN access as well as cellular networks, thereby allowing these devices to provide mobile telephony communications capability when within the enterprise as well as when away from the enterprise. However, these networks cannot currently commercially support carrier-class VoIP telephony services. In addition, enterprise calls shall be integrated with the IMS network architecture. This is achieved by the present invention in that instead of a VoIP call, a circuit-switched call is established. In particular, a network node (404) is operable, responsive to receiving (408) a SIP INVITE request from an enterprise user (118) to initiate origination of an outgoing cellular call to a called party (120), for establishing (418) a first call leg to the enterprise user (118) by sending a circuit-switched call that identifies an enterprise address of the enterprise user (118) as a calling line identity. The network node (404) includes functionality for establishing (430) a second call leg to the called party (120). The first and second call legs are then patched to establish an end-to-end communications path between the enterprise user (118) and the called party (120), wherein the enterprise address instead of the non-enterprise address is presented to the called party (120) as a calling line identity with respect to the outgoing cellular call from the enterprise user (118).

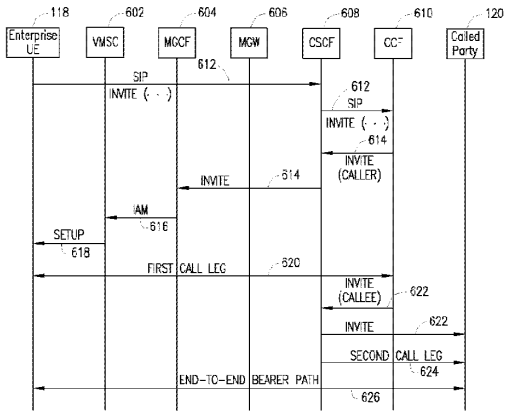


FIG. 6

EP 1 988 698 A1

Description

CROSS-REFERECE TO RELATED APPLICATION(S)

[0001] This application discloses subject matter that is related to the subject matter of the following U.S. patent application(s): (i) "SYSTEM AND METHOD FOR PRESENTING MEDIA TO MULTIPLE PARTIES IN A SIP ENVIRONMENT" (Docket No. 30761-2-US-PAT), Application No.:_____, filed even date herewith, in the name(s) of Andrew Allen, Adrian Buckley, Richard George, Brian Oliver, Lap Luu and Dalsu Lee; and (ii) "SYSTEM AND METHOD FOR INTEGRATING AN OUTGOING CELLULAR CALL AS AN ENTERPRISE CALL" (Docket No. 30761-US-PAT), Application No.:_____, filed even date herewith, in the name(s) of Andrew Allen, Adrian Buckley, Richard George, Brian Oliver, Lap Luu and Dalsu Lee, which is (are) hereby incorporated by reference.

FIELD OF THE DISCLOSURE

[0002] The present patent disclosure generally relates to communications networks. More particularly, and not by way of any limitation, the present patent disclosure is directed to a system and method for integrating an outgoing cellular call as an enterprise call in an IP Multimedia Subsystem (IMS) network environment.

BACKGROUND

[0003] Many enterprise networks are replacing their existing Private Branch Exchange (PBX)- and Central Office Exchange (CENTREX)-based telephony systems with systems based upon Voice-over-IP (VoIP) and Session Initiation Protocol (SIP)-based signaling systems that utilize the existing enterprise IP infrastructure, e.g., Local Area Network (LAN) and Wireless LAN (WLAN) technologies. It is not uncommon for enterprise employees to regularly use mobile communications devices when away from the enterprise, which interoperate with cellular networks such as, e.g., the Global System for Mobile Communications (GSM) networks, Code Division Multiple Access (CDMA) networks, and Universal Mobile Telecommunications System (UMTS) networks, to keep in touch with other employees of the enterprise and to conduct business communications with other people outside the enterprise. Additionally, mobile communications devices are being enhanced to provide SIP-based communications (including VoIP) over WLAN access as well as cellular networks, thereby allowing these devices to provide mobile telephony communications capability when within the enterprise as well as when away from the enterprise. It is expected that such developments may allow replacement of the ubiquitous wired desktop phone in the enterprise with dual-mode, WLAN-capable mobile devices.

[0004] Although cellular telephony networks have deployed IP-based data communications capabilities through exploitation of well-known technologies, it is generally understood that these networks cannot currently commercially support carrier-class VoIP telephony services due to issues of delay, Quality of Service (QoS) and efficiency, which prevent cost-effective usage of such networks for purposes of providing acceptable quality voice services. Accordingly, for the foreseeable future, telephony services based upon the existing network infrastructure are likely to continue to utilize conventional circuit-switched network technology for telephony calls.

[0005] Based on the foregoing, it should appreciated that the integration of VoIP enterprise networks with carrier cellular telephony networks in order to serve an enterprise user within the enterprise as well as while away is fraught with numerous difficulties. Moreover, in such scenarios it may be desirable for enterprises to have certain control over the calls made by their employees for tracking and monitoring purposes. In addition, it would be desirable to provide value-added enterprise call integration services within the context of ongoing development of current 3rd Generation Partnership Project (3GPP) standards which specify an Internet Protocol (IP)-based core network architecture referred to as the IP Multimedia Subsystem (IMS).

SUMMARY

[0006] The present patent disclosure is broadly directed to a scheme for integrating an outgoing cellular call as an enterprise call within an IMS environment wherein an enterprise user's enterprise address is presented to the called party instead of the enterprise user's non-enterprise address (e.g., cellular telephony number). In one aspect, disclosed herein is an embodiment of a method for integrating an outgoing cellular call as an enterprise call in an IMS environment, wherein the outgoing cellular call is originated by an enterprise user towards a called party, the enterprise user having an enterprise address and a non-enterprise address. The claimed embodiment comprises one or more of the following: receiving a SIP INVITE request from the enterprise user for initiating the outgoing cellular call to the called party; establishing a first call leg to the enterprise user, e.g., by providing a SIP INVITE message back to the enterprise user; establishing a second call leg to the called party; and patching the first and second call legs to establish an end-to-end communications path between the enterprise user and the called party, wherein the enterprise address is presented

Ex.1002 / Page 486 of 1173
Cisco Systems, Inc.

instead of the non-enterprise address to the called party as a calling line identity with respect to the outgoing cellular call from the enterprise user.

[0007] In another aspect, disclosed herein is an embodiment of an IMS network node for integrating an outgoing cellular call as an enterprise call, wherein the outgoing cellular call is originated by an enterprise user towards a called party, the enterprise user having an enterprise address and a non-enterprise address. The claimed embodiment comprises one or more of the following: means for receiving a SIP INVITE request from the enterprise user for initiating the outgoing cellular call to the called party; means for establishing a first call leg to the enterprise user; means for establishing a second call leg to the called party; and means for patching the first and second call legs to establish an end-to-end communications path between the enterprise user and the called party, wherein the enterprise address is presented instead of the non-enterprise address to the called party as a calling line identity with respect to the outgoing cellular call from the enterprise user.

[0008] In a further aspect, disclosed herein is an embodiment of an IMS-capable user equipment (UE) device operable to generate an outgoing cellular call as an enterprise call to a called party. The claimed embodiment comprises one or more of the following: means for generating a SIP INVITE request with respect to initiating an outgoing cellular call to a called party, the SIP INVITE request being directed to an IMS network node; and means for establishing a call leg with the IMS network node responsive to receiving a SIP INVITE message back from the IMS network node.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] A more complete understanding of the embodiments of the present patent disclosure may be had by reference to the following Detailed Description when taken in conjunction with the accompanying drawings wherein:

[0010] FIG. 1 depicts an exemplary network environment wherein one or more embodiments of the present patent disclosure may be practiced for purposes of integrating an outgoing cellular call as an enterprise call;

[0011] FIG. 2 depicts a flowchart of the present patent disclosure according to one embodiment;

[0012] FIG. 3 depicts another flowchart of the present patent disclosure according to one embodiment;

[0013] FIG. 4 depicts an exemplary message flow diagram according to one embodiment of the present patent disclosure;

[0014] FIG. 5 depicts an exemplary IMS network environment wherein one or more embodiments of the present patent disclosure may be practiced for purposes of integrating an outgoing cellular call as an enterprise call;

[0015] FIG. 6 depicts an exemplary message flow diagram according to another embodiment of the present patent disclosure;

[0016] FIG. 7 depicts another flowchart of the present patent disclosure according to one embodiment; and

[0017] FIG. 8 depicts a block diagram of an embodiment of a communication device operable for purposes of the present patent disclosure.

DETAILED DESCRIPTION OF THE DRAWINGS

[0018] A system and method of the present patent disclosure will now be described with reference to various examples of how the embodiments can best be made and used. Like reference numerals are used throughout the description and several views of the drawings to indicate like or corresponding parts, wherein the various elements are not necessarily drawn to scale. Referring now to the drawings, and more particularly to FIG. 1, an exemplary network environment 100 is depicted wherein one or more embodiments of the present patent disclosure may be practiced for integrating an outgoing cellular call as an enterprise call. As depicted, the network environment 100 includes a generalized network infrastructure 102 wherein certain portions may form an enterprise network whereas the remaining portions may comprise an external network arrangement such as one or several service provider networks that serve as intermediary networks with respect to the enterprise network and the well-known PSTN/PLMN infrastructure 114. For purposes herein, an enterprise network may be any communications network internal to a company, office, or organization, and may comprise wireline and/or wireless network infrastructure. Regardless of the actual implementation, the network infrastructure 102 includes an integration server (also referred to as a Unified Communications Platform (UCP) element) 104, a switching element such as a SIP-capable Private Branch Exchange (PBX) 110 and a gateway (GW) element such as a SIP/PSTN GW 112. As alluded to previously, one or more of these elements may be incorporated within an enterprise network infrastructure in one embodiment. Alternatively, one or more of these elements or their functionalities may be hosted in a service provider network. In either arrangement, the functionalities of the elements may be integrated or redistributed into separate network entities. Accordingly, for purposes of the present patent disclosure, a "network node" may comprise a generalized network entity that effectuates or facilitates at least a portion of the functionalities set forth hereinbelow with respect to call integration.

[0019] An enterprise user is operable to effectuate communications (e.g., Voice/data/Video calls or multimedia sessions, and the like) in a number of scenarios within the context of the network environment 100 with respect to a called

Ex.1002 / Page 487 of 1173
Cisco Systems, Inc.

party 120. In general, the enterprise user is capable of initiating communications using one of two addresses: an enterprise address that may be used for calls made from within the enterprise network and a non-enterprise address for calls made from outside the enterprise network. In one application, the enterprise user may be provided with two separate pieces of user equipment (UE) 118: a wireline telephony equipment having the enterprise address that is used when the enterprise user is on the enterprise premises and a mobile communications device (MCD) having a cellular telephony number (i.e., non-enterprise address) that may be used when the enterprise user is away. Alternatively, where local wireless connectivity to the enterprise network is supported, a single wireless UE device operable in two different radio access technologies (RATs) may be provided. In this scenario, when the wireless UE device is attached to the enterprise network via any known or heretofore unknown Wireless Local Area Network (WLAN) technology, calls originated by the enterprise user may have the enterprise address as the calling party number. On the other hand, calls originated when the wireless UE device is attached to a wide area cellular network (WACN) such as the Public Land Mobile Network (PLMN) 114 may have the non-enterprise address (e.g., cellular telephony number) as the calling party number. Accordingly, it should be appreciated that the enterprise user equipment 118 may be a conventional cellular phone having data channel capability (e.g., Short Message Service or SMS capability) or a dual-mode MCD having WLAN capability (for enterprise operation) and WACN capability (for remote operation). Additionally, for purposes of further generalization, the enterprise UE device 118 may also comprise any personal computer (e.g., desktops, laptops, palmtops, personal digital assistants (PDAs) or other handheld computing devices) equipped with a suitable wireless modem, as well as a communications device operable in both circuit-switched (CS) and packet-switched (PS) communications that may even be capable of effectuating an inter-technology handoff between both CS and PS domains.

[0020] Based on the foregoing, it may be realized that the enterprise and non-enterprise addresses for an enterprise user may take on different forms, depending on the equipment and service provisioning. For instance, the enterprise address may comprise a SIP Uniform Resource Identifier (URI) or an E-164 number. Likewise, the non-enterprise address and the called party address may also comprise either SIP URIs, E.164 numbers, or other identifiers.

[0021] An enterprise data server 116 may be disposed in association with at least a portion of the network 102, preferably with the UCP node 104 when provisioned as part of an enterprise network. A data communications path 122 may be effectuated between the enterprise UE 118 and the enterprise network over the PLMN data network infrastructure via the enterprise data server 116. Regardless of whether integrated within an enterprise network or disposed in a service provider network, UCP node 104 preferably includes a Call Manager functionality 106 as well as a SIP Back-to-Back User Agent (B2BUA) 108 that is operable to perform third-party call control in order to combine multiple call legs together. In general, all enterprise SIP calls may be routed via the UCP node 104 and it is the role of the UCP node 104 to trigger the routing of the incoming SIP calls to the enterprise user regardless of whether UE 118 is attached via the enterprise WLAN or via the PLMN cellular network. Further, as will be described in detail below, the enterprise data server 116 can also receive a trigger message (i.e., a request to originate an outgoing cellular call) from UE 118 that is attached to the PLMN cellular network 114 via the cellular network's data network (such as GPRS or CDMA packet data network, for example) to request that the UCP node 104 establish a call between the enterprise UE 118 and the equipment 120 of the called party.

[0022] Taking reference to FIGS. 1 and 2 together, a generalized scheme 200 for integrating outgoing calls from the enterprise UE 118 when it is attached to the cellular network may be set forth as follows. The enterprise user using its equipment sends a request message to a serving network node (i.e., the UCP element 104 shown in FIG. 1) via the cellular network's data network (block 202). Additionally or alternatively, the request message may also be mediated via an enterprise data server. In one embodiment, the request may comprise a SIP Request such as a SIP REFER message or some other SIP Request (e.g., a SIP INVITE message) either sent directly to the enterprise data server 116 via the cellular network's data network or routed to the UCP node 104 via the cellular network's SIP based infrastructure such as the IP Multimedia Subsystem (IMS). Alternatively, the message may not be a SIP Message at all and could be any message that contains the necessary information to enable the UCP node 104 to establish a call between the enterprise UE 118 and the called party's equipment 120 that the enterprise user is attempting to call (e.g., an SMS message, an Unstructured Supplementary Service Data (USSD) message, or an IP based message). In accordance with an embodiment, the following pieces of information may be transmitted as part of the request message: (i) the enterprise address (e.g., SIP URI or E.164 number) that the enterprise user is reachable at; (ii) the non-enterprise address (e.g., E.164 number) that the enterprise UE is reachable at when it is attached to the cellular network; (iii) the E.164 number or SIP URI of the called party; and (iv) an indication of whether privacy is required. Upon receiving the request message from the enterprise UE (block 204), the service logic at the UCP node 104 uses the received information to effectuate two call legs in association with a switching node such as a SIP-capable PBX/CENTREX node, a first call leg between the switching node and the enterprise UE and a second call leg between the called party's UE and the switching node wherein the enterprise user's enterprise address is presented to the called party instead of the non-enterprise address associated with the UE (i.e., the cellular number) (block 206). Thereafter, the first and second call legs are patched together wherein the two respective Session Description Protocol (SDP) streams associated with the call legs are joined in order to establish an end-to-end bearer communications path between the enterprise user and

Ex.1002 / Page 488 of 1173
Cisco Systems, Inc.

the called party (block 208).

[0023] Set forth below is an example of how a SIP REFER request can be used to trigger the UCP node 104 to establish an outgoing call within the context of the scheme described above:

Table I

```
REFER sip: IntegrationServer@companyXXX.com; SIP/2.0
Via: SIP/2.0/UDP PIN12345678.blackberry.com
     ;branch=z9hG4bKhjhs8ass83

Max-Forwards: 70
To: <sip: IntegrationServer@companyXXX.com>
From: Mike <sip:Mike@companyXXX.com>;tag=32331
Call-ID: d432fa84b4c76e66710
Cseq: 2 REFER
Contact: <sip:PIN12345678.blackberry.com>
Refer-To: <cid:cn35t8jf02@companyXXX.com>
Require: multiple-refer
Content-Type: application/resource-lists+xml
Content-Disposition: recipient-list
Content-Length: 362
Content-ID: <cn35t8jf02@example.com>

<?xml version="1.0" encoding="UTF-8"?>
<resource-lists  xmlns+"um:ietf:params:xml:ns:resource-
lists"
     Xmins:xsi="http://www.w3.org/2001/XML.Schema-
instance">
<list>
<entry uri="tel: 098-765-4321"/>
<entry uri="tel: 123-456-7890"/>
</list>
</resource-lists>
```

[0024] Those skilled in the art will recognize that the above SIP REFER request embodiment uses the Resource List mechanism defined in draft-ietf-sip-multiple-refer and draft-ietf-simple-xcap-list-user to trigger the sending of a SIP INVITE request towards both the enterprise UE 118 and the called party equipment 120 using the list entry uri elements to deliver both the E.164 number that the enterprise UE is reachable at via the cellular network and the E.164 number of the party being called. Accordingly, when the UCP node 104 receives the SIP REFER request or other trigger message, it uses SIP Third Party Call Control to establish two SIP Call legs; one SIP leg to the enterprise UE via the PBX, SIP-PSTN Gateway and the circuit-switched cellular network; the other SIP leg to the called party. As pointed out previously, these two call legs are joined together at the UCP node 104 in order to form a single end-to-end call between the enterprise user and the called party. The SIP INVITE requests sent contain the enterprise address of the enterprise UE terminal which can be in the form of SIP URI or as an E.164 number in a TEL URI along with the appropriate privacy setting if requested in the SIP REFER request. Alternatively, the privacy setting may be required by the enterprise network based on certain service provisioning policies and profiles. The enterprise address of the enterprise UE terminal can be transported in the SIP INVITE request using the SIP From header, Referred-By header, P-Asserted-Identity header, Identity header or Remote-Party-ID header. If a SIP URI is used as the enterprise address of the enterprise UE terminal, the SIP-PBX 110 may translate this address to the corresponding E.164 number that represents the enterprise address of the device. The SIP-PSTN GW 112 includes the E.164 number that represents the enterprise address of the enterprise UE terminal in the Calling Line Identity in the circuit-switched signaling messages.

Ex.1002 / Page 489 of 1173
Cisco Systems, Inc.

[0025] With respect to the behavior of the enterprise UE for purposes of facilitating integration of an outgoing cellular call, reference may now be taken to FIG. 3 wherein a flowchart is depicted. When a request message for initiating an outgoing cellular call to a called party is transmitted to the network infrastructure, there is an expectation to receive an incoming circuit-switched call back from the network within a time window (block 302). Accordingly, a timer mechanism may be started at the application level to determine when to receive the circuit-switched call back in response to the outgoing request message. In one embodiment, if the timer expires, the enterprise UE device may try a number of times until a limit is reached, whereupon the call is considered to have failed. When the enterprise UE device receives a call establishment SETUP signaling request via the circuit-switched PSTN/PMLN signaling, the logic executing on the device is operable to identify that the circuit-switched call contains the enterprise address as the Calling Line Identity (block 304) (that is, the Calling Line Identity in the SETUP is the enterprise UE's enterprise address), and based thereon, the logic determines that this incoming call is related to the requested outgoing call (requested via the SIP REFER request or other message) (block 306). Accordingly, the logic operates to suppress generation of an alert to the enterprise user but establishes the circuit-switched call and stops the application timer (block 306). Further, the enterprise UE may provide an indication to the network that the call leg has been established (block 308). Accordingly, in one embodiment, the UCP node may wait until it receives such an acknowledgement of the establishment of the call leg with the enterprise UE device before attempting to establish the call leg to the called user by sending an SIP INVITE request in order to avoid the possibility of the called party answering before the call leg with the enterprise UE device is established (i.e., avoidance of a race condition). In the meantime, until the call legs are patched, there may be a delay experienced at the enterprise UE from the time the circuit-switched call leg with the network is established. Appropriate delay handling mechanisms(s) may therefore be provided to mitigate the delay.

[0026] When the called party's equipment receives the circuit-switched SETUP message (or SIP INVITE request if the called party is using a SIP phone within the enterprise SIP network or an external SIP network), the Calling Line Identity in the case of the circuit-switched SETUP message (or From header, Referred-By header, P-Asserted-Identity header, Identity header or Remote-Party-ID header in the case of SIP INVITE message) contains the enterprise address (e.g., E.164 number or SIP URI) of the enterprise UE device to be presented to the called party for Calling Line Identity Presentation (if provided based on the privacy setting). The called phone rings the user and returns an ALERTING message in the case of a circuit-switched call (or a SIP 180 "Ringing" response in the case of a SIP call). An ALERTING message will be translated by the SIP-PSTN gateway to a SIP 180 "Ringing" response. When the SIP 180 "Ringing" response is received at the UCP node, the service logic operable thereat may send a notification of "Ringing" back to the enterprise UE terminal via the cellular network's data network. In the case that the call establishment was triggered using a SIP REFER request, this notification may be in the form of a SIP NOTIFY request as specified in RFC 3515. In the case a message other than a SIP REFER request was used, the notification of "Ringing" may be sent using some other message. It is necessary to use the connection via the cellular network's data network to notify the "Ringing" since the call leg that is established with the enterprise UE terminal via the circuit-switched network is "in the wrong direction" to be able to indicate ALERTING using the circuit-switched signaling protocol.

[0027] Upon answering by the enterprise user, the UE terminal sends the circuit-switched CONNECT message (or SIP 200 "OK" response if the called party is using a SIP phone within the enterprise SIP network or an external SIP network). A CONNECT message will be translated by the SIP-PSTN GW to a SIP 200 "OK" response. When the SIP 200 "OK" response is received at the UCP node 104, it can send a notification of "OK" back to the enterprise UE terminal via the cellular network's data network. In the case that the call establishment was triggered using a SIP REFER request, this notification will be in the form of a SIP NOTIFY request as specified in RFC 3515. In the case a message other than a SIP REFER request was used, the notification of "OK" may be sent using some other message. At this point the call is established via the cellular network between the enterprise UE terminal and the called party, with the enterprise address of the enterprise UE terminal being displayed as the identity of the calling party.

[0028] FIG. 4 depicts an exemplary message flow diagram according to an embodiment of the process set forth above. As illustrated, a UCP node 402 and a network node 404 are exemplified to highlight the message flow between the enterprise UE 118 and the network infrastructure in particular detail. Upon blocking all incoming calls to the enterprise UE 108 (block 406), a request with respect to an outgoing call is initiated (reference numeral 408). In response, the UCP node 402 sends a message to the network node 404 (e.g., SIP-PBX) to block calls to the enterprise UE 118. A confirmation 412 is then propagated from the network node 404 to enterprise UE 118 via the UCP node 412, whereupon incoming calls from the network may be allowed (block 414). The UCP node 402 transmits a message 416 to the network node 404 to invite the enterprise user (i.e., caller) with respect to establishing a CS call 418 through the cellular network to the enterprise UE 118. Service logic at the enterprise UE 118 is operable to intercept the incoming CS call setup and identify that the enterprise address of the enterprise user is the CLI (block 420). Thereafter, a SIP 200 "OK" message 424 is generated by the network node 404 towards the UCP node 402 with respect to caller SDP. In response, an acknowledgement (ACK) 426 is generated by the UCP node 402. The UCP node 402 also generates a message 428 towards the network node 404 to invite the called party (i.e., callee) with respect to establishing a CS call 430 therewith through the PSTN/PLMN. As shown in block 422, appropriate service logic may be provided for handling the delay before

Ex.1002 / Page 490 of 1173
Cisco Systems, Inc.

patching the call legs. Pursuant to joining the audio paths (block 432), a SIP 200 "OK" message 434 is generated by the network node 404 towards the UCP node 402 with respect to callee SDP. In response, an acknowledgement (ACK) 436 is generated by the UCP node 402. A message 438 is provided thereafter by the UCP node 402 to the network node 404 in order to unblock calls to the enterprise UE 118, resulting in a confirmation 440 by the network node 404.

[0029] An embodiment of the foregoing call integration mechanism may also be implemented within an IMS-based network environment in a different application wherein the functionality of the UCP node is provided as an IMS node. Referring now to FIG. 5, an exemplary IMS-based network environment 500 is depicted wherein an embodiment of the present patent disclosure may be practiced for effectuating call integration with respect to an enterprise call originated by a UE device. As depicted, the network environment 500 is generalized to include an access space 504 comprised of a number of access technologies available to one or more enterprise UE devices 502-1 through 502-N. As generalized previously, a UE device may be any tethered or untethered communications device, and may include any personal computer (e.g., desktops, laptops, palmtops, or handheld computing devices) equipped with a suitable wireless modem or a mobile communications device (e.g., cellular phones or data-enabled handheld devices capable of receiving and sending messages, web browsing, et cetera), or any enhanced PDA device or integrated information appliance capable of email, video mail, Internet access, corporate data access, messaging, calendaring and scheduling, information management, and the like. Further, as alluded to hereinabove, the UE device may also capable of operating in multiple modes in that it can engage in both CS-based as well as PS-based communications, and can transition from one mode of communications to another mode of communications without loss of continuity.

[0030] The access space 504 may be comprised of both CS and PS networks, which may involve wireless technologies, wireline technologies, broadband access technologies, etc. For example, reference numeral 506 refers to wireless technologies such as GSM and CDMA networks, although it is envisaged that the teachings hereof may be extended to any 3rd Generation Partnership Project (3GPP)-compliant cellular network (e.g., 3GPP or 3GPP2) as well. Reference numeral 508 refers to broadband access networks including WLANs, Wi-MAX networks as well as fixed networks such as DSL, cable broadband, etc. Thus, for purposes of the present disclosure, the access technologies may comprise RATs selected from IEEE 802.11a technology, IEEE 802.11b technology, IEEE 802.11g technology, IEEE 802.11n technology, GSM/EDGE Radio Access Network (GERAN) technology (both CS and PS domains), and UMTS technology, and Evolution - Data Optimized (EVDO) technology, and so on. Additionally, also exemplified as part of the access space 504 is the conventional wireline PSTN infrastructure 510 available to the enterprise UEs as illustrated in FIG. 5.

[0031] An IMS core network 512 is coupled to the various access networks set forth above, including any CS-based networks. As is well known, the IMS standard defined by the 3GPP is designed to allow service providers manage a variety of services that can be delivered via IP over any network type, wherein IP is used to transport both bearer traffic and SIP-based signaling traffic. Broadly, IMS is a framework for managing the applications (i.e., services) and networks (i.e., access) that is capable of providing multimedia services. IMS defines an "application server" as a network element that delivers services subscribers use, e.g., voice call continuity (VCC), Push-To-Talk (PTT), etc. IMS manages applications by defining common control components that each application server (AS) is required to have, e.g., subscriber profiles, IMS mobility, network access, authentication, service authorization, charging and billing, inter-operator functions, and interoperation with the legacy phone network.

[0032] It should be understood that whereas IMS is defined by the 3GPP standards body which mainly addresses GSM networks, another group, 3GPP2, is involved in defining a closely analogous architecture referred to as Multimedia Domain (MMD). MMD is essentially an IMS for CDMA networks, and since MMD and IMS are roughly equivalent, the term "IMS" may be used in this present patent disclosure to refer collectively to both IMS and MMD where applicable. In addition, fixed network standards for NGN (Next Generation Networks) that are based on and/or reuse IMS are also being developed by bodies such as ETSI TISPAN, Cablelabs and the ITU-T. NGN and IMS are roughly equivalent, and accordingly the term "IMS" may also be used in this present patent disclosure to refer collectively to both IMS and NGN where applicable.

[0033] Continuing to refer to FIG. 5, reference numerals 514-1 to 514-N refer to a plurality of AS nodes operable to support various services, e.g., VCC, PTT, etc., as alluded to hereinabove. Further, a call integration AS node having an IMS CS Control Function (ICCF, or CCF for short) may also be disposed within the core network for controlling call integration with respect to calls originated by one or more enterprise UE devices. Accordingly, it should be appreciated that at least one of the AS nodes is operable equivalent to the functionality of UCP node 104 described in detail hereinabove. Further, an AS node, e.g., AS 514-N, may be provided as part of the enterprise users' home IMS core network which implements functionality referred to as call continuity control function (CCCF) 516 and network domain selection (NeDS) 518. In essence, the CCCF portion 516 of AS 514-N is operable as a new IMS application server element that resides in the home IMS network and tracks all call sessions and related mobile VoIP bearer traffic, including call handover/routing between CS and IMS domains. The NeDS portion 518 of AS 114-N is responsible for performing, *inter alia,* registration/de-registration management between the IMS and CS networks (e.g., GSM or CDMA). Despite being potentially separate functions, it is possible to integrate both the CCCF and NeDS functionalities into a single IMS-compatible network element 514-N as illustrated in FIG. 5. Also, a suitable session control function (SCF) 520 may be

Ex.1002 / Page 491 of 1173
Cisco Systems, Inc.

provided as part of the AS node 514-N with respect to applicable radio access technology, e.g., gsmSCF. Additional related functional entities may include the following: Domain Transfer Function (DTF) (also referred to as Functional Entity FE-A), CS Adaptation Function (CSAF) (also referred to as FE-B), CAMEL Service (also referred to as FE-C), and Domain Selection Function (DSF) (also referred to as FE-D). Accordingly, for purposes of the present disclosure, the term "network node" with reference to an IMS core network may comprise one or more of the foregoing functionalities in any combination as applicable as well as the call integration functionality described herein.

[0034] Furthermore, although not shown in FIG. 5, a master user database, referred to as a Home Subscriber Server or HSS, may also be provided as part of the home IMS network 512, for supporting the various IMS network entities that actually manage calls or sessions such as UCP/AS node 514-N. In general, the HSS database may contain user profiles (i.e., subscription-related information), including various user and device identifies such as International Mobile Subscriber Identity (IMSI), Temporal Mobile Subscriber Identity (TMSI), International Mobile Equipment Identity (IMEI), Mobile Subscriber ISDN Number (MSISDN), Universally Unique Identifier (UUID), as well as additional IMS-specific identities such as IM Multimedia Private Identity (IMPI) and IP Multimedia Public Identity (IMPU) that are implemented as Tel-URIs or SIP-URIs.

[0035] FIG. 6 depicts an exemplary message flow diagram according to another embodiment of the present patent disclosure for call integration in an IMS-based environment such as the network environment 500 described in the foregoing sections. Network functionalities such as Visited Mobile Switching Center (VMSC) 602, Media Gateway Control Function (MGCF) 604, Media Gateway (MGW) 606 are operable with respect to IMS functionalities such as Call/Session Control Function (CSCF) 608 and CCF 610 for purposes of mediating an originating call by the enterprise UE 118 towards the call party 120. As illustrated, the enterprise UE 118 is operable to generate a SIP INVITE message 612 including the enterprise user information, called party information, as well as privacy setting information, as described hereinabove, towards CSCF node 608 which propagates SIP INVITE 612 to ICCF 610 embodying the call integration functionality. For purposes of establishing a first call leg, ICCF 610 generates a SIP INVITE message 614 towards the calling party, i.e., the enterprise UE 118, which is received by MGCF 604. In response, an Initial Address Message (IAM) 616 is generated towards VMSC 602, which in turn sends a SETUP message 618 to the enterprise UE 118. Thereafter, a first call leg is 610 is established between the enterprise UE 118 and the IMS network node. Further, ICCF 610 generates another SIP INVITE message 622 towards the called party 120, which is also mediated via CSCF 608. As a result, a second call leg 624 is established, which is patched with the first call leg 620 for establishing an end-to-end path 626 between the enterprise UE 118 and called party 120. Those skilled in the art will recognize that suitable timing mechanisms and delay handling mechanisms may also be implemented at the device side and/or the network side in order to avoid the race conditions and other operational issues set forth in detail with reference to the previously described embodiments.

[0036] FIG. 7 depicts another flowchart of the present patent disclosure according to one embodiment 700 which describes the IMS node functionality for effectuating call integration. As described above, an enterprise user sends a SIP INVITE request to initiate an outgoing call to a called party (block 702). A serving IMS network node receives the request from the enterprise user (block 704), whereupon it establishes two call legs in association with a CSCF node: one call leg between the IMS network and the enterprise user and another call leg between the IMS network and the called party. Using the information provided in the SIP INVITE message, the enterprise user's enterprise address is presented as a Calling Line Identity to the called party instead of the non-enterprise address of the enterprise user (block 706). The two call legs are then patched in order to establish the communication path between the parties (block 708). It should be appreciated that the various operations set forth herein may be accomplished via a number of means, including software (e.g., program code), firmware, hardware, or in any combination, usually in association with a processing system. Where the processes are embodied in software, such software may comprise program instructions that form a computer program product, uploadable service application software, or software downloadable from a remote station, and the like.

[0037] FIG. 8 depicts a block diagram of an embodiment of a communications device 800 operable as a UE device, e.g., the enterprise UE 118, for purposes of the present patent disclosure. It will be recognized by those skilled in the art upon reference hereto that although an embodiment of UE 118 may comprise an arrangement similar to one shown in FIG. 8, there can be a number of variations and modifications, in hardware, software or firmware, with respect to the various modules depicted. Further, a UE device 800 for purposes of the present disclosure may comprise a mobile equipment (ME) device without a removable storage module and/or a mobile device coupled with such a storage module. Accordingly, the arrangement of FIG. 8 should be taken as illustrative rather than limiting with respect to the embodiments of the present patent disclosure. A microprocessor 802 providing for the overall control of an embodiment of UE 800 is operably coupled to a communication subsystem 804 that may preferably be capable of multi-mode communications (e.g., CS domain and PS domain). The communication subsystem 804 generally includes one or more receivers 808 and one or more transmitters 814 as well as associated components such as one or more local oscillator (LO) modules 810 and a processing module such as a digital signal processor (DSP) 812. As will be apparent to those skilled in the field of communications, the particular design of the communication module 804 may be dependent upon the communications networks with which the mobile device is intended to operate (e.g., a CDMA network, a GSM network, or a

Ex.1002 / Page 492 of 1173
Cisco Systems, Inc.

WLAN, et cetera). Regardless of the particular design, however, signals received by antenna 806 through appropriate access infrastructure 805 (e.g., cellular base station towers, WLAN hot spots, etc.) are provided to receiver 808, which may perform such common receiver functions as signal amplification, frequency down conversion, filtering, channel selection, analog-to-digital (A/D) conversion, and the like. Similarly, signals to be transmitted are processed, including modulation and encoding, for example, by DSP 812, and provided to transmitter 814 for digital-to-analog (D/A) conversion, frequency up conversion, filtering, amplification and transmission over the air-radio interface via antenna 816.

[0038] Microprocessor 802 may also interface with further device subsystems such as auxiliary input/output (I/O) 818, serial port 820, display 822, keyboard/keypad 824, speaker 826, microphone 828, random access memory (RAM) 830, a short-range communications subsystem 832, and any other device subsystems, e.g., timer mechanisms, generally labeled as reference numeral 833. To control access, a USIM/RUIM interface 834 may also be provided in communication with the microprocessor 802. In one implementation, USIM/RUIM interface 834 is operable with a USIM/RUIM card having a number of key configurations 844 and other information 846 such as identification and subscriber-related data.

[0039] Operating system software and applicable service logic software may be embodied in a persistent storage module (i.e., non-volatile storage) such as Flash memory 835. In one implementation, Flash memory 835 may be segregated into different areas, e.g., storage area for computer programs 836 (e.g., service processing logic), as well as data storage regions such as device state 837, address book 839, other personal information manager (PIM) data 841, and other data storage areas generally labeled as reference numeral 843. A transport stack 845 may be provided to effectuate one or more appropriate radio-packet transport protocols. In addition, enterprise call request messaging logic 848, including memory storage for storing pertinent address information, is provided for facilitating integration of outgoing calls as set forth hereinabove.

[0040] It is believed that the operation and construction of the embodiments of the present patent application will be apparent from the Detailed Description set forth above. While the exemplary embodiments shown and described may have been characterized as being preferred, it should be readily understood that various changes and modifications could be made therein without departing from the scope of the present disclosure as set forth in the following claims.

Claims

1. A method for integrating an outgoing cellular call as an enterprise call in an IP Multimedia Subsystem (IMS) environment (500), wherein said outgoing cellular call is originated by an enterprise user (118) towards a called party (120), said enterprise user (118) having an enterprise address and a non-enterprise address, comprising:

   receiving (704) a Session Initiation Protocol (SIP) INVITE request (612) from said enterprise user (118) for initiating said outgoing cellular call to said called party (120);
   establishing (706) a first call leg (620) to said enterprise user (118);
   establishing (706) a second call leg (624) to said called party (120); and
   patching (708) said first and second call legs (620, 624) to establish an end-to-end communications path (626) between said enterprise user (118) and said called party (120), wherein said enterprise address is presented instead of said non-enterprise address to said called party (120) as a calling line identity with respect to said outgoing cellular call from said enterprise user (118).

2. The method as recited in claim 1, wherein said SIP INVITE request (612) includes said enterprise address, said non-enterprise address, said called party's address, and a privacy indication.

3. The method as recited in claim 2, wherein said enterprise address comprises one of a SIP Uniform Resource Identifier (URI) and an E-164 number.

4. The method as recited in claim 2, wherein said non-enterprise address comprises a cellular telephony network number in E-164 format.

5. The method as recited in claim 2, wherein said called party's address comprises one of a SIP Uniform Resource Identifier (URI) and an E-164 number.

6. The method as recited in claim 1, wherein said establishment (706) of said first call leg (620) is facilitated by sending a SIP INVITE message (614) towards said enterprise user (118).

7. The method as recited in claim 1, wherein said establishment (706) of said second call leg (624) is facilitated sending a SIP INVITE message (622) towards said called party (120).

Ex.1002 / Page 493 of 1173
Cisco Systems, Inc.

8. An IP Multimedia Subsystem (IMS) network node (610) for integrating an outgoing cellular call as an enterprise call, wherein said outgoing cellular call is originated by an enterprise user (118) towards a called party (120), said enterprise user having an enterprise address and a non-enterprise address, comprising:

means for receiving (704) a Session Initiation Protocol (SIP) INVITE request (612) from said enterprise user (118) for initiating said outgoing cellular call to said called party (120);
means for establishing (706) a first call leg (620) to said enterprise user (118);
means for establishing (706) a second call leg (624) to said called party (120); and
means for patching (708) said first and second call legs (620, 624) to establish an end-to-end communications path (626) between said enterprise user (118) and said called party (120), wherein said enterprise address is presented instead of said non-enterprise address to said called party (120) as a calling line identity with respect to said outgoing cellular call from said enterprise user (118) .

9. The IMS network node (610) as recited in claim 8, wherein said SIP INVITE request (612) includes said enterprise address, said non-enterprise address, said called party's address, and a privacy indication.

10. The IMS network node (610) as recited in claim 9, wherein said enterprise address comprises one of a SIP Uniform Resource Identifier (URI) and an E-164 number.

11. The IMS network node (610) as recited in claim 9, wherein said called party's address comprises one of a SIP Uniform Resource Identifier (URI) and an E-164 number.

12. The IMS network node (610) as recited in claim 9, wherein said non-enterprise address comprises a cellular telephony network number in E-164 format.

13. The IMS network node (610) as recited in claim 8, further including means for sending a SIP INVITE message (614) towards said enterprise user (118) with respect to establishment of said first call leg (620).

14. The IMS network node (610) as recited in claim 8, further including means for sending a SIP INVITE message (622) towards said called party (120) with respect to establishment of said second call leg (624).

15. An IP Multimedia Subsystem (IMS)-capable user equipment (UE) device (800), comprising:

means for generating (802, 848) a Session Initiation Protocol (SIP) INVITE request (612) with respect to initiating an outgoing cellular call to a called party (120), said SIP INVITE request (612) being directed to an IMS network node (610); and
means for establishing (802, 848) a call leg (620) with said IMS network node (610) responsive to receiving a control message (618) that is provided responsive to a SIP INVITE message (614) from said IMS network node (610).

16. The IMS-capable UE device (800) as recited in claim 15, further comprising means for providing (802, 848) an indication to said IMS network node (610) that said call leg (620) is established between said UE device (800) and said network node (610).

17. The IMS-capable UE device (800) as recited in claim 15 or claim 16, wherein said request (612) includes an enterprise address and a non-enterprise address each associated with an enterprise user, said called party's address, and a privacy indication.

18. The IMS-capable UE device (800) as recited in claim 17, wherein said enterprise address comprises one of a SIP Uniform Resource Identifier (URI) and an E-164 number.

19. The IMS-capable UE device (800) as recited in claim 17, wherein said called party's address comprises one of a SIP Uniform Resource Identifier (URI) and an E-164 number.

20. The IMS-capable UE device (800) as recited in claim 18, wherein said non-enterprise address comprises a cellular telephony network number in E-164 format.

Ex.1002 / Page 494 of 1173
Cisco Systems, Inc.

Amended claims in accordance with Rule 137(2) EPC.

1. A method for integrating an outgoing cellular call as an enterprise call in an IP Multimedia Subsystem (IMS) environment (500), wherein said outgoing cellular call is originated by an enterprise user (118) towards a called party (120), said enterprise user (118) having an enterprise address and a non-enterprise address, comprising:

receiving (704) a Session Initiation Protocol (SIP) INVITE request (612) from said enterprise user (118) for initiating said outgoing cellular call to said called party (120);
establishing (706) a first call leg (620) to said enterprise user (118), wherein said enterprise address is presented to said enterprise user as a calling line identity;
establishing (706) a second call leg (624) to said called party (120); and
patching (708) said first and second call legs (620, 624) to establish an end-to-end communications path (626) between said enterprise user (118) and said called party (120), wherein said enterprise address is presented instead of said non-enterprise address to said called party (120) as a calling line identity with respect to said outgoing cellular call from said enterprise user (118).

2. The method as recited in claim 1, wherein said SIP INVITE request (612) includes said enterprise address, said non-enterprise address, said called party's address, and a privacy indication.

3. The method as recited in claim 2, wherein said enterprise address comprises one of a SIP Uniform Resource Identifier (URI) and an E-164 number.

4. The method as recited in claim 2, wherein said non-enterprise address comprises a cellular telephony network number in E-164 format.

5. The method as recited in claim 2, wherein said called party's address comprises one of a SIP Uniform Resource Identifier (URI) and an E-164 number.

6. The method as recited in claim 1, wherein said establishment (706) of said first call leg (620) is facilitated by sending a SIP INVITE message (614) towards said enterprise user (118).

7. The method as recited in claim 1, wherein said establishment (706) of said second call leg (624) is facilitated sending a SIP INVITE message (622) towards said called party (120).

8. An IP Multimedia Subsystem (IMS) network node (610) for integrating an outgoing cellular call as an enterprise call when said outgoing cellular call is originated by an enterprise user (118) towards a called party (120), said enterprise user having an enterprise address and a non-enterprise address, the network node comprising:

means for receiving (704) a Session Initiation Protocol (SIP) INVITE request (612) from said enterprise user (118) for initiating said outgoing cellular call to said called party (120);
means for establishing (706) a first call leg (620) to said enterprise user (118) and for presenting said enterprise address to said enterprise user as a calling line identity;
means for establishing (706) a second call leg (624) to said called party (120); and
means for patching (708) said first and second call legs (620, 624) to establish an end-to-end communications path (626) between said enterprise user (118) and said called party (120), wherein the network node is configured to present said enterprise address instead of said non-enterprise address to said called party (120) as a calling line identity with respect to said outgoing cellular call from said enterprise user (118).

9. The IMS network node (610) as recited in claim 8, configured to include in said SIP INVITE request (612) said enterprise address, said non-enterprise address, said called party's address, and a privacy indication.

10. The IMS network node (610) as recited in claim 9, configured to include said enterprise address as one of a SIP Uniform Resource Identifier (URI) and an E-164 number.

11. The IMS network node (610) as recited in claim 9, configured to include said called party's address as one of a SIP Uniform Resource Identifier (URI) and an E-164 number.

12. The IMS network node (610) as recited in claim 9, configured to include said non-enterprise address as a cellular

Ex.1002 / Page 495 of 1173
Cisco Systems, Inc.

telephony network number in E-164 format.

13. The IMS network node (610) as recited in claim 8, further including means for sending a SIP INVITE message (614) towards said enterprise user (118) with respect to establishment of said first call leg (620).

14. The IMS network node (610) as recited in claim 8, further including means for sending a SIP INVITE message (622) towards said called party (120) with respect to establishment of said second call leg (624).

Ex.1002 / Page 496 of 1173
Cisco Systems, Inc.

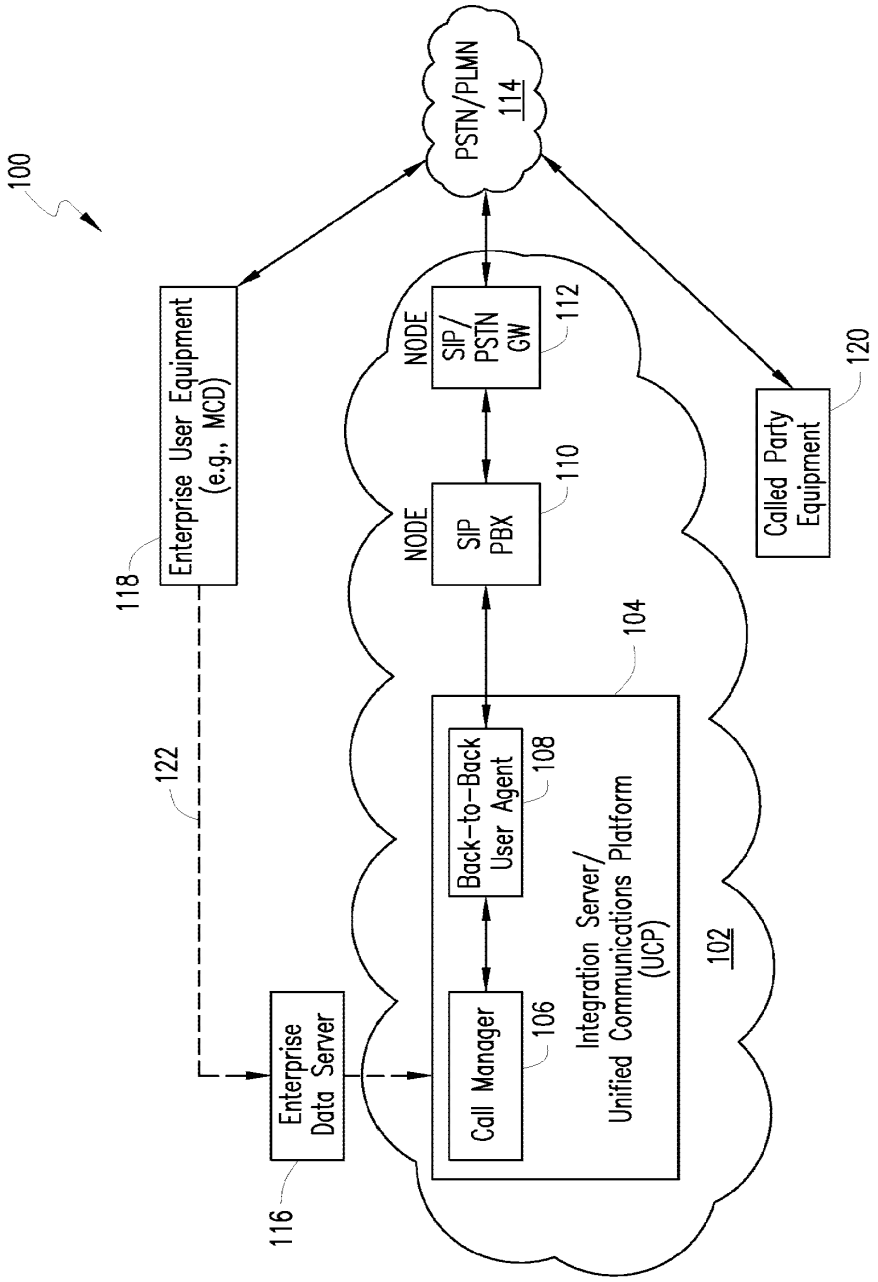

100
PSTN/PLMN
114
Enterprise User Equipment
(e.g., MCD)
118
NODE
SIP/
PSTN
GW
112
NODE
SIP
PBX
110
Called Party
Equipment
120
104
Back-to-Back
User Agent
108
Integration Server/
Unified Communications Platform
(UCP)
102
122
Enterprise
Data Server
116
Call Manager
106

FIG. 1

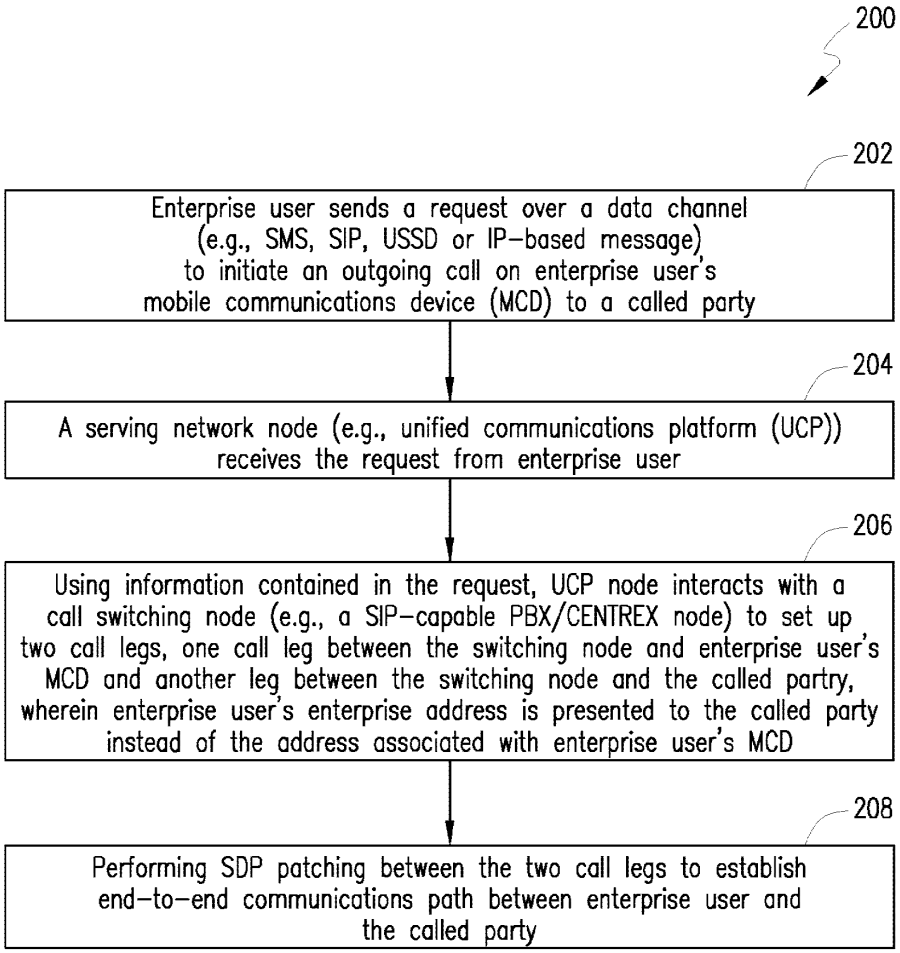


FIG. 2

Ex.1002 / Page 498 of 1173
Cisco Systems, Inc.

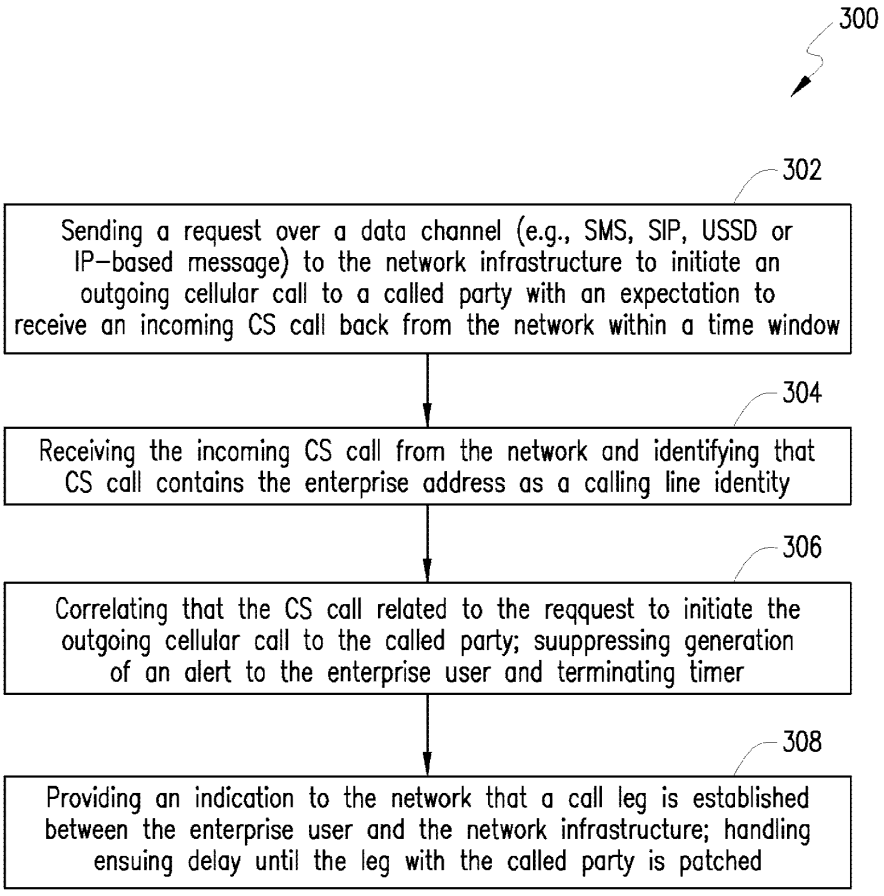

300
302
Sending a request over a data channel (e.g., SMS, SIP, USSD or IP-based message) to the network infrastructure to initiate an outgoing cellular call to a called party with an expectation to receive an incoming CS call back from the network within a time window
304
Receiving the incoming CS call from the network and identifying that CS call contains the enterprise address as a calling line identity
306
Correlating that the CS call related to the reqquest to initiate the outgoing cellular call to the called party; suuppressing generation of an alert to the enterprise user and terminating timer
308
Providing an indication to the network that a call leg is established between the enterprise user and the network infrastructure; handling ensuing delay until the leg with the called party is patched

FIG. 3

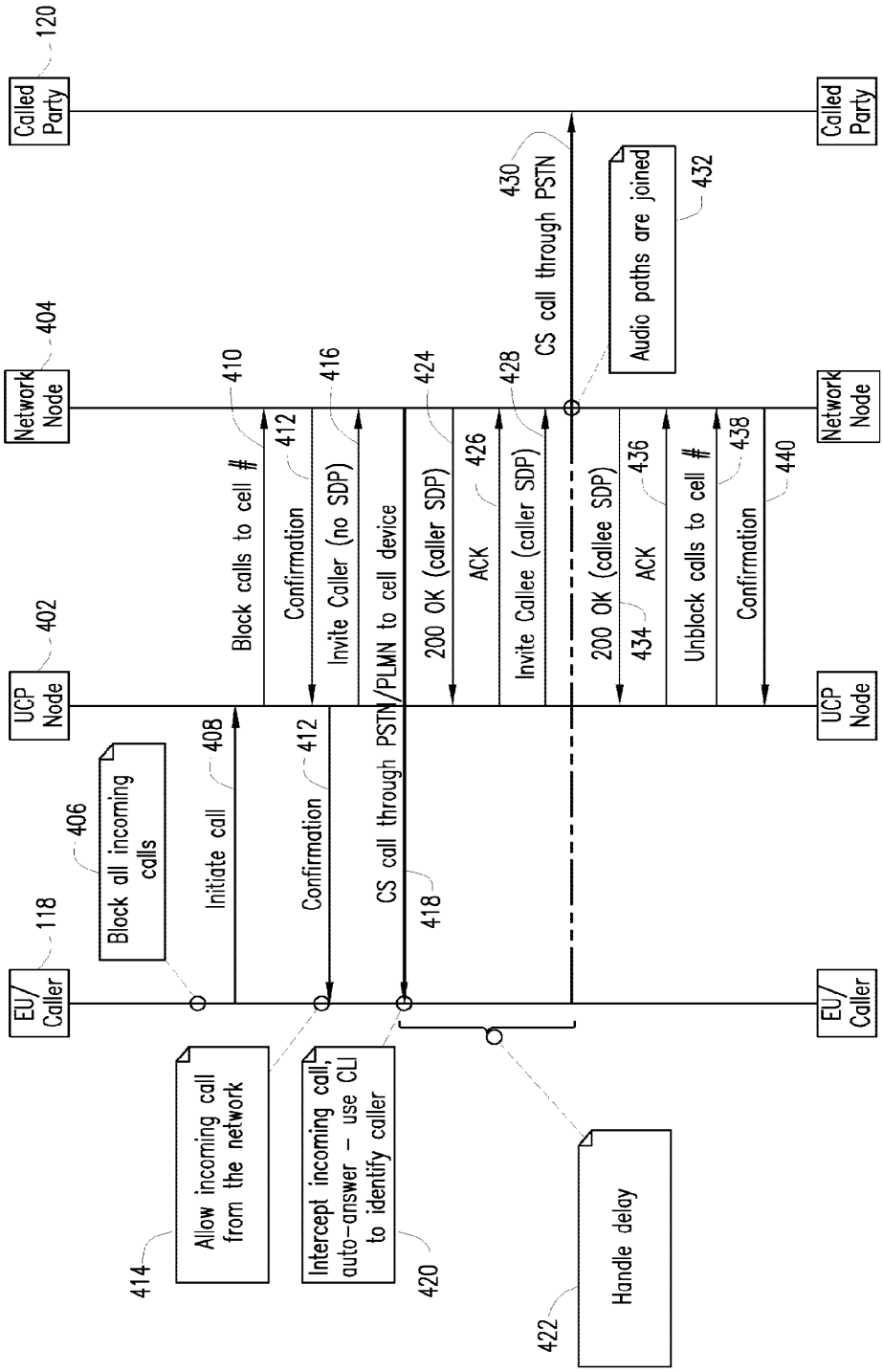

Called Party
120
Network Node
404
UCP Node
402
EU/ Caller
118
Block all incoming calls
406
Initiate call
408
Block calls to cell #
410
Confirmation
412
Invite Caller (no SDP)
416
CS call through PSTN/PLMN to cell device
418
200 OK (caller SDP)
424
ACK
426
Invite Callee (caller SDP)
428
CS call through PSTN
430
Audio paths are joined
432
200 OK (callee SDP)
434
ACK
436
Unblock calls to cell #
438
Confirmation
440
Allow incoming call from the network
414
Intercept incoming call, auto-answer – use CLI to identify caller
420
Handle delay
422

FIG. 4

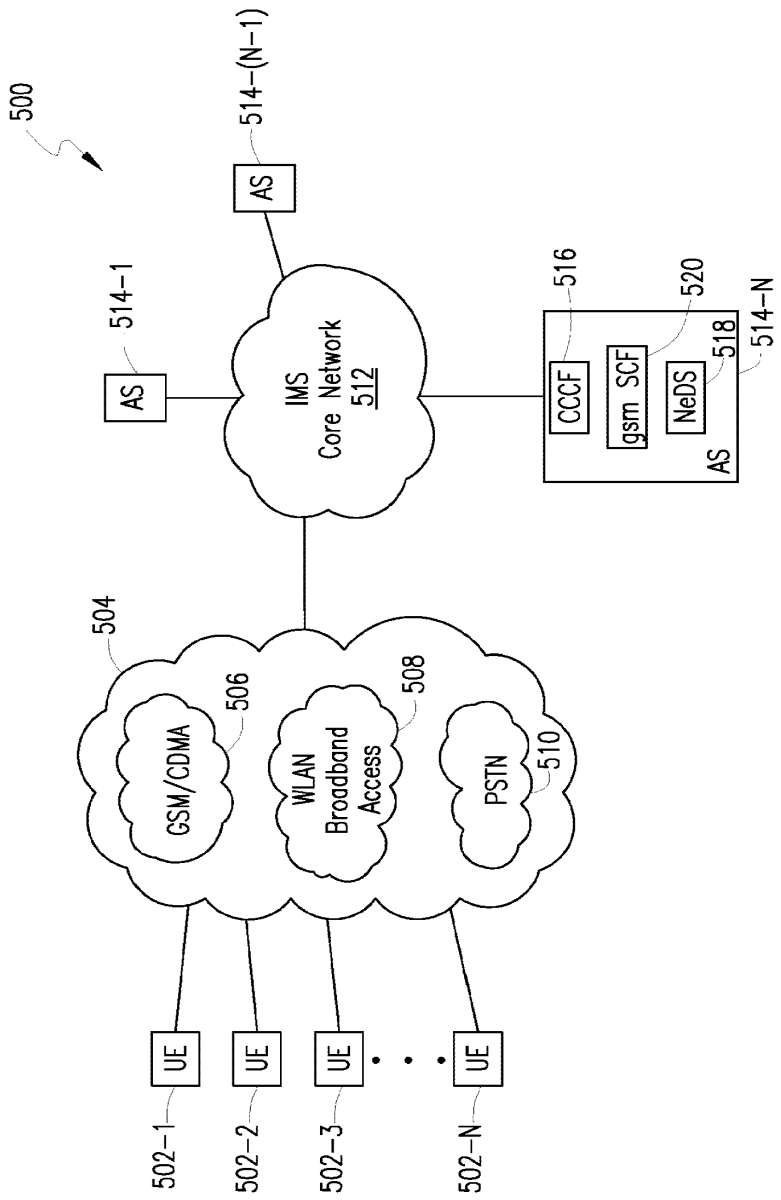

500
514-(N-1)
AS
514-1
AS
IMS
Core Network
512
516
520
518
514-N
CCCF
gsm SCF
NeDS
AS
504
GSM/CDMA
506
WLAN
Broadband
Access
508
PSTN
510
UE
UE
UE
UE
502-1
502-2
502-3
502-N

FIG. 5

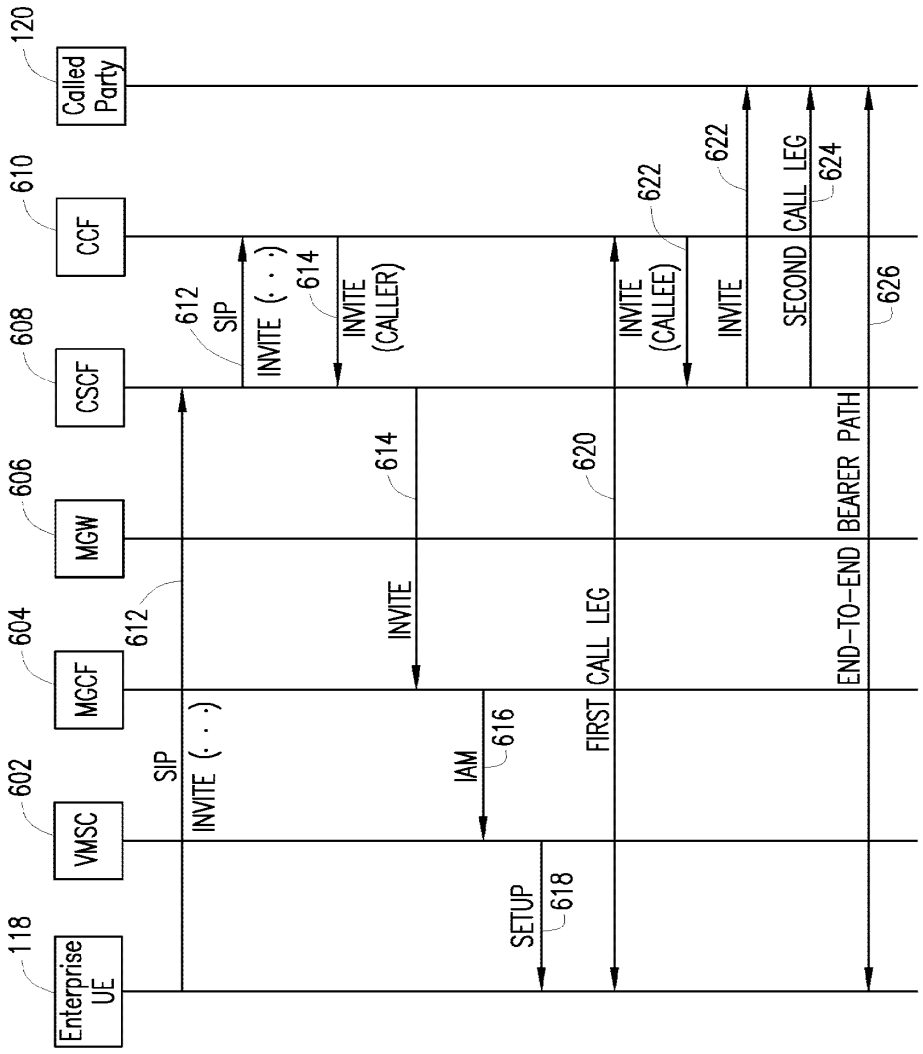

Enterprise UE
118
VMSC
602
MGCF
604
MGW
606
CSCF
608
CCF
610
Called Party
120
SIP
INVITE (· · ·)
612
SETUP
618
IAM
616
INVITE
614
FIRST CALL LEG
620
INVITE (CALLER)
INVITE (CALLEE)
622
INVITE
SECOND CALL LEG
624
END-TO-END BEARER PATH
626

FIG. 6

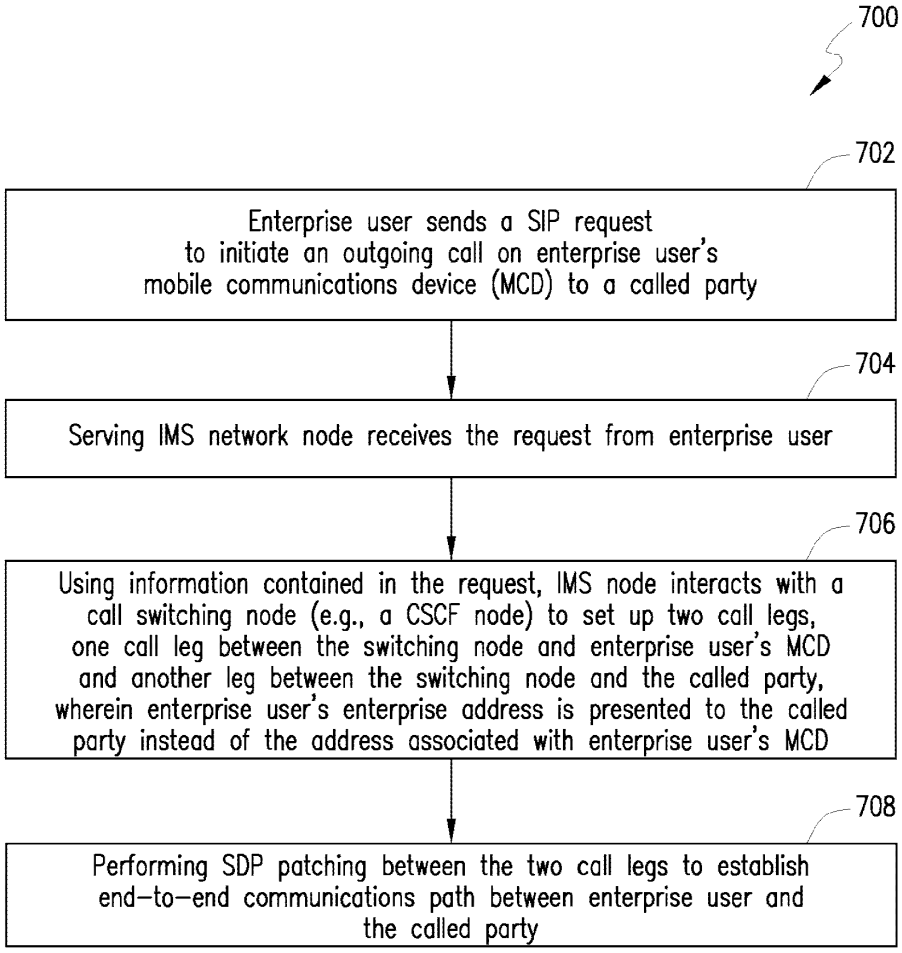

700
702
Enterprise user sends a SIP request to initiate an outgoing call on enterprise user's mobile communications device (MCD) to a called party
704
Serving IMS network node receives the request from enterprise user
706
Using information contained in the request, IMS node interacts with a call switching node (e.g., a CSCF node) to set up two call legs, one call leg between the switching node and enterprise user's MCD and another leg between the switching node and the called party, wherein enterprise user's enterprise address is presented to the called party instead of the address associated with enterprise user's MCD
708
Performing SDP patching between the two call legs to establish end-to-end communications path between enterprise user and the called party

FIG. 7

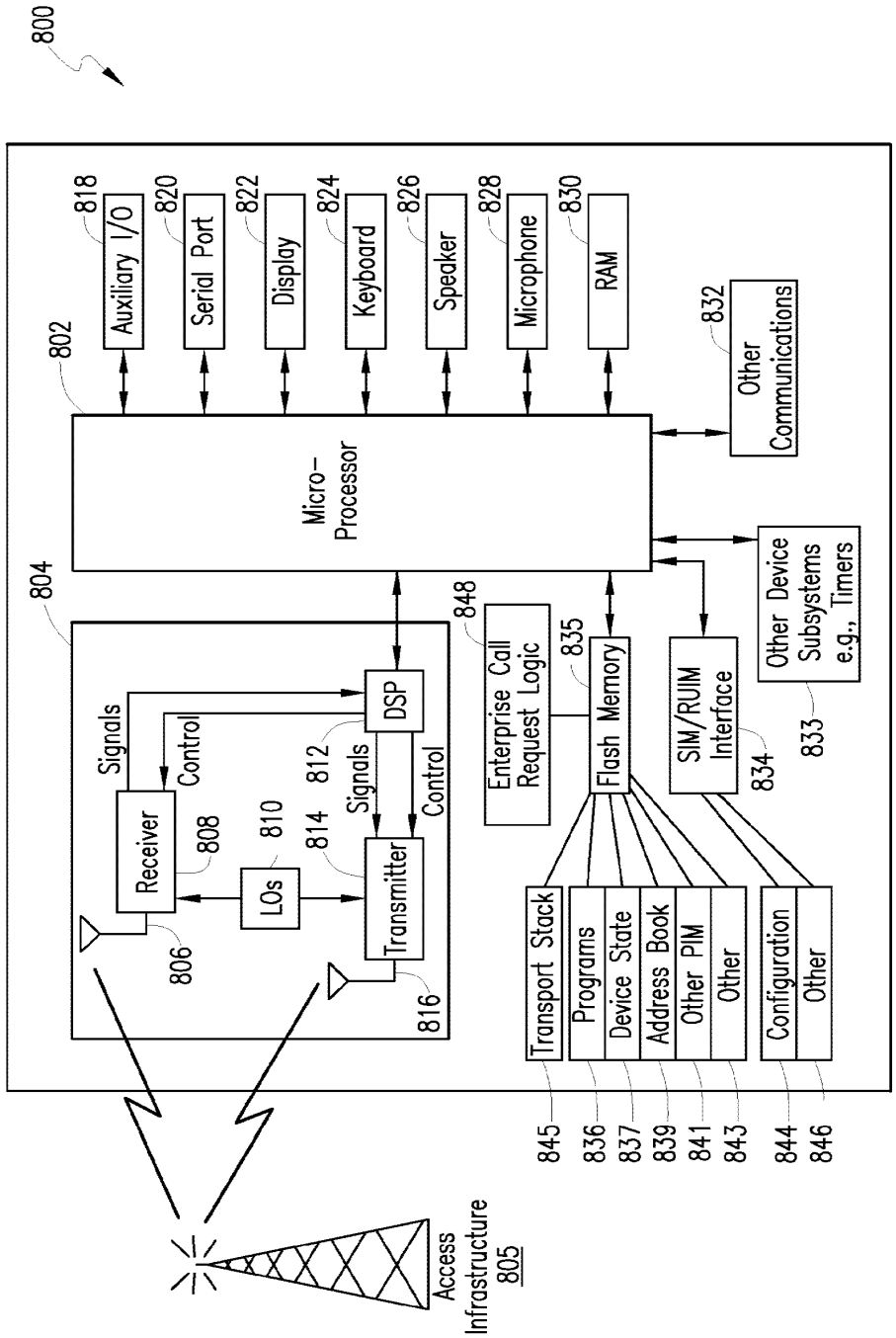

800
802
804
Micro-Processor
Auxiliary I/O
818
Serial Port
820
Display
822
Keyboard
824
Speaker
826
Microphone
828
RAM
830
Other Communications
832
Other Device Subsystems e.g., Timers
833
SIM/RUIM Interface
834
Flash Memory
835
Enterprise Call Request Logic
848
DSP
812
Signals
Control
Receiver
808
LOs
810
814
Transmitter
806
816
Transport Stack
Programs
Device State
Address Book
Other PIM
Other
Configuration
Other
845
836
837
839
841
843
844
846
Access Infrastructure 805

FIG. 8

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 07 10 7248

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
Y	GB 2 342 536 A (ORANGE PERSONAL COMM SERV LTD [GB]) 12 April 2000 (2000-04-12) * page 8, line 10 - page 9, line 12; figure 3 *	1-20	INV. H04M7/12 H04L29/06 H04M1/253 H04M1/725
Y	US 2007/015535 A1 (LABAUVE LANCE [US] ET AL) 18 January 2007 (2007-01-18) * paragraph [0078] *	1-20	
A	DE VRIENDT, J.; HANSON, G.; URIE, A.: "Network migration strategies towards IMS" ALCATEL TELECOMMUNICATIONS REVIEW, ALCATEL, PARIS CEDEX, FR, 2005, XP007903135 ISSN: 1267-7167 *Mobile operator migration path*	1-20	

TECHNICAL FIELDS SEARCHED (IPC)

H04M
H04Q
H04L

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	17 October 2007	Cremer, Jan

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

Ex.1002 / Page 505 of 1173
Cisco Systems, Inc.

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 07 10 7248

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

17-10-2007

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
GB 2342536 A	12-04-2000	AU 6214899 A	01-05-2000
		EP 1118240 A1	25-07-2001
		WO 0022863 A1	20-04-2000
US 2007015535 A1	18-01-2007	US 2007015536 A1	18-01-2007

EPO FORM P0459

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

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 988 697 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
05.11.2008 Bulletin 2008/45

(51) Int Cl.:
H04M 7/12 *(2006.01)* ***H04L 29/06*** *(2006.01)*
H04M 1/253 *(2006.01)* ***H04M 1/725*** *(2006.01)*

(21) Application number: **07107246.6**

(22) Date of filing: **30.04.2007**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC MT NL PL PT RO SE SI SK TR
Designated Extension States:
AL BA HR MK RS

(71) Applicant: **Research In Motion Limited**
Waterloo, Ontario N2L 3W8 (CA)

(72) Inventors:
- **Allen, Andrew**
  Mundelein, IL 60060 (US)
- **Buckley, Adrian**
  Tracy, CA 95376 (US)
- **George, Richard**
  Waterloo, Ontario N2T 2S3 (CA)
- **Oliver, Brian**
  Fergus, Ontario N1M 1C8 (CA)
- **Luu, Lap**
  Markham, Ontario, L6C 2X7 (CA)
- **Lee, Dalsu**
  Thornhill, Ontario, L4J 7Y8 (CA)

(74) Representative: **Roberts, Gwilym Vaughan et al**
Kilburn & Strode
20 Red Lion Street
London WC1R 4PJ (GB)

Remarks:
Amended claims in accordance with Rule 137(2) EPC.

(54) **Hybrid VoWLAN-cellular system and method for establishing an outgoing cellular call as an enterprise call**

(57) The application relates to systems based upon Voice-over-IP and Session Initiation Protocol-based signaling systems that utilize the existing enterprise IP infrastructure. Mobile communication devices are being enhanced to provide SIP-based communications (including VoIP) over WLAN access as well as cellular networks, thereby allowing these devices to provide mobile telephony communications capability when within the enterprise as well as when away from the enterprise. However, these networks cannot currently commercially support carrier-class VoIP telephony services. This problem is solved by the invention in that instead of a VoIP call, a circuit-switched call is established. In particular, a network node (404) is operable, responsive to receiving (408) a request from an enterprise user (118) to initiate origination of an outgoing cellular call to a called party (120), for establishing (418) a first call leg to the enterprise user (118) by sending a circuit-switched call that identifies an enterprise address of the enterprise user (118) as a calling line identity. The network node (404) includes functionality for establishing (430) a second call leg to the called party (120) upon receiving an indication from the enterprise user (118) that the first call leg has been established. The first and second call legs are then patched to establish an end-to-end communications path between the enterprise user (118) and the called party (120), wherein the enterprise address instead of the non-enterprise address is presented to the called party (120) as a calling line identity with respect to the outgoing cellular call from the enterprise user (118).

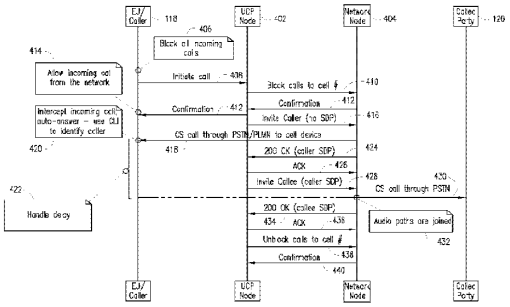


FIG. 4

EP 1 988 697 A1

Description

CROSS-REFERECE TO RELATED APPLICATION(S)

[0001] This application discloses subject matter that is related to the subject matter of the following U.S. patent application(s): (i) "SYSTEM AND METHOD FOR PRESENTING MEDIA TO MULTIPLE PARTIES IN A SIP ENVIRONMENT" (Docket No. 30761-2-US-PAT), Application No.:_, filed even date herewith, in the name(s) of Andrew Allen, Adrian Buckley, Richard George, Brian Oliver, Lap Luu and Dalsu Lee; and (ii) "SYSTEM AND METHOD FOR INTEGRATING AN OUTGOING CELLULAR CALL AS AN ENTERPRISE CALL IN AN IMS ENVIRONMENT" (Docket No. 30761-1-US-PAT), Application No.:_, filed even date herewith, in the name(s) of Andrew Allen, Adrian Buckley, Richard George, Brian Oliver, Lap Luu and Dalsu Lee, which is (are) hereby incorporated by reference.

FIELD OF THE DISCLOSURE

[0002] The present patent disclosure generally relates to communications networks. More particularly, and not by way of any limitation, the present patent disclosure is directed to a system and method for integrating an outgoing cellular call as an enterprise call in a network environment.

BACKGROUND

[0003] Many enterprise networks are replacing their existing Private Branch Exchange (PBX)- and Central Office Exchange (CENTREX)-based telephony systems with systems based upon Voice-over-IP (VoIP) and Session Initiation Protocol (SIP)-based signaling systems that utilize the existing enterprise IP infrastructure, e.g., Local Area Network (LAN) and Wireless LAN (WLAN) technologies. It is not uncommon for enterprise employees to regularly use mobile communications devices when away from the enterprise, which interoperate with cellular networks such as, e.g., the Global System for Mobile Communications (GSM) networks, Code Division Multiple Access (CDMA) networks, and Universal Mobile Telecommunications System (UMTS) networks, to keep in touch with other employees of the enterprise and to conduct business communications with other people outside the enterprise. Additionally, mobile communications devices are being enhanced to provide SIP-based communications (including VoIP) over WLAN access as well as cellular networks, thereby allowing these devices to provide mobile telephony communications capability when within the enterprise as well as when away from the enterprise. It is expected that such developments may allow replacement of the ubiquitous wired desktop phone in the enterprise with dual-mode, WLAN-capable mobile devices.

[0004] Although cellular telephony networks have deployed IP-based data communications capabilities through exploitation of well-known technologies, it is generally understood that these networks cannot currently commercially support carrier-class VoIP telephony services due to issues of delay, Quality of Service (QoS) and efficiency, which prevent cost-effective usage of such networks for purposes of providing acceptable quality voice services. Accordingly, for the foreseeable future, telephony services based upon the existing network infrastructure are likely to continue to utilize conventional circuit-switched network technology for telephony calls.

[0005] Based on the foregoing, it should appreciated that the integration of VoIP enterprise networks with carrier cellular telephony networks in order to serve an enterprise user within the enterprise as well as while away is fraught with numerous difficulties. Moreover, in such scenarios it may be desirable for enterprises to have certain control over the calls made by their employees for tracking and monitoring purposes.

SUMMARY

[0006] The present patent disclosure is broadly directed to a scheme for integrating an outgoing cellular call as an enterprise call wherein an enterprise user's enterprise address is presented to the called party instead of the enterprise user's non-enterprise address (e.g., cellular telephony number). In one aspect, disclosed herein is an embodiment of a method for facilitating integration of an outgoing cellular call as an enterprise call, wherein the outgoing cellular call is originated by an enterprise user towards a called party, the enterprise user having an enterprise address and a non-enterprise address. The claimed embodiment comprises one or more of the following: sending a request to a network node for initiating the outgoing cellular call to the called party with an expectation to receive an incoming circuit-switched call back from the network node within a time window; receiving the incoming circuit-switched call from the network node and identifying that the incoming circuit-switched call contains the enterprise address as a calling line identity; correlating that the incoming circuit-switched call is related to the request to initiate origination of the outgoing cellular call; and providing an indication to the network node (which could be optional in some embodiments) that a call leg is established between the enterprise user and the network node.

[0007] In another aspect, disclosed herein is an embodiment of a method for integrating an outgoing cellular call as

Ex.1002 / Page 508 of 1173
Cisco Systems, Inc.

an enterprise call by an enterprise user having an enterprise address and a non-enterprise address. The claimed embodiment comprises one or more of the following: receiving a request from the enterprise user for initiating the outgoing cellular call to the called party; establishing a first call leg to the enterprise user by sending a circuit-switched call that identifies the enterprise address as a calling line identity; establishing a second call leg to the called party, preferably upon receiving an indication that the first call leg has been established; and patching the first and second call legs to establish an end-to-end communications path between the enterprise user and the called party, wherein the enterprise address is presented instead of the non-enterprise address to the called party as a calling line identity with respect to the outgoing cellular call from the enterprise user.

[0008] In a further aspect, disclosed herein is an embodiment of a user equipment (UE) device operable to generate an outgoing cellular call as an enterprise call to a called party. The claimed embodiment comprises one or more of the following: means for sending a request to a network node to initiate origination of the outgoing cellular call to the called party with an expectation to receive an incoming circuit-switched call back from the network node within a time window; and means for correlating that the incoming circuit-switched call is related to the request to initiate origination of the outgoing cellular call by identifying that the incoming circuit-switched call contains an enterprise address of the enterprise user as a calling line identity.

[0009] In a still further aspect, disclosed herein is an embodiment of a network node for integrating an outgoing cellular call as an enterprise call. The claimed embodiment comprises one or more of the following: means, responsive to receiving a request from the enterprise user to initiate origination of the outgoing cellular call to the called party, for establishing a first call leg to the enterprise user by sending a circuit-switched call that identifies the enterprise address as a calling line identity; means for establishing a second call leg to the called party upon receiving an indication from the enterprise user that the first call leg has been established; and means for patching the first and second call legs to establish an end-to-end communications path between the enterprise user and the called party, wherein an enterprise address of the enterprise user instead of its non-enterprise address is presented to the called party as a calling line identity with respect to the outgoing cellular call from the enterprise user.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] A more complete understanding of the embodiments of the present patent disclosure may be had by reference to the following Detailed Description when taken in conjunction with the accompanying drawings wherein:

[0011] FIG. 1 depicts an exemplary network environment wherein one or more embodiments of the present patent disclosure may be practiced for purposes of integrating an outgoing cellular call as an enterprise call;

[0012] FIG. 2 depicts a flowchart of the present patent disclosure according to one embodiment;

[0013] FIG. 3 depicts another flowchart of the present patent disclosure according to one embodiment;

[0014] FIG. 4 depicts an exemplary message flow diagram according to one embodiment of the present patent disclosure; and

[0015] FIG. 5 depicts a block diagram of an embodiment of a communications device operable for purposes of the present patent disclosure.

DETAILED DESCRIPTION OF THE DRAWINGS

[0016] A system and method of the present patent disclosure will now be described with reference to various examples of how the embodiments can best be made and used. Like reference numerals are used throughout the description and several views of the drawings to indicate like or corresponding parts, wherein the various elements are not necessarily drawn to scale. Referring now to the drawings, and more particularly to FIG. 1, an exemplary network environment 100 is depicted wherein an embodiment of the present patent disclosure may be practiced for integrating an outgoing cellular call as an enterprise call. As depicted, the network environment 100 includes a generalized network infrastructure 102 wherein certain portions may form an enterprise network whereas the remaining portions may comprise an external network arrangement such as one or several service provider networks that serve as intermediary networks with respect to the enterprise network and the well-known PSTN/PLMN infrastructure 114. For purposes herein, an enterprise network may be any communications network internal to a company, office, or organization, and may comprise wireline and/or wireless network infrastructure. Regardless of the actual implementation, the network infrastructure 102 includes an integration server (also referred to as a Unified Communications Platform (UCP) element) 104, a switching element such as a SIP-capable Private Branch Exchange (PBX) 110 and a gateway (GW) element such as a SIP/PSTN GW 112. As alluded to previously, one or more of these elements may be incorporated within an enterprise network infrastructure in one embodiment. Alternatively, one or more of these elements or their functionalities may be hosted in a service provider network. In either arrangement, the functionalities of the elements may be integrated or redistributed into separate network entities. Accordingly, for purposes of the present patent disclosure, a "network node" may comprise a generalized network entity that effectuates or facilitates at least a portion of the functionalities set forth hereinbelow

Ex.1002 / Page 509 of 1173
Cisco Systems, Inc.

with respect to call integration.

[0017] An enterprise user is operable to effectuate communications (e.g., Voice/data/Video calls or multimedia sessions, and the like) in a number of scenarios within the context of the network environment 100 with respect to a called party 120. In general, the enterprise user is capable of initiating communications using one of two addresses: an enterprise address that may be used for calls made from within the enterprise network and a non-enterprise address for calls made from outside the enterprise network. In one application, the enterprise user may be provided with two separate pieces of user equipment (UE) 118: a wireline telephony equipment having the enterprise address that is used when the enterprise user is on the enterprise premises and a mobile communications device (MCD) having a cellular telephony number (i.e., non-enterprise address) that may be used when the enterprise user is away. Alternatively, where local wireless connectivity to the enterprise network is supported, a single wireless UE device operable in two different radio access technologies (RATs) may be provided. In this scenario, when the wireless UE device is attached to the enterprise network via any known or heretofore unknown Wireless Local Area Network (WLAN) technology, calls originated by the enterprise user may have the enterprise address as the calling party number. On the other hand, calls originated when the wireless UE device is attached to a wide area cellular network (WACN) such as the Public Land Mobile Network (PLMN) 114 may have the non-enterprise address (e.g., cellular telephony number) as the calling party number. Accordingly, it should be appreciated that the enterprise user equipment 118 may be a conventional cellular phone having data channel capability (e.g., Short Message Service or SMS capability) or a dual-mode MCD having WLAN capability (for enterprise operation) and WACN capability (for remote operation). Additionally, for purposes of further generalization, the enterprise UE device 118 may also comprise any personal computer (e.g., desktops, laptops, palmtops, personal digital assistants (PDAs) or other handheld computing devices) equipped with a suitable wireless modem, as well as a communications device operable in both circuit-switched (CS) and packet-switched (PS) communications that may even be capable of effectuating an inter-technology handoff between both CS and PS domains.

[0018] Based on the foregoing, it may be realized that the enterprise and non-enterprise addresses for an enterprise user may take on different forms, depending on the equipment and service provisioning. For instance, the enterprise address may comprise a SIP Uniform Resource Identifier (URI) or an E-164 number. Likewise, the non-enterprise address and the called party address may also comprise either SIP URIs, E.164 numbers, or other identifiers.

[0019] An enterprise data server 116 may be disposed in association with at least a portion of the network 102, preferably with the UCP node 104 when provisioned as part of an enterprise network. A data communications path 122 may be effectuated between the enterprise UE 118 and the enterprise network over the PLMN data network infrastructure via the enterprise data server 116. Regardless of whether integrated within an enterprise network or disposed in a service provider network, UCP node 104 preferably includes a Call Manager functionality 106 as well as a SIP Back-to-Back User Agent (B2BUA) 108 that is operable to perform third-party call control in order to combine multiple call legs together. In general, all enterprise SIP calls may be routed via the UCP node 104 and it is the role of the UCP node 104 to trigger the routing of the incoming SIP calls to the enterprise user regardless of whether UE 118 is attached via the enterprise WLAN or via the PLMN cellular network. Further, as will be described in detail below, the enterprise data server 116 can also receive a trigger message (i.e., a request to originate an outgoing cellular call) from UE 118 that is attached to the PLMN cellular network 114 via the cellular network's data network (such as GPRS or CDMA packet data network, for example) to request that the UCP node 104 establish a call between the enterprise UE 118 and the equipment 120 of the called party.

[0020] Taking reference to FIGS. 1 and 2 together, a generalized scheme 200 for integrating outgoing calls from the enterprise UE 118 when it is attached to the cellular network may be set forth as follows. The enterprise user using its equipment sends a request message to a serving network node (i.e., the UCP element 104 shown in FIG. 1) via the cellular network's data network (block 202). Additionally or alternatively, the request message may also be mediated via an enterprise data server. In one embodiment, the request may comprise a SIP Request such as a SIP REFER message or some other SIP Request (e.g., a SIP INVITE message) either sent directly to the enterprise data server 116 via the cellular network's data network or routed to the UCP node 104 via the cellular network's SIP based infrastructure such as the IP Multimedia Subsystem (IMS). Alternatively, the message may not be a SIP Message at all and could be any message that contains the necessary information to enable the UCP node 104 to establish a call between the enterprise UE 118 and the called party's equipment 120 that the enterprise user is attempting to call (e.g., an SMS message, an Unstructured Supplementary Service Data (USSD) message, or an IP based message). In accordance with an embodiment, the following pieces of information may be transmitted as part of the request message: (i) the enterprise address (e.g., SIP URI or E.164 number) that the enterprise user is reachable at; (ii) the non-enterprise address (e.g., E.164 number) that the enterprise UE is reachable at when it is attached to the cellular network; (iii) the E.164 number or SIP URI of the called party; and (iv) an indication of whether privacy is required. Upon receiving the request message from the enterprise UE (block 204), the service logic at the UCP node 104 uses the received information to effectuate two call legs in association with a switching node such as a SIP-capable PBX/CENTREX node, a first call leg between the switching node and the enterprise UE and a second call leg between the called party's UE and the switching node wherein the enterprise user's enterprise address is presented to the called party instead of the non-

Ex.1002 / Page 510 of 1173
Cisco Systems, Inc.

enterprise address associated with the UE (i.e., the cellular number) (block 206). Thereafter, the first and second call legs are patched together wherein the two respective Session Description Protocol (SDP) streams associated with the call legs are joined in order to establish an end-to-end bearer communications path between the enterprise user and the called party (block 208).

[0021] Set forth below is an example of how a SIP REFER request can be used to trigger the UCP node 104 to establish an outgoing call within the context of the scheme described above:

Table I

```
REFER sip: IntegrationServer@companyXXX.com; SIP/2.0
Via: SIP/2.0/UDP PIN12345678.blackberry.com
     ;branch=z9hG4bKhjhs8ass83

Max-Forwards: 70
To: <sip: IntegrationServer@companyXXX.com>
From: Mike <sip:Mike@companyXXX.com>;tag=32331
Call-ID: d432fa84b4c76e66710
Cseq: 2 REFER
Contact: <sip:PIN12345678.blackberry.com>
Refer-To: <cid:cn35t8jf02@companyXXX.com>
Require: multiple-refer
Content-Type: application/resource-lists+xml
Content-Disposition: recipient-list
Content-Length: 362
Content-ID: <cn35t8jf02@example.com>

<?xml version="1.0" encoding="UTF-8"?>
<resource-lists  xmlns+"um:ietf:params:xml:ns:resource-
lists"
          Xmins:xsi="http://www.w3.org/2001/XML.Schema-
instance">
<list>
<entry uri="tel: 098-765-4321"/>
<entry uri="tel: 123-456-7890"/>
</list>
</resource-lists>
```

[0022] Those skilled in the art will recognize that the above SIP REFER request embodiment uses the Resource List mechanism defined in draft-ietf-sip-multiple-refer and draft-ietf-simple-xcap-list-user to trigger the sending of a SIP INVITE request towards both the enterprise UE 118 and the called party equipment 120 using the list entry uri elements to deliver both the E.164 number that the enterprise UE is reachable at via the cellular network and the E.164 number of the party being called. Accordingly, when the UCP node 104 receives the SIP REFER request or other trigger message, it uses SIP Third Party Call Control to establish two SIP Call legs; one SIP leg to the enterprise UE via the PBX, SIP-PSTN Gateway and the circuit-switched cellular network; the other SIP leg to the called party. As pointed out previously, these two call legs are joined together at the UCP node 104 in order to form a single end-to-end call between the enterprise user and the called party. The SIP INVITE requests sent contain the enterprise address of the enterprise UE terminal which can be in the form of SIP URI or as an E.164 number in a TEL URI along with the appropriate privacy setting if requested in the SIP REFER request. Alternatively, the privacy setting may be required by the enterprise network based on certain service provisioning policies and profiles. The enterprise address of the enterprise UE terminal can be transported in the SIP INVITE request using the SIP From header, Referred-By header, P-Asserted-Identity header, Identity header or Remote-Party-ID header. If a SIP URI is used as the enterprise address of the enterprise UE

Ex.1002 / Page 511 of 1173
Cisco Systems, Inc.

terminal, the SIP-PBX 110 may translate this address to the corresponding E.164 number that represents the enterprise address of the device. The SIP-PSTN GW 112 includes the E.164 number that represents the enterprise address of the enterprise UE terminal in the Calling Line Identity in the circuit-switched signaling messages.

[0023] With respect to the behavior of the enterprise UE for purposes of facilitating integration of an outgoing cellular call, reference may now be taken to FIG. 3 wherein a flowchart is depicted. When a request message for initiating an outgoing cellular call to a called party is transmitted to the network infrastructure, there is an expectation to receive an incoming circuit-switched call back from the network within a time window (block 302). Accordingly, a timer mechanism may be started at the application level to determine when to receive the circuit-switched call back in response to the outgoing request message. In one embodiment, if the timer expires, the enterprise UE device may try a number of times until a limit is reached, whereupon the call is considered to have failed. When the enterprise UE device receives a call establishment SETUP signaling request via the circuit-switched PSTN/PMLN signaling, the logic executing on the device is operable to identify that the circuit-switched call contains the enterprise address as the Calling Line Identity (block 304) (that is, the Calling Line Identity in the SETUP is the enterprise UE's enterprise address), and based thereon, the logic determines that this incoming call is related to the requested outgoing call (requested via the SIP REFER request or other message) (block 306). Accordingly, the logic operates to suppress generation of an alert to the enterprise user but establishes the circuit-switched call and stops the application timer (block 306). Further, the enterprise UE may provide an indication to the network that the call leg has been established (block 308). Accordingly, in one embodiment, the UCP node may wait until it receives such an acknowledgement of the establishment of the call leg with the enterprise UE device before attempting to establish the call leg to the called user by sending an SIP INVITE request in order to avoid the possibility of the called party answering before the call leg with the enterprise UE device is established (i.e., avoidance of a race condition). In the meantime, until the call legs are patched, there may be a delay experienced at the enterprise UE from the time the circuit-switched call leg with the network is established. Appropriate delay handling mechanisms(s) may therefore be provided to mitigate the delay.

[0024] When the called party's equipment receives the circuit-switched SETUP message (or SIP INVITE request if the called party is using a SIP phone within the enterprise SIP network or an external SIP network), the Calling Line Identity in the case of the circuit-switched SETUP message (or From header, Referred-By header, P-Asserted-Identity header, Identity header or Remote-Party-ID header in the case of SIP INVITE message) contains the enterprise address (e.g., E.164 number or SIP URI) of the enterprise UE device to be presented to the called party for Calling Line Identity Presentation (if provided based on the privacy setting). The called phone rings the user and returns an ALERTING message in the case of a circuit-switched call (or a SIP 180 "Ringing" response in the case of a SIP call). An ALERTING message will be translated by the SIP-PSTN gateway to a SIP 180 "Ringing" response. When the SIP 180 "Ringing" response is received at the UCP node, the service logic operable thereat may send a notification of "Ringing" back to the enterprise UE terminal via the cellular network's data network. In the case that the call establishment was triggered using a SIP REFER request, this notification may be in the form of a SIP NOTIFY request as specified in RFC 3515. In the case a message other than a SIP REFER request was used, the notification of "Ringing" may be sent using some other message. It is necessary to use the connection via the cellular network's data network to notify the "Ringing" since the call leg that is established with the enterprise UE terminal via the circuit-switched network is "in the wrong direction" to be able to indicate ALERTING using the circuit-switched signaling protocol.

[0025] Upon answering by the enterprise user, the UE terminal sends the circuit-switched CONNECT message (or SIP 200 "OK" response if the called party is using a SIP phone within the enterprise SIP network or an external SIP network). A CONNECT message will be translated by the SIP-PSTN GW to a SIP 200 "OK" response. When the SIP 200 "OK" response is received at the UCP node 104, it can send a notification of "OK" back to the enterprise UE terminal via the cellular network's data network. In the case that the call establishment was triggered using a SIP REFER request, this notification will be in the form of a SIP NOTIFY request as specified in RFC 3515. In the case a message other than a SIP REFER request was used, the notification of "OK" may be sent using some other message. At this point the call is established via the cellular network between the enterprise UE terminal and the called party, with the enterprise address of the enterprise UE terminal being displayed as the identity of the calling party.

[0026] FIG. 4 depicts an exemplary message flow diagram according to an embodiment of the process set forth above. As illustrated, a UCP node 402 and a network node 404 are exemplified to highlight the message flow between the enterprise UE 118 and the network infrastructure in particular detail. Upon blocking all incoming calls to the enterprise UE 118 (block 406), a request with respect to an outgoing call is initiated (reference numeral 408). In response, the UCP node 402 sends a message to the network node 404 (e.g., SIP-PBX) to block calls to the enterprise UE 118. A confirmation 412 is then propagated from the network node 404 to enterprise UE 118 via the UCP node 412, whereupon incoming calls from the network may be allowed (block 414). The UCP node 402 transmits a message 416 to the network node 404 to invite the enterprise user (i.e., caller) with respect to establishing a CS call 418 through the cellular network to the enterprise UE 118. Service logic at the enterprise UE 118 is operable to intercept the incoming CS call setup and identify that the enterprise address of the enterprise user is the CLI (block 420). Thereafter, a SIP 200 "OK" message 424 is generated by the network node 404 towards the UCP node 402 with respect to caller SDP. In response, an

Ex.1002 / Page 512 of 1173
Cisco Systems, Inc.

acknowledgement (ACK) 426 is generated by the UCP node 402. The UCP node 402 also generates a message 428 towards the network node 404 to invite the called party (i.e., callee) with respect to establishing a CS call 430 therewith through the PSTN/PLMN. As shown in block 422, appropriate service logic may be provided for handling the delay before patching the call legs. Pursuant to joining the audio paths (block 432), a SIP 200 "OK" message 434 is generated by the network node 404 towards the UCP node 402 with respect to callee SDP. In response, an acknowledgement (ACK) 436 is generated by the UCP node 402. A message 438 is provided thereafter by the UCP node 402 to the network node 404 in order to unblock calls to the enterprise UE 118, resulting in a confirmation 440 by the network node 404. It should be appreciated that the various operations set forth herein may be accomplished via a number of means, including software (e.g., program code), firmware, hardware, or in any combination, usually in association with a processing system. Where the processes are embodied in software, such software may comprise program instructions that form a computer program product, uploadable service application software, or software downloadable from a remote station, and the like.

[0027] FIG. 5 depicts a block diagram of an embodiment of a communications device 500 operable as a UE device, e.g., the enterprise UE 118, for purposes of the present patent disclosure. It will be recognized by those skilled in the art upon reference hereto that although an embodiment of UE 118 may comprise an arrangement similar to one shown in FIG. 5, there can be a number of variations and modifications, in hardware, software or firmware, with respect to the various modules depicted. Further, a UE device 500 for purposes of the present disclosure may comprise a mobile equipment (ME) device without a removable storage module and/or a mobile device coupled with such a storage module. Accordingly, the arrangement of FIG. 5 should be taken as illustrative rather than limiting with respect to the embodiments of the present patent disclosure. A microprocessor 502 providing for the overall control of an embodiment of UE 500 is operably coupled to a communication subsystem 504 that may preferably be capable of multi-mode communications (e.g., CS domain and PS domain). The communication subsystem 504 generally includes one or more receivers 508 and one or more transmitters 514 as well as associated components such as one or more local oscillator (LO) modules 510 and a processing module such as a digital signal processor (DSP) 512. As will be apparent to those skilled in the field of communications, the particular design of the communication module 504 may be dependent upon the communications networks with which the mobile device is intended to operate (e.g., a CDMA network, a GSM network, WLAN, et cetera). Regardless of the particular design, however, signals received by antenna 506 through appropriate access infrastructure 505 (e.g., cellular base station towers, WLAN hot spots, etc.) are provided to receiver 508, which may perform such common receiver functions as signal amplification, frequency down conversion, filtering, channel selection, analog-to-digital (A/D) conversion, and the like. Similarly, signals to be transmitted are processed, including modulation and encoding, for example, by DSP 512, and provided to transmitter 514 for digital-to-analog (D/A) conversion, frequency up conversion, filtering, amplification and transmission over the air-radio interface via antenna 516.

[0028] Microprocessor 502 may also interface with further device subsystems such as auxiliary input/output (I/O) 518, serial port 520, display 522, keyboard/keypad 524, speaker 526, microphone 528, random access memory (RAM) 530, a short-range communications subsystem 532, and any other device subsystems, e.g., timer mechanisms, generally labeled as reference numeral 533. To control access, a USIM/RUIM interface 534 may also be provided in communication with the microprocessor 602. In one implementation, USIM/RUIM interface 534 is operable with a USIM/RUIM card having a number of key configurations 544 and other information 546 such as identification and subscriber-related data.

[0029] Operating system software and applicable service logic software may be embodied in a persistent storage module (i.e., non-volatile storage) such as Flash memory 535. In one implementation, Flash memory 535 may be segregated into different areas, e.g., storage area for computer programs 536 (e.g., service processing logic), as well as data storage regions such as device state 537, address book 539, other personal information manager (PIM) data 541, and other data storage areas generally labeled as reference numeral 543. A transport stack 545 may be provided to effectuate one or more appropriate radio-packet transport protocols. In addition, enterprise call request messaging logic 548, including memory storage for storing pertinent address information, is provided for facilitating integration of outgoing calls as set forth hereinabove.

[0030] It is believed that the operation and construction of the embodiments of the present patent application will be apparent from the Detailed Description set forth above. While the exemplary embodiments shown and described may have been characterized as being preferred, it should be readily understood that various changes and modifications could be made therein without departing from the scope of the present disclosure as set forth in the following claims.

Claims

1. A method for facilitating integration of an outgoing cellular call as an enterprise call, wherein said outgoing cellular call is originated by an enterprise user (118) towards a called party (120), said enterprise user (118) having an enterprise address and a non-enterprise address, comprising:

sending (302) a request to a network node (104) for initiating said outgoing cellular call to said called party (120) with an expectation to receive an incoming circuit-switched call back from said network node (104) within a time window;
receiving (304) said incoming circuit-switched call from said network node (104) and identifying that said incoming circuit-switched call contains said enterprise address as a calling line identity;
correlating (306) that said incoming circuit-switched call is related to said request to initiate origination of said outgoing cellular call; and
providing (308) an indication to said network node (104) that a call leg is established between said enterprise user (118) and said network node (104).

2. The method as recited in claim 1, wherein said request is sent as one of a Short Message Service (SMS) message, an Unstructured Supplementary Service Data (USSD)-based message, a Session Initiation Protocol (SIP) message, and an Internet Protocol (IP)-based message.

3. The method as recited in claim 1 or claim 2, wherein said request includes said enterprise address, said non-enterprise address, said called party's address, and a privacy indication.

4. The method as recited in claim 3, wherein said enterprise address comprises one of a SIP Uniform Resource Identifier (URI) and an E-164 number.

5. The method as recited in claim 3, wherein said non-enterprise address comprises a cellular telephony network number in E-164 format.

6. The method as recited in claim 3, wherein said called party's address comprises one of a SIP Uniform Resource Identifier (URI) and an E-164 number.

7. The method as recited in claim 1, wherein said time window is effectuated based on commencing a timer with respect to sending said request.

8. The method as recited in claim 7, wherein said timer is terminated upon receipt of said incoming circuit-switched call from said network node (104).

9. The method as recited in claim 1, further comprising determining whether said time window has elapsed without receiving said incoming circuit-switched call from said network node (104), and if so, continuing to send said request a select number of times.

10. A method for integrating an outgoing cellular call as an enterprise call, wherein said outgoing cellular call is originated by an enterprise user (118) towards a called party (120), said enterprise user (118) having an enterprise address and a non-enterprise address, comprising:

receiving (204) a request from said enterprise user (118) for initiating said outgoing cellular call to said called party (120);
establishing (206) a first call leg to said enterprise user (118) by sending a circuit-switched call that identifies said enterprise address as a calling line identity;
establishing (206) a second call leg to said called party (120) upon receiving an indication that said first call leg has been established; and
patching (208) said first and second call legs to establish an end-to-end communications path between said enterprise user (118) and said called party (120), wherein said enterprise address is presented instead of said non-enterprise address to said called party (120) as a calling line identity with respect to said outgoing cellular call from said enterprise user (118).

11. The method as recited in claim 10, wherein said request is received as one of a Short Message Service (SMS) message, an Unstructured Supplementary Service Data (USSD)-based message, a Session Initiation Protocol (SIP) message, and an Internet Protocol (IP)-based message.

12. The method as recited in claim 10 or claim 11, wherein said request includes said enterprise address, said non-enterprise address, said called party's address, and a privacy indication.

Ex.1002 / Page 514 of 1173
Cisco Systems, Inc.

13. The method as recited in claim 12, wherein said enterprise address comprises one of a SIP Uniform Resource Identifier (URI) and an E-164 number.

14. The method as recited in claim 12, wherein said non-enterprise address comprises a cellular telephony network number in E-164 format.

15. The method as recited in claim 12, wherein said called party's address comprises one of a SIP Uniform Resource Identifier (URI) and an E-164 number.

16. A user equipment (UE) device (500) operable to generate an outgoing cellular call as an enterprise call, wherein said outgoing cellular call is originated towards a called party (118), comprising:

means for sending (302) a request to a network node (104) to initiate origination of said outgoing cellular call to said called party (118) with an expectation to receive an incoming circuit-switched call back from said network node (104) within a time window; and
means for correlating (306) that said incoming circuit-switched call is related to said request to initiate origination of said outgoing cellular call.

17. The UE device (500) as recited in claim 16, further comprising means for providing (308) an indication to said network node (104) that a call leg is established between said UE device (500) and said network node (104).

18. The UE device (500) as recited in claim 16 or claim 17, wherein said request comprises one of a Short Message Service (SMS) message, an Unstructured Supplementary Service Data (USSD)-based message, a Session Initiation Protocol (SIP) REFER message, a SIP INVITE message, and an Internet Protocol (IP)-based message.

19. The UE device (500) as recited in claim 18, wherein said request includes said enterprise address, said non-enterprise address, said called party's address, and a privacy indication.

20. A network node (104) for integrating an outgoing cellular call as an enterprise call, wherein said outgoing cellular call is originated by an enterprise user (118) towards a called party (120), said enterprise user (118) having an enterprise address and a non-enterprise address, comprising:

means, responsive to receiving (204) a request from said enterprise user (118) to initiate origination of said outgoing cellular call to said called party (120), for establishing (206) a first call leg to said enterprise user (118) by sending a circuit-switched call that identifies said enterprise address as a calling line identity;
means for establishing (206) a second call leg to said called party (120) upon receiving an indication from said enterprise user (118) that said first call leg has been established; and
means for patching (208) said first and second call legs to establish an end-to-end communications path between said enterprise user (118) and said called party (120), wherein said enterprise address is presented instead of said non-enterprise address to said called party (120) as a calling line identity with respect to said outgoing cellular call from said enterprise user (118).

21. The network node (104) as recited in claim 20, wherein said request comprises one of a Short Message Service (SMS) message, an Unstructured Supplementary Service Data (USSD)-based message, a Session Initiation Protocol (SIP) REFER message, a SIP INVITE message, and an Internet Protocol (IP)-based message.

22. The network node (104) as recited in claim 20 or claim 21, wherein said request includes said enterprise address, said non-enterprise address, said called party's address, and a privacy indication.

23. The network node (104) as recited in claim 22, wherein said enterprise address comprises one of a SIP Uniform Resource Identifier (URI) and an E-164 number.

24. The network node as recited in claim 22, wherein said called party's address comprises one of a SIP Uniform Resource Identifier (URI) and an E-164 number.

Ex.1002 / Page 515 of 1173
Cisco Systems, Inc.

Amended claims in accordance with Rule 137(2) EPC.

1. A method for facilitating integration of an outgoing cellular call as an enterprise call, wherein said outgoing cellular call is originated by an enterprise user (118) towards a called party (120), said enterprise user (118) having an enterprise address and a non-enterprise address, comprising:

sending (302) a request to a network node (104) for initiating said outgoing cellular call to said called party (120) with an expectation to receive an incoming circuit-switched call back from said network node (104) within a time window;
receiving (304) said incoming circuit-switched call from said network node (104) and identifying that said incoming circuit-switched call contains said enterprise address as a calling line identity;
correlating (306) that said incoming circuit-switched call is related to said request to initiate origination of said outgoing cellular call; and
providing (308) an indication to said network node (104) that a call leg is established between said enterprise user (118) and said network node (104).

2. The method as recited in claim 1, wherein said request is sent as one of a Short Message Service (SMS) message, an Unstructured Supplementary Service Data (USSD)-based message, a Session Initiation Protocol (SIP) message, and an Internet Protocol (IP)-based message.

3. The method as recited in claim 1 or claim 2, wherein said request includes said enterprise address, said non-enterprise address, said called party's address, and a privacy indication.

4. The method as recited in claim 3, wherein said enterprise address comprises one of a SIP Uniform Resource Identifier (URI) and an E-164 number.

5. The method as recited in claim 3, wherein said non-enterprise address comprises a cellular telephony network number in E-164 format.

6. The method as recited in claim 3, wherein said called party's address comprises one of a SIP Uniform Resource Identifier (URI) and an E-164 number.

7. The method as recited in claim 1, wherein said time window is effectuated based on commencing a timer with respect to sending said request.

8. The method as recited in claim 7, wherein said timer is terminated upon receipt of said incoming circuit-switched call from said network node (104).

9. The method as recited in claim 1, further comprising determining whether said time window has elapsed without receiving said incoming circuit-switched call from said network node (104), and if so, continuing to send said request a select number of times.

10. A user equipment (UE) device (500) operable to generate an outgoing cellular call as an enterprise call, wherein said outgoing cellular call is originated towards a called party (118), comprising:

means for sending (302) a request to a network node (104) to initiate origination of said outgoing cellular call to said called party (118) with an expectation to receive an incoming circuit-switched call back from said network node (104) within a time window;
means for receiving (304) said incoming circuit-switched call from said network node (104) and for identifying that said incoming circuit-switched call contains an enterprise address associated with said UE device as a calling line identity; and
means for correlating (306) that said incoming circuit-switched call is related to said request to initiate origination of said outgoing cellular call.

11. The UE device (500) as recited in claim 10, further comprising means for providing (308) an indication to said network node (104) that a call leg is established between said UE device (500) and said network node (104).

12. The UE device (500) as recited in claim 10 or claim 11, wherein said request comprises one of a Short Message

Ex.1002 / Page 516 of 1173
Cisco Systems, Inc.

Service (SMS) message, an Unstructured Supplementary Service Data (USSD)-based message, a Session Initiation Protocol (SIP) REFER message, a SIP INVITE message, and an Internet Protocol (IP)-based message.

13. The UE device (500) as recited in claim 12, wherein said request includes said enterprise address, said non-enterprise address, said called party's address, and a privacy indication.

Ex.1002 / Page 517 of 1173
Cisco Systems, Inc.

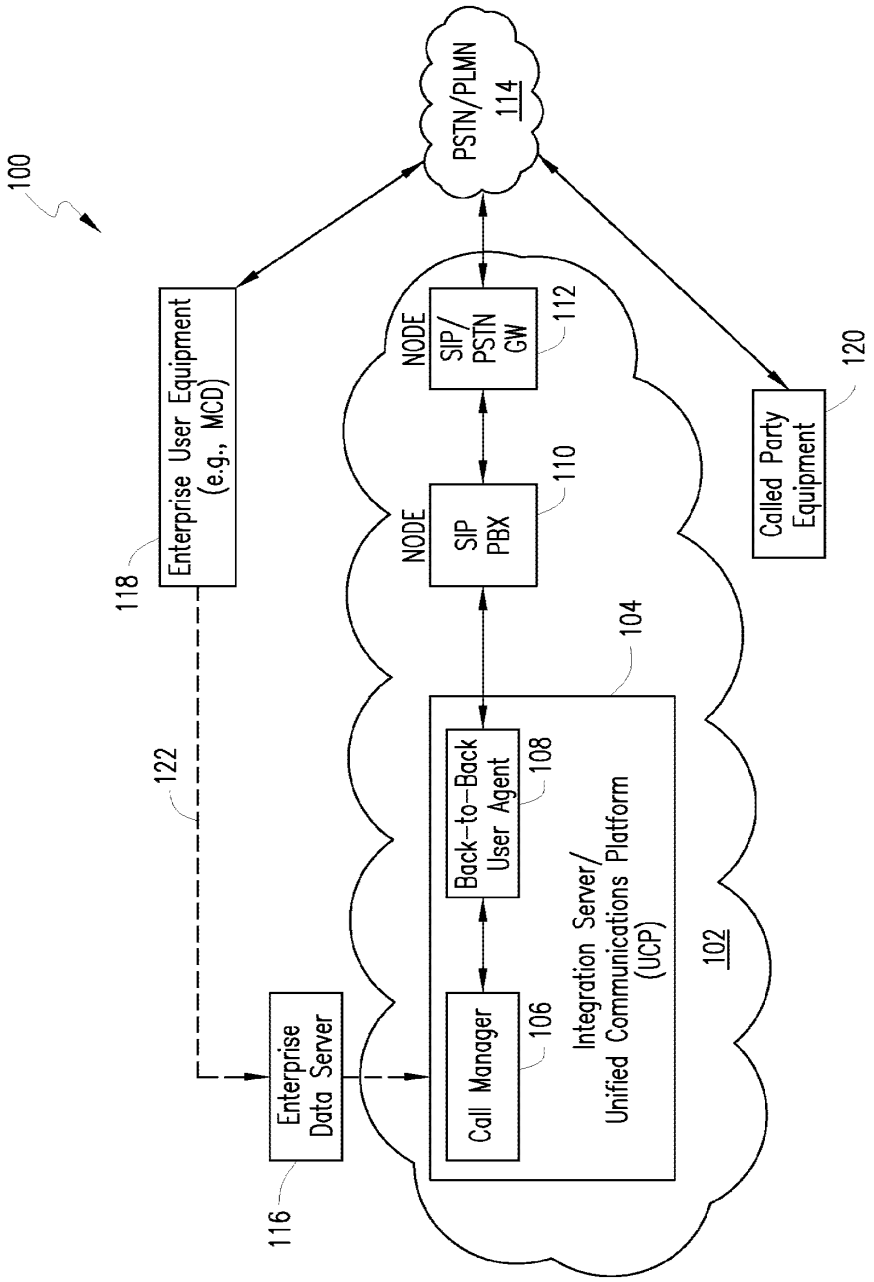

100
PSTN/PLMN
114
Enterprise User Equipment
(e.g., MCD)
118
NODE
SIP/
PSTN
GW
112
NODE
SIP
PBX
110
Called Party
Equipment
120
104
Back-to-Back
User Agent
108
Integration Server/
Unified Communications Platform
(UCP)
102
Call Manager
106
Enterprise
Data Server
116
122

FIG. 1

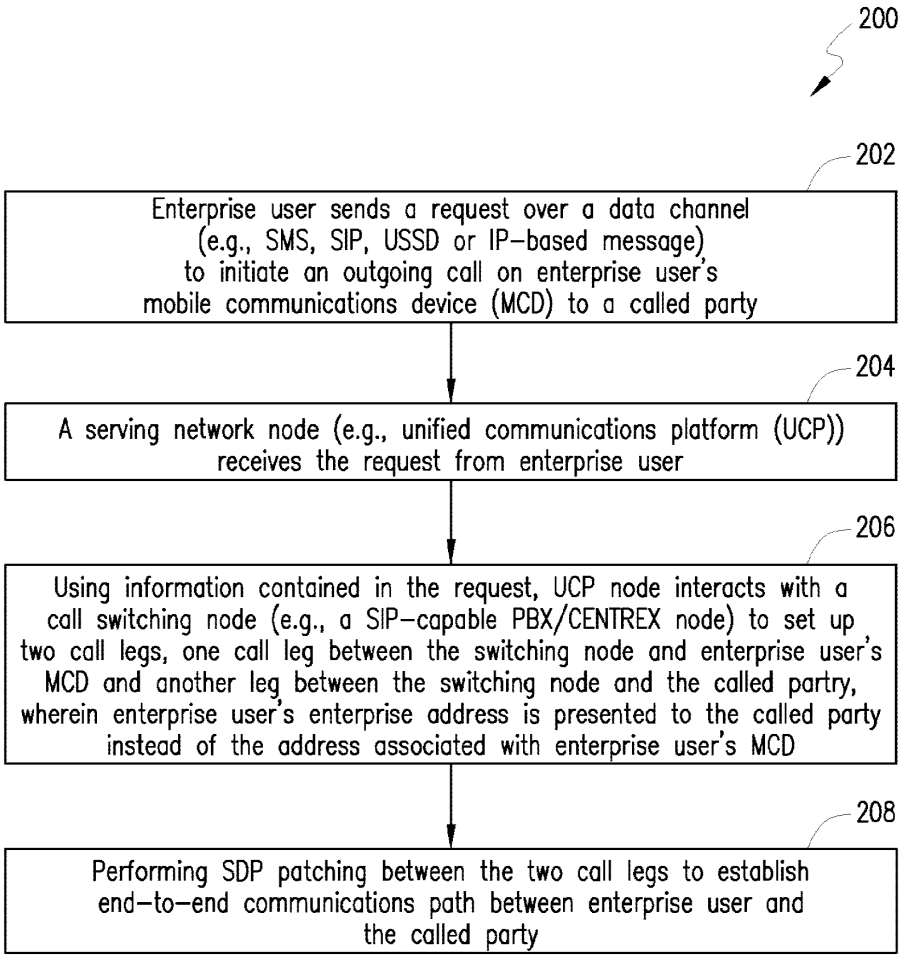


FIG. 2

Ex.1002 / Page 519 of 1173
Cisco Systems, Inc.

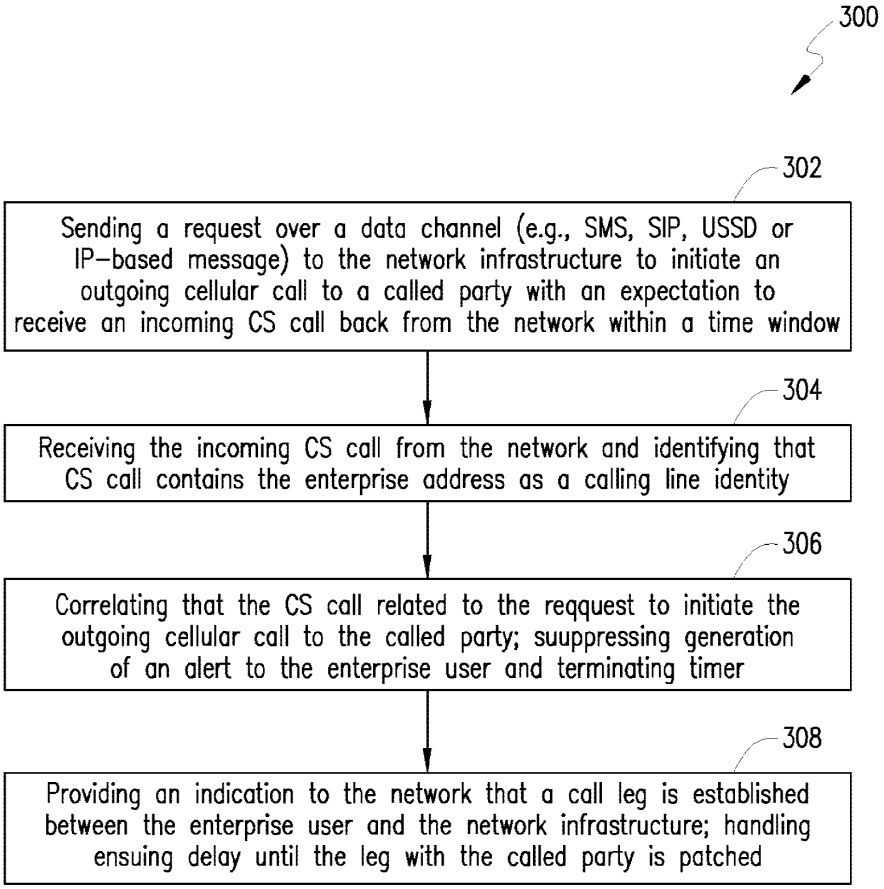

300
302
Sending a request over a data channel (e.g., SMS, SIP, USSD or IP-based message) to the network infrastructure to initiate an outgoing cellular call to a called party with an expectation to receive an incoming CS call back from the network within a time window
304
Receiving the incoming CS call from the network and identifying that CS call contains the enterprise address as a calling line identity
306
Correlating that the CS call related to the reqquest to initiate the outgoing cellular call to the called party; suuppressing generation of an alert to the enterprise user and terminating timer
308
Providing an indication to the network that a call leg is established between the enterprise user and the network infrastructure; handling ensuing delay until the leg with the called party is patched

FIG. 3

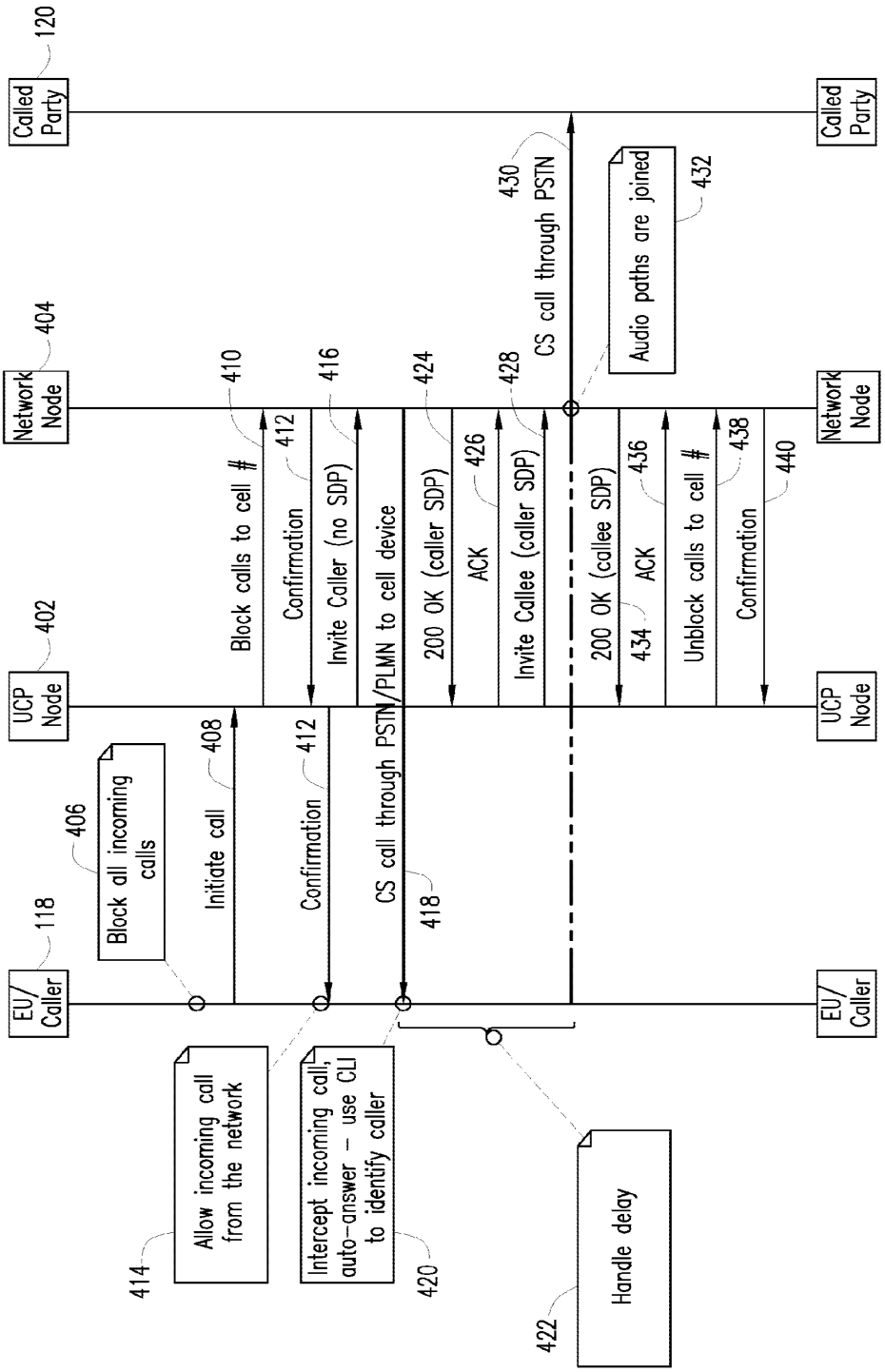


FIG. 4

Ex.1002 / Page 521 of 1173
Cisco Systems, Inc.

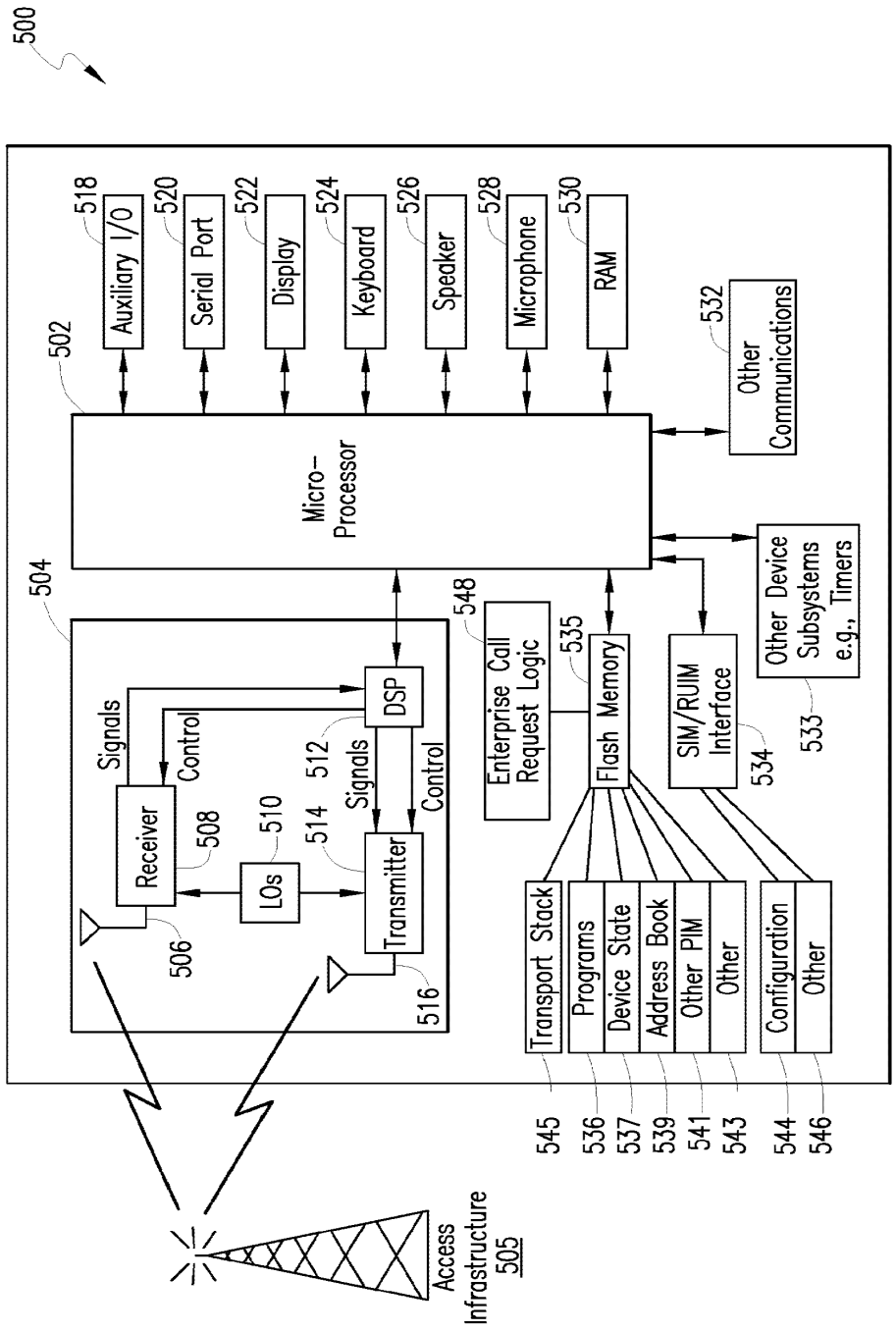

500
502
Micro-Processor
504
Auxiliary I/O
518
Serial Port
520
Display
522
Keyboard
524
Speaker
526
Microphone
528
RAM
530
Other Communications
532
Other Device Subsystems e.g., Timers
533
SIM/RUIM Interface
534
Flash Memory
535
Enterprise Call Request Logic
548
DSP
Signals
Control
512
Receiver
508
LOs
510
514
Transmitter
506
516
Transport Stack
Programs
Device State
Address Book
Other PIM
Other
Configuration
Other
545
536
537
539
541
543
544
546
Access Infrastructure
505

FIG. 5

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 07 10 7246

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	GB 2 342 536 A (ORANGE PERSONAL COMM SERV LTD [GB]) 12 April 2000 (2000-04-12)	1-9, 11-19, 21-24	INV. H04M7/12 H04L29/06
Y	* page 8, line 10 - page 9, line 12; figure 3 *	10,20	H04M1/253 H04M1/725
Y	US 2007/015535 A1 (LABAUVE LANCE [US] ET AL) 18 January 2007 (2007-01-18) * paragraph [0078] *	10,20	
A	EP 0 582 440 A2 (AMERICAN TELEPHONE & TELEGRAPH [US] AT & T CORP [US]) 9 February 1994 (1994-02-09) * figures 5,6 *	1,16	

TECHNICAL FIELDS SEARCHED (IPC)

H04M
H04Q
H04L

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	28 September 2007	Cremer, Jan

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

Ex.1002 / Page 523 of 1173
Cisco Systems, Inc.

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 07 10 7246

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

28-09-2007

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
GB 2342536 A	12-04-2000	AU 6214899 A	01-05-2000
		EP 1118240 A1	25-07-2001
		WO 0022863 A1	20-04-2000
US 2007015535 A1	18-01-2007	US 2007015536 A1	18-01-2007
EP 0582440 A2	09-02-1994	CA 2101395 A1	06-02-1994
		DE 69332300 D1	24-10-2002
		DE 69332300 T2	15-05-2003
		ES 2181683 T3	01-03-2003
		JP 3369263 B2	20-01-2003
		JP 6197172 A	15-07-1994
		MX 9304689 A1	31-05-1994
		US 5311583 A	10-05-1994

EPO FORM P0459

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

Ex.1002 / Page 524 of 1173
Cisco Systems, Inc.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 638 275 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
22.03.2006 Bulletin 2006/12

(51) Int Cl.:
H04L 12/56 (2006.01)

(21) Application number: 05255066.2

(22) Date of filing: 17.08.2005

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC NL PL PT RO SE SI SK TR
Designated Extension States:
AL BA HR MK YU

(30) Priority: 18.08.2004 GB 0418379

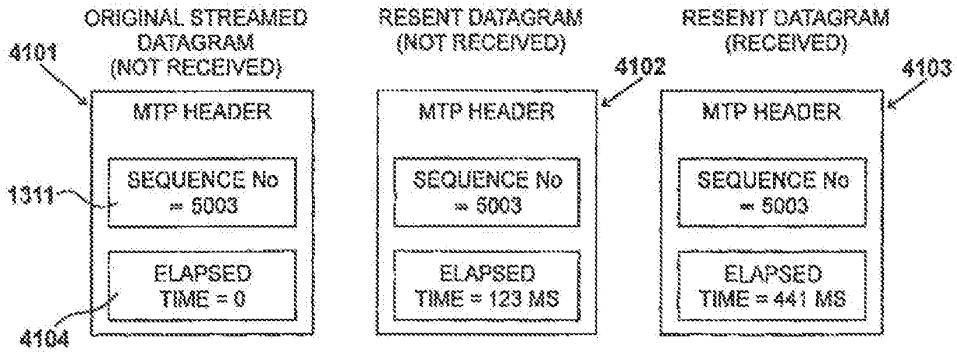
(71) Applicant: Wecomm Limited
Austin Friars,
London EC2N 2HA (GB)

(72) Inventors:
- Sturrock, Oliver
London W12 8NT (GB)
- Wentford, Timothy John
Pinner HA5 1NB (GB)

(74) Representative: Chapman, Paul Nicholas et al
Atkinson Burrington Limited
29 President Buildings
President Way
Sheffield S4 7UR (GB)

(54) Transmitting packets of data

(57) Data packet transmission involves transmitting a first data packet from a first station over a network to create a first transmission with the intention of the first transmission being received at a second station. Said first data packet is retransmitted from the first station to the second station to create a second transmission, wherein said second transmission of said first data packet includes latency information indicating the time between said first transmission and said second transmission. The second station processes said latency information to determine a resend latency measurement.



RESEND LATENCY = ELAPSED TIME IN RECEIVED DATAGRAM

RECEIVE EMPTY DATAGRAM Y REDUCE RESEND LATENCY
NO DATAGRAMS RECEIVED Y INCREASE RESEND LATENCY

APPLICATION LATENCY = CONNECTION LATENCY + PROTOCOL LATENCY

Figure 41

EP 1 638 275 A2

Printed by Jouve, 75001 PARIS (FR)