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.
14/667,516	11/24/2015	9198117	RALEP007C11C4	5348

106963 7590 11/04/2015

Headwater Partners I LLC
555 Twin Dolphin Drive, Suite 310
Redwood Shores, CA 94065

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):

Gregory G. Raleigh, Woodside, CA;
Headwater Partners I LLC, Redwood City, CA;

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.

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.
14/667,516	03/24/2015	Gregory G. Raleigh	RALEP007C11C4	5348

106963 7590 10/22/2015

Headwater Partners I LLC
555 Twin Dolphin Drive, Suite 310
Redwood Shores, CA 94065

EXAMINER	
RUDY, ANDREW J	

ART UNIT	PAPER NUMBER
3687	

NOTIFICATION DATE	DELIVERY MODE
10/22/2015	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patent@headwaterllc.com
krista@jacobseniplaw.com

Corrected Notice of Allowability	**Application No.** 14/667,516	**Applicant(s)** RALEIGH, GREGORY G.	
	Examiner ANDREW JOSEPH RUDY	**Art Unit** 3687	**AIA (First Inventor to File) Status** No

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

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

1. ☒ This communication is responsive to *the 09 October 2015 IDS's*.
   ☐ 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 *2-19*. 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 _____
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
5. ☐ Examiner's Amendment/Comment
6. ☐ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/ANDREW JOSEPH RUDY/
Primary Examiner
Art Unit: 3687

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	14667516
Filing Date	2015-03-24
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP007C11C4

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	5974439	A	1999-10-26	Bollella, Gregory	
	2	6882718	B1	2005-04-19	Smith, Benjamin V.	
	3	8644813	B1	2014-02-04	Gailloux et al.	
	4	7058022	B1	2006-06-06	Carolan et al.	
	5	7149521	B2	2006-12-12	Sundar et al.	
	6	7162237	B1	2007-01-09	Silver et al.	
	7	7200112	B2	2007-04-03	Sundar et al.	
	8	7266371	B1	2007-09-04	Amin et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C4

	9	7366654	B2	2008-04-29	Moore, Robert C.	
	10	7391724	B2	2008-06-24	Alakoski et al.	
	11	7395244	B1	2008-07-01	Kingsford, Bryan	
	12	7411930	B2	2008-08-12	Montojo et al.	
	13	8667542	B1	2014-03-04	Bertz et al.	
	14	7508799	B2	2009-03-24	Sumner et al.	
	15	7554983	B1	2009-06-30	Muppala, Suresh	
	16	7564799	B2	2009-07-21	Holland et al.	
	17	7817615	B1	2010-10-19	Breau et al.	
	18	7844034	B1	2010-11-30	Oh et al.	
	19	7849477	B2	2010-12-07	Cristofalo et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C4

	20	7899039	B2	2011-03-01	Andreasen et al.	
	21	7978686	B2	2011-07-12	Goyal et al.	
	22	7987496	B2	2011-07-26	Bryce et al.	
	23	8104080	B2	2012-01-24	Burns et al.	
	24	8150394	B2	2012-04-03	Bianconi et al.	
	25	8190122	B1	2012-05-29	Alexander et al.	
	26	8793304	B2	2014-07-29	Lu et al.	
	27	8503455	B2	2013-08-06	Heikens, Heico	
	28	9002342	B2	2015-04-07	Tenhunen et al.	
	29	RE44412		2013-08-06	Naqvi et al.	
If you wish to add additional U.S. Patent citation information please click the Add button.						Add
U.S.PATENT APPLICATION PUBLICATIONS						Remove

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C4

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	20040260766	A1	2004-12-23	Barros et al.	
	2	20050041617	A1	2005-02-24	Huotari et al.	
	3	20060095517	A1	2006-05-04	O'Connor et al.	
	4	20080018494	A1	2008-01-24	Waite et al.	
	5	20080034063	A1	2008-02-07	Yee, Robert	

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] ¡	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]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C4

	1		☐

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

EXAMINER SIGNATURE

Examiner Signature	/Andrew Joseph Rudy/	Date Considered	10/17/2015

*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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

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	14667516
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C4

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
/A.R./	1	7860088		2010-12-28	Lioy, Marcello	
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	14667516
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C4

	1		☐

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

EXAMINER SIGNATURE

Examiner Signature	/Andrew Joseph Rudy/	Date Considered	10/17/2015

*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.

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	14667516
Filing Date	2015-03-24
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP007C11C4

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	5974439	A	1999-10-26	Bollella, Gregory	
	2	6882718	B1	2005-04-19	Smith, Benjamin V.	
	3	8644813	B1	2014-02-04	Gailloux et al.	
	4	7058022	B1	2006-06-06	Carolan et al.	
	5	7149521	B2	2006-12-12	Sundar et al.	
	6	7162237	B1	2007-01-09	Silver et al.	
	7	7200112	B2	2007-04-03	Sundar et al.	
	8	7266371	B1	2007-09-04	Amin et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C4

	9	7366654	B2	2008-04-29	Moore, Robert C.	
	10	7391724	B2	2008-06-24	Alakoski et al.	
	11	7395244	B1	2008-07-01	Kingsford, Bryan	
	12	7411930	B2	2008-08-12	Montojo et al.	
	13	8667542	B1	2014-03-04	Bertz et al.	
	14	7508799	B2	2009-03-24	Sumner et al.	
	15	7554983	B1	2009-06-30	Muppala, Suresh	
	16	7564799	B2	2009-07-21	Holland et al.	
	17	7817615	B1	2010-10-19	Breau et al.	
	18	7844034	B1	2010-11-30	Oh et al.	
	19	7849477	B2	2010-12-07	Cristofalo et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C4

	20	7899039	B2	2011-03-01	Andreasen et al.	
	21	7978686	B2	2011-07-12	Goyal et al.	
	22	7987496	B2	2011-07-26	Bryce et al.	
	23	8104080	B2	2012-01-24	Burns et al.	
	24	8150394	B2	2012-04-03	Bianconi et al.	
	25	8190122	B1	2012-05-29	Alexander et al.	
	26	8793304	B2	2014-07-29	Lu et al.	
	27	8503455	B2	2013-08-06	Heikens, Heico	
	28	9002342	B2	2015-04-07	Tenhunen et al.	
	29	RE44412		2013-08-06	Naqvi et al.	
If you wish to add additional U.S. Patent citation information please click the Add button.						Add
U.S.PATENT APPLICATION PUBLICATIONS						Remove

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C4

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	20040260766	A1	2004-12-23	Barros et al.	
	2	20050041617	A1	2005-02-24	Huotari et al.	
	3	20060095517	A1	2006-05-04	O'Connor et al.	
	4	20080018494	A1	2008-01-24	Waite et al.	
	5	20080034063	A1	2008-02-07	Yee, Robert	

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	14667516
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C4

	1		☐

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	14667516
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C4

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.

☒ Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ None

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	/James E. Harris/	Date (YYYY-MM-DD)	2015-10-08
Name/Print	James E. Harris	Registration Number	40013

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.

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	14667516
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C4

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	7860088		2010-12-28	Lioy, Marcello	
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] ¡	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	14667516
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C4

	1		☐

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	14667516
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C4

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.

☒ Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ None

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	/James E. Harris/	Date (YYYY-MM-DD)	2015-10-08
Name/Print	James E. Harris	Registration Number	40013

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.

Electronic Patent Application Fee Transmittal	
Application Number:	14667516
Filing Date:	24-Mar-2015
Title of Invention:	Network System With Common Secure Wireless Message Service Serving Multiple Applications on Multiple Wireless Devices
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Filer:	James E. Harris/Ann Taylor
Attorney Docket Number:	RALEP007C11C4
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:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	2806	1	90	90
		Total in USD ($)		**90**

Electronic Acknowledgement Receipt	
EFS ID:	23748260
Application Number:	14667516
International Application Number:	
Confirmation Number:	5348
Title of Invention:	Network System With Common Secure Wireless Message Service Serving Multiple Applications on Multiple Wireless Devices
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	James E. Harris/Ann Taylor
Filer Authorized By:	James E. Harris
Attorney Docket Number:	RALEP007C11C4
Receipt Date:	09-OCT-2015
Filing Date:	24-MAR-2015
Time Stamp:	18:56:24
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$90
RAM confirmation Number	4530
Deposit Account	505876
Authorized User	TAYLOR, ANN
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	P007C11C4_IDS1.pdf	612834 2b11f0ae161560430b3fd9e8989ad04ed99b9098	no	7
Warnings:					
Information:					
2	Information Disclosure Statement (IDS) Form (SB08)	P007C11C4_IDS2.pdf	611819 3e8ead67a99d27cc4f4ac82daa55c35e24f5ea29	no	4
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30773 05d705aa03a2a7520f60d71cbba4eb91d4db7279	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1255426		

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

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

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

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

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)

106963 7590 10/07/2015
Headwater Partners I LLC
555 Twin Dolphin Drive, Suite 310
Redwood Shores, CA 94065

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.

Ann Taylor	(Depositor's name)
	(Signature)
October 9, 2015	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/667,516	03/24/2015	Gregory G. Raleigh	RALEP007C11C4	5348

TITLE OF INVENTION: Network System With Common Secure Wireless Message Service Serving Multiple Applications on Multiple Wireless Devices

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	01/07/2016

EXAMINER	ART UNIT	CLASS-SUBCLASS
RUDY, ANDREW J	3687	705-028000

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 James E. Harris
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: Headwater Partners I LLC

(B) RESIDENCE: (CITY and STATE OR COUNTRY): Redwood City, CA

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 505876 (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 October 8, 2015
Typed or printed name James E. Harris Registration No. 40013

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:	14667516			
Filing Date:	24-Mar-2015			
Title of Invention:	Network System With Common Secure Wireless Message Service Serving Multiple Applications on Multiple Wireless Devices			
First Named Inventor/Applicant Name:	Gregory G. Raleigh			
Filer:	James E. Harris/Ann Taylor			
Attorney Docket Number:	RALEP007C11C4			
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:	23748638
Application Number:	14667516
International Application Number:	
Confirmation Number:	5348
Title of Invention:	Network System With Common Secure Wireless Message Service Serving Multiple Applications on Multiple Wireless Devices
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	James E. Harris/Ann Taylor
Filer Authorized By:	James E. Harris
Attorney Docket Number:	RALEP007C11C4
Receipt Date:	09-OCT-2015
Filing Date:	24-MAR-2015
Time Stamp:	19:25:47
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$480
RAM confirmation Number	4818
Deposit Account	505876
Authorized User	TAYLOR, ANN
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

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

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

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

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	P007C11C4_IssueFee.pdf	401224 06a0bc29c7ab0049b1a6c0587abb7753b0c6bd99	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30630 317f69155f3e52b410f9def4123386e89a7e6247	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	431854		

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

106963 7590 10/07/2015

Headwater Partners I LLC
555 Twin Dolphin Drive, Suite 310
Redwood Shores, CA 94065

EXAMINER	
RUDY, ANDREW J	
ART UNIT	PAPER NUMBER
3687	

DATE MAILED: 10/07/2015

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/667,516	03/24/2015	Gregory G. Raleigh	RALEP007C11C4	5348

TITLE OF INVENTION: Network System With Common Secure Wireless Message Service Serving Multiple Applications on Multiple Wireless Devices

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	01/07/2016

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.

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)

106963 7590 10/07/2015
Headwater Partners I LLC
555 Twin Dolphin Drive, Suite 310
Redwood Shores, CA 94065

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.
14/667,516	03/24/2015	Gregory G. Raleigh	RALEP007C11C4	5348

TITLE OF INVENTION: Network System With Common Secure Wireless Message Service Serving Multiple Applications on Multiple Wireless Devices

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	01/07/2016

EXAMINER	ART UNIT	CLASS-SUBCLASS
RUDY, ANDREW J	3687	705-028000

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.
14/667,516	03/24/2015	Gregory G. Raleigh	RALEP007C11C4	5348

106963 7590 10/07/2015

Headwater Partners I LLC
555 Twin Dolphin Drive, Suite 310
Redwood Shores, CA 94065

EXAMINER	
RUDY, ANDREW J	

ART UNIT	PAPER NUMBER
3687	

DATE MAILED: 10/07/2015

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.

Notice of Allowability	Application No. 14/667,516	Applicant(s) RALEIGH, GREGORY G.	
	Examiner ANDREW JOSEPH RUDY	Art Unit 3687	AIA (First Inventor to File) Status No

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

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

1. ☒ This communication is responsive to *the 25 March 2015 Amendment*.
   ☐ 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 *2-19*. 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 _____
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
5. ☒ Examiner's Amendment/Comment
6. ☒ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application is being examined under the pre-AIA first to invent provisions.

2. Further pertinent references of interest are noted on the attached PTO-892.

3. Applicant's six (6) Information Disclosure Statements (IDS's) submitted have been reviewed. Note the attached IDS's.

Allowable Subject Matter

4. Claims 2-19 are allowed.

The following is an examiner's statement of reasons for allowance: Claims 2-19 are allowed as the prior art, either alone or in combination, does not disclose Applicant's inventive claim language. It is noted that the claims have been reviewed in light of Alice Corporation Pty. Ltd. v. CLS Bank International, et al., 573 U. S. ___ (2014). The claims are not drawn to an abstract idea.

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

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to ANDREW JOSEPH RUDY whose telephone number is (571)272-6789. The examiner can normally be reached on Monday thru Friday.

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.

/ANDREW JOSEPH RUDY/
Primary Examiner
Art Unit 3687

Notice of References Cited	Application/Control No. 14/667,516	Applicant(s)/Patent Under Reexamination RALEIGH, GREGORY G.	
	Examiner ANDREW JOSEPH RUDY	Art Unit 3687	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-8,966,018 B2	02-2015	Bugwadia; Jamsheed	G06F9/4411	709/220
*	B	US-8,572,256 B2	10-2013	Babbar; Uppinder Singh	H04L67/322	709/227
*	C	US-8,527,662 B2	09-2013	Biswas; Sanjit	H04L41/04	370/389
*	D	US-8,522,337 B2	08-2013	Adusumilli; Koteshwerrao S.	H04L63/04	380/270
*	E	US-8,073,427 B2	12-2011	Koch; Robert	H04W28/14	340/568.1
*	F	US-7,894,431 B2	02-2011	Goring; Bryan R.	H04L12/5693	370/392
*	G	US-7,849,161 B2	12-2010	Koch; Robert	H04W8/08	455/411
*	H	US-7,627,767 B2	12-2009	Sherman; Stephen	H04W28/14	710/263
*	I	US-7,047,276 B2	05-2006	Liu; Hsiang-Min	H04L67/04	709/201
*	J	US-6,397,259 B1	05-2002	Lincke; Scott D.	G06F17/3089	707/E17.116
*	K	US-6,393,014 B1	05-2002	Daly; Brian Kevin	H04W4/18	370/331
	L	US-				
	M	US-				

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

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

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

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	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

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	20020022472		2002-02-21	WATLER et al.	
	2	20020120540		2002-08-29	KENDE et al.	
	3	20020131404		2002-09-19	MEHTA et al.	
	4	20020138601		2002-09-26	PIPONIUS et al.	
	5	20020176377		2002-11-28	HAMILTON, Thomas E.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	6	20020199001		2002-12-26	WENOCUR et al.	
	7	20030004937		2003-01-02	SALMENKAITA et al.	
	8	20030005112		2003-01-02	KRAUTKREMER, Todd Joseph	
	9	20030013434		2003-01-16	ROSENBERG et al.	
	10	20030018524		2003-01-23	FISHMAN et al.	
	11	20030046396		2003-03-06	RICHTER et al.	
	12	20030050070		2003-03-13	MASHINSKY et al.	
	13	20030050837		2003-03-13	KIM, Do Sik	
	14	20030088671		2003-05-08	KLINKER et al.	
	15	20030133408		2003-07-17	CHENG et al.	
	16	20030161265		2003-08-28	CAO et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	17	20030182420		2003-09-25	JONES et al.	
	18	20030182435		2003-09-25	REDLICH et al.	
	19	20030220984		2003-11-27	JONES et al.	
	20	20030224781		2003-12-04	MILFORD et al.	
	21	20030229900		2003-12-11	REISMAN, Richard	
	22	20030236745		2003-12-25	HARTSELL et al.	
	23	20040019539		2004-01-29	RAMAN et al.	
	24	20040021697		2004-02-05	BEATON et al.	
	25	20040030705		2004-02-12	BOWMAN-AMUAH, Michel K.	
	26	20040044623		2004-03-04	WAKE et al.	
	27	20040047358		2004-03-11	CHEN et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	28	20040073672		2004-04-15	FASCENDA, Anthony C.	
	29	20040082346		2004-04-29	SKYTT et al.	
	30	20040098715		2004-05-20	AGHERA et al.	
	31	20040103193		2004-05-27	PANDYA et al.	
	32	20040107360		2004-06-03	HERRMANN et al.	
	33	20040127200		2004-07-01	SHAW et al.	
	34	20040132427		2004-07-08	LEE et al.	
	35	20040168052		2004-08-26	CLISHAM et al.	
	36	20040198331		2004-10-07	COWARD et al.	
	37	20040236547		2004-11-25	RAPPAPORT et al.	
	38	20040249918		2004-12-09	SUNSHINE, Roger N.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	39	20050021995		2005-01-27	LAL et al.	
	40	20050048950		2005-03-03	MORPER, Hans-Jochen	
	41	20050055291		2005-03-10	BEVENTE et al.	
	42	20050055309		2005-03-10	WILLIAMS et al.	
	43	20050060266		2005-03-17	DEMELLO et al.	
	44	20050097516		2005-05-05	DONNELLY et al.	
	45	20050107091		2005-05-19	VANNITHAMBY et al.	
	46	20050128967		2005-06-16	SCOBBIE, Donald MacGregor	
	47	20050166043		2005-07-28	ZHANG et al.	
	48	20050183143		2005-08-18	ANDERHOLM et al.	
	49	20050198377		2005-09-08	FERGUSON et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	50	20050216421		2005-09-29	BARRY et al.	
	51	20050228985		2005-10-13	YLIKOSKI et al.	
	52	20050238046		2005-10-27	HASSAN et al.	
	53	20050246282		2005-11-03	NASLUND et al.	
	54	20050250508		2005-11-10	GUO et al.	
	55	20050254435		2005-11-17	MOAKLEY et al.	
	56	20050266825		2005-12-01	CLAYTON, Steve	
	57	20050266880		2005-12-01	GUPTA, Vivek G.	
	58	20060014519		2006-01-19	MARSH et al.	
	59	20060019632		2006-01-26	CUNNINGHAM et al.	
	60	20060026679		2006-02-02	ZAKAS, Philip H.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	61	20060034256		2006-02-16	ADDAGATLA et al.	
	62	20060040642		2006-02-23	BORIS et al.	
	63	20060045245		2006-03-02	AARON et al.	
	64	20060048223		2006-03-02	LEE et al.	
	65	20060072646		2006-04-06	FEHER, Kamilo	
	66	20060085543		2006-04-20	HRASTAR et al.	
	67	20060112016		2006-05-25	ISHIBASHI, Yoshihito	
	68	20060143098		2006-06-29	LAZARIDIS, Mihal	
	69	20060165060		2006-07-27	DUA, Robin	
	70	20060178917		2006-08-10	MERRIAM et al.	
	71	20060178918		2006-08-10	MIKURAK, Michael G.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	72	20060183462		2006-08-17	KOLEHMAINEN, Mikko	
	73	20060190314		2006-08-24	HERNANDEZ, Rick	
	74	20060199608		2006-09-07	DUNN et al.	
	75	20060206904		2006-09-14	WATKINS et al.	
	76	20060218395		2006-09-28	MAES, Stephane H.	
	77	20060233108		2006-10-19	KRISHNAN, Murali R.	
	78	20060233166		2006-10-19	BOU-DIAB et al.	
	79	20060236095		2006-10-19	SMITH et al.	
	80	20060242685		2006-10-26	HEARD et al.	
	81	20060258341		2006-11-16	MILLER et al.	
	82	20060291477		2006-12-28	CROAK et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	83	20070019670		2007-01-25	FALARDEAU, Eric	
	84	20070022289		2007-01-25	ALT et al.	
	85	20070036312		2007-02-15	CAI et al.	
	86	20070055694		2007-03-08	RUGE et al.	
	87	20070061243		2007-03-15	RAMER et al.	
	88	20070076616		2007-04-05	NGO et al.	
	89	20070093243		2007-04-26	KAPADEKAR et al.	
	90	20070100981		2007-05-03	ADAMCZYK et al.	
	91	20070101426		2007-05-03	LEE et al.	
	92	20070104126		2007-05-10	CALHOUN et al.	
	93	20070130315		2007-06-07	FRIEND et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	94	20070140113		2007-06-21	GEMELOS, Steven	
	95	20070140275		2007-06-21	BOWMAN et al.	
	96	20070198656		2007-08-23	MAZZAFERRI et al.	
	97	20070220251		2007-09-20	ROSENBERG et al.	
	98	20070226225		2007-09-27	YIU et al.	
	99	20070243862		2007-10-18	COSKUN et al.	
	100	20070248100		2007-10-25	ZUBERI et al.	
	101	20070254675		2007-11-01	ZORLU OZER et al.	
	102	20070255848		2007-11-01	SEWALL et al.	
	103	20070259673		2007-11-08	WILLARS et al.	
	104	20070263558		2007-11-15	SALOMONE, Leonardo	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	105	20070274327		2007-11-29	KAARELA et al.	
	106	20070282896		2007-12-06	WYDROUG et al.	
	107	20070294395		2007-12-20	STRUB et al.	
	108	20070298764		2007-12-27	CLAYTON, Steve	
	109	20080005285		2008-01-03	ROBINSON et al.	
	110	20080005561		2008-01-03	BROWN et al.	
	111	20080010452		2008-01-10	HOLTZMAN et al.	
	112	20080039102		2008-02-14	SEWALL et al.	
	113	20080049630		2008-02-28	KOZISEK et al.	
	114	20080052387		2008-02-28	HEINZ et al.	
	115	20080059474		2008-03-06	LIM, Keng	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	116	20080059743		2008-03-06	BYCHKOV et al.	
	117	20080060066		2008-03-06	WYNN et al.	
	118	20080062900		2008-03-13	RAO, Bindu Rama	
	119	20080064367		2008-03-13	NATH et al.	
	120	20080066149		2008-03-13	LIM, Keng	
	121	20080066150		2008-03-13	LIM, Keng	
	122	20080082643		2008-04-03	STORRIE et al.	
	123	20080083013		2008-04-03	SOLIMAN et al.	
	124	20080095339		2008-04-24	ELLIOTT et al.	
	125	20080098062		2008-04-24	BALIA, Hinal K.	
	126	20080109679		2008-05-08	WRIGHT et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	127	20080120688		2008-05-22	QIU et al.	
	128	20080127304		2008-05-29	GINTER et al.	
	129	20080130534		2008-06-05	TOMIOKA, Tazuko	
	130	20080130656		2008-06-05	KIM et al.	
	131	20080132268		2008-06-05	CHOI-GROGAN et al.	
	132	20080134330		2008-06-05	KAPOOR et al.	
	133	20080147454		2008-06-19	WALKER et al.	
	134	20080160958		2008-07-03	ABICHANDANI et al.	
	135	20080162637		2008-07-03	ADAMCZYK et al.	
	136	20080162704		2008-07-03	POPLETT et al.	
	137	20080164304		2008-07-10	NARASIMHAN et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	138	20080167027		2008-07-10	GAUTIER et al.	
	139	20080167033		2008-07-10	BECKERS, Michel	
	140	20080168523		2008-07-10	ANSARI et al.	
	141	20080177998		2008-07-24	APSANGI et al.	
	142	20080183812		2008-07-31	PAUL et al.	
	143	20080184127		2008-07-31	RAFEY et al.	
	144	20080189760		2008-08-07	ROSENBERG et al.	
	145	20080207167		2008-08-28	BUGENHAGEN, Michael K.	
	146	20080212470		2008-09-04	CASTANEDA et al.	
	147	20080221951		2008-09-11	STANFORTH et al.	
	148	20080222692		2008-09-11	ANDERSSON et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	149	20080225748		2008-09-18	KHEMANI et al.	
	150	20080229385		2008-09-18	FEDER et al.	
	151	20080229388		2008-09-18	MAES, Stephane H.	
	152	20080256593		2008-10-16	VINBERG et al.	
	153	20080268813		2008-10-30	MAES, Stephane H.	
	154	20080298230		2008-12-04	LUFT et al.	
	155	20080305793		2008-12-11	GALLAGHER et al.	
	156	20080311885		2008-12-18	DAWSON et al.	
	157	20080316923		2008-12-25	FEDDERS et al.	
	158	20080318547		2008-12-25	BALLOU et al.	
	159	20080318550		2008-12-25	DeATLEY, Dallas	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	160	20080319879		2008-12-25	CARROLL et al.	
	161	20090005005		2009-01-01	FORSTALL et al.	
	162	20090013157		2009-01-08	BEAULE, Stephane	
	163	20090054030		2009-02-26	GOLDS, David	
	164	20090068984		2009-03-12	BURNETT, R. Alan	
	165	20090077622		2009-03-19	BAUM et al.	
	166	20090079699		2009-03-26	SUN, Jian	
	167	20090113514		2009-04-30	HU, Q. James	
	168	20090125619		2009-05-14	ANTANI, Snehal S.	
	169	20090180391		2009-07-16	PETERSEN et al.	
	170	20090197585		2009-08-06	AARON, Jeffrey A.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	171	20090257379		2009-10-15	ROBINSON et al.	
	172	20090271514		2009-10-29	THOMAS et al.	
	173	20090286507		2009-11-19	O'NEIL et al.	
	174	20090287921		2009-11-19	ZHU et al.	
	175	20090288140		2009-11-19	HUBER et al.	
	176	20100017506		2010-01-21	FADELL, Anthony	
	177	20100042675		2010-02-18	FUJII, Hiroshi	
	178	20100043068		2010-02-18	VARADHAN et al.	
	179	20100071053		2010-03-18	ANSARI et al.	
	180	20100082431		2010-04-01	RAMER et al.	
	181	20100103820		2010-04-29	FULLER et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	182	20100188975		2010-07-29	RALEIGH, Gregory G.	
	183	20100188990		2010-07-29	RALEIGH, Gregory G.	
	184	20100188992		2010-07-29	RALEIGH, Gregory G.	
	185	20100188994		2010-07-29	RALEIGH, Gregory G.	
	186	20100191576		2010-07-29	RALEIGH, Gregory G.	
	187	20100191612		2010-07-29	RALEIGH, Gregory G.	
	188	20100191846		2010-07-29	RALEIGH, Gregory G.	
	189	20100192170		2010-07-29	RALEIGH, Gregory G.	
	190	20100192212		2010-07-29	RALEIGH, Gregory G.	
	191	20100195503		2010-08-05	RALEIGH, Gregory G.	
	192	20100197268		2010-08-05	RALEIGH, Gregory G.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	193	20100198698		2010-08-05	RALEIGH et al.	
	194	20100198939		2010-08-05	RALEIGH, Gregory G.	
	195	20100325420		2010-12-23	KANEKAR, Tushar	
	196	20110126141		2011-05-26	KING et al.	
	197	20080132201		2008-06-05	KARLBERG, Johan	
	198	20080081606		2008-04-03	COLE, Terry L.	
	199	20090248883		2009-10-01	SURYANARAYANA et al.	
	200	20100144310		2010-06-10	BEDINGFIELD, James Carlton	
	201	20080085707		2008-04-10	FADELL, Tony	
	202	20090046723		2009-02-19	RAHMAN, Reshad A. et al.	
	203	20080219268		2008-09-11	DENNISON, Larry R.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	204	20080005285		2008-01-03	ROBINSON, James David et al.	
	205	20090315735		2009-12-24	BHAVANI, Neeraj S. et al.	
	206	20090219170		2009-09-03	CLARK, Ryan C. et al.	
	207	20090067372		2009-03-12	SHAH, Keyur C. et al.	
	208	20080262798		2008-10-23	KIM, Eun Ah et al.	
	209	20100103820		2010-04-29	FULLER, Randy et al.	
	210	20100153781		2010-06-17	HANNA, Stephen R.	
	211	20090307746		2009-12-10	DI, Jinwen et al.	
	212	20050009499		2005-01-13	KOSTER, Karl	
	213	20010053694		2001-12-20	IGARASHI, Yoichiro et al.	
	214	20100041364		2010-02-18	LOTT, Robert Wayne et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	215	20100027469		2010-02-04	GURAJALA, Ravindra Babu et al.	
	216	20090299857		2009-12-03	BRUBAKER, Curtis M.	
	217	20080051076		2008-02-28	O'Shaughnessy, John et al.	
	218	20080313730		2008-12-18	Iftimie, Sorin et al.	
	219	20110173678		2011-07-14	KAIPPALLIMALIL, John et al.	
	220	20080235511		2008-09-25	O'BRIEN, William G. et al.	
	221	20080240373		2008-10-02	WILHELM, Robert D.	
	222	20100027559		2010-02-04	LIN, Hung-Ming et al.	
	223	20020116338		2002-08-22	GONTHIER, Jean-Charles et al.	
	224	20070061878		2007-03-15	HAGIU, Costin et al. et al.	
	225	20100020822		2010-01-28	ZERILLO, Anthony J. et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	226	20040203755		2004-10-14	BRUNET, Jeffrey et al.	
	227	20090172077		2009-07-02	ROXBURGH, David et al.	
	228	20080120668		2008-05-22	Yau, Frank Chuen-Foo	
	229	20030171112		2003-09-11	Lupper, Alfred et al.	
	230	20070300252		2007-12-27	Acharya, Swarup et al.	
	231	20050007993		2005-01-13	Chambers, Mahdi et al.	
	232	20020164983		2002-11-07	Raviv, Li-On et al.	
	233	20070280453		2007-12-06	Kelley, Sean S.	
	234	20100241544		2010-09-23	Benson, Dan et al.	
	235	20090157792		2009-06-18	Fiatal, Trevor	
	236	20070109983		2007-05-17	Shankar, Rohit et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	237	20020049074		2002-04-25	Eisinger, Bernd et al.	
	238	20020161601		2002-10-31	Nauer, Bernhard et al.	
	239	20040132427		2004-07-08	Lee, Wan-Yeon et al.	
	240	20060068796		2006-03-30	Millen, Stephanie L. et al.	
	241	20010048738		2001-12-06	Baniak, Paul G. et al.	
	242	20070033197		2007-02-08	Scherzer, Shimon et al.	
	243	20110013569		2011-01-20	Scherzer, Shimon et al.	
	244	20110159818		2011-06-30	Scherzer, Shimon et al.	
	245	20120020296		2012-01-26	Scherzer, Shimon et al.	
	246	20120196644		2012-08-02	Scherzer, Shimon et al.	
	247	20120238287		2012-09-20	Scherzer, Shimon	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	248	20130058274		2013-03-07	Scherzer, Shimon et al.	
	249	20130084835		2013-04-04	Scherzer, Shimon et al.	
	250	20090005000		2009-01-01	Baker, Matthew et al.	
	251	20090006116		2009-01-01	Baker, Matthew et al.	
	252	20090006200		2009-01-01	Baker, Matthew et al.	
	253	20110081881		2011-04-07	Baker, Matthew Donald et al.	
	254	20110082790		2011-04-07	Baker, Matthew Donald et al.	
	255	20130029653		2013-01-31	Baker, Matthew Donald et al.	
	256	20130065555		2013-03-14	Baker, Matthew Donald et al.	
	257	20060135144		2006-06-22	Jothipragasam, Premkumar	
	258	20080089295		2008-04-17	Keeler, James D. et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	259	20080022354		2008-01-24	Grewal, Karanvir et al.	
	260	20040102182		2004-05-27	Reith, Lothar et al.	
	261	20030233332		2003-12-18	Keeler, James D. et al.	
	262	20080250053		2008-10-09	Aaltonen, Janne et al.	
	263	20070155365		2007-07-05	Kim, Sung-Jun et al.	
	264	20130144789		2013-06-06	Aaltonen, Janne et al.	
	265	20100131584		2010-05-27	Johnson, William J.	
	266	20100080202		2010-04-01	Hanson, Mark	
	267	20070147324		2007-06-28	McGary, Faith	
	268	20070168499		2007-07-19	Chu, Jing-Long	
	269	20070025301		2007-02-01	Petersson, Justus et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	270	20070140145		2007-06-21	Kumar, Surender et al.	
	271	20080120129		2008-05-22	Seubert, Michael et al.	
	272	20060174035		2006-08-03	Tufail, Mudassir	
	273	20110264923		2011-10-27	Kocher, Paul C. et al.	
	274	20080201266		2008-08-21	Chua, Huina et al.	
	275	20060156398		2006-07-13	Ross, Alan D. et al.	
	276	20060173959		2006-08-03	McKelvie, Samuel J. et al.	
	277	20100284327		2010-11-11	Miklos, Gyorgy	
	278	20070033194		2007-02-08	Srinivas, Davanum M. et al.	
	279	20050079863		2005-04-14	Macaluso, Anthony G.	
	280	20060114832		2006-06-01	Hamilton, Thomas E. et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	281	20040225898		2004-11-11	Frost, D. Gabriel et al.	
	282	20080070550		2008-03-20	Hose, David Alan	
	283	20110019574		2011-01-27	Malomsoky, Szaboles et al.	
	284	20030188117		2003-10-02	Yoshino, Kenji et al.	
	285	20040255145		2004-12-16	Chow, Jerry	
	286	20050055595		2005-03-10	Frazer, Mark et la.	
	287	20070259656		2007-11-08	Jeong, Jong Woo	
	288	20080263348		2008-10-23	Zaltsman, Etai et al.	
	289	20080313315		2008-12-18	Karaoguz, Jeyhan et al.	
	290	20090282127		2009-11-12	LeBlanc, Michael et al.	
	291	20100167696		2010-07-01	Smith, Christopher David et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	292	20030188006		2003-10-02	Bard, Steven R.	
	293	20060160536		2006-07-20	Chou, Joey	
	294	20060168128		2006-07-27	Sistla, Amber et al.	
	295	20040203833		2004-10-14	Rathunde, Dale F. et al.	
	296	20050186948		2005-08-25	Gallagher, Michael D. et al.	
	297	20070147317		2007-06-28	Smith, Brian K. et al.	
	298	20080270212		2008-10-30	Blight, Jeffrey et al.	
	299	20080056273		2008-03-06	Pelletier, Ghyslain et al.	
	300	20110110309		2011-05-12	Bennett, James D.	

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]

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	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]
	1		☐

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

EXAMINER SIGNATURE

Examiner Signature	/Andrew Joseph Rudy/	Date Considered	09/28/2015

*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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

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	14667516
Filing Date	2015-03-24
First Named Inventor	Raleigh
Art Unit	2431
Examiner Name	not yet assigned
Attorney Docket Number	RALEP007C11C4

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	8447980		2013-05-21	Godfrey, James A. et al.	
	2	8429403		2013-04-23	Moret, Eric et al.	
	3	8411587		2013-04-02	Curtis, William et al.	
	4	8396929		2013-03-12	Helfman, Nadav et al.	
	5	8363658		2013-01-29	Delker, Jason R. et al.	
	6	8265004		2012-09-11	Toutonghi, Michael J.	
	7	8233895		2012-07-31	Tysowski, Piotr Konrad	
	8	7685254		2010-03-23	Pandya, Ashish A.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	9	7181017		2007-02-20	Nagel, Robert H. et al.	
	10	6965872		2005-11-15	Grdina, Jerome M.	
	11	8402540		2013-03-19	Kapoor, Harsh et al.	
	12	8135657		2012-03-13	Kapoor, Harsh et al.	
	13	8271992		2012-09-18	Chatley, Scott P. et al.	
	14	8315999		2012-11-20	Chatley, Scott P. et al.	
	15	8332375		2012-12-11	Chatley, Scott P. et al.	
	16	8468337		2013-06-18	Gaur, Santosh P. et al.	
	17	8477778		2013-07-02	Lehmann Jr., L. Curtis et al.	
	18	6640097		2003-10-28	Corrigan, Louis et al.	
	19	7039713		2006-05-02	Van Gunter, David et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	20	5915008		1999-06-22	Dulman, Scott	
	21	8126476		2012-02-28	Vardi, Yosef et al.	
	22	8000276		2011-08-16	Scherzer, Shimon et al.	
	23	8358638		2013-01-22	Scherzer, Tamir et al.	
	24	8356336		2013-01-15	Johnston, Keith et al.	
	25	8307067		2012-11-06	Ryan, Nicholas M.	
	26	7286848		2007-10-23	Vireday, Richard P. et al.	
	27	7313237		2007-12-25	Bahl, Paramvir et al.	
	28	7444669		2008-10-28	Bahl, Paramvir et al.	
	29	7548976		2009-06-16	Bahl, Paramvir et al.	
	30	8027339		2011-09-27	Short, Joel E. et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	31	8095112		2012-01-10	Chow, Richard et al.	
	32	7881697		2011-02-01	Baker, Matthew Donald et al.	
	33	7899438		2011-03-01	Baker, Matthew Donald et al.	
	34	7945238		2011-05-17	Baker, Matthew Donald et al.	
	35	8078140		2011-12-13	Baker, Matthew Donald et al.	
	36	8285249		2012-10-09	Baker, Matthew Donald et al.	
	37	7493659		2009-02-17	Wu, Handong et al.	
	38	7801985		2010-09-21	Pitkow, Jim et al.	
	39	8242959		2012-08-14	Mia, Rashidus S. et al.	
	40	8326319		2012-12-04	Davis, Richard W.	
	41	7102620		2006-09-05	Harries, Andrew Stanely Guy et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	42	7139569		2006-11-21	Kato, Akira	
	43	7529204		2009-05-05	Bourlas, Yair et al.	
	44	7720960		2010-05-18	Pruss, Richard Manfred et al.	
	45	7969950		2011-06-28	Iyer, Pradeep J. et al.	
	46	8032409		2011-10-04	Mikurak, Michael G.	
	47	8045973		2011-10-25	Chambers, Michael D.	
	48	8116781		2012-02-14	Chen, Xixian et al.	
	49	8126396		2012-02-28	Bennett, James D.	
	50	8351898		2013-01-08	Raleigh, Gregory G.	
	51	5630159		1997-05-13	Zancho, William F.	
	52	5633484		1997-05-27	Zancho, William F. et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	53	5814798		1998-09-29	Zancho, William F.	
	54	7039403		2006-05-02	Wong, Gregory A.	
	55	7583964		2009-09-01	Wong, Gregory A.	
	56	7593730		2009-09-22	Khandelwal, Deepak et al.	
	57	7948953		2011-05-24	Melkote, Keerti G. et al.	
	58	8200509		2012-06-12	Kenedy, Andrew Alexander et al.	
	59	8270972		2012-09-18	Otting, Marcia J. et al.	
	60	7929959		2011-04-19	DeAtley, Dallas et al.	
	61	7478420		2009-01-13	Wright, Michael et al.	
	62	7502672		2009-03-10	Kolls, H. Brock	
	63	7756757		2010-07-13	Oakes III, Charles Lee	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	64	7930446		2011-04-19	Kesselman, Alex et al.	
	65	8078163		2011-12-13	Lemond, Eric et al.	
	66	8068829		2011-11-29	Lemond, Eric et al.	
	67	8086497		2011-12-27	Oakes III, Charles Lee	
	68	8166040		2012-04-24	Brindisi, Richard G. et al.	
	69	6934249		2005-08-23	Bertin, Olivier et al.	
	70	7774456		2010-08-10	Lownsbrough, Derek Leigh et al.	
	71	8447607		2013-05-21	Weider, Chris et al.	
	72	8504729		2013-08-06	Pezzutti, David A.	
	73	8495227		2013-07-23	Kaminsky, David L. et al.	
	74	8472371		2013-06-25	Bari, Farooq et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	75	8134954		2012-03-13	Godfrey, James A. et al.	
	76	7535880		2009-05-19	Hinman, Brian L. et al.	
	77	7499438		2009-03-03	Hinman, Brian L. et al.	
	78	7496652		2009-02-24	Pezzutti, David	
	79	6957067		2005-10-18	Iyer, Pradeep J. et al.	
	80	6654814		2003-11-25	Britton, Kathryn H. et al.	
	81	8374592		2013-02-12	Proctor, Jr. James A. et al.	
	82	8325638		2012-12-04	Jin, Haipeng et al.	
	83	8116749		2012-02-14	Proctor Jr., James Arthur et al.	
	84	8090616		2012-01-03	Proctor Jr., James Arthur et al.	
	85	8090359		2012-01-03	Proctor Jr., James Arthur et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	86	8150431		2012-04-03	Wolovitz, Lionel et al.	
	87	8483135		2013-07-09	Cai, Yigang et al.	
	88	6104700		2000-08-15	Haddock, Stephen R. et al.	
	89	8185127		2012-05-22	Cai, Zheng et al.	
	90	8521110		2013-08-27	Rofougaran, Ahmadreza	
	91	7310424		2007-12-18	Gehring, Stephan Walter et al.	
	92	7356011		2008-04-08	Waters, Christopher J.F. et al.	
	93	7546460		2009-06-09	Maes, Stephane H.	
	94	7921463		2011-04-05	Sood, Kapil et al.	
	95	7940751		2011-05-10	Hansen, Christopher J.	
	96	8122249		2012-02-21	Falk, Rainer et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	97	8495360		2013-07-23	Falk, Rainer et al.	
	98	8520589		2013-08-27	Bhatt, Yogesh et al.	
	99	6542992		2003-04-01	Peirce, Kenneth L. et al.	
	100	8185093		2012-05-22	Jheng, Yu-Syuan et al.	
	101	8296404		2012-10-23	McDysan, Dave et al.	
	102	8195163		2012-06-05	Gisby, Doug et al.	
	103	8437734		2013-05-07	Ray, Amar N. et al.	
	104	7460837		2008-12-02	Diener, Neil R.	
	105	7653394		2010-01-26	McMillin, Brian K.	
	106	8130793		2012-03-06	Edwards, Stephen K. et al.	
	107	8509082		2013-08-13	Heinz, John M. et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	108	8526329		2013-09-03	Mahany, Ronald L. et al.	
	109	5983270		1999-11-09	Abraham, Dalen M. et al.	
	110	6598034		2003-07-22	Kloth, Axel K.	
	111	7032072		2006-04-18	Quinn, Michael J. et al.	
	112	7580356		2009-08-25	Mishra, Sanjeev K. et al.	
	113	7742406		2010-06-22	Muppala, Suresh	
	114	7953877		2011-05-31	Vemula, Narendra et al.	
	115	7957381		2011-06-07	Clermidy, Fabien et al.	
	116	8031601		2011-10-04	Feroz, Azeem et al.	
	117	8255534		2012-08-28	Assadzadeh, Alireza	
	118	8489720		2013-07-16	Morford, Michael Robert et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	119	7774323		2010-08-10	Helfman, Nadav	
	120	7043268		2006-05-09	Yukie, Satoru et al.	
	121	7113780		2006-09-26	McKenna, Daniel Bernard et al.	
	122	8166554		2012-04-24	John, Pramod	
	123	7697540		2010-04-13	Haddad, Reda et al.	
	124	6748195		2004-06-08	Phillips, W. Garland	
	125	8583499		2013-11-12	De Judicibus, Dario et al.	
	126	8352360		2013-01-08	De Judicibus, Dario et al.	
	127	8463232		2013-06-11	Tuli, Amol et al.	
	128	7958029		2011-06-07	Bobich, Thomas et al.	
	129	7540408		2009-06-02	Levine, Judah Joseph et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	130	7826427		2010-11-02	Sood, Kapil et al.	
	131	8483694		2013-07-09	Lewis, Allan D. et al.	
	132	8351592		2013-01-08	Freeny, Jr., Charles C. et al.	
	133	7610396		2009-10-27	Taglienti, Claudio et al.	
	134	7984511		2011-07-19	Kocher, Paul Carl et al.	
	135	7987510		2011-07-26	Kocher, Paul C. et al.	
	136	8571993		2013-10-29	Kocher, Paul C. et al.	
	137	8543265		2013-09-24	Ekhaguere, David E. et al.	
	138	6873988		2005-03-29	Hermann, Conrad K. et al.	
	139	7013469		2006-03-14	Smith, Adam W. et al.	
	140	7203169		2007-04-10	Okholm, Jon Eric et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	141	7286834		2007-10-23	Walter, Edward	
	142	7555757		2009-06-30	Smith, Adam W. et al.	
	143	7574509		2009-08-11	Nixon, Mark J. et al.	
	144	7826607		2010-11-02	de Carvalho Resende, Mauricio Guilherme et al.	
	145	7940685		2011-05-10	Breslau, Lee Michel et al.	
	146	8196199		2012-06-05	Hrastar, Scott E. et al.	
	147	8204505		2012-06-19	Jin, Haipeng et al.	
	148	8228818		2012-07-24	Chase, Christopher J. et al.	
	149	8320244		2012-11-27	Muqattash, Alaa et al.	
	150	8411691		2013-04-02	Aggarwal, Rahul	
	151	8461958		2013-06-11	Saenz, Jorge E. et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	152	8484327		2013-07-09	Werner, Eran et al.	
	153	8522039		2013-08-27	Hyndman, Arn et al.	
	154	8544105		2013-09-24	Mclean, Ivan H. et al.	
	155	8571474		2013-10-29	Chavez, Timothy R. et al.	
	156	5774532		1998-06-30	Gottlieb, Louis G. et al.	
	157	8095124		2012-01-10	Balia, Hinal K.	
	158	7797060		2010-09-14	Grgic, Richard J. et al.	
	159	7930327		2011-04-19	Craft, David Jones et al.	
	160	8264965		2012-09-11	Dolganow, Andrew et a.	
	161	6885997		2005-04-26	Roberts, David T.	
	162	8229394		2012-07-24	Karlberg, Johan	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	163	8495700		2013-07-23	Shahbazi, Majid	
	164	8548427		2013-10-01	Chow, Paulo S.T. et al.	
	165	8572117		2013-10-29	Rappaport, Theodore S.	
	166	8589955		2013-11-19	Roundtree, Brian et al.	
	167	8660853		2014-02-25	Robb, Terence A. et al.	
	168	8601125		2013-12-03	Huang, Shibi et al	
	169	8046449		2011-10-25	Yoshiuchi, Hideya	
	170	8635164		2014-01-21	Rosenhaft, Matthew et al.	
	171	8566236		2013-10-22	Busch, James David	
	172	8528068		2013-09-03	Weglein, Joseph et al.	
	173	8442015		2013-05-14	Behzad, Arya et al	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	174	7853255		2010-12-14	Karaoguz, Jeyhan et al	
	175	7720464		2010-05-18	Batta, Puneet	
	176	8300575		2012-10-30	Willars, Per	
	177	8666395		2014-03-04	Silver, Andrew	
	178	8315593		2012-11-20	Gallant, John K. et al.	
	179	8180881		2012-05-15	Seo, Kyoung-Il et al.	
	180	7539132		2009-05-26	Werner, Carl E. et al.	
	181	7805606		2010-09-28	Birger, Chet et al.	
	182	8347378		2013-01-01	Merkin, Aaron E. et al.	
	183	6185576		2001-02-06	McIntosh, Lowrie	
	184	8175574		2012-05-08	Panda, Biswaranjan et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	185	8375128		2013-02-12	Tofighbakhsh, Mostafa et al.	
	186	8527410		2013-09-03	Markki, Outi et al.	
	187	7320029		2008-01-15	Rinne, Janne Petri et al.	
	188	8275415		2012-09-25	Huslak, Nicholas S.	
	189	8554876		2013-10-08	Winsor, Gerald W.	
	190	8191124		2012-05-29	Wynn, Simon et al.	
	191	7805140		2010-09-28	Friday, Robert J. et al.	
	192	8605691		2013-12-10	Soomro, Amjad et al.	
	193	8655357		2014-02-18	Gazzard, Daryl Robert et al.	
	194	8706863		2014-04-22	Fadell, Anthony	
	195	6640334		2003-10-28	Rasmussen, John H.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	196	7668612		2010-02-23	Okkonen, Harri	
	197	5325532		1994-06-28	Crosswy, Wm. Caldwell et al.	
	198	7614051		2009-11-03	Glaum, Jeffrey D. et al.	
	199	5131020		1992-07-14	Liebesny, John P. et al.	
	200	8370483		2013-02-05	Choong et al.	
	201	8670334		2014-03-11	Keohane et al.	
	202	8693323		2014-04-08	McDysan, David E.	
	203	7409447		2008-08-05	Assadzadeh, Alireza	
	204	8725899		2014-05-13	Short, Joel et al.	
	205	8676925		2014-03-18	Liu, Jiawei et al.	
	206	8645518		2014-02-04	David, Scott L.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	207	7756056		2010-07-13	Kim et al	
	208	8131281		2012-03-06	Hildner et al.	
	209	8160598		2012-04-17	Savoor, Raghvendra	
	210	8375136		2013-02-12	Roman et al.	
	211	6119933		2000-09-19	Wong et al.	
	212	8694772		2014-04-08	Kao et al.	
	213	8719423		2014-05-06	Wyld, Jeremy	
	214	8347104		2013-01-01	Pathiyal, Krishna K.	
	215	7149229		2006-12-12	Leung, Kent K.	
	216	7242668		2007-07-10	Kan, Chao et al.	
	217	8095640		2012-01-10	Guingo, Pierrick et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	218	8780857		2014-07-15	Balasubramanian, Srinivasan et al.	
	219	8811991		2014-08-19	Jain, Nikhil et al.	
	220	7809351		2010-10-05	Panda et al.	
	221	8346210		2013-01-01	Balsan, Damien et al.	
	222	8355696		2013-01-15	Olding et al.	
	223	8422988		2013-04-16	Keshav, Srinivasan	
	224	8488597		2013-07-16	Nie et al.	
	225	6438575		2002-08-20	Khan et al.	
	226	7222304		2007-05-22	Beaton et al.	
	227	7561899		2009-07-14	Lee, Changseok	
	228	8200200		2012-06-12	Belser et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	229	8229914		2012-07-24	Ramer et al.	
	230	8522249		2013-08-27	Beaule, Stephane	
	231	8701015		2014-04-15	Bonnat, Pierre	
	232	6697821		2004-02-24	Ziff et al.	
	233	6763226		2004-07-13	McZeal Jr., Alfred	
	234	6982733		2006-01-03	McNally et al.	
	235	6983370		2006-01-03	Eaton, et al.	
	236	7318111		2008-01-08	Zhao, Wen	
	237	8064418		2011-11-22	Maki, Lasse	
	238	8249601		2012-08-21	Emberson et al.	
	239	8514927		2013-08-20	Sundararajan et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

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]	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	1538730A	CN		2004-10-20	Zhongxing Communication Co., Ltd.		☐
	2	101115248A	CN		2008-01-30	Lenovo Beijing Ltd.		☐
	3	101341764A	CN		2009-01-07	Telefonaktiebolaget LM Ericsson		☐
	4	2007068288A1	WO		2007-06-21	Telefonaktiebolaget LM Ericsson		☐
	5	1802839A	CN		2006-07-12	Motorola Inc.		☐
	6	2004064306A2	WO		2004-07-29	Motorola Inc.		☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	7	101123553A	CN		2007-09-11	SouTheast University		☐
	8	1937511A	CN		2007-03-28	ZTE		☐
	9	1999027723 A1	WO		1999-06-03	Telefonaktiebolaget LM Ericsson		☐
	10	2007133844	WO		2007-11-22	Camiant, Inc.		☐
	11	101183958A	CN		2008-05-21	Huawei Tech. Co. Ltd.		☐
	12	1801829A	CN		2006-07-12	Kunda Computer Technology (Kunshan) Co., Ltd.		☐
	13	1867024A	CN		2006-11-22	Huawei Technologies Co., Ltd.		☐
	14	101815275A	CN		2010-08-25	Yang, Liu		☐

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]
	1	VerizonWireless.com news, "Verizon Wireless Adds to Portfolio of Cosumer-Friendly Tools With Introduction of Usage Controls, Usage Controls and Chaperone 2.0 Offer Parents Full Family Security Solution," August 18, 2008	☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	2	"The Construction of Intelligent Residential District in Use of Cable Television Network," Shandong Science, Vol. 13, No. 2, June 2000	☐
	3	"Communication Concepts for Mobile Agent Systems," by Joachim Baumann et al.; Inst. Of Parallel and Distributed High-Performance Systems, Univ. of Stuttgart, Germany, pp. 123-135, 1997	☐
	4	"End to End QoS Solution for Real-time Multimedia Application;" Computer Engineering and Applications, 2007, 43 (4): 155-159, by Tan Zu-guo, Wang Wen-juan; Information and Science School, Zhanjian Normal College, Zhan jiang, Guangdong 524048, China	☐
	5	"ASA/PIX: Allow Split Tunneling for VPN Clients on the ASA Configuration Example," Document ID 70917, January 10, 2008	☐

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

EXAMINER SIGNATURE

Examiner Signature	/Andrew Joseph Rudy/	Date Considered	09/28/2015

*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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

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	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

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	20100030890		2010-02-04	Dutta, Satadip et al.	
	2	20080025230		2008-01-31	Patel, Alpesh et al.	
	3	20040170191		2004-09-02	Guo, Zihua et al.	
	4	20020188732		2002-12-12	Buckman, Charles R. et al.	
	5	20080034419		2008-02-07	Mullick, Amarnath et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	6	20080010379		2008-01-10	Zhao, Hang	
	7	20080139210		2008-06-12	Gisby, Doug et al.	
	8	20040243992		2004-12-02	Gustafson, James P. et al.	
	9	20070226775		2007-09-27	Andreasen, Flemming Stig et al.	
	10	20100235329		2010-09-16	Koren, David et al	
	11	20090254857		2009-10-08	Romine, Christopher et al.	
	12	20080166993		2008-07-10	Gautier et al.	
	13	20040137890		2004-07-15	Kalke, Catherine	
	14	20070143824		2007-06-21	Shahbazi, Majid	
	15	20070266422		2007-11-15	Germano et al.	
	16	20090044185		2009-02-12	Krivopaltsev, Eugene	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	17	20040039792		2004-02-26	Nakanishi, Tomoaki	
	18	20050075115		2005-04-07	Corneille et al.	
	19	20050239447		2005-10-27	Holzman et al.	
	20	20070213054		2007-09-13	Han, Seung-Wook	
	21	20080032715		2008-02-07	Jia et al.	
	22	20090163173		2009-06-25	Williams, Timothy D.	
	23	20100075666		2010-03-25	Garner, Neil Robert	
	24	20080293395		2008-11-27	Matthews, Ajit et al.	
	25	20050245241		2005-11-03	Durand, Terry et al.	
	26	20080125079		2008-05-29	O'Neil, Douglas et al.	
	27	20050135264		2005-06-23	Popoff, Jeff et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	28	20070165630		2007-07-19	Rasanen, Jorma	
	29	20100287599		2010-11-11	HE, Xianhui	
	30	20070060200		2007-03-15	Boris et al.	
	31	20060030306		2006-02-09	Kuhn, Brian Gerald	
	32	20060035631		2006-02-16	White et al.	
	33	20060206709		2006-09-14	Labrou et al.	
	34	20090046707		2009-02-19	Smires et al.	
	35	20100311402		2010-12-09	Srinivasan et al.	
	36	20110277019		2011-11-10	Pritchard Jr., John Russell	
	37	20050250536		2005-11-10	Deng et al.	
	38	20070192460		2007-08-16	Choi et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	39	20080080457		2008-04-03	Cole, Terry L.	
	40	20090049518		2009-02-19	Roman et al.	
	41	20100248719		2010-09-30	Scholaert, Hugh	

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] ¡	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	1310401A	CN		2000-02-22	Wang, Di Xing		☐
	2	1878160A	CN		2006-12-13	Jiang, Yong		☐
	3	101127988A	CN		2008-02-20	ZTE Corporation		☐
	4	1503548 A1	EP		2005-02-02	FG Microtec GmbH		☐
	5	3148713 B2	JP		2001-03-26	ATR Kankyo Tekio Tsushin Kenkyusho		☐
	6	2009-218773	JP		2009-09-24	Advanced Telecommunication Research Institute Inte		☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	7	2006093961	WO		2006-09-08	Kyocera Wireless Corp.		☐
	8	2007-318354	JP		2007-12-06	Fujitsu Ten Ltd.		☐
	9	2007126352	WO		2007-11-08	Telefonaktiebolaget LM Ericsson		☐
	10	2009-212707	JP		2009-09-17	Fujitsu Ltd.		☐
	11	2008-301121	JP		2008-12-11	Kyocera Corp.		☐

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]
	1	Dixon et al., "Triple Play Digital Services: Comcast and Verizon (Digital Phone, Television, and Internet), August 2007	☐

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

EXAMINER SIGNATURE

Examiner Signature	/Andrew Joseph Rudy/	Date Considered	09/28/2015

*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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

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	14667516
Filing Date	2015-03-24
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP007C11C4

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	6578076	B1	2003-06-10	Putzolu, David Matthew	
	2	7084775	B1	2006-08-01	Smith, Michael R.	
	3	7133695	B2	2006-11-07	Beyda, William J.	
	4	7260382	B1	2007-08-21	Lamb et al.	
	5	7271765	B2	2007-09-18	Stilp et al.	
	6	7627872	B2	2009-12-01	Hebeler et al.	
	7	7684370	B2	2010-03-23	Kezys, Vytautas Robertas	
	8	7685530	B2	2010-03-23	Sherrard et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C4

	9	7760137	B2	2010-07-20	Martucci et al.	
	10	7843843	B1	2010-11-30	Albert L. Papp et al.	
	11	7925778	B1	2011-04-12	Wijnands et al.	
	12	7936736	B2	2011-05-03	Proctor, Jr. et al.	
	13	7937450	B2	2011-05-03	Janik, Craig M.	
	14	8010082	B2	2011-08-30	Sutaria et al.	
	15	8019846	B2	2011-09-13	ROELENS et al.	
	16	8050705	B2	2011-11-01	Sicher et al.	
	17	8086791	B2	2011-12-27	Caulkins, Jason	
	18	8103285	B2	2012-01-24	Kalhan, Amit	
	19	8155666	B2	2012-04-10	Alizadeh-Shabdiz, Farshid	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C4

	20	8233433	B2	2012-07-31	Kalhan, Amit	
	21	8259692	B2	2012-09-04	Bajko, Gabor	
	22	8406736	B2	2013-03-26	Das et al.	
	23	8489110	B2	2013-07-16	Frank et al.	
	24	8495181	B2	2013-07-23	Venkatraman et al.	
	25	8532610	B2	2013-09-10	Manning Cassett et al.	
	26	8571598	B2	2013-10-29	Valavi, John J.	
	27	8634425	B2	2014-01-21	Gorti et al.	
	28	8739035	B2	2014-05-27	Trethewey, Jim	
	29	8825109	B2	2014-09-02	Montemurro et al.	
	30	8831561	B2	2014-09-09	Sutaria et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C4

	31	8880047	B2	2014-11-04	Konicek et al.	
	32	8930238	B2	2015-01-06	Coffman et al.	
	33	8977284	B2	2015-03-10	Reed, Mark J.	
	34	9014973	B2	2015-04-21	Ruckart, John	

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	20040259534	A1	2004-12-23	Chaudhari et al.	
	2	20060072451	A1	2006-04-06	Ross, Alan D.	
	3	20070005795	A1	2007-01-04	Gonzalez, Ruben	
	4	20070293191	A1	2007-12-20	Mir et al.	
	5	20070294410	A1	2007-12-20	Pandya et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C4

	6	20080050715	A1	2008-02-28	Golczewski et al.	
	7	20080282319	A1	2008-11-13	Fontijn et al.	
	8	20090197612	A1	2009-08-06	Kiiskinen, Arto	
	9	20100151866	A1	2010-06-17	Karpov et al.	
	10	20110145920	A1	2011-06-16	Mahaffey et al.	
	11	20130326356	A9	2013-12-05	Zheng 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	101080055	CN	A	2007-11-28	Tencent Technology (Shenzhen) Co., Ltd.		☐
	2	101335666	CN	A	2008-12-31	Hangzhou H3C Technologies Co., Ltd.		☐
	3	1567818	CN	A	2005-01-19	Huawei Tech. Co. Ltd.		☐

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C4

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]
	1	Ahmed et al., "A Context-Aware Vertical Handover Decision Algorithm for Multimode Mobile Terminals and Its Performance," BenQ Mobile, Munich Germany; University of Klagenfurt, Klagenfurt, Austria; 2006	☐
	2	Kassar et al., "An overview of vertical handover decision strategies in heterogeneous wireless networks," ScienceDirect, University Pierre & Marie Curie, Paris, France, 6/5/2007	☐
	3	Sadeh et al., "Understanding and Capturing People's Privacy Policies in a Mobile Social Networking Application," ISR School of Computer Science, Carnegie Mellon University, 2007	☐
	4	Schiller et al., "Location-Based Services," The Morgan Kaufmann Series in Data Management Systems, 2004	☐

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

EXAMINER SIGNATURE			
Examiner Signature	/Andrew Joseph Rudy/	Date Considered	09/28/2015

*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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

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	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

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	5577100		1996-11-19	McGREGOR et al.	
	2	5794142		1998-08-11	VANTTILA et al.	
	3	5892900		1999-04-06	GINTER et al.	
	4	5903845		1999-05-11	BUHRMANN et al.	
	5	5933778		1999-08-03	BUHRMANN et al.	
	6	5940472		1999-08-17	NEWMAN et al.	
	7	6047268		2000-04-04	BARTOLI et al.	
	8	6078953		2000-06-20	VAID et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	9	6098878		2000-08-08	DENT et al.	
	10	6141686		2000-10-31	JACKOWSKI et al.	
	11	6148336		2000-11-14	THOMAS et al.	
	12	6198915		2001-03-06	McGREGOR et al.	
	13	6263055		2001-07-17	GARLAND et al.	
	14	6317584		2001-11-13	ABU-AMARA et al.	
	15	6418147		2002-07-09	WIEDEMAN, Robert A.	
	16	6449479		2002-09-10	SANCHEZ, Eduardo	
	17	6532235		2003-03-11	BENSON et al.	
	18	6532579		2003-03-11	SATO et al.	
	19	6539082		2003-03-25	LOWE et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	20	6563806		2003-05-13	YANO et al.	
	21	6574321		2003-06-03	COX et al.	
	22	6574465		2003-06-03	MARSH et al.	
	23	6603969		2003-08-05	VUORISTO et al.	
	24	6639975		2003-10-28	O'NEAL et al.	
	25	6650887		2003-11-18	McGREGOR et al.	
	26	6651101		2003-11-18	GAI et al.	
	27	6658254		2003-12-02	PURDY et al.	
	28	6684244		2004-01-27	GOLDMAN et al.	
	29	6725031		2004-04-20	WATLER et al.	
	30	6765864		2004-07-20	NATARAJAN et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	31	6785889		2004-08-31	WILLIAMS, Peter	
	32	6829596		2004-12-07	FRAZEE, Steve	
	33	6829696		2004-12-07	BALMER et al.	
	34	6920455		2005-07-19	WESCHLER, Paul	
	35	6952428		2005-10-04	NECKA et al.	
	36	6965667		2005-11-15	TRABANDT et al.	
	37	6996076		2006-02-07	FORBES et al.	
	38	6998985		2006-02-14	REISMAN et al.	
	39	7024200		2006-04-04	McKENNA et al.	
	40	7027408		2006-04-11	NABKEL et al.	
	41	7042988		2006-05-09	JUITT et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	42	7058968		2006-06-06	ROWLAND et al.	
	43	7069248		2006-06-27	HUBER, Adriano	
	44	7092696		2006-08-15	HOSAIN et al.	
	45	7142876		2006-11-28	TROSSEN et al.	
	46	7158792		2007-01-02	COOK et al.	
	47	7174174		2007-02-06	BORIS et al.	
	48	7180855		2007-02-20	LIN , Wei	
	49	7197321		2007-03-27	ERSKINE et al.	
	50	7242920		2007-07-10	MORRIS, Robert P.	
	51	7245901		2007-07-17	McGREGOR et al.	
	52	7280816		2007-10-09	FRATTI et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	53	7280818		2007-10-09	CLAYTON, Steve	
	54	7289489		2007-10-30	KUNG et al.	
	55	7290283		2007-10-30	COPELAND III, John A.	
	56	7317699		2008-01-08	GODFREY et al.	
	57	7322044		2008-01-22	HRASTAR, Scott E.	
	58	7324447		2008-01-29	MORFORD, Michael Robert	
	59	7325037		2008-01-29	LAWSON, Karen L.	
	60	7349695		2008-03-25	OOMMEN et al.	
	61	7353533		2008-04-01	WRIGHT et al.	
	62	7356337		2008-04-08	FLORENCE, Shahar	
	63	7366497		2008-04-29	NAGATA, Hideaki	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	64	7373136		2008-05-13	WATLER et al.	
	65	7388950		2008-06-17	ELSEY et al.	
	66	7401338		2008-07-15	BOWEN et al.	
	67	7403763		2008-07-22	MAES, Stephane H.	
	68	7418253		2008-08-26	KAVANAH, Alan	
	69	7421004		2008-09-02	FEHER, Kamilo	
	70	7450591		2008-11-11	KORLING et al.	
	71	7450927		2008-11-11	CRESWELL et al.	
	72	7486185		2009-02-03	CULPEPPER et al.	
	73	7499537		2009-03-03	ELSEY et al.	
	74	7516219		2009-04-07	MOGHADDAM et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	75	7574731		2009-08-11	FASCENDA, Anthony C.	
	76	7580857		2009-08-25	VanFLEET et al.	
	77	7610328		2009-10-27	HAASE et al.	
	78	7617516		2009-11-10	HUSLAK et al.	
	79	7620065		2009-11-17	FALARDEAU, Eric	
	80	7620162		2009-11-17	AARON et al.	
	81	7647047		2010-01-12	MOGHADDAM et al.	
	82	7650137		2010-01-19	JOBS et al.	
	83	7668903		2010-02-23	EDWARDS et al.	
	84	7693720		2010-04-06	KENNEWICK et al.	
	85	7720505		2010-05-18	GOPI et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	86	7734784		2010-06-08	ARAUJO et al.	
	87	7747240		2010-06-29	BRISCOE et al.	
	88	7747699		2010-06-29	PRUEITT et al.	
	89	7792708		2010-09-07	ALVA, Jessi	
	90	7797204		2010-09-14	BALENT, Bruce F.	
	91	7797401		2010-09-14	STEWART et al.	
	92	7822837		2010-10-26	URBAN et al.	
	93	7848768		2010-12-07	OMORI et al.	
	94	7868778		2011-01-11	KENWRIGHT, David Norris	
	95	7873705		2011-01-18	KALISH, Dan	
	96	7882029		2011-02-01	WHITE, Craig R.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	97	7929960		2011-04-19	MARTIN et al.	
	98	7937069		2011-05-03	RASSAM, Frederic	
	99	7941184		2011-05-10	PRENDERGAST et al.	
	100	7949529		2011-05-24	WEIDER et al.	
	101	7957511		2011-06-07	DRUDIS et al.	
	102	7975184		2011-07-05	GOFF et al.	
	103	7984130		2011-07-19	BOGINENI et al.	
	104	7986935		2011-07-26	D'SOUZA et al.	
	105	8005459		2011-08-23	BALSILLIE, Jim	
	106	8010080		2011-08-30	THENTHIRUPERAI et al.	
	107	8010081		2011-08-30	ROSKOWSKI, Steve	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	108	8015133		2011-09-06	WU et al.	
	109	8015234		2011-09-06	LUM et al.	
	110	8019687		2011-09-13	WANG et al.	
	111	8023425		2011-09-20	RALEIGH, Gregory G.	
	112	8095666		2012-01-10	SCHMIDT et al.	
	113	8099077		2012-01-17	CHOWDHURY et al.	
	114	8099517		2012-01-17	JIA et al.	
	115	8144591		2012-03-27	GHAI et al.	
	116	8170553		2012-05-01	BENNETT, James D.	
	117	6606744		2003-08-12	MIKURAK, Michael G.	
	118	7336960		2008-02-26	ZAVALKOVSKY et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	119	8190675		2012-05-29	TRIBBETT, David	
	120	8194549		2012-06-05	HUBER et al.	
	121	8200775		2012-06-12	MOORE, James F.	
	122	8135392		2012-03-13	MARCELLINO et al.	
	123	7953808		2011-05-31	SHARP et al.	
	124	6502131		2002-12-31	VAID, Aseem et al.	
	125	6505114		2003-01-07	LUCIANI, Sergio	
	126	6763000		2004-07-13	WALSH, Peter J.	
	127	6967958		2005-11-22	ONO, Yoshiyuki et al.	
	128	7644267		2010-01-05	YLIKOSKI, Martti et al.	
	129	7710932		2010-05-04	MUTHUSWAMY, Sivakumar et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	130	7881199		2011-02-01	KRSTULICH, Zlatko	
	131	7886047		2011-02-08	POTLURI, Dora	
	132	7911975		2011-03-22	DROZ, Patrick et al.	
	133	8050275		2011-11-01	IYER, Jayaraman R.	
	134	8194553		2012-06-05	LIANG, Zhi Yong et al.	
	135	8239520		2012-08-07	GRAH, Adrian	
	136	7890084		2011-02-15	Dudziak, Thaddeus Jude et al.	
	137	7890111		2011-02-15	Bugenhagen, Michael K.	
	138	6226277		2001-05-01	Chuah, Mooi Choo	
	139	6839340		2005-01-04	Voit, Eric A. et al.	
	140	6922562		2005-07-26	Ward, Stephen L. et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	141	7620041		2009-11-17	Dunn, Jeffrey H. et al.	
	142	7627314		2009-12-01	Carlson, Steven I. et al.	
	143	7792538		2010-09-07	Kozisek, Steven E.	
	144	7801523		2010-09-21	Kenderov, Stoyan	
	145	7877090		2011-01-25	Maes, Stephane H.	
	146	7912025		2011-03-22	Pattenden, Christopher E. S. et al.	
	147	7948968		2011-05-24	Voit, Eric A. et al.	
	148	7970426		2011-06-28	Poe, Brian R. et al.	
	149	8185158		2012-05-22	Tamura, Motoshi et al.	
	150	8254915		2012-08-28	Kozisek, Steven E.	
	151	7418257		2008-08-26	Kim, Myong-Ju	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	152	8126123		2012-02-28	Cai, Yigang et al.	
	153	7903553		2011-03-08	Liu, Enhui	
	154	8155620		2012-04-10	Wang, Jun et al.	
	155	8238287		2012-08-07	Gopi, Paramesh et al.	
	156	7113997		2006-09-26	Jayapalan, Jay et al.	
	157	5594777		1997-01-14	Makkonen, Matti et al.	
	158	8244241		2012-08-14	Montemurro, Michael	
	159	7756534		2010-07-13	Anupam, Vinod et al.	
	160	7636574		2009-12-22	Poosala, Viswanath	
	161	6678516		2004-01-13	Nordman, Ian et al.	
	162	6477670		2002-11-05	Ahmadvand, Nima	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	163	6038452		2000-03-14	Strawczynski, Leo et al.	
	164	8108520		2012-01-31	Ruutu, Jussi et al.	
	165	7778643		2010-08-17	Laroia, Rajiv et al.	
	166	7668176		2010-02-23	Chuah, Mooi Choo	
	167	7515608		2009-04-07	Yuan, Yuan et al.	
	168	7251218		2007-07-31	Jorgensen, Jacob W.	
	169	7002920		2006-02-21	Ayyagari, Deepak et al.	
	170	7685131		2010-03-23	Batra, Vishal Singh et al.	
	171	7283561		2007-10-16	Picher-Dempsey, Heidi	
	172	7212491		2007-05-01	Koga, Takahiro	
	173	6683853		2004-01-27	Kannas, Chris et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	174	7609700		2009-10-27	Ying, Wen-Ping et al.	
	175	8255515		2012-08-28	MELMAN, David et al.	
	176	7945240		2011-05-17	KLOCK, Jacqueline et al.	
	177	7912056		2011-03-22	BRASSEM, Wayne	
	178	7920529		2011-04-05	MAHLER, Roger et al.	
	179	8184530		2012-05-22	SWAN, Tim L. et al.	
	180	8214536		2012-07-03	ZHAO, Wen	
	181	8213363		2012-07-03	YING, Wen-Ping et al.	
	182	8255689		2012-08-28	KIM, Eun Ah et al.	
	183	7746854		2010-06-29	AMBE, Shekhar et al.	
	184	7068600		2006-06-27	CAIN, Joseph Bibb	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	185	6876653		2005-04-05	AMBE, Shekhar et al.	
	186	6631122		2003-10-07	ARUNACHALAM, Vaidhyanathan et al.	
	187	7599288		2009-10-06	COLE, Raymond E. et al.	
	188	7546629		2009-06-09	ALBERT, Anthony et al.	
	189	7747730		2010-06-29	HARLOW, James D.	
	190	7609650		2009-10-27	ROSKOWSKI, Steve et al.	
	191	6581092		2003-06-17	MOTOYAMA, Tetsuro	
	192	7283963		2007-10-16	FITZPATRICK, John E. et al.	
	193	8271049		2012-09-18	SILVER, Andrew et al.	
	194	7644151		2010-01-05	JERRIM, John et al.	
	195	8291238		2012-10-16	GINTER, Karl L. et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	196	8068824		2011-11-29	SHAN, Xueshan et al.	
	197	7228354		2007-06-05	CHAMBLISS, David Darden et al.	
	198	5283904		1994-02-01	CARSON, David G. et al.	
	199	8208919		2012-06-26	KOTECHA, Lalit Ratilal	
	200	8185152		2012-05-22	GOLDNER, Alla	
	201	7844728		2010-11-30	ANDERSON, Thomas W. et al.	
	202	7873344		2011-01-18	BOWSER, Robert et al.	
	203	7856226		2010-12-21	WONG, Ellis L. et al.	
	204	7948952		2011-05-24	HURTTA, Tuija et al.	
	205	7957020		2011-06-07	MINE, Ryuta et al.	
	206	7346410		2008-03-18	UCHIYAMA, Kenji	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	207	7167078		2007-01-23	POURCHOT, Shawn C.	
	208	8102814		2012-01-24	RAHMAN, Shahriar I. et al.	
	209	7970350		2011-06-28	SHEYNMAN, Arnold	
	210	8094551		2012-01-10	HUBER, Kurt Donald et al.	
	211	8135388		2012-03-13	Gailloux, Michael A. et al.	
	212	6947723		2005-09-20	Gurnani, Roger et al.	
	213	8350700		2013-01-08	Fast, Raymond D. et al.	
	214	8204190		2012-06-19	Bang, Jung-Hee et al.	
	215	7865182		2011-01-04	Macaluso, Anthony G.	
	216	7962622		2011-06-14	Friend, John et al.	
	217	7583964		2009-09-01	Wong, Gregory A.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	218	7565141		2009-07-21	Macaluso, Anthony G.	
	219	7373179		2008-05-13	Stine, Ted et al.	
	220	7236780		2007-06-26	Benco, David S.	
	221	7039403		2006-05-02	Wong, Gregory A.	
	222	8370477		2013-02-05	Short, Joel E. et al.	
	223	8364806		2013-01-29	Short, Joel E. et al.	
	224	8279067		2012-10-02	BERGER, Thomas R. et al.	
	225	8213296		2012-07-03	SHANNON, Frank M. et al.	
	226	8019868		2011-09-13	RAO, Goutham et al.	
	227	8005988		2011-08-23	MAES, Stephane H.	
	228	7978627		2011-07-12	TAYLOR, William Scott et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	229	7711848		2010-05-04	MAES, Stephane H.	
	230	6782412		2004-08-24	BROPHY, Kevin et al.	
	231	6081591		2000-06-27	SKOOG, Frederick H.	
	232	6064878		2000-05-16	DENKER, John Stewart et al.	
	233	7730123		2010-06-01	ERICKSON, Richard R. et al.	
	234	8024397		2011-09-20	ERICKSON, Richard R. et al.	
	235	8156206		2012-04-10	KILEY, Kevin J. et al.	
	236	8126722		2012-02-28	ROBB, Terence Alan et al.	
	237	6754470		2004-06-22	Hendrickson, Keith et al.	
	238	8122128		2012-02-21	Burke, II, Robert M. et al.	
	239	8149823		2012-04-03	Turcan, Diane Brown et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	240	8131256		2012-03-06	MARTTI, Jyrki et al.	
	241	6381316		2002-04-30	JOYCE, Simon James et al.	
	242	7965983		2011-06-21	SWAN, Tim et al.	
	243	8284740		2012-10-09	O'CONNOR, Dennis M.	
	244	8116223		2012-02-14	TIAN, Dan et al.	
	245	6154738		2000-11-28	CALL, Charles Gainor	
	246	8423016		2013-04-16	BUCKLEY, Adrian et al.	
	247	6035281		2000-03-07	Crosskey, James P. et al.	
	248	6996393		2006-02-07	Pyhalammi, Seppo et al.	
	249	7760711		2010-07-20	Kung, Fen-Chung et al.	
	250	8000318		2011-08-16	Wiley, William L. et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	251	8098579		2012-01-17	Ray, Amar N. et al.	
	252	8155670		2012-04-10	Fullam, Scott et al.	
	253	8374090		2013-02-12	Morrill, Robert J. et al.	
	254	7457265		2008-11-25	Julka, Vibhor et al.	
	255	7729326		2010-06-01	Sekhar, Ramesh	
	256	7929973		2011-04-19	Zavalkovsky, Arthur et al.	
	257	7945945		2011-05-17	Graham, Richard et al.	
	258	8059530		2011-11-15	Cole, Terry L.	
	259	8280354		2012-10-02	Smith, Christopher et al.	
	260	8266681		2012-09-11	Deshpande, Sumit B. et al.	
	261	8331293		2012-12-11	Sood, Kapil	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	262	8019820		2011-09-13	Son, Giyeong et al.	
	263	8155155		2012-04-10	Chow, Albert T. et al.	
	264	8191116		2012-05-29	Gazzard, Daryl	
	265	6292828		2001-09-18	Williams, David L.	
	266	7043226		2006-05-09	Yamauchi, Toshiaki	
	267	7472189		2008-12-30	Mallya, Arvind R. et al.	
	268	7944948		2011-05-17	Chow, Albert T. et al.	
	269	7802724		2010-09-28	Nohr, Steven Paul	
	270	8005009		2011-08-23	McKee, Neil et al.	
	271	7760861		2010-07-20	Croak, Marian et al.	
	272	8060463		2011-11-15	Spiegel, Joel R.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	273	8224773		2012-07-17	Spiegel, Joel R.	
	274	8352980		2013-01-08	Howcroft, Jerald Robert	
	275	8386386		2013-02-26	Zhu, Kevin	
	276	8340718		2012-12-25	Colonna, Massimo et al.	
	277	8385896		2013-02-26	Proctor Jr., James A. et al.	
	278	8320949		2012-11-27	Matta, Sudheer Poorna Chandra	
	279	8279864		2012-10-02	Wood, Daniel M.	
	280	8271045		2012-09-18	Parolkar, Satish et al.	
	281	8233883		2012-07-31	De Froment, Eric	
	282	8224382		2012-07-17	Bultman, Michael J.	
	283	8184590		2012-05-22	Rosenblatt, Ariel	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	284	8174970		2012-05-08	Adamczyk, Maria et al.	
	285	8165576		2012-04-24	Raju, Vishwanath et al.	
	286	8073721		2011-12-06	Lewis, Lundy	
	287	8032899		2011-10-04	Archer, Charles J. et al.	
	288	7974624		2011-07-05	Gallagher, Michael D. et al.	
	289	7907970		2011-03-15	Park, Vincent D. et al.	
	290	7778176		2010-08-17	Morford, Michael Robert	
	291	7725570		2010-05-25	Lewis, Lundy	
	292	7634388		2009-12-15	Archer, Charles J. et al.	
	293	7633438		2009-12-15	Tysowski, Piotr Konrad	
	294	7593417		2009-09-22	Wang, James et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	295	7551922		2009-06-23	Roskowski, Steve et al.	
	296	7545782		2009-06-09	Rayment, Stephen G. et al.	
	297	7039037		2006-05-02	Wang, Jiwei R. et al.	
	298	6928280		2005-08-09	Xanthos, James et al.	
	299	6765925		2004-07-20	Sawyer, Wilson et al.	
	300	5889477		1999-03-30	Fastenrath, Ulrich	

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]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	1	1463238	EP		2004-09-29	Alcatel		☐
	2	1739518	EP		2007-01-03	Research In Motion Limited		☐
	3	1772988	EP		2007-04-11	Huawei Technologies Co., Ltd.		☐
	4	1978772	EP		2008-10-08	British Telecommunications Public Limited Company		☐
	5	1999065185	WO		1999-12-16	British Telecommunications Public Limited Company		☐
	6	2003014891	WO		2003-02-20	The Boeing Company		☐
	7	2003058880	WO		2003-07-17	Telia AB		☐
	8	2004028070	WO		2004-04-01	Credant Technologies, Inc.		☐
	9	2004077797	WO		2004-09-10	Boston Communications Group, Inc. (Erskine)		☐
	10	2004095753	WO		2004-11-04	Motorola Inc.		☐
	11	2006004467	WO		2006-01-12	Telefonaktiebolaget LM Ericsson		☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	12	2006050758	WO		2006-05-18	Telefonaktiebolaget LM Ericsson		☐
	13	2006073837	WO		2006-07-13	Symbol Technologies, Inc.		☐
	14	2006077481	WO		2006-07-27	TrueContext Corporation		☐
	15	2006130960	WO		2006-12-14	Mobidia, Inc.		☐
	16	2007001833	WO		2007-01-04	Symbol Technologies, Inc.		☐
	17	2007014630	WO		2007-02-08	Telefonaktiebolaget LM Ericsson		☐
	18	2007018363	WO		2007-02-15	Upresto, Inc.		☐
	19	2007053848	WO		2007-05-10	Mobile Armor, LLC		☐
	20	2007069245	WO		2007-06-21	Yoggie Security Systems, Inc.		☐
	21	2007107701	WO		2007-09-27	British Telecommunications Public Limited Company		☐
	22	2008017837	WO		2008-02-14	Symbian Software Limited		☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	23	2008051379	WO		2008-05-02	Verizon Services Corp.		☐
	24	2008066419	WO		2008-06-05	Telefonaktiebolaget LM Ericsson		☐
	25	2008080139	WO		2008-07-03	Integrated Mobile, Inc.		☐
	26	2008080430	WO		2008-07-10	Telecom Italia S.P.A.		☐
	27	2008099802	WO		2008-08-21	NEC Corporation		☐
	28	2010088413	WO		2010-08-05	Headwater Partners I LLC		☐
	29	2006120558	WO		2006-11-16	Nokia Corp.		☐
	30	1889777A	CN		2006-07-19	Huawei Tech. Co. Ltd.		☐
	31	101155343A	CN		2006-09-29	Huawei Tech. Co. Ltd.		☐
	32	101035308A	CN		2006-03-09	Huawei Tech. Co. Ltd.		☐
	33	2007124279	WO		2007-11-01	Cisco Technology, Inc., et al.		☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	34	2005008995	WO		2005-01-27	Starhub Ltd.		☐
	35	1998058505	WO		1998-12-23	Sonera Oy		☐
	36	2007097786	WO		2007-08-30	Sony Ericsson Mobile Communications AB		☐

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	3rd Generation Partnership Project, "Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) Enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) Access," Release 8, Document No. 3GPP TS 23.401, V8.4.0, December 2008	☐
	2	3rd Generation Partnership Project, "Technical Specification Group Services and System Aspects; Policy and Charging Control Architecture," Release 8, Document No. 3GPP TS 23.203, V8.4.0, December 2008	☐
	3	ALONISTIOTI et al., "Intelligent Architectures Enabling Flexible Service Provision and Adaptability," 2002	☐
	4	Amazon Technologies, Inc., "Kindle™ User's Guide," 3rd Edition, Copyright 2004-2009	☐
	5	CHANDRASEKHAR et al., "Femtocell Networks: A Survey," June 28, 2008	☐
	6	CHAOUCHI et al., "Policy Based Networking in the Integration Effort of 4G Networks and Services," 2004 IEEE	☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	7	Cisco Systems, Inc., "Cisco Mobile Exchange (CMX) Solution Guide: Chapter 2 - Overview of GSM, GPRS, and UMTS," November 4, 2008	☐
	8	DIKAIAKOS et al., "A Distributed Middleware Infrastructure for Personalized Services," November 24, 2003	☐
	9	European Commission, "Data Roaming Tariffs - Transparency Measures," [online] retrieved from http://web.archive.org/web/20081220232754/http://ec.europa.eu/information_society/activities/roaming/data/measures/index_en.htm, December 20, 2008 [retrieved May 16, 2012]	☐
	10	FAROOQ et al., "An IEEE 802.16 WiMax Module for the NS-3 Simulator," March 2-6, 2009	☐
	11	HAN et al., "Information Collection Services for Qos-Aware Mobile Applications," 2005	☐
	12	HARTMANN et al., "Agent-Based Banking Transactions & Information Retrieval - What About Performance Issues?" 1999	☐
	13	Hewlett-Packard Development Company, LP, "IP Multimedia Services Charging," white paper, January 2006	☐
	14	HOSSAIN et al., "Gain-Based Selection of Ambient Media Services in Pervasive Environments," Mobile Networks and Applications. 03 October 2008	☐
	15	KNIGHT et al., "Layer 2 and 3 Virtual Private Networks: Taxonomy, Technology, and Standarization Efforts," IEEE Communications Magazine, June 2004	☐
	16	KOUTSOPOULOU et al., "Middleware Platform for the Support of Charging Reconfiguration Actions," 2005	☐
	17	KYRIAKAKOS et al., "Ubiquitous Service Provision in Next Generation Mobile Networks," Proceedings of the 13th IST Mobile and Wireless Communications Summit, Lyon, France, June 2004	☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	18	LI, Yu, "Dedicated E-Reading Device: The State of the Art and The Challenges," Scroll, Vol. 1, No. 1, 2008	☐
	19	NILSSON et al., "A Novel MAC Scheme for Solving the QoS Parameter Adjustment Problem in IEEE802.11e EDCA," February 2006	☐
	20	OPPLIGER, Rolf, "Internet Security: Firewalls and Bey," Communications of the ACM, May 1997, Vol. 40. No. 5	☐
	21	RAO et al., "Evolution of Mobile Location-Based Services," Communication of the ACM, December 2003	☐
	22	STEGLICH, Stephan, "I-Centric User Interaction," November 21, 2003	☐
	23	VAN EIJK, et al., "GigaMobile, Agent Technology for Designing Personalized Mobile Service Brokerage," July 1, 2002	☐
	24	ZHU et al., "A Survey of Quality of Service in IEEE 802.11 Networks," IEEE Wireless Communications, August 2004	☐
	25	ANTON, B. et al., "Best Current Practices for Wireless Internet Service Provider (WISP) Roaming"; Release Date February 2003, Version 1.0; Wi-Fi Alliance – Wireless ISP Roaming (WISPr)	☐

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

EXAMINER SIGNATURE

Examiner Signature	/Andrew Joseph Rudy/	Date Considered	09/28/2015

*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.

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

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	14667516
Filing Date	2015-03-24
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP007C11C4

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	5572528	A	1996-11-05	Shuen, Pauline	
	2	5754953	A	1998-05-19	Briancon et al.	
	3	6628934	A	2003-09-30	Rosenberg et al.	
	4	6662014	B1	2003-12-09	Walsh, Patrick Jay	
	5	6757717	B1	2004-06-29	Goldstein, Leonid	
	6	6901440	B1	2005-05-31	Bimm et al.	
	7	6970692	B2	2005-11-29	Tysor, Arthur James	
	8	7007295	B1	2006-02-28	Rose et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C4

	9	7203752	B2	2007-04-10	Rice et al.	
	10	7222190	B2	2007-05-22	Klinker et al.	
	11	7224968	B2	2007-05-29	Dobson et al.	
	12	7379731	B2	2008-05-27	Natsuno et al.	
	13	7457870	B1	2008-11-25	Lownsbrough et al.	
	14	7515926	B2	2009-04-07	Bu et al.	
	15	7536695	B2	2009-05-19	Alam et al.	
	16	7586871	B2	2009-09-08	Hamilton et al.	
	17	7752330	B2	2010-07-06	Olsen et al.	
	18	7792257	B1	2010-09-07	Vanier et al.	
	19	7801783	B2	2010-09-21	Kende et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C4

	20	7865187	B2	2011-01-04	Ramer et al.	
	21	7933274	B2	2011-04-26	Verma et al.	
	22	8005726	B1	2011-08-23	Bao, Yulin	
	23	8050690	B2	2011-11-01	Neeraj, Chawla	
	24	8086398	B2	2011-12-27	Sanchez et al.	
	25	8107953	B2	2012-01-31	Zimmerman et al.	
	26	8112435	B2	2012-02-07	Epstein et al.	
	27	8174378	B2	2012-05-08	Richman et al.	
	28	8195661	B2	2012-06-05	Kalavade, Asawaree	
	29	8200163	B2	2012-06-12	Hoffman, George E.	
	30	8200818	B2	2012-06-12	Freund et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C4

	31	8208788	B2	2012-06-26	Ando et al.	
	32	8254880	B2	2012-08-28	Aaltonen et al.	
	33	8270955	B2	2012-09-18	Ramer et al.	
	34	8326828	B2	2012-12-04	Zhou et al.	
	35	8331223	B2	2012-12-11	Hill et al.	
	36	8358975	B2	2013-01-22	Bahl et al.	
	37	8533775	B2	2013-09-10	Alcorn et al.	
	38	8538394	B2	2013-09-17	Zimmerman et al.	
	39	8538458	B2	2013-09-17	Haney, Richard D.	
	40	8565746	B2	2013-10-22	Hoffman, George E.	
	41	8571501	B2	2013-10-29	Miller et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C4

	42	8644702	B1	2014-02-04	Kalajan, Kevin E.	
	43	8713535	B2	2014-04-29	Malhotra et al.	
	44	8713641	B1	2014-04-29	Pagan et al.	
	45	8730842	B2	2014-05-20	Collins et al.	
	46	8732808	B2	2014-05-20	Sewall et al.	
	47	8761711	B2	2014-06-24	Grignani et al.	
	48	9049010		2015-06-02	Jueneman et al.	
	49	6445777		2002-09-03	Clark, Curtis	
	50	7039027		2006-05-02	Bridgelall, Raj	
	51	7990049		2011-08-02	Shioya, Shunsuke	
	52	8180886		2012-05-15	Overcash et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C4

	53	8339991		2012-12-25	Biswas et al.	

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	20020154751	A1	2002-10-24	Thompson et al.	
	2	20030084321	A1	2003-05-01	Tarquini et al.	
	3	20040133668	A1	2004-07-08	Nicholas III, Henry T.	
	4	20060136882	A1	2006-06-22	Noonan et al.	
	5	20060143066	A1	2006-06-29	Calabria	
	6	20070073899	A1	2007-03-29	Judge et al.	
	7	20070174490	A1	2007-07-26	Choi et al.	
	8	20070234402	A1	2007-10-04	Khosravi et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C4

	9	20090048913	A1	2009-02-19	Shenfield et al.	
	10	20090181662	A1	2009-07-16	Fleischman et al.	
	11	20020191573		2002-12-19	Whitehill et al.	
	12	20060098627		2006-05-11	Karaoguz, Jeyhan et al.	
	13	20090070379		2009-03-12	Rappaport, Theodore R.	

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	2688553	CA	A1	2008-12-04	Yoggie Security Systems, Inc.		☐
	2	1508734	CN	A	2004-06-30	Chinese Creative Corp.		☐
	3	1850575	EP	A1	2007-10-31	Research In Motion		☐
	4	2009111919	JP		2009-05-21	Kyocera Communications Systems		☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C4

	5	2009232107	JP	A	2009-10-08	Fujitsu Ltd.		☐
	6	2006012610	WO	A2	2006-02-02	Citrix Systems, Inc.		☐

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	"Ads and movies on the run," the Gold Coast Bulletin, Southport, Qld, Jan. 29, 2008	☐
	2	"Jentro Technologies launches Zenlet platform to accelerate location-based content delivery to mobile devices," The Mobile Internet, Boston, MA, Feb. 2008	☐
	3	Jing et al., "Client-Server Computing in Mobile Environments," GTE Labs. Inc., Purdue University, ACM Computing Surveys, Vol. 31, No. 2, June 1999	☐
	4	Kim, "Free wireless a high-wire act; MetroFi needs to draw enough ads to make service add profits," San Francisco Chronicle, Aug. 21, 2006	☐
	5	Koutsopoulou et al., "Charging, Accounting and Billing Management Schemes In Mobile Telecommunication Networks and the Internet," IEEE Communications Surveys & Tutorials, First Quarter 2004, Vol. 6, No. 1	☐
	6	Loopt User Guide, metroPCS, 7/17/2008	☐
	7	Nuzman et al., "A compund model for TCP connection arrivals for LAN and WAN applications," Oct. 22, 2002	☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C4

	8	Richtel, "Cellphone consumerism; If even a debit card is too slow, now you have a new way to act on impulse: [National Edition]," National Post, Canada, Oct. 2, 2007	☐
	9	Rivadeneyra et al., "A communication architecture to access data services through GSM," San Sebastian, Spain, 1998	☐
	10	Sabat, "The evolving mobile wireless value chain and market structure," Nov. 2002	☐
	11	Sun et al., "Towards Connectivity Management Adaptability: Context Awareness in Policy Representation and End-to-end Evaluation Algorithm," Dept. of Electrical and Information Engineering, Univ. of Oulu, Finland, 2004	☐

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

EXAMINER SIGNATURE

Examiner Signature	/Andrew Joseph Rudy/	Date Considered	09/28/2015

*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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

Search Notes	Application/Control No.	Applicant(s)/Patent under Reexamination	
	14/667,516	RALEIGH, GREGORY G.	
	Examiner	Art Unit	
	ANDREW JOSEPH RUDY	3687	

SEARCHED			
Class	Subclass	Date	Examiner
709	203, 204, 206, 207, 217,219	9/28/2015	AJR
709	223	9/28/2015	AJR
713	168-170	9/28/2015	AJR
705	28,30	9/28/2015	AJR
455	405,406	9/28/2015	AJR
455	411	9/28/2015	AJR
455	414.1	9/28/2015	AJR

INTERFERENCE SEARCHED			
Class	Subclass	Date	Examiner
709	**206,207**	**9/28/2015**	**AJR**
713	168	9/28/2015	AJR

SEARCH NOTES (INCLUDING SEARCH STRATEGY)		
	DATE	EXMR
Continuity data reviewed.	9/28/2015	AJR
Inventor name search conducted.	9/28/2015	AJR
Bibliographic data updated.	9/28/2015	AJR

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14667516	RALEIGH, GREGORY G.
	Examiner	**Art Unit**
	ANDREW JOSEPH RUDY	3687

CPC						
Symbol					**Type**	**Version**
H04W		48	/	14	F	2013-01-01
G06Q		10	/	06375	I	2013-01-01
G06Q		20	/	102	I	2013-01-01
G06Q		20	/	20	I	2013-01-01
G06Q		20	/	40	I	2013-01-01
G06Q		30	/	0207	I	2013-01-01
G06Q		30	/	0283	I	2013-01-01
G06Q		30	/	0284	I	2013-01-01
G06Q		30	/	04	I	2013-01-01
G06Q		30	/	0601	I	2013-01-01
G06Q		40	/	00	I	2013-01-01
H04L		12	/	14	I	2013-01-01
H04L		41	/	0893	A	2013-01-01
H04L		41	/	5003	I	2013-01-01
H04L		41	/	5025	A	2013-01-01
H04M		15	/	00	I	2013-01-01
H04M		15	/	58	I	2013-01-01
H04M		2215	/	0188	A	2013-01-01
H04W		4	/	24	I	2013-01-01
H04W		4	/	26	I	2013-01-01
G06F		15	/	177	I	2013-01-01
G06Q		30	/	0241	I	2013-01-01
H04L		9	/	32	I	2013-01-01
H04L		63	/	10	I	2013-01-01
H04W		28	/	02	I	2013-01-01
H04W		12	/	08	I	2013-01-01
H04W		4	/	001	I	2013-01-01
H04W		8	/	02	A	2013-01-01
H04L		47	/	2408	I	2013-01-01
H04L		63	/	08	I	2013-01-01
H04L		67	/	306	I	2013-01-01

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 18	
/ANDREW JOSEPH RUDY/ Primary Examiner.Art Unit 3687 (Primary Examiner)	9/28/2015 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 16

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14667516	RALEIGH, GREGORY G.
	Examiner	Art Unit
	ANDREW JOSEPH RUDY	3687

G06Q		40	/ 12	I	2013-12-03
H04W		8	/ 20	I	2013-01-01
H04W		28	/ 12	I	2013-01-01
H04W		88	/ 08	I	2013-01-01
H04W		4	/ 20	I	2013-01-01
H04W		12	/ 00	I	2013-01-01
H04M		15	/ 88	I	2013-01-01
H04W		28	/ 0268	I	2013-01-01
H04M		15	/ 61	I	2013-01-01
H04W		24	/ 08	I	2013-01-01
H04W		84	/ 04	A	2013-01-01
H04W		84	/ 12	A	2013-01-01
H04W		12	/ 02	I	2013-01-01
H04L		51	/ 046	I	2013-01-01
H04L		63	/ 0428	I	2013-01-01
H04W		4	/ 12	I	2013-01-01
H04W		4	/ 18	I	2013-01-01
H04W		8	/ 18	I	2013-01-01
H04W		72	/ 0453	I	2013-01-01

CPC Combination Sets					
Symbol			Type	Set	Ranking	Version
		/				
		/				

NONE (Assistant Examiner)	(Date)	Total Claims Allowed: 18	
/ANDREW JOSEPH RUDY/ Primary Examiner.Art Unit 3687 (Primary Examiner)	9/28/2015 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 16

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14667516	RALEIGH, GREGORY G.
	Examiner	**Art Unit**
	ANDREW JOSEPH RUDY	3687

US ORIGINAL CLASSIFICATION		INTERNATIONAL CLASSIFICATION										
CLASS	SUBCLASS	CLAIMED					NON-CLAIMED					
709	206	G	0	6	F	15 / 16 (2006.01.01)						
CROSS REFERENCE(S)		H	0	4	L	9 / 32 (2006.01.01)						
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)											
713	168											

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 18	
/ANDREW JOSEPH RUDY/ Primary Examiner.Art Unit 3687 (Primary Examiner)	9/28/2015 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 16

U.S. Patent and Trademark Office

Part of Paper No. 20150928

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14667516	RALEIGH, GREGORY G.
	Examiner	**Art Unit**
	ANDREW JOSEPH RUDY	3687

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

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	18	
/ANDREW JOSEPH RUDY/ Primary Examiner.Art Unit 3687	9/28/2015	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	16

U.S. Patent and Trademark Office Part of Paper No. 20150928

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. 5348

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
14/667,516	03/24/2015 RULE	705	3687	RALEP007C11C4

APPLICANTS
Headwater Partners I LLC, Redwood City, CA;

INVENTORS
Gregory G. Raleigh, Woodside, CA;

**** CONTINUING DATA ***************************
This application is a CON of 14/263,604 04/28/2014 PAT 9037127
which is a CON of 12/380,780 03/02/2009 PAT 8839388
which claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009

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

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED **** ** SMALL ENTITY **
04/02/2015

Foreign Priority claimed ☐ Yes ☑ No 35 USC 119(a-d) conditions met ☐ Yes ☑ No Verified and Acknowledged /ANDREW JOSEPH RUDY/ Examiner's Signature	☐ Met after Allowance Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
		CA	106	18	1

ADDRESS
Headwater Partners I LLC
555 Twin Dolphin Drive, Suite 310
Redwood Shores, CA 94065
UNITED STATES

TITLE
Network System With Common Secure Wireless Message Service Serving Multiple Applications on Multiple Wireless Devices

FILING FEE RECEIVED		
1530	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).

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	14667516
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C4

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	5572528	A	1996-11-05	Shuen, Pauline	
	2	5754953	A	1998-05-19	Briancon et al.	
	3	6628934	A	2003-09-30	Rosenberg et al.	
	4	6662014	B1	2003-12-09	Walsh, Patrick Jay	
	5	6757717	B1	2004-06-29	Goldstein, Leonid	
	6	6901440	B1	2005-05-31	Bimm et al.	
	7	6970692	B2	2005-11-29	Tysor, Arthur James	
	8	7007295	B1	2006-02-28	Rose et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C4

	9	7203752	B2	2007-04-10	Rice et al.	
	10	7222190	B2	2007-05-22	Klinker et al.	
	11	7224968	B2	2007-05-29	Dobson et al.	
	12	7379731	B2	2008-05-27	Natsuno et al.	
	13	7457870	B1	2008-11-25	Lownsbrough et al.	
	14	7515926	B2	2009-04-07	Bu et al.	
	15	7536695	B2	2009-05-19	Alam et al.	
	16	7586871	B2	2009-09-08	Hamilton et al.	
	17	7752330	B2	2010-07-06	Olsen et al.	
	18	7792257	B1	2010-09-07	Vanier et al.	
	19	7801783	B2	2010-09-21	Kende et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C4

	20	7865187	B2	2011-01-04	Ramer et al.	
	21	7933274	B2	2011-04-26	Verma et al.	
	22	8005726	B1	2011-08-23	Bao, Yulin	
	23	8050690	B2	2011-11-01	Neeraj, Chawla	
	24	8086398	B2	2011-12-27	Sanchez et al.	
	25	8107953	B2	2012-01-31	Zimmerman et al.	
	26	8112435	B2	2012-02-07	Epstein et al.	
	27	8174378	B2	2012-05-08	Richman et al.	
	28	8195661	B2	2012-06-05	Kalavade, Asawaree	
	29	8200163	B2	2012-06-12	Hoffman, George E.	
	30	8200818	B2	2012-06-12	Freund et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C4

	31	8208788	B2	2012-06-26	Ando et al.	
	32	8254880	B2	2012-08-28	Aaltonen et al.	
	33	8270955	B2	2012-09-18	Ramer et al.	
	34	8326828	B2	2012-12-04	Zhou et al.	
	35	8331223	B2	2012-12-11	Hill et al.	
	36	8358975	B2	2013-01-22	Bahl et al.	
	37	8533775	B2	2013-09-10	Alcorn et al.	
	38	8538394	B2	2013-09-17	Zimmerman et al.	
	39	8538458	B2	2013-09-17	Haney, Richard D.	
	40	8565746	B2	2013-10-22	Hoffman, George E.	
	41	8571501	B2	2013-10-29	Miller et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C4

	42	8644702	B1	2014-02-04	Kalajan, Kevin E.	
	43	8713535	B2	2014-04-29	Malhotra et al.	
	44	8713641	B1	2014-04-29	Pagan et al.	
	45	8730842	B2	2014-05-20	Collins et al.	
	46	8732808	B2	2014-05-20	Sewall et al.	
	47	8761711	B2	2014-06-24	Grignani et al.	
	48	9049010		2015-06-02	Jueneman et al.	
	49	6445777		2002-09-03	Clark, Curtis	
	50	7039027		2006-05-02	Bridgelall, Raj	
	51	7990049		2011-08-02	Shioya, Shunsuke	
	52	8180886		2012-05-15	Overcash et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C4

	53	8339991		2012-12-25	Biswas et al.	

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	20020154751	A1	2002-10-24	Thompson et al.	
	2	20030084321	A1	2003-05-01	Tarquini et al.	
	3	20040133668	A1	2004-07-08	Nicholas III, Henry T.	
	4	20060136882	A1	2006-06-22	Noonan et al.	
	5	20060143066	A1	2006-06-29	Calabria	
	6	20070073899	A1	2007-03-29	Judge et al.	
	7	20070174490	A1	2007-07-26	Choi et al.	
	8	20070234402	A1	2007-10-04	Khosravi et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C4

	9	20090048913	A1	2009-02-19	Shenfield et al.	
	10	20090181662	A1	2009-07-16	Fleischman et al.	
	11	20020191573		2002-12-19	Whitehill et al.	
	12	20060098627		2006-05-11	Karaoguz, Jeyhan et al.	
	13	20090070379		2009-03-12	Rappaport, Theodore R.	

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	2688553	CA	A1	2008-12-04	Yoggie Security Systems, Inc.		☐
	2	1508734	CN	A	2004-06-30	Chinese Creative Corp.		☐
	3	1850575	EP	A1	2007-10-31	Research In Motion		☐
	4	2009111919	JP		2009-05-21	Kyocera Communications Systems		☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C4

	5	2009232107	JP	A	2009-10-08	Fujitsu Ltd.		☐
	6	2006012610	WO	A2	2006-02-02	Citrix Systems, Inc.		☐

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	"Ads and movies on the run," the Gold Coast Bulletin, Southport, Qld, Jan. 29, 2008	☐
	2	"Jentro Technologies launches Zenlet platform to accelerate location-based content delivery to mobile devices," The Mobile Internet, Boston, MA, Feb. 2008	☐
	3	Jing et al., "Client-Server Computing in Mobile Environments," GTE Labs. Inc., Purdue University, ACM Computing Surveys, Vol. 31, No. 2, June 1999	☐
	4	Kim, "Free wireless a high-wire act; MetroFi needs to draw enough ads to make service add profits," San Francisco Chronicle, Aug. 21, 2006	☐
	5	Koutsopoulou et al., "Charging, Accounting and Billing Management Schemes In Mobile Telecommunication Networks and the Internet," IEEE Communications Surveys & Tutorials, First Quarter 2004, Vol. 6, No. 1	☐
	6	Loopt User Guide, metroPCS, 7/17/2008	☐
	7	Nuzman et al., "A compund model for TCP connection arrivals for LAN and WAN applications," Oct. 22, 2002	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C4

	8	Richtel, "Cellphone consumerism; If even a debit card is too slow, now you have a new way to act on impulse: [National Edition]," National Post, Canada, Oct. 2, 2007	☐
	9	Rivadeneyra et al., "A communication architecture to access data services through GSM," San Sebastian, Spain, 1998	☐
	10	Sabat, "The evolving mobile wireless value chain and market structure," Nov. 2002	☐
	11	Sun et al., "Towards Connectivity Management Adaptability: Context Awareness in Policy Representation and End-to-end Evaluation Algorithm," Dept. of Electrical and Information Engineering, Univ. of Oulu, Finland, 2004	☐

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	14667516
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C4

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.

☐ Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ None

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	/James E. Harris/	Date (YYYY-MM-DD)	2015-09-17
Name/Print	James E. Harris	Registration Number	40013

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)).

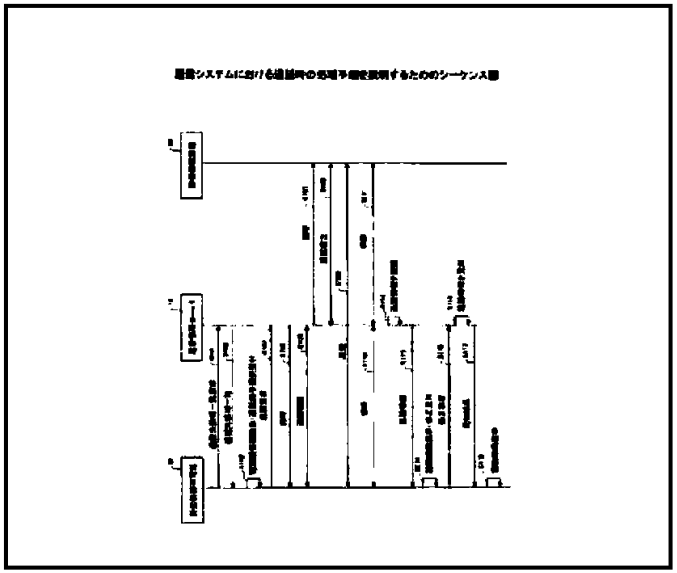
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under 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.

(11)Publication number 2009-232107
(43)Date of publication of application 08.10.2009
(51)Int.Cl. *H04M 15/00 (2006.01)*

(21)Application number 2008-074306
(22)Date of filing 21.03.2008
(71)Applicant FUJITSU LTD
(72)Inventor TSUJIUCHI HIDETOSHI



(54)SPEECH COMMUNICATION INFORMATION RECORDING PROGRAM, SPEECH COMMUNICATION INFORMATION RECORDING APPARATUS AND SPEECH COMMUNICATION INFORMATION RECORDING METHOD

(57)Abstract
PROBLEM TO BE SOLVED: To provide a speech communication information recording program, a speech communication information recording apparatus and a speech communication information recording method, for appropriately dividing the burden origin of a call charge for one telephone number.
SOLUTION: A computer is made to execute: a procedure of receiving information specifying a call originating telephone number and information specifying a call terminating telephone number from a telephone set on a call originating side; a speech communication relay procedure of establishing speech communication between the telephone set on the call originating side and the telephone set on the call terminating side on the basis of the received information; a billing destination determination procedure of determining a billing destination for the call terminating telephone number using a management means for managing the identification information of the billing destination of the call charge by telephone number; and a billing destination recording procedure of relating the identification information of the determined billing destination and the identification information of the speech communication and recording them in a storage device.

(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2009-232107
(P2009-232107A)
(43)公開日　平成21年10月8日(2009.10.8)

(51)Int.Cl.		F I		テーマコード（参考）
H04M 15/00	(2006.01)	H04M 15/00	E	5K025

審査請求 未請求　請求項の数 7　OL　（全 21 頁）

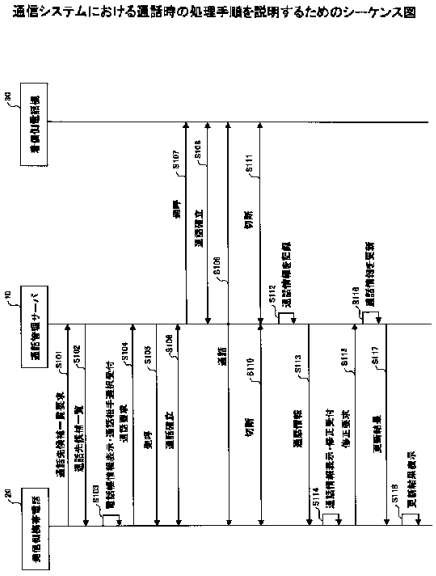
(21)出願番号　特願2008-74306 (P2008-74306)
(22)出願日　平成20年3月21日 (2008.3.21)

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100070150
弁理士　伊東　忠彦
(72)発明者　辻内　秀敏
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

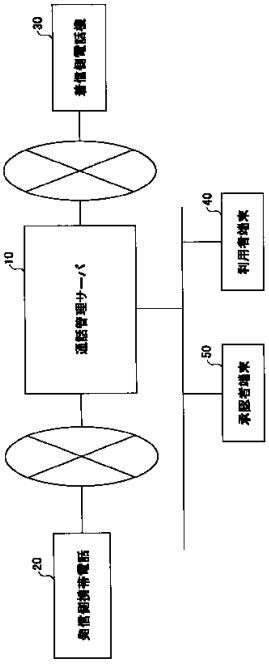
Ｆターム(参考)　5K025 AA01　CC01　CC07　GG10　GG12

(54)【発明の名称】通話情報記録プログラム、通話情報記録装置、及び通話情報記録方法

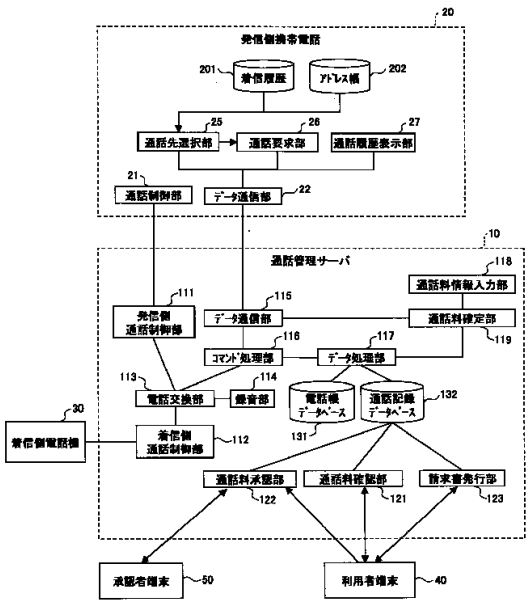
(57)【要約】
【課題】一つの電話番号に対する通話料の負担元を適切に区分することのできる通話情報記録プログラム、通話情報記録装置、及び通話情報記録方法の提供を目的とする。
【解決手段】コンピュータに、発信側の電話機より発信電話番号を特定する情報と着信電話番号を特定する情報とを受信する手順と、受信された情報に基づいて前記発信側の電話機と着信側の電話機との間の通話を確立する通話中継手順と、電話番号ごとに通話料の請求先の識別情報を管理する管理手段を用いて、前記着信電話番号に対する請求先を判定する請求先判定手順と、判定された請求先の識別情報と前記通話の識別情報とを関連付けて記憶装置に記録する請求先記録手順とを実行させることにより上記課題を解決する。
【選択図】図４



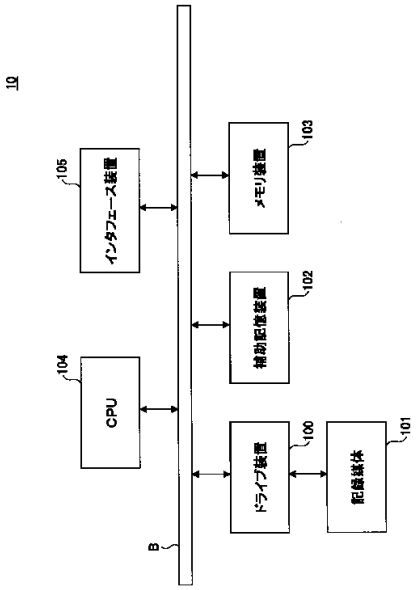
本発明の実施の形態における通信システム構成例を示す図



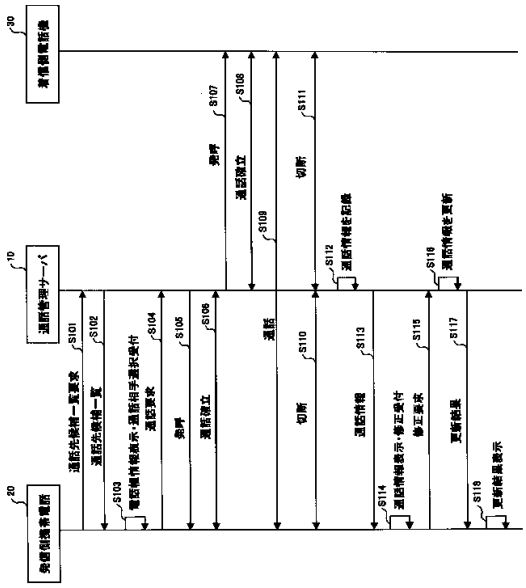
本発明の実施の形態における通信システムの機能構成例を示す図



本発明の実施の形態における通話管理サーバのハードウェア構成例を示す図



通信システムにおける通話時の処理手順を説明するためのシーケンス図

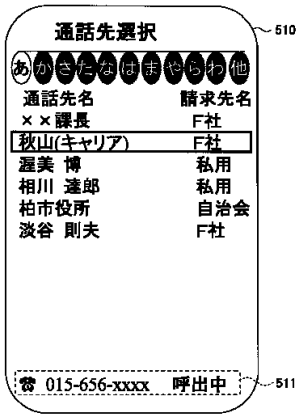


電話帳データベースの構成例を示す図

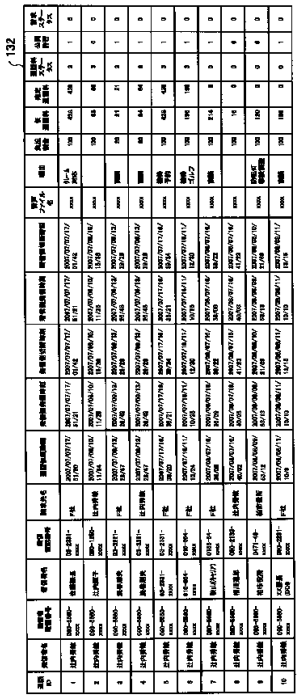
131

発信者名	発信者電話番号	通話先名	通話先電話番号	関係	請求先名	メールアドレス
辻内秀敏	090-5560-xxxx	辻内匡子	090-1250-xxxx	妻	辻内秀敏	xxx@xxxxxxx
辻内秀敏	090-5560-xxxx	渡谷則夫	03-3221-xxxx	松上電器	F社	xxx@xxxxxxx
辻内秀敏	090-5560-xxxx	柏市役所	0471-48-xxxx	自治会	柏市役所	xxx@xxxxxxx
辻内秀敏	090-5560-xxxx	佐藤課長	03-2331-xxxx	OO商事	F社	xxx@xxxxxxx
辻内秀敏	090-5560-xxxx	秋山(キャリア)	0156-64-xxxx	F社	F社	xxx@xxxxxxx
辻内秀敏	090-5560-xxxx	相川達郎	050-2133-xxxx	親戚	辻内秀敏	
辻内秀敏	090-5560-xxxx	××課長	090-2231-xxxx	顧客	F社	xxx@xxxxxxx

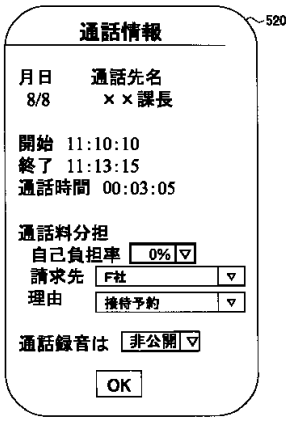
通話先選択画面の表示例を示す図



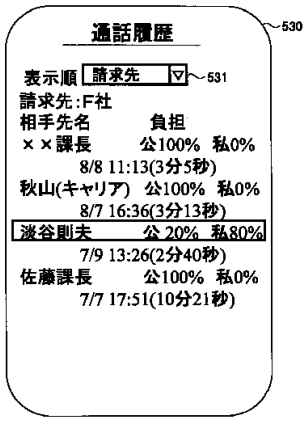
通話記録データベースの構成例を示す図



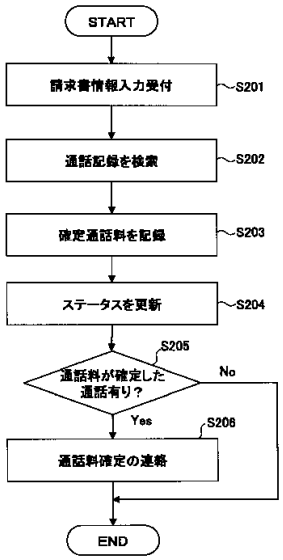
通話情報画面の表示例を示す図



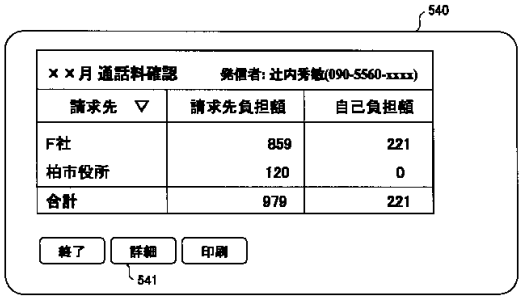
通話履歴画面の表示例を示す図



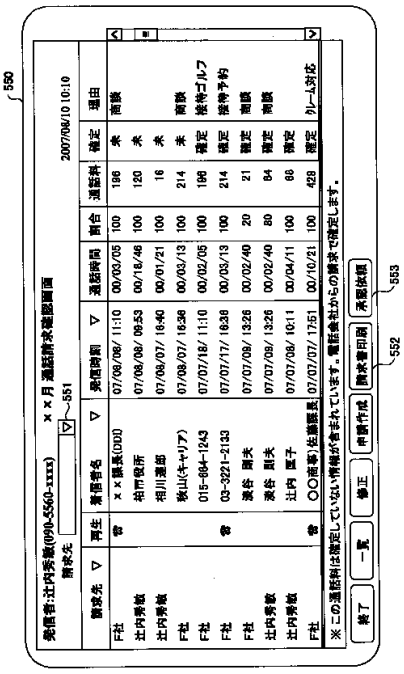
通話料の請求に応じて通話管理サーバによって実行される通話料の確定処理の処理手順を説明するためのフローチャート



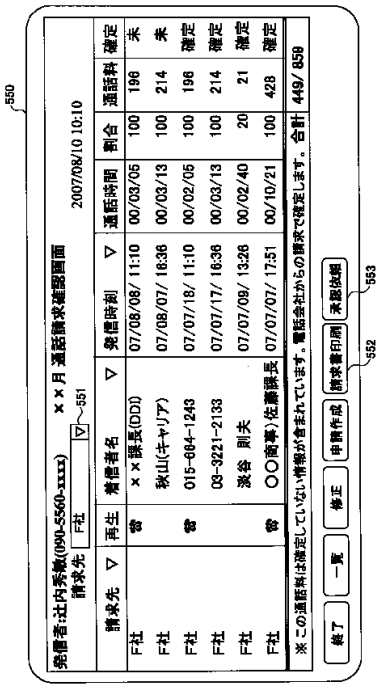
通話料確認画面の表示例を示す図



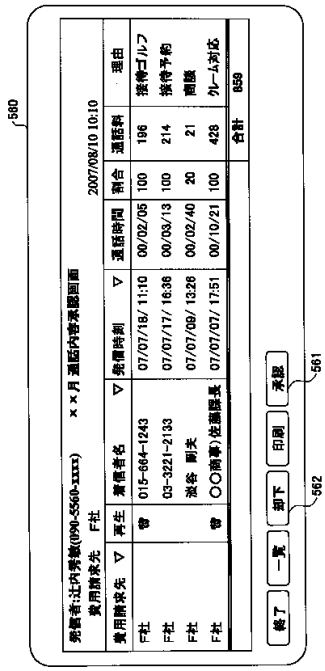
通話料確認詳細画面の表示例を示す図



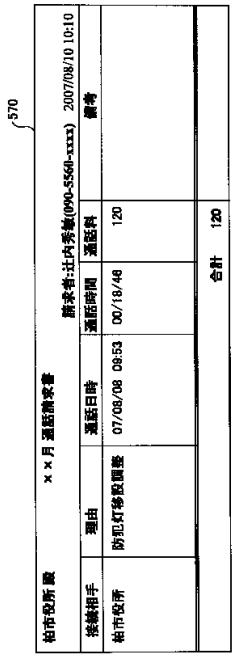
請求先が所属企業に絞り込まれた場合の通話料詳細画面の表示例を示す図



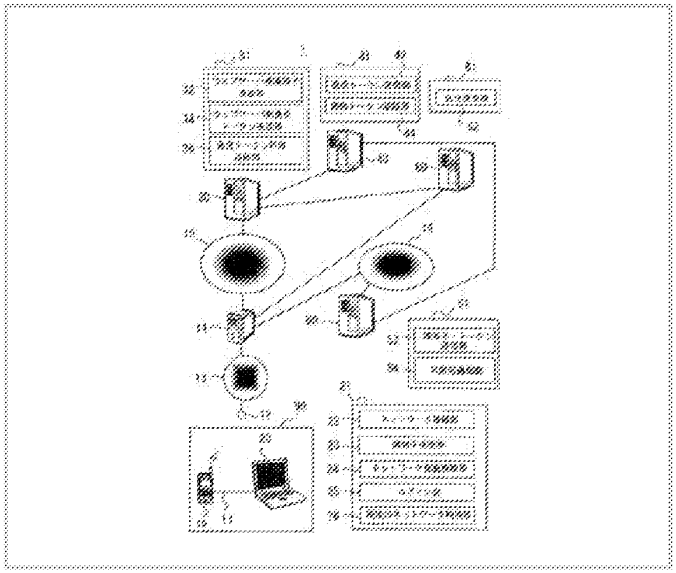
承認画面の表示例を示す図



請求書画面の表示例を示す図



(11)Publication number 2009-111919
(43)Date of publication of application 21.05.2009
(51)Int.Cl. *H04L 12/56 (2006.01)*
H04M 15/00 (2006.01)
H04M 11/00 (2006.01)
(21)Application number 2007-284415
(22)Date of filing 31.10.2007
(71)Applicant KYOCERA COMMUNICATION SYSTEMS CO LTD
(72)Inventor MASUDA KEIICHI



(54)SYSTEM, PROGRAM AND RECORDING MEDIUM FOR BILLING DATA COMMUNICATION FEE, AND METHOD OF BILLING DATA COMMUNICATION FEE

(57)Abstract
PROBLEM TO BE SOLVED: To provide a system or the like for billing a data communication fee, which can make account separately between official and private expenses when accessing a predetermined network 16 in a business-related matter, and which is also highly reliable as viewed from the carrier side.
SOLUTION: When a mobile party purchases a communication token T for a given network 16, the mobile party transmits the ID of the mobile phone 10 to a communication token issuing server 40 through the web server 30. The communication token T is generated based on the ID and transmitted to a PC 20 through the web server 30 and the mobile phone 10. After once disconnecting between the mobile phone and the network 15 for contents of the mobile phone, the mobile party tests the use of the predetermined network 16 through an authentication server 50 using the ID and the communication token T. The ID and the communication token T are transmitted to the communication token issuing server 40 and the validity of the communication token T is authenticated. The amount of the fee for data communication of the mobile phone 10, from which the fee for the communication token T is deducted, is charged to a billing destination on the mobile phone 10 side, and the fee for the communication token T is charged to another billing destination.

(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2009-111919
(P2009-111919A)
(43)公開日　平成21年5月21日(2009.5.21)

(51)Int.Cl.		F I		テーマコード（参考）
H04L 12/56	(2006.01)	H04L 12/56	C	5K025
H04M 15/00	(2006.01)	H04M 15/00	G	5K030
H04M 11/00	(2006.01)	H04M 15/00	E	5K201
		H04M 11/00	302	

審査請求 有　請求項の数 23　ＯＬ　（全 26 頁）

(21)出願番号　特願2007-284415 (P2007-284415)
(22)出願日　平成19年10月31日 (2007.10.31)

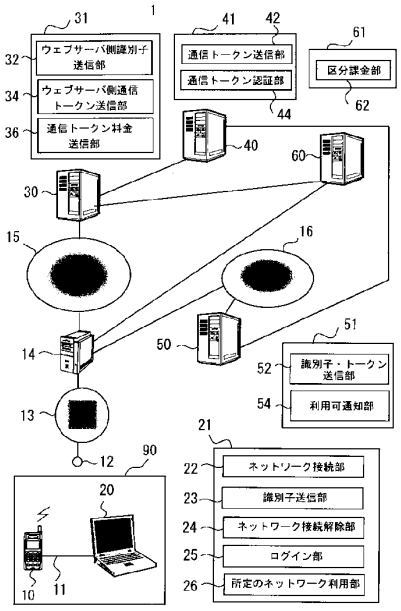
(71)出願人　596100812
京セラコミュニケーションシステム株式会社
京都府京都市伏見区竹田鳥羽殿町６番地
(74)代理人　100108372
弁理士　谷田　拓男
(72)発明者　増田　景一
京都府京都市伏見区竹田鳥羽殿町６番地
京セラコミュニケーションシステム株式会社内

Ｆターム(参考)　5K025 BB08 CC09 DD06 EE19 EE24 FF22 GG10 GG18
5K030 GA15 GA19 HA08 HB08 HB11 HC01 JA10 JT02 KA04 KA06 LB01 MC07

最終頁に続く

(54)【発明の名称】データ通信料金課金システム、プログラム、記録媒体およびデータ通信料金課金方法

(57)【要約】
【課題】業務上所定のネットワーク１６へアクセスする場合に公私分計することができ且つキャリヤ側からみて信頼度が高いデータ通信料金課金システム等を提供する。
【解決手段】所定のネットワーク１６用の通信トークンＴを購入する際、携帯電話器１０のＩＤをウェブサーバ３０経由で通信トークン発行サーバ４０へ送信する。ＩＤに基づき通信トークンＴが生成されウェブサーバ３０及び携帯電話器１０を介してＰＣ２０へ送信される。携帯電話コンテンツ用ネットワーク１５との接続を一旦解除した後、ＩＤ及び通信トークンＴを用い認証サーバ５０を介し所定のネットワーク１６の利用を試す。ＩＤ及び通信トークンＴは通信トークン発行サーバ４０へ送信され通信トークンＴの正当性が認証される。携帯電話器１０のデータ通信に対する料金から通信トークンＴの料金を控除した額が携帯電話器１０側の請求先に課金され通信トークンＴの料金は他の請求先に課金される。
【選択図】　図１



【特許請求の範囲】
【請求項１】
移動通信機能を有する移動通信部と情報処理機能を有する情報処理部とを備えた移動情報端末の該移動通信部に掛かるデータ通信料金を該移動通信部側の請求先と他の請求先とに区分して課金するデータ通信料金課金システムであって、該移動通信部が移動通信部側ネットワークに接続する際の認証課金を行う通信事業者側サーバと、該移動通信部側ネットワークに接続されソフトウェアの配信を行う配信サイトが稼動するウェブサーバと、該ウェブサーバと接続され所定のネットワークの利用権を示す通信トークンを発行する通信トークン発行サーバと、該ウェブサーバと接続され該移動通信部に掛かるデータ通信料金を課金する課金サーバと、該所定のネットワークに接続された認証サーバとを備え、
前記移動情報端末は、
前記移動通信部を介して移動通信部側ネットワークに接続する移動通信部側ネットワーク接続手段と、
前記通信トークンの購入に際し前記移動通信部の識別子を前記ウェブサーバへ送信する識別子送信手段と、
前記ウェブサーバ側から前記移動通信部を介して前記通信トークンが送信された後、前記移動通信部側ネットワーク接続手段により接続された移動通信部側ネットワークとの接続を解除する移動通信部側ネットワーク接続解除手段と、
前記移動通信部の識別子及び前記ウェブサーバ側から送信された通信トークンを用い、前記移動通信部及び前記認証サーバを介して前記所定のネットワークの利用を試みるログイン手段と、
前記認証サーバから前記所定のネットワークの利用を認める通知が送信された場合、該認証サーバを介して該所定のネットワークの利用を行う所定のネットワーク利用手段とを備え、
前記ウェブサーバは、
前記識別子送信手段により送信された識別子を前記通信トークン発行サーバへ送信するウェブサーバ側識別子送信手段と、
前記通信トークン発行サーバから送信された通信トークンを前記移動通信部を介して前記情報処理部へ送信するウェブサーバ側通信トークン送信手段と、
前記課金サーバへ前記ウェブサーバ側通信トークン送信手段により送信された通信トークンの料金を送信する通信トークン料金送信手段とを備え、
前記認証サーバは、
前記ログイン手段により用いられた識別子及び通信トークンを前記通信トークン発行サーバへ送信する識別子・通信トークン送信手段と、
前記通信トークン発行サーバにより前記通信トークンの正当性が認証された場合、前記移動通信部を介して前記情報処理部へ前記所定のネットワークの利用を認める通知を送信する利用可通知手段とを備え、
前記通信トークン発行サーバは、
前記ウェブサーバ側識別子送信手段により送信された識別子に基づき通信トークンを生成して前記ウェブサーバへ送信する通信トークン送信手段と、
前記識別子・通信トークン送信手段により送信された識別子及び通信トークンに基づき該通信トークンの正当性を認証する通信トークン認証手段とを備え、
前記課金サーバは、
前記通信事業者側サーバから送信された所定の期間における前記移動通信部のデータ通信に対する料金から、該所定の期間における前記通信トークン料金送信手段により送信された通信トークンの料金を控除した額を該移動通信部側の請求先に課金し、該通信トークンの料金を他の請求先に課金する区分課金手段とを備えたことを特徴とするデータ通信料金課金システム。
【請求項２】
請求項１記載のデータ通信料金課金システムにおいて、前記移動通信部が無線ＬＡＮを

介して前記所定のネットワークの利用を行う場合、
前記通信トークン料金送信手段により送信された通信トークンの料金は無線ＬＡＮ回線使用料金を含み、
前記ログイン手段は、前記移動通信部の識別子及び前記ウェブサーバ側通信トークン送信手段により送信された該通信トークンを用い無線ＬＡＮ基地局及び前記認証サーバを介して所定のネットワークの利用を試み、
前記利用可通知手段は、前記通信トークン認証手段により前記通信トークンの正当性が認証された場合、無線ＬＡＮ基地局を介して前記情報処理部へ前記所定のネットワークの利用を認める通知を送信することを特徴とするデータ通信料金課金システム。
【請求項３】
請求項１又は２記載のデータ通信料金課金システムにおいて、前記所定のネットワークへの接続が認証を要する場合、前記ウェブサーバが該認証を行うウェブサーバ側認証手段をさらに備えたことを特徴とするデータ通信料金課金システム。
【請求項４】
請求項１乃至３のいずれかに記載のデータ通信料金課金システムにおいて、
前記通信トークン送信手段は、前記ウェブサーバ側識別子送信手段により送信された識別子と所定の鍵と所定の乱数とに基づき該通信トークンを生成して該ウェブサーバへ送信し、該所定の乱数は該識別子と関連付けて記録しておき、
前記通信トークン認証手段は、前記識別子・通信トークン送信手段により送信された識別子及び通信トークンと、前記所定の鍵と、前記通信トークン送信手段により該識別子と関連付けて記録された所定の乱数とに基づき前記通信トークンの正当性を認証することを特徴とするデータ通信料金課金システム。
【請求項５】
請求項１乃至４のいずれかに記載のデータ通信料金課金システムにおいて、前記移動情報端末及び前記課金サーバは該移動通信部の１以上の識別子と該１以上の識別子に各々対応する前記他の請求先との対応表をさらに備え、
前記識別子送信手段は、前記通信トークンの購入に際し前記対応表に基づき前記移動通信部の１以上の識別子の内の一つの識別子を前記ウェブサーバへ送信し、
前記通信トークン料金送信手段は、前記課金サーバへ前記ウェブサーバ側通信トークン送信手段により送信された通信トークンの料金と前記識別子送信手段により送信された識別子とを送信し、
前記区分課金手段は、前記通信事業者側サーバから送信された所定の期間における前記移動通信部のデータ通信に対する料金から、該所定の期間における前記通信トークン料金送信手段により送信された通信トークンの料金を控除した額を該移動通信部側の請求先に課金し、該通信トークンの料金を前記通信トークン料金送信手段により送信された識別子に対応する前記対応表中の他の請求先に課金することを特徴とするデータ通信料金課金システム。
【請求項６】
請求項１乃至５のいずれかに記載のデータ通信料金課金システムにおいて、前記移動通信部側の請求先は該移動通信部の所有者又は利用者側であり、前記他の請求先は該所有者又は該利用者に対して所定の関係を有する側であることを特徴とするデータ通信料金課金システム。
【請求項７】
請求項１乃至６のいずれかに記載のデータ通信料金課金システムにおいて、前記移動通信部は携帯電話器であり、前記情報処理部はパーソナルコンピュータであり、該携帯電話器と該パーソナルコンピュータとは脱着可能に接続されたことを特徴とするデータ通信料金課金システム。
【請求項８】
移動通信機能を有する移動通信部と情報処理機能を有する情報処理部とを備えた移動情報端末が実行するプログラムであって、該情報処理部のコンピュータを、

前記移動通信部を介して移動通信部側ネットワークに接続する移動通信部側ネットワーク接続手段、

前記移動通信部側ネットワークに接続されソフトウェアの配信を行う配信サイトが稼動するウェブサーバへ、所定のネットワークの利用権を示す通信トークンの購入に際し該移動通信部の識別子を送信する識別子送信手段、

前記ウェブサーバ側から前記移動通信部を介して前記通信トークンが送信された後、前記移動通信部側ネットワーク接続手段により接続された移動通信部側ネットワークとの接続を解除する移動通信部側ネットワーク接続解除手段、

前記移動通信部の識別子及び前記ウェブサーバ側から送信された通信トークンを用い、前記移動通信部及び前記所定のネットワークに接続された認証サーバを介して該所定のネットワークの利用を試みるログイン手段、

前記認証サーバから前記所定のネットワークの利用を認める通知が送信された場合、該認証サーバを介して該所定のネットワークの利用を行う所定のネットワーク利用手段として機能させるためのプログラムであり、

前記識別子送信手段により前記ウェブサーバへ送信された識別子は、該ウェブサーバにより、該ウェブサーバと接続され通信トークンを発行する通信トークン発行サーバへ送信され、該通信トークン発行サーバにより、送信された該識別子に基づき通信トークンが生成され、該通信トークンは該ウェブサーバへ送信され、該ウェブサーバにより、送信された該通信トークンは前記移動通信部を介して前記情報処理部へ送信され、該ウェブサーバと接続され前記移動通信部に掛かるデータ通信料金を課金する課金サーバへ、該通信トークンの料金が送信されるものであり、

前記ログイン手段により用いられた識別子及び通信トークンは、前記認証サーバにより前記通信トークン発行サーバへ送信され、該通信トークン発行サーバにより、送信された識別子及び通信トークンに基づき通信トークンの正当性が認証され、該通信トークンの正当性が認証された場合、該認証サーバにより、前記移動通信部を介して前記情報処理部へ該所定のネットワークの利用を認める通知が送信され、

前記課金サーバにより、前記移動通信部が前記移動通信部側ネットワークに接続する際の認証課金を行う通信事業者側サーバから送信された所定の期間における該移動通信部のデータ通信に対する料金から、該所定の期間における前記ウェブサーバにより送信された通信トークンの料金を控除した額が該移動通信部側の請求先に課金され、該通信トークンの料金が他の請求先に課金されることを特徴とするプログラム。

【請求項９】

請求項８記載のプログラムにおいて、前記移動情報端末が無線ＬＡＮを介して前記所定のネットワークの利用を行う場合、

前記ウェブサーバ側から前記課金サーバ側へ送信された通信トークンの料金は無線ＬＡＮ回線使用料金を含み、

前記ログイン手段は、前記移動情報端末の識別子及び前記ウェブサーバ側から送信された通信トークンを用い無線ＬＡＮ基地局及び前記認証サーバを介して前記所定のネットワークの利用を試み、

前記通信トークン発行サーバにより前記通信トークンの正当性が認証された場合、前記認証サーバにより、無線ＬＡＮ基地局を介して前記情報処理部へ前記所定のネットワークの利用を認める通知が送信されることを特徴とするプログラム。

【請求項１０】

請求項８又は９記載のプログラムにおいて、前記移動情報端末及び前記課金サーバは該移動通信部の１以上の識別子と該１以上の識別子に各々対応する前記他の請求先との対応表をさらに備え、

前記識別子送信手段は、前記通信トークンの購入に際し前記対応表に基づき前記移動通信部の１以上の識別子の内の一つの識別子を前記ウェブサーバへ送信し、

前記ウェブサーバにより、前記課金サーバへ、前記移動通信部を介して前記情報処理部へ送信された通信トークンの料金と前記識別子送信手段により送信された識別子とが送信

され、
前記課金サーバにより、前記通信事業者側サーバから送信された所定の期間における前記移動通信部のデータ通信に対する料金から、該所定の期間における前記ウェブサーバにより送信された通信トークンの料金を控除した額を該移動通信部側の請求先に課金し、該通信トークンの料金を前記ウェブサーバにより送信された識別子に対応する前記対応表中の他の請求先に課金することを特徴とするプログラム。
【請求項１１】
移動通信機能を有する移動通信部と情報処理機能を有する情報処理部とを備えた移動情報端末の該移動通信部に掛かるデータ通信料金を課金する課金サーバが該移動通信部に掛かるデータ通信料金を該移動通信部側の請求先と他の請求先とに区分して課金するためのプログラムであって、課金サーバのコンピュータを、
前記移動通信部が移動通信部側ネットワークに接続する際の認証課金を行う通信事業者側サーバから送信された所定の期間における該移動通信部のデータ通信に対する料金から、該移動通信部側ネットワークに接続されソフトウェアの配信を行う配信サイトが稼動するウェブサーバから前記課金サーバへ送信された該所定の期間における所定のネットワークの利用権を示す通信トークンの料金を控除した額を該移動通信部側の請求先に課金し、該通信トークンの料金を他の請求先に課金する区分課金手段として機能させるためのプログラムであり、
前記移動情報端末により、該移動通信部を介して前記移動通信部側ネットワークに接続し、通信トークンの購入に際し該移動通信部の識別子が前記ウェブサーバへ送信され、該ウェブサーバにより、送信された該識別子が該ウェブサーバと接続され通信トークンを発行する通信トークン発行サーバへ送信され、該通信トークン発行サーバにより、送信された該識別子に基づき通信トークンが生成され、該通信トークンは該ウェブサーバへ送信され、該ウェブサーバにより、送信された該通信トークンが該移動通信部を介して該情報処理部へ送信され、前記課金サーバへ該通信トークンの料金が送信されるものであり、
前記移動情報端末により、従前に接続された前記移動通信部側ネットワークとの接続が解除され、前記移動通信部の識別子及び前記ウェブサーバから送信された前記通信トークンを用い、該移動通信部及び前記所定のネットワークに接続された認証サーバを介して該所定のネットワークの利用が試みられ、該認証サーバにより、移動情報端末により用いられた該識別子及び該通信トークンが前記通信トークン発行サーバへ送信され、該通信トークン発行サーバにより、送信された該識別子及び該通信トークンに基づき該通信トークンの正当性が認証された場合、該移動通信部を介して該情報処理部へ該所定のネットワークの利用を認める通知が送信され、該移動情報端末により、該認証サーバを介して該所定のネットワークの利用が行なわれることを特徴とするプログラム。
【請求項１２】
請求項１１記載のプログラムにおいて、前記移動通信部が無線ＬＡＮを介して前記所定のネットワークの利用を行う場合、
前記ウェブサーバから前記課金サーバへ送信された通信トークンの料金は無線ＬＡＮ回線使用料金を含み、
前記移動情報端末により、前記移動通信部の識別子及び前記ウェブサーバ側から該移動通信部を介して該情報処理部へ送信された前記通信トークンを用い無線ＬＡＮ基地局及び前記認証サーバを介して所定のネットワークの利用が試みられ、
前記通信トークン発行サーバにより前記通信トークンの正当性が認証された場合、前記認証サーバにより、無線ＬＡＮ基地局を介して前記情報処理部へ前記所定のネットワークの利用を認める通知が送信されることを特徴とするプログラム。
【請求項１３】
請求項１１又は１２記載のプログラムにおいて、前記移動情報端末及び前記課金サーバは該移動通信部の１以上の識別子と該１以上の識別子に各々対応する前記他の請求先との対応表をさらに備え、
前記移動情報端末により、前記通信トークンの購入に際し前記対応表に基づき前記移動

通信部の１以上の識別子の内の一つの識別子が前記ウェブサーバへ送信され、
前記ウェブサーバにより、前記課金サーバへ、前記移動通信部を介して前記情報処理部へ送信された通信トークンの料金と前記移動情報端末により送信された識別子とが送信され、
前記区分課金手段は、前記通信事業者側サーバから送信された所定の期間における前記移動通信部のデータ通信に対する料金から、該所定の期間における前記通信トークン料金送信手段により送信された通信トークンの料金を控除した額を該移動通信部側の請求先に課金し、該通信トークンの料金を前記通信トークン料金送信手段により送信された識別子に対応する前記対応表中の他の請求先に課金することを特徴とするプログラム。
【請求項１４】
請求項８乃至１３のいずれかに記載のプログラムにおいて、前記移動通信部側の請求先は該移動通信部の所有者又は利用者側であり、前記他の請求先は該所有者又は該利用者に対して所定の関係を有する側であることを特徴とするプログラム。
【請求項１５】
請求項８乃至１４のいずれかに記載のプログラムにおいて、前記移動通信部は携帯電話器であり、前記情報処理部はパーソナルコンピュータであり、該携帯電話器と該パーソナルコンピュータとは脱着可能に接続されたことを特徴とするプログラム。
【請求項１６】
請求項８乃至１５のいずれかに記載のプログラムを記録したコンピュータ読取り可能な記録媒体。
【請求項１７】
移動通信機能を有する移動通信部と情報処理機能を有する情報処理部とを備えた移動情報端末の該移動通信部に掛かるデータ通信料金を該移動通信部側の請求先と他の請求先とに区分して課金するデータ通信料金課金方法であって、
前記移動情報端末が、
前記移動通信部を介して移動通信部側ネットワークに接続する移動通信部側ネットワーク接続ステップと、
前記移動通信部側ネットワーク接続ステップで接続された移動通信部側ネットワークに接続されソフトウェアの配信を行う配信サイトが稼動するウェブサーバへ、所定のネットワークの利用権を示す通信トークンの購入に際し該移動通信部の識別子を送信する識別子送信ステップと、
前記ウェブサーバが、
前記ウェブサーバと接続され前記通信トークンを発行する通信トークン発行サーバへ、前記識別子送信ステップで送信された識別子を送信するウェブサーバ側識別子送信ステップと、
前記通信トークン発行サーバが、
前記ウェブサーバ側識別子送信ステップで送信された識別子に基づき通信トークンを生成して前記ウェブサーバへ送信する通信トークン送信ステップと、
前記ウェブサーバが、
前記通信トークン送信ステップで送信された通信トークンを前記移動通信部を介して前記情報処理部へ送信するウェブサーバ側通信トークン送信ステップと、
前記ウェブサーバと接続され前記移動通信部に掛かるデータ通信料金を課金する課金サーバへ、前記ウェブサーバ側通信トークン送信ステップで送信された通信トークンの料金を送信する通信トークン料金送信ステップと、
前記移動情報端末が、
前記移動通信部側ネットワーク接続ステップで接続された移動通信部側ネットワークとの接続を解除する移動通信部側ネットワーク接続解除ステップと、
前記移動通信部の識別子及び前記ウェブサーバ側通信トークン送信ステップで送信された通信トークンを用い、前記移動通信部及び前記所定のネットワークに接続された認証サーバを介して該所定のネットワークの利用を試みるログインステップと、

前記認証サーバが、
前記ログインステップで用いられた識別子及び通信トークンを前記通信トークン発行サーバへ送信する識別子・通信トークン送信ステップと、
前記通信トークン発行サーバが、
前記識別子・通信トークン送信ステップで送信された識別子及び通信トークンに基づき該通信トークンの正当性を認証する通信トークン認証ステップと、
前記認証サーバが、
前記通信トークン認証ステップで通信トークンの正当性が認証された場合、前記移動通信部を介して前記情報処理部へ前記所定のネットワークの利用を認める通知を送信する利用可通知ステップと、
前記移動情報端末が、
前記利用通知ステップで前記認証サーバから前記所定のネットワークの利用を認める通知が送信された場合、該認証サーバを介して前記所定のネットワークの利用を行う所定のネットワーク利用ステップと、
前記課金サーバが、
前記移動通信部が前記移動通信部側ネットワークに接続する際の認証課金を行う通信事業者側サーバから送信された所定の期間における該移動通信部のデータ通信に対する料金から、該所定の期間における前記通信トークン料金送信ステップで送信された通信トークンの料金を控除した額を該移動通信部側の請求先に課金し、該通信トークンの料金を他の請求先に課金する区分課金ステップとを備えたことを特徴とするデータ通信料金課金方法。
【請求項１８】
請求項１７記載のデータ通信料金課金方法において、前記移動通信部が無線ＬＡＮを介して該所定のネットワークの利用を行う場合、
前記通信トークン料金送信ステップで送信された該通信トークンの料金は無線ＬＡＮ回線使用料金を含み、
前記ログインステップは、前記移動通信部の識別子及び前記ウェブサーバ側通信トークン送信ステップで送信された通信トークンを用い前記無線ＬＡＮ基地局及び前記認証サーバを介して前記所定のネットワークの利用を試み、
前記利用可通知ステップは、前記通信トークン認証ステップで通信トークンの正当性が認証された場合、無線ＬＡＮ基地局を介して前記情報端末装置へ前記所定のネットワークの利用を認める通知を送信することを特徴とするデータ通信料金課金方法。
【請求項１９】
請求項１７又は１８記載のデータ通信料金課金方法において、前記所定のネットワークへの接続が認証を要する場合、前記ウェブサーバ側識別子送信ステップに先立ち、前記ウェブサーバが該認証を行うウェブサーバ側認証ステップをさらに備えたことを特徴とするデータ通信料金課金方法。
【請求項２０】
請求項１７乃至１９のいずれかに記載のデータ通信料金課金方法において、
前記通信トークン送信ステップは、前記通信トークン発行サーバが、前記ウェブサーバ側識別子送信ステップで送信された識別子と所定の鍵と所定の乱数とに基づき通信トークンを生成して前記ウェブサーバへ送信し、該所定の乱数は該識別子と関連付けて記録しておき、
前記通信トークン認証ステップは、前記通信トークン発行サーバが、前記識別子・通信トークン送信ステップで送信された識別子及び通信トークンと、前記所定の鍵と、前記通信トークン送信ステップで該識別子と関連付けて記録された所定の乱数とに基づき該通信トークンの正当性を認証することを特徴とするデータ通信料金課金方法。
【請求項２１】
請求項１７乃至２０のいずれかに記載のデータ通信料金課金方法において、前記移動情報端末及び前記課金サーバは該移動通信部の１以上の識別子と該１以上の識別子に各々対

応する前記他の請求先との対応表をさらに備え、
前記識別子送信ステップは、前記通信トークンの購入に際し前記対応表に基づき前記移動通信部の１以上の識別子の内の一つの識別子を前記ウェブサーバへ送信し、
前記通信トークン料金送信ステップは、前記課金サーバへ前記ウェブサーバ側通信トークン送信ステップで送信された通信トークンの料金と前記識別子送信ステップで送信された識別子とを送信し、
前記区分課金ステップは、前記通信事業者側サーバから送信された所定の期間における前記移動通信部のデータ通信に対する料金から、該所定の期間における前記通信トークン料金送信ステップで送信された通信トークンの料金を控除した額を該移動通信部側の請求先に課金し、該通信トークンの料金を前記通信トークン料金送信ステップで送信された識別子に対応する前記対応表中の他の請求先に課金することを特徴とするデータ通信料金課金方法。
【請求項２２】
請求項１７乃至２１のいずれかに記載のデータ通信料金課金方法において、前記移動通信部側の請求先は該移動通信部の所有者又は利用者側であり、前記他の請求先は該所有者又は該利用者に対して所定の関係を有する側であることを特徴とするデータ通信料金課金方法。
【請求項２３】
請求項１７乃至２２のいずれかに記載のデータ通信料金課金方法において、前記移動通信部は携帯電話器であり、前記情報処理部はパーソナルコンピュータであり、該携帯電話器と該パーソナルコンピュータとは脱着可能に接続されたことを特徴とするデータ通信料金課金方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、移動情報端末装置のデータ通信料金を当該移動情報端末装置側の請求先と他の請求先とに区分して課金するデータ通信料金課金システム等に関する。
【背景技術】
【０００２】
近年、社外で携帯電話器とパーソナルコンピュータ（以下、「ＰＣ」と省略する。）とを用いてモバイル通信を行うことにより、業務を行う必要に迫られているビジネスマン等が増加している。所持している携帯電話器はビジネスマン等の個人契約によるものであることが多く、この場合、モバイル通信によるアクセスで発生したパケット通信料はビジネスマン等へ請求されることになる。ビジネスマン等は当該請求の明細書を用いて会社にパケット通信料を請求することは可能であるが、業務上であるのか個人使用であるのかという、いわゆる公私区分の事務処理は極めて面倒且つ困難である。このため、当該パケット通信料はビジネスマン等の個人負担になってしまうことが多いというのが実情である。
【０００３】
従来、携帯電話器の通話の分野では、公私区分の事務処理を容易にするために、相手の電話番号の前にいわゆる特番と呼ばれる認識番号を入力することにより、会社と個人とで通話料金を区分する公私分計サービスが行われている（非特許文献１参照）。
【０００４】
携帯電話器を用いたデータ通信向けの種々の公私分計サービスも既に行われている。例えば、パケットカウントを行うソフトウェアをＰＣ上に予めインストールしておくことにより、リアルタイムにデータ通信料およびデータ通信料金の概算を表示することもできる（非特許文献２参照）。
【０００５】
予めアクセス先を登録しておくことにより、パケットの宛先が登録されている場合には、個人使用の携帯電話器へのパケット通信料の請求を免除し、会社側へ請求するという仕組みも存在する。あるいは、企業側ネットワークへアクセスする場合を業務利用とし、他

のインターネット上のサーバへアクセスする場合を私的利用として、両者を分けて課金する通信料金分別方法も存在する（特許文献１参照）。

【０００６】

【非特許文献１】日経ＢＰ社、ITpro 、Network“ケータイonBussiness”、［online］、２００４年９月１６日、［平成１９年２月１日検索］、インターネット<URL: http://itpro.nikkeibp.co.jp/free/TIS/keitai/20040915/149943/?ST=keitai&P=2>

【非特許文献２】ＫＤＤＩ、モバイル通信、各種ソフトダウンロード“パケットカウンター”、［online］、［平成１９年２月１日検索］、インターネット<URL: http:// http://www.au.kddi.com/mobile/soft/packet_counter/index.html>

【特許文献１】国際公開第ＷＯ２００４／０７７７６５号

【発明の開示】

【発明が解決しようとする課題】

【０００７】

上述のように、携帯電話器の通話の分野では特番を用いることにより会社と個人とで通話料金を区分する公私分計サービスが行われている。しかし、通話の場合と比較してデータ通信の場合、パケットは同時に複数の箇所にアクセスすることができるため、特番のような認識番号を付加することにより公私分計することは困難であるという問題があった。

上述のように、パケットカウントを行うソフトウェアをＰＣ上に予めインストールしておく公私分計サービスも行われている。しかし、当該分計は概算にすぎない上、ＰＣ上でのパケットカウントはユーザがカウントしたものと同様であるため、当該分計はキャリヤ側からみて信頼度が低く、従って当該分計はキャリヤ側の請求に反映できるものではないという問題があった。上述のように、パケットの宛先が登録されている場合には、個人使用の携帯電話器へのパケット通信料の請求を免除し、会社側へ請求するという仕組みも存在する。しかし、この場合、宛先を登録する必要があるという問題があった。企業側ネットワークへアクセスする場合を業務利用とし、他の一般のインターネット上のサーバへアクセスする場合を私的利用として、両者を分けて課金する通信料金分別方法も存在する。しかし、業務上、インターネット上のサーバへアクセスする場合は私的利用となってしまうため、業務利用として分けて課金することができないという問題があった。

【０００８】

そこで、本発明の目的は、上記問題を解決するためになされたものであり、携帯電話器の通話の分野で行われている特番のような認識番号を用いることなく、パケットカウントを行うソフトウェアをＰＣ上に予めインストールしておくことなく、パケットの宛先の登録の必要もなく、業務上、インターネット上のサーバへアクセスする場合であっても公私分計することができ且つキャリヤ側からみて信頼度が高いデータ通信料金課金システム等を提供することにある。

【課題を解決するための手段】

【０００９】

この発明のデータ通信料金課金システムは、移動通信機能を有する移動通信部と情報処理機能を有する情報処理部とを備えた移動情報端末の該移動通信部に掛かるデータ通信料金を該移動通信部側の請求先と他の請求先とに区分して課金するデータ通信料金課金システムであって、該移動通信部が移動通信部側ネットワークに接続する際の認証課金を行う通信事業者側サーバと、該移動通信部側ネットワークに接続されソフトウェアの配信を行う配信サイトが稼動するウェブサーバと、該ウェブサーバと接続され所定のネットワークの利用権を示す通信トークンを発行する通信トークン発行サーバと、該ウェブサーバと接続され該移動通信部に掛かるデータ通信料金を課金する課金サーバと、該所定のネットワークに接続された認証サーバとを備え、前記移動情報端末は、前記移動通信部を介して移動通信部側ネットワークに接続する移動通信部側ネットワーク接続手段と、前記通信トークンの購入に際し前記移動通信部の識別子を前記ウェブサーバへ送信する識別子送信手段と、前記ウェブサーバ側から前記移動通信部を介して前記通信トークンが送信された後、前記移動通信部側ネットワーク接続手段により接続された移動通信部側ネットワークとの

接続を解除する移動通信部側ネットワーク接続解除手段と、前記移動通信部の識別子及び前記ウェブサーバ側から送信された通信トークンを用い、前記移動通信部及び前記認証サーバを介して前記所定のネットワークの利用を試みるログイン手段と、前記認証サーバから前記所定のネットワークの利用を認める通知が送信された場合、該認証サーバを介して該所定のネットワークの利用を行う所定のネットワーク利用手段とを備え、前記ウェブサーバは、前記識別子送信手段により送信された識別子を前記通信トークン発行サーバへ送信するウェブサーバ側識別子送信手段と、前記通信トークン発行サーバから送信された通信トークンを前記移動通信部を介して前記情報処理部へ送信するウェブサーバ側通信トークン送信手段と、前記課金サーバへ前記ウェブサーバ側通信トークン送信手段により送信された通信トークンの料金を送信する通信トークン料金送信手段とを備え、前記認証サーバは、前記ログイン手段により用いられた識別子及び通信トークンを前記通信トークン発行サーバへ送信する識別子・通信トークン送信手段と、前記通信トークン発行サーバにより前記通信トークンの正当性が認証された場合、前記移動通信部を介して前記情報処理部へ前記所定のネットワークの利用を認める通知を送信する利用可通知手段とを備え、前記通信トークン発行サーバは、前記ウェブサーバ側識別子送信手段により送信された識別子に基づき通信トークンを生成して前記ウェブサーバへ送信する通信トークン送信手段と、前記識別子・通信トークン送信手段により送信された識別子及び通信トークンに基づき該通信トークンの正当性を認証する通信トークン認証手段とを備え、前記課金サーバは、前記通信事業者側サーバから送信された所定の期間における前記移動通信部のデータ通信に対する料金から、該所定の期間における前記通信トークン料金送信手段により送信された通信トークンの料金を控除した額を該移動通信部側の請求先に課金し、該通信トークンの料金を他の請求先に課金する区分課金手段とを備えたことを特徴とする。

【００１０】

ここで、この発明のデータ通信料金課金システムにおいて、前記移動通信部が無線ＬＡＮを介して前記所定のネットワークの利用を行う場合、前記通信トークン料金送信手段により送信された通信トークンの料金は無線ＬＡＮ回線使用料金を含み、前記ログイン手段は、前記移動通信部の識別子及び前記ウェブサーバ側通信トークン送信手段により送信された該通信トークンを用い無線ＬＡＮ基地局及び前記認証サーバを介して所定のネットワークの利用を試み、前記利用可通知手段は、前記通信トークン認証手段により前記通信トークンの正当性が認証された場合、無線ＬＡＮ基地局を介して前記情報処理部へ前記所定のネットワークの利用を認める通知を送信することができる。

【００１１】

ここで、この発明のデータ通信料金課金システムにおいて、前記所定のネットワークへの接続が認証を要する場合、前記ウェブサーバが該認証を行うウェブサーバ側認証手段をさらに備えることができる。

【００１２】

ここで、この発明のデータ通信料金課金システムにおいて、前記通信トークン送信手段は、前記ウェブサーバ側識別子送信手段により送信された識別子と所定の鍵と所定の乱数とに基づき該通信トークンを生成して該ウェブサーバへ送信し、該所定の乱数は該識別子と関連付けて記録しておき、前記通信トークン認証手段は、前記識別子・通信トークン送信手段により送信された識別子及び通信トークンと、前記所定の鍵と、前記通信トークン送信手段により該識別子と関連付けて記録された所定の乱数とに基づき前記通信トークンの正当性を認証することができる。

【００１３】

ここで、この発明のデータ通信料金課金システムにおいて、前記移動情報端末及び前記課金サーバは該移動通信部の１以上の識別子と該１以上の識別子に各々対応する前記他の請求先との対応表をさらに備え、前記識別子送信手段は、前記通信トークンの購入に際し前記対応表に基づき前記移動通信部の１以上の識別子の内の一つの識別子を前記ウェブサーバへ送信し、前記通信トークン料金送信手段は、前記課金サーバへ前記ウェブサーバ側通信トークン送信手段により送信された通信トークンの料金と前記識別子送信手段により

送信された識別子とを送信し、前記区分課金手段は、前記通信事業者側サーバから送信された所定の期間における前記移動通信部のデータ通信に対する料金から、該所定の期間における前記通信トークン料金送信手段により送信された通信トークンの料金を控除した額を該移動通信部側の請求先に課金し、該通信トークンの料金を前記通信トークン料金送信手段により送信された識別子に対応する前記対応表中の他の請求先に課金することができる。

【００１４】

ここで、この発明のデータ通信料金課金システムにおいて、前記移動通信部側の請求先は該移動通信部の所有者又は利用者側であり、前記他の請求先は該所有者又は該利用者に対して所定の関係を有する側であるものとすることができる。

【００１５】

ここで、この発明のデータ通信料金課金システムにおいて、前記移動通信部は携帯電話器であり、前記情報処理部はパーソナルコンピュータであり、該携帯電話器と該パーソナルコンピュータとは脱着可能に接続されたものとすることができる。

【００１６】

この発明のプログラムは、移動通信機能を有する移動通信部と情報処理機能を有する情報処理部とを備えた移動情報端末が実行するプログラムであって、該情報処理部のコンピュータを、前記移動通信部を介して移動通信部側ネットワークに接続する移動通信部側ネットワーク接続手段、前記移動通信部側ネットワークに接続されソフトウェアの配信を行う配信サイトが稼動するウェブサーバへ、所定のネットワークの利用権を示す通信トークンの購入に際し該移動通信部の識別子を送信する識別子送信手段、前記ウェブサーバ側から前記移動通信部を介して前記通信トークンが送信された後、前記移動通信部側ネットワーク接続手段により接続された移動通信部側ネットワークとの接続を解除する移動通信部側ネットワーク接続解除手段、前記移動通信部の識別子及び前記ウェブサーバ側から送信された通信トークンを用い、前記移動通信部及び前記所定のネットワークに接続された認証サーバを介して該所定のネットワークの利用を試みるログイン手段、前記認証サーバから前記所定のネットワークの利用を認める通知が送信された場合、該認証サーバを介して該所定のネットワークの利用を行う所定のネットワーク利用手段として機能させるためのプログラムであり、前記識別子送信手段により前記ウェブサーバへ送信された識別子は、該ウェブサーバにより、該ウェブサーバと接続され通信トークンを発行する通信トークン発行サーバへ送信され、該通信トークン発行サーバにより、送信された該識別子に基づき通信トークンが生成され、該通信トークンは該ウェブサーバへ送信され、該ウェブサーバにより、送信された該通信トークンは前記移動通信部を介して前記情報処理部へ送信され、該ウェブサーバと接続され前記移動通信部に掛かるデータ通信料金を課金する課金サーバへ、該通信トークンの料金が送信されるものであり、前記ログイン手段により用いられた識別子及び通信トークンは、前記認証サーバにより前記通信トークン発行サーバへ送信され、該通信トークン発行サーバにより、送信された識別子及び通信トークンに基づき通信トークンの正当性が認証され、該通信トークンの正当性が認証された場合、該認証サーバにより、前記移動通信部を介して前記情報処理部へ該所定のネットワークの利用を認める通知が送信され、前記課金サーバにより、前記移動通信部が前記移動通信部側ネットワークに接続する際の認証課金を行う通信事業者側サーバから送信された所定の期間における該移動通信部のデータ通信に対する料金から、該所定の期間における前記ウェブサーバにより送信された通信トークンの料金を控除した額が該移動通信部側の請求先に課金され、該通信トークンの料金が他の請求先に課金されることを特徴とするプログラムである。

【００１７】

ここで、この発明のプログラムにおいて、前記移動情報端末が無線ＬＡＮを介して前記所定のネットワークの利用を行う場合、前記ウェブサーバ側から前記課金サーバ側へ送信された通信トークンの料金は無線ＬＡＮ回線使用料金を含み、前記ログイン手段は、前記移動情報端末の識別子及び前記ウェブサーバ側から送信された通信トークンを用い無線ＬＡＮ基地局及び前記認証サーバを介して前記所定のネットワークの利用を試み、前記通信

トークン発行サーバにより前記通信トークンの正当性が認証された場合、前記認証サーバにより、無線ＬＡＮ基地局を介して前記情報処理部へ前記所定のネットワークの利用を認める通知が送信されることができる。

【００１８】

ここで、この発明のプログラムにおいて、前記移動情報端末及び前記課金サーバは該移動通信部の１以上の識別子と該１以上の識別子に各々対応する前記他の請求先との対応表をさらに備え、前記識別子送信手段は、前記通信トークンの購入に際し前記対応表に基づき前記移動通信部の１以上の識別子の内の一つの識別子を前記ウェブサーバへ送信し、前記ウェブサーバにより、前記課金サーバへ、前記移動通信部を介して前記情報処理部へ送信された通信トークンの料金と前記識別子送信手段により送信された識別子とが送信され、前記課金サーバにより、前記通信事業者側サーバから送信された所定の期間における前記移動通信部のデータ通信に対する料金から、該所定の期間における前記ウェブサーバにより送信された通信トークンの料金を控除した額を該移動通信部側の請求先に課金し、該通信トークンの料金を前記ウェブサーバにより送信された識別子に対応する前記対応表中の他の請求先に課金することができる。

【００１９】

この発明のプログラムは、移動通信機能を有する移動通信部と情報処理機能を有する情報処理部とを備えた移動情報端末の該移動通信部に掛かるデータ通信料金を課金する課金サーバが該移動通信部に掛かるデータ通信料金を該移動通信部側の請求先と他の請求先とに区分して課金するためのプログラムであって、課金サーバのコンピュータを、前記移動通信部が移動通信部側ネットワークに接続する際の認証課金を行う通信事業者側サーバから送信された所定の期間における該移動通信部のデータ通信に対する料金から、該移動通信部側ネットワークに接続されソフトウェアの配信を行う配信サイトが稼動するウェブサーバから前記課金サーバへ送信された該所定の期間における所定のネットワークの利用権を示す通信トークンの料金を控除した額を該移動通信部側の請求先に課金し、該通信トークンの料金を他の請求先に課金する区分課金手段として機能させるためのプログラムであり、前記移動情報端末により、該移動通信部を介して前記移動通信部側ネットワークに接続し、通信トークンの購入に際し該移動通信部の識別子が前記ウェブサーバへ送信され、該ウェブサーバにより、送信された該識別子が該ウェブサーバと接続され通信トークンを発行する通信トークン発行サーバへ送信され、該通信トークン発行サーバにより、送信された該識別子に基づき通信トークンが生成され、該通信トークンは該ウェブサーバへ送信され、該ウェブサーバにより、送信された該通信トークンが該移動通信部を介して該情報処理部へ送信され、前記課金サーバへ該通信トークンの料金が送信されるものであり、前記移動情報端末により、従前に接続された前記移動通信部側ネットワークとの接続が解除され、前記移動通信部の識別子及び前記ウェブサーバから送信された前記通信トークンを用い、該移動通信部及び前記所定のネットワークに接続された認証サーバを介して該所定のネットワークの利用が試みられ、該認証サーバにより、移動情報端末により用いられた該識別子及び該通信トークンが前記通信トークン発行サーバへ送信され、該通信トークン発行サーバにより、送信された該識別子及び該通信トークンに基づき該通信トークンの正当性が認証された場合、該移動通信部を介して該情報処理部へ該所定のネットワークの利用を認める通知が送信され、該移動情報端末により、該認証サーバを介して該所定のネットワークの利用が行なわれることを特徴とするプログラムである。

【００２０】

ここで、この発明のプログラムにおいて、前記移動通信部が無線ＬＡＮを介して前記所定のネットワークの利用を行う場合、前記ウェブサーバから前記課金サーバへ送信された通信トークンの料金は無線ＬＡＮ回線使用料金を含み、前記移動情報端末により、前記移動通信部の識別子及び前記ウェブサーバ側から該移動通信部を介して該情報処理部へ送信された前記通信トークンを用い無線ＬＡＮ基地局及び前記認証サーバを介して所定のネットワークの利用が試みられ、前記通信トークン発行サーバにより前記通信トークンの正当性が認証された場合、前記認証サーバにより、無線ＬＡＮ基地局を介して前記情報処理部

へ前記所定のネットワークの利用を認める通知が送信されることができる。

【００２１】

ここで、この発明のプログラムにおいて、前記移動情報端末及び前記課金サーバは該移動通信部の１以上の識別子と該１以上の識別子に各々対応する前記他の請求先との対応表をさらに備え、前記移動情報端末により、前記通信トークンの購入に際し前記対応表に基づき前記移動通信部の１以上の識別子の内の一つの識別子が前記ウェブサーバへ送信され、前記ウェブサーバにより、前記課金サーバへ、前記移動通信部を介して前記情報処理部へ送信された通信トークンの料金と前記移動情報端末により送信された識別子とが送信され、前記区分課金手段は、前記通信事業者側サーバから送信された所定の期間における前記移動通信部のデータ通信に対する料金から、該所定の期間における前記通信トークン料金送信手段により送信された通信トークンの料金を控除した額を該移動通信部側の請求先に課金し、該通信トークンの料金を前記通信トークン料金送信手段により送信された識別子に対応する前記対応表中の他の請求先に課金することができる。

【００２２】

ここで、この発明のプログラムにおいて、前記移動通信部側の請求先は該移動通信部の所有者又は利用者側であり、前記他の請求先は該所有者又は該利用者に対して所定の関係を有する側であるものとすることができる。

【００２３】

ここで、この発明のプログラムにおいて、前記移動通信部は携帯電話器であり、前記情報処理部はパーソナルコンピュータであり、該携帯電話器と該パーソナルコンピュータとは脱着可能に接続されたものとすることができる。

【００２４】

この発明の記録媒体は、本発明のいずれかのプログラムを記録したコンピュータ読取り可能な記録媒体である。

【００２５】

この発明のデータ通信料金課金方法は、移動通信機能を有する移動通信部と情報処理機能を有する情報処理部とを備えた移動情報端末の該移動通信部に掛かるデータ通信料金を該移動通信部側の請求先と他の請求先とに区分して課金するデータ通信料金課金方法であって、前記移動情報端末が、前記移動通信部を介して移動通信部側ネットワークに接続する移動通信部側ネットワーク接続ステップと、前記移動通信部側ネットワーク接続ステップで接続された移動通信部側ネットワークに接続されソフトウェアの配信を行う配信サイトが稼動するウェブサーバへ、所定のネットワークの利用権を示す通信トークンの購入に際し該移動通信部の識別子を送信する識別子送信ステップと、前記ウェブサーバが、前記ウェブサーバと接続され前記通信トークンを発行する通信トークン発行サーバへ、前記識別子送信ステップで送信された識別子を送信するウェブサーバ側識別子送信ステップと、前記記通信トークン発行サーバが、前記ウェブサーバ側識別子送信ステップで送信された識別子に基づき通信トークンを生成して前記ウェブサーバへ送信する通信トークン送信ステップと、前記ウェブサーバが、前記通信トークン送信ステップで送信された通信トークンを前記移動通信部を介して前記情報処理部へ送信するウェブサーバ側通信トークン送信ステップと、前記ウェブサーバと接続され前記移動通信部に掛かるデータ通信料金を課金する課金サーバへ、前記ウェブサーバ側通信トークン送信ステップで送信された通信トークンの料金を送信する通信トークン料金送信ステップと、前記移動情報端末が、前記移動通信部側ネットワーク接続ステップで接続された移動通信部側ネットワークとの接続を解除する移動通信部側ネットワーク接続解除ステップと、前記移動通信部の識別子及び前記ウェブサーバ側通信トークン送信ステップで送信された通信トークンを用い、前記移動通信部及び前記所定のネットワークに接続された認証サーバを介して該所定のネットワークの利用を試みるログインステップと、前記認証サーバが、前記ログインステップで用いられた識別子及び通信トークンを前記通信トークン発行サーバへ送信する識別子・通信トークン送信ステップと、前記通信トークン発行サーバが、前記識別子・通信トークン送信ステップで送信された識別子及び通信トークンに基づき該通信トークンの正当性を認証する

通信トークン認証ステップと、前記認証サーバが、前記通信トークン認証ステップで通信トークンの正当性が認証された場合、前記移動通信部を介して前記情報処理部へ前記所定のネットワークの利用を認める通知を送信する利用可通知ステップと、前記移動情報端末が、前記利用通知ステップで前記認証サーバから前記所定のネットワークの利用を認める通知が送信された場合、該認証サーバを介して前記所定のネットワークの利用を行う所定のネットワーク利用ステップと、前記課金サーバが、前記移動通信部が前記移動通信部側ネットワークに接続する際の認証課金を行う通信事業者側サーバから送信された所定の期間における該移動通信部のデータ通信に対する料金から、該所定の期間における前記通信トークン料金送信ステップで送信された通信トークンの料金を控除した額を該移動通信部側の請求先に課金し、該通信トークンの料金を他の請求先に課金する区分課金ステップとを備えたことを特徴とする。

【００２６】

ここで、この発明のデータ通信料金課金方法において、前記移動通信部が無線ＬＡＮを介して該所定のネットワークの利用を行う場合、前記通信トークン料金送信ステップで送信された該通信トークンの料金は無線ＬＡＮ回線使用料金を含み、前記ログインステップは、前記移動通信部の識別子及び前記ウェブサーバ側通信トークン送信ステップで送信された通信トークンを用い前記無線ＬＡＮ基地局及び前記認証サーバを介して前記所定のネットワークの利用を試み、前記利用可通知ステップは、前記通信トークン認証ステップで通信トークンの正当性が認証された場合、無線ＬＡＮ基地局を介して前記情報端末装置へ前記所定のネットワークの利用を認める通知を送信することができる。

【００２７】

ここで、この発明のデータ通信料金課金方法において、前記所定のネットワークへの接続が認証を要する場合、前記ウェブサーバ側識別子送信ステップに先立ち、前記ウェブサーバが該認証を行うウェブサーバ側認証ステップをさらに備えることができる。

【００２８】

ここで、この発明のデータ通信料金課金方法において、前記通信トークン送信ステップは、前記通信トークン発行サーバが、前記ウェブサーバ側識別子送信ステップで送信された識別子と所定の鍵と所定の乱数とに基づき通信トークンを生成して前記ウェブサーバへ送信し、該所定の乱数は該識別子と関連付けて記録しておき、前記通信トークン認証ステップは、前記通信トークン発行サーバが、前記識別子・通信トークン送信ステップで送信された識別子及び通信トークンと、前記所定の鍵と、前記通信トークン送信ステップで該識別子と関連付けて記録された所定の乱数とに基づき該通信トークンの正当性を認証することができる。

【００２９】

ここで、この発明のデータ通信料金課金方法において、前記移動情報端末及び前記課金サーバは該移動通信部の１以上の識別子と該１以上の識別子に各々対応する前記他の請求先との対応表をさらに備え、前記識別子送信ステップは、前記通信トークンの購入に際し前記対応表に基づき前記移動通信部の１以上の識別子の内の一つの識別子を前記ウェブサーバへ送信し、前記通信トークン料金送信ステップは、前記課金サーバへ前記ウェブサーバ側通信トークン送信ステップで送信された通信トークンの料金と前記識別子送信ステップで送信された識別子とを送信し、前記区分課金ステップは、前記通信事業者側サーバから送信された所定の期間における前記移動通信部のデータ通信に対する料金から、該所定の期間における前記通信トークン料金送信ステップで送信された通信トークンの料金を控除した額を該移動通信部側の請求先に課金し、該通信トークンの料金を前記通信トークン料金送信ステップで送信された識別子に対応する前記対応表中の他の請求先に課金することができる。

【００３０】

ここで、この発明のデータ通信料金課金方法において、前記移動通信部側の請求先は該移動通信部の所有者又は利用者側であり、前記他の請求先は該所有者又は該利用者に対して所定の関係を有する側であるものとすることができる。

【００３１】
ここで、この発明のデータ通信料金課金方法において、前記移動通信部は携帯電話器であり、前記情報処理部はパーソナルコンピュータであり、該携帯電話器と該パーソナルコンピュータとは脱着可能に接続されたものとすることができる。
【発明の効果】
【００３２】
本発明のデータ通信料金課金システム等によれば、所定のネットワーク用の通信トークンを携帯電話コンテンツ用ネットワークに接続された配信サイトが稼動するウェブサーバ経由で購入するに際し、好適には携帯電話器およびＰＣから構成される移動情報端末のＰＣから携帯電話器を介して携帯電話器の識別子ＩＤをウェブサーバへ送信する。送信された識別子ＩＤはウェブサーバにより通信トークン発行サーバへ送信される。通信トークン発行サーバは送信された携帯電話器の識別子ＩＤに基づき通信トークンを生成し、この生成された通信トークンをウェブサーバへ送信する。生成した通信トークンは携帯電話器の識別子ＩＤと紐付けされた状態で記録しておく。送信された通信トークンはウェブサーバにより携帯電話器を介してＰＣへ送信される。その後、携帯電話コンテンツ用ネットワークとの接続を一旦解除した後、改めて携帯電話器の識別子ＩＤおよび上記通信トークンを用い、ＰＣ側から携帯電話器および認証サーバを介して所定のネットワークの利用を試みる。認証サーバは携帯電話器の識別子ＩＤおよび通信トークンを通信トークン発行サーバへ送信する。通信トークン発行サーバは送信された識別子ＩＤおよび通信トークンに基づき当該通信トークンの正当性を認証する。従前に、生成された通信トークンＴ（従前）は携帯電話器の識別子ＩＤ（従前）と紐付けされた状態で記録されているため、送信された識別子ＩＤおよび通信トークンと、記録されている識別子ＩＤ（従前）および通信トークン（従前）とが一致する場合、従前に携帯電話コンテンツ用ネットワークを介して通信トークン（従前）を購入する際に用いられた携帯電話器と、現在所定のネットワークの利用を試みようとしている際に用いられている携帯電話器とが同一であると認証することができる。認証結果はウェブサーバ側へ通知される。以上のように、上記通信トークン購入時における認証（コンテンツ認証）と購入後における認証（通信認証）とを対応させることができる。この結果、携帯電話コンテンツ用ネットワークから所定のネットワークへの通信の切替を行った場合であってもユーザ（携帯電話器）の対応が付けられる。このため、課金サーバは通信事業者側サーバから送信された所定の期間（例えば、1ヶ月間）におけるユーザ所有の携帯電話器のデータ通信に対する料金から、当該所定の期間におけるウェブサーバにより送信された通信トークンの料金を控除した額を携帯電話器側の請求先（携帯電話器の所有者または利用者であるユーザ）に課金し、当該通信トークンの料金を他の請求先（上記ユーザに対して所定の関係を有する側）に課金することができる。従って、ユーザが業務上、インターネット（所定のネットワークの一例）上のサーバへアクセスする場合であっても、上述した通信トークンを用いることにより容易に公私分計することができる。さらに、本発明のデータ通信料金課金システムはキャリヤ側の設備だけで実現することができるため、キャリヤ側からみて極めて信頼度の高いシステムである。この結果、携帯電話器の通話の分野で行われている特番のような認識番号を用いることなく、パケットカウントを行うソフトウェアをＰＣ上に予めインストールしておくことなく、パケットの宛先の登録の必要もなく、業務上、インターネット上のサーバへアクセスする場合であっても公私分計することができ且つキャリヤ側からみて信頼度が高いデータ通信料金課金システム等を提供することができるという効果がある。
【発明を実施するための最良の形態】
【００３３】
以下、各実施例について図面を参照して詳細に説明する。
【実施例１】
【００３４】
図１は、本発明の実施例１におけるデータ通信料金課金システム１を示す。図１において、符号９０は移動通信機能を有する移動通信部１０と情報処理機能を有する情報処理部

２０とを備えた移動情報端末である。移動情報端末９０は移動通信部１０と情報処理部２０とを備えた１台の装置として構成することができる。あるいは移動情報端末９０は、好適には移動通信部１０を携帯電話器１０とし、好適には情報処理部２０をパーソナルコンピュータＰＣ２０とし、携帯電話器１０とＰＣ２０とを脱着可能に接続した構成とすることもできる。以下では、移動情報端末９０は携帯電話器１０とＰＣ２０とが脱着可能に接続した構成であるものとする。携帯電話器１０のユーザは携帯電話器１０の所有者または利用者と想定する。携帯電話器１０とＰＣ２０との間の接続は脱着可能な接続方式、例えばＵＳＢ（Universal Serial Bus）ケーブル１１を用いることが好適である。しかし、ＵＳＢ等の接続方式に限定されるものではなく、無線等であってもよいことは勿論である。なお本明細書において、「携帯電話器」は携帯電話装置または携帯電話機と呼んでもよい。続いて、符号１３は移動体通信網、１４は移動体通信網１３に接続された通信事業者側サーバ、１２は移動体通信網１３に接続された基地局であり、携帯電話器１０は基地局１２のエリア内に在圏しているものと想定する。符号１５は通信事業者側サーバ１４と接続された携帯電話コンテンツ用ネットワーク（移動通信部側ネットワーク）、３０は携帯電話コンテンツ用ネットワーク１５に接続されソフトウェアの配信を行う配信サイトが稼動するウェブ（Ｗｅｂ）サーバである。通信事業者側サーバ１４は携帯電話器１０が携帯電話コンテンツ用ネットワーク１５に接続する際の認証課金を行う。続いて、符号４０はウェブサーバ３０と接続され所定のネットワーク１６の利用権を示す通信トークン（ワンタイム通信トークン）を発行する通信トークン発行サーバ、６０はウェブサーバ３０と接続され移動情報端末９０の携帯電話器１０に掛かるデータ通信料金を課金する課金サーバ、５０は所定のネットワーク１６に接続された認証サーバである。所定のネットワークとしては、携帯電話器１０のユーザが業務上使用する企業内ネットワーク、インターネット等が好適である。認証サーバ５０は通信トークン発行サーバ４０と接続されている。図１に示されるように、携帯電話器１０は移動体通信網１３および携帯電話コンテンツ用ネットワーク１５を介してウェブサーバ３０と接続されている。ウェブサーバ３０と通信トークン発行サーバ４０との間の接続、ウェブサーバ３０と課金サーバ６０との間の接続、通信事業者側サーバ１４と課金サーバ６０との間の接続、認証サーバ５０と通信トークン発行サーバ４０との間の各接続はＶＰＮ（Virtual Private Network）等の専用通信網によることが好適である。上述のように、移動通信部の例として携帯電話器１０を用いて説明するが、移動通信部１０は携帯電話器１０に限定されるものではなく、ＰＨＳ（Personal Handyphone System）等であってもよい。同様に、情報処理部２０の例としてＰＣ２０を用いて説明するが、ＰＣ２０に限定されるものではなく、ＰＤＡ（Personal Digital Assistant）等、携帯電話器１０と接続可能な情報処理装置であれば他の装置であってもよい。

【００３５】

図１において、符号２１はＰＣ２０が備える機能を示す機能ブロックである。機能ブロック２１において、符号２２は携帯電話器１０を介して携帯電話コンテンツ用ネットワーク１５に接続するネットワーク接続部（移動通信部側ネットワーク接続手段）、２３は、例えば携帯電話器１０のユーザが業務上必要とする所定のネットワーク１６用の通信トークンを自己が所有する携帯電話器１０を用いて上記配信サイト経由で購入するに際し、携帯電話器１０の識別子（例えば携帯電話器１０の電話番号等）をウェブサーバ３０へ送信する識別子送信部（識別子送信手段）、２４はウェブサーバ３０側から携帯電話器１０を介して通信トークンが携帯コンテンツとみなされて送信された後、ネットワーク接続部２２により接続された携帯電話コンテンツ用ネットワーク１５との接続を解除するネットワーク接続解除部（移動通信部側ネットワーク接続解除手段）、２５は携帯電話器１０の識別子およびウェブサーバ３０側から送信された通信トークンを用い、携帯電話器１０および認証サーバ５０を介して所定のネットワーク１６の利用を試みるログイン部（ログイン手段）、２６は認証サーバ５０から所定のネットワーク１６の利用を認める通知が送信された場合、認証サーバ５０を介して所定のネットワーク１６の利用を行う所定のネットワーク利用部（所定のネットワーク利用手段）である。以上のＰＣ２０が備える機能は、ＰＣ２０に配置されＰＣ２０のコンピュータに上述の各機能を実行させるための通信認証接

続ソフトウェアとして実現することができる。識別子送信部２３がウェブサーバ３０へ送信する識別子は、携帯電話器１０の識別子に限定されるものではなく、ＰＣ２０の識別子（例えばＰＣ２０の製造番号等）であってもよい。あるいは、携帯電話器１０およびＰＣ２０から構成される移動情報端末９０の識別子とすることもできる。

【００３６】

図１において、符号３１はウェブサーバ３０が備える機能を示す機能ブロックである。機能ブロック３１において、符号３２は識別子送信部２３により送信された識別子を通信トークン発行サーバ４０へ送信するウェブサーバ側識別子送信部（ウェブサーバ側識別子送信手段）、３４は通信トークン発行サーバ４０から送信された通信トークンを携帯電話器１０を介してＰＣ２０へ送信するウェブサーバ側通信トークン送信部（ウェブサーバ側通信トークン送信手段）、３６は課金サーバ６０へウェブサーバ側通信トークン送信部３４により送信された通信トークンの料金を送信する通信トークン料金送信部（通信トークン料金送信手段）である。携帯電話器１０のユーザが通信トークンを購入する時点では、通常、通信トークンの料金は予め定まっているが、未確定であってもよい。後述するように、課金サーバ６０が通信料金の公私分計を行うため、携帯電話器１０のユーザは業務上使用する通信トークンの料金を考慮する必要はない。

【００３７】

図１において、符号５１は認証サーバ５０が備える機能を示す機能ブロックである。機能ブロック５１において、符号５２はログイン部２５により用いられた携帯電話器１０の識別子および通信トークンを通信トークン発行サーバ４０へ送信する識別子・通信トークン送信部（識別子・通信トークン送信手段）、５４は通信トークン発行サーバ４０により上記通信トークンの正当性が認証された場合、携帯電話器１０を介してＰＣ２０へ所定のネットワーク１６の利用を認める通知を送信する利用可通知部（利用可通知手段）である。

【００３８】

図１において、符号４１は通信トークン発行サーバ４０が備える機能を示す機能ブロックである。機能ブロック４１において、符号４２はウェブサーバ側識別子送信部３２により送信された携帯電話器１０の識別子に基づき上記通信トークンを生成し、この生成された通信トークンをウェブサーバ３０へ送信する通信トークン送信部（通信トークン送信手段）、４４は識別子・通信トークン送信部５２により送信された識別子および通信トークンに基づき当該通信トークンの正当性を認証する通信トークン認証部（通信トークン認証手段）である。通信トークン送信部４２は、生成した通信トークンを携帯電話器１０の識別子と紐付けされた状態で記録しておく。通信トークン認証部４４の認証結果は認証サーバ５０側へ通知される。

【００３９】

図１において、符号６１は課金サーバ６０が備える機能を示す機能ブロックである。機能ブロック６１において、符号６２は、通信事業者側サーバ１４から送信された所定の期間（例えば、1ヶ月間）における携帯電話器１０のデータ通信に対する料金から、当該所定の期間における通信トークン料金送信部３６により送信された通信トークンの料金を控除した額を携帯電話器１０側の請求先（携帯電話器１０の所有者または利用者であるユーザ等）に課金し、当該通信トークンの料金を他の請求先（携帯電話器１０の所有者または利用者であるユーザに対して所定の関係を有する側等）に課金する区分課金部（区分課金手段）である。以上により、携帯電話器１０のユーザが業務上必要とする所定のネットワーク１６用の通信トークンを自己が所有する携帯電話器１０を用いて上記配信サイト経由で購入した場合、業務上用いた通信トークンの料金は上記他の請求先に課金されることになる。この結果、携帯電話器１０のユーザが私用で用いたデータ通信料金と業務上用いたデータ通信料金(通信トークンの料金)とが公私分計されることになる。所定の関係を有する側としては、例えばユーザが会社員である場合、当該会社員の雇用者、即ち会社であるものとすることができる。当該会社員が自社のネットワーク（所定のネットワーク１６）にログインする場合、業務上用いた当該自社のネットワークに関する通信トークンの料金

は会社側に課金されることになり、公私分計されることになる。あるいは、所定の関係を有する側としては、例えばユーザがコンシューマー向けの会員制情報提供サービスの会員である場合、当該コンシューマー向けの会員制情報提供サービスの提供者であるものとすることもできる。当該会員が当該会員制情報提供サービスのネットワーク（所定のネットワーク１６）にログインする場合、利用した当該会員制情報提供サービスのネットワークに関する通信トークンの料金は、当該会員制情報提供サービスの提供者側に課金されることになり、一種の分計が行なわれることになる。

【００４０】

図２は、データ通信料金課金システム１の構成要素であるＰＣ２０、ウェブサーバ３０、通信トークン発行サーバ４０、認証サーバ５０、課金サーバ６０で実行される各プログラムの流れまたはデータ通信料金課金方法をフローチャートで示す。図２において、左側からＰＣ２０で実行されるプログラム等のフローチャート、ウェブサーバ３０で実行されるプログラム等のフローチャート、通信トークン発行サーバ４０で実行されるプログラム等のフローチャート、認証サーバ５０で実行されるプログラム等のフローチャート、課金サーバ６０で実行されるプログラム等のフローチャートであり、各構成要素間の通信は点線で示す。

【００４１】

図２に示されるように、まず、ＰＣ２０が、携帯電話器１０を介して携帯電話コンテンツ用ネットワーク１５に接続する（移動通信部側ネットワーク接続ステップ。ステップＳ２２）。移動通信部側ネットワーク接続ステップ（ステップＳ２２）で接続された携帯電話コンテンツ用ネットワーク１５に接続されソフトウェアの配信を行う配信サイトが稼動するウェブサーバ３０へ、所定のネットワーク１６の利用権を示す通信トークンの購入を行うために、携帯電話器１０の識別子ＩＤを送信する（識別子送信ステップ。ステップＳ２３）。

【００４２】

次に、ウェブサーバ３０が、ウェブサーバ３０と接続され通信トークンを発行する通信トークン発行サーバ４０へ、識別子送信ステップ（ステップＳ２３）で送信された識別子ＩＤを送信する（ウェブサーバ側識別子送信ステップ。ステップＳ３２）。

【００４３】

続いて、通信トークン発行サーバ４０が、ウェブサーバ側識別子送信ステップ（ステップＳ３２）で送信された識別子ＩＤに基づき通信トークンＴを生成してウェブサーバ３０へ送信する（通信トークン送信ステップ。ステップＳ４２）。通信トークン発行サーバ４０は生成した通信トークンＴを携帯電話器１０の識別子ＩＤと紐付けした状態で記録しておく。

【００４４】

ウェブサーバ３０が、通信トークン送信ステップ（ステップＳ４２）で送信された通信トークンＴを携帯電話器１０を介してＰＣ２０へ送信する（ウェブサーバ側通信トークン送信ステップ。ステップＳ３４）。ウェブサーバ３０と接続され携帯電話器１０のデータ通信料金を課金する課金サーバ６０へ、ウェブサーバ側通信トークン送信ステップ（ステップＳ３４）で送信された通信トークンＴの料金Ｂを送信する（通信トークン料金送信ステップ。ステップＳ３６）。

【００４５】

ＰＣ２０が、移動通信部側ネットワーク接続ステップ（ステップＳ２２）で接続された携帯電話コンテンツ用ネットワーク１５との接続を解除する（移動通信部側ネットワーク接続解除ステップ。ステップＳ２４）。携帯電話器１０の識別子ＩＤおよびウェブサーバ側通信トークン送信ステップ（ステップＳ３４）で送信された通信トークンＴを用い、携帯電話器１０および所定のネットワーク１６に接続された認証サーバ５０を介して所定のネットワーク１６の利用を試みる（ログインステップ。ステップＳ２５）。

【００４６】

認証サーバ５０が、ログインステップ（ステップＳ２５）で用いられた識別子ＩＤおよ

び通信トークンＴを通信トークン発行サーバ４０へ送信する（識別子・通信トークン送信ステップ。ステップＳ５２）。

【００４７】

通信トークン発行サーバ４０が、識別子・通信トークン送信ステップ（ステップＳ５２）で送信された識別子ＩＤおよび通信トークンＴに基づき通信トークンＴの正当性を認証する（通信トークン認証ステップ。ステップＳ４４）。上述のように、通信トークンＴ（従前）は携帯電話器１０の識別子ＩＤ（従前）と紐付けされた状態で記録されているため、識別子・通信トークン送信ステップ（ステップＳ５２）で送信された識別子ＩＤおよび通信トークンＴと、記録されている識別子ＩＤ（従前）および通信トークンＴ（従前）とが一致する場合、通信トークン発行サーバ４０は従前に携帯電話コンテンツ用ネットワーク１５を介して通信トークンＴを購入する際に用いられた携帯電話器１０と、現在所定のネットワーク１６の利用を試みようとしている際に用いられている携帯電話器１０とが同一であると認証することができる。通信トークン認証ステップ（ステップＳ４４）において、上記認証結果Ｎは認証サーバ５０側へ通知される。

【００４８】

認証サーバ５０は、通信トークン認証ステップ（ステップＳ４４）で通信トークンＴの正当性が認証された場合、すなわち通知された認証結果Ｎが正当性を認証したことを示す場合、携帯電話器１０を介してＰＣ２０へ所定のネットワーク１６の利用を認める通知Ｍを送信する（利用可通知ステップ。ステップＳ５４）。

【００４９】

ＰＣ２０は、認証サーバ５０から所定のネットワーク１６の利用を認める通知Ｍが送信された場合、認証サーバ５０を介して所定のネットワーク１６の利用を行う（所定のネットワーク利用ステップ。ステップＳ２６）。

【００５０】

課金サーバ６０は、携帯電話器１０が携帯電話コンテンツ用ネットワーク１５に接続する際の認証課金を行う通信事業者側サーバ１４から送信された所定の期間における携帯電話器１０のデータ通信に対する料金から、当該所定の期間における通信トークン料金送信ステップ（ステップＳ３６）で送信された通信トークンＴの料金Ｂを控除した額を携帯電話器１０側の請求先に課金し、通信トークンＴの料金Ｙを他の請求先に課金する（区分課金ステップ。ステップＳ６２）。

【００５１】

以上より、本発明の実施例１によれば、識別子送信部２３は所定のネットワーク１６用の通信トークンＴを配信サイト経由で購入するに際し、携帯電話器１０の識別子ＩＤをウェブサーバ３０へ送信する。識別子送信部２３により送信された識別子ＩＤはウェブサーバ側識別子送信部３２により通信トークン発行サーバ４０へ送信される。通信トークン送信部４２はウェブサーバ側識別子送信部３２により送信された携帯電話器１０の識別子ＩＤに基づき通信トークンＴを生成し、この生成された通信トークンＴをウェブサーバ３０へ送信する。通信トークン送信部４２は生成した通信トークンＴを携帯電話器１０の識別子ＩＤと紐付けした状態で記録しておく。送信された通信トークンＴはウェブサーバ側通信トークン送信部３４により携帯電話器１０を介してＰＣ２０へ送信される。その後、ネットワーク接続解除部２４がネットワーク接続部２２により接続された携帯電話コンテンツ用ネットワーク１５との接続を解除する。携帯電話器１０とＰＣ２０との間は接続状態のままでよい。一旦携帯電話コンテンツ用ネットワーク１５との接続が解除された後、改めてログイン部２５が携帯電話器１０の識別子ＩＤおよび上記通信トークンＴを用い、携帯電話器１０および認証サーバ５０を介して所定のネットワーク１６の利用を試みる。識別子・通信トークン送信部５２はログイン部２５により用いられた携帯電話器１０の識別子ＩＤおよび通信トークンＴを通信トークン発行サーバ４０へ送信する。通信トークン認証部４４は識別子・通信トークン送信部５２により送信された識別子ＩＤおよび通信トークンＴに基づき当該通信トークンＴの正当性を認証する。従前に通信トークン送信部４２により生成された通信トークンＴ（従前）は携帯電話器１０の識別子ＩＤ（従前）と紐付

けされた状態で記録されているため、識別子・通信トークン送信部５２により送信された識別子ＩＤおよび通信トークンＴと、記録されている識別子ＩＤ（従前）および通信トークンＴ（従前）とが一致する場合、通信トークン認証部４４は、従前に携帯電話コンテンツ用ネットワーク１５を介して通信トークンＴ（従前）を購入する際に用いられた携帯電話器１０と、現在所定のネットワーク１６の利用を試みようとしている際に用いられている携帯電話器１０とが同一であると認証することができる。通信トークン認証部４４の認証結果Ｎは認証サーバ５０側へ通知される。

【００５２】

以上のように、上記通信トークンＴ購入時における認証（コンテンツ認証）と購入後における認証（通信認証）とを対応させることができる。この結果、携帯電話コンテンツ用ネットワーク１５から所定のネットワーク１６への通信の切替を行った場合であってもユーザ（携帯電話器１０のユーザ）の対応が付けられる。このため、区分課金部６２は通信事業者側サーバ１４から送信された所定の期間（例えば、1ヶ月間）におけるユーザ所有の携帯電話器１０のデータ通信に対する料金（＝Ａ）から、当該所定の期間における通信トークン料金送信部３６により送信された通信トークンＴの料金（＝Ｂ）を控除した額（＝Ａ－Ｂ）を携帯電話器１０側の請求先（携帯電話器１０の所有者または利用者であるユーザ）に課金し、当該通信トークンＴの料金（＝Ｂ）を他の請求先（上記ユーザに対して所定の関係を有する側、例えば雇用者側）に課金することができる。従って、ユーザが業務上、インターネット（所定のネットワーク１６の一例）上のサーバへアクセスする場合であっても、上述した通信トークンＴを用いることにより即時に公私分計することができる。さらに、本発明のデータ通信料金課金システム１はキャリヤ側の設備だけで実現することができるため、キャリヤ側からみて極めて信頼度の高いシステムである。この結果、携帯電話器１０の通話の分野で行われている特番のような認識番号を用いることなく、パケットカウントを行うソフトウェアをＰＣ２０上に予めインストールしておくことなく、パケットの宛先の登録の必要もなく、業務上、インターネット１６上のサーバへアクセスする場合であっても公私分計することができ且つキャリヤ側からみて信頼度が高いデータ通信料金課金システム等を提供することができる。

【実施例２】

【００５３】

実施例２では、携帯電話器１０が無線ＬＡＮを介して所定のネットワーク１６の利用を行う場合について説明する。

【００５４】

図３は、本発明の実施例２におけるデータ通信料金課金システム２を示す。図２で図１と同じ符号を付した箇所は同じ要素を示すため説明は省略する。図２に示されるデータ通信料金課金システム２が図１に示されるデータ通信料金課金システム１と異なる点は、ＰＣ２０が無線ＬＡＮ１７を介して所定のネットワーク１６の利用を行う場合のために、無線ＬＡＮ１７および無線ＬＡＮ１７に接続された無線ＬＡＮ基地局１８が追加された点と、当該追加に伴い、ＰＣ２０のログイン部２５の機能および認証サーバ５０の利用可通知部５４の機能が一部変更された点とである（各々、ログイン部２５’、利用可通知部５４’と示す）。

【００５５】

データ通信料金課金システム２では、通信トークン料金送信部３６により送信された通信トークンＴ’の料金Ｂ’には、実施例１で説明した所定のネットワーク１６の利用料に加えて無線ＬＡＮ１７の回線使用料金が含まれている。この無線ＬＡＮ１７の回線使用料金は、例えば無線ＬＡＮ基地局１８があるホットスポットの臨時課金である。ログイン部２５’は、携帯電話器１０の識別子ＩＤおよびウェブサーバ側通信トークン送信部３４により送信された通信トークンＴ’を用いて、無線ＬＡＮ基地局１８および認証サーバ５０を介して所定のネットワーク１６の利用を試みる。利用可通知部５４’は、通信トークン認証部４４により通信トークンＴ’の正当性が認証された場合、無線ＬＡＮ基地局１８を介してＰＣ２０へ所定のネットワーク１６の利用を認める通知Ｍ’を送信する。他の処理

は実施例１と同様であるため説明は省略する。

【００５６】

実施例２のデータ通信料金課金方法は、上述した実施例１のデータ通信料金課金方法において、通信トークン料金送信ステップ（ステップＳ３６）で送信された通信トークンＴ’の料金Ｂ’が無線ＬＡＮ１７の回線使用料金を含み、ログインステップ（ステップＳ２５）は、携帯電話器１０の識別子ＩＤおよびウェブサーバ側通信トークン送信ステップ（ステップＳ３４）で送信された通信トークンＴを用いて、無線ＬＡＮ基地局１８および認証サーバ５０を介して所定のネットワーク１６の利用を試みることになる。利用可通知ステップ（ステップＳ５４）は、通信トークン認証ステップ（ステップＳ４４）で通信トークンＴの正当性が認証された場合、無線ＬＡＮ基地局１８を介してＰＣ２０へ所定のネットワーク１６の利用を認める通知Ｍ’を送信することになる。他の処理は図２に示される実施例１の処理と同様であるため説明は省略する。

【００５７】

以上より、本発明の実施例２によれば、データ通信料金課金システム２における通信トークンＴ’の料金Ｂに、所定のネットワーク１６の利用料に加えて無線ＬＡＮ１７の回線使用料金を含ませておく。ログイン部２５’は、携帯電話器１０の識別子ＩＤおよびウェブサーバ側通信トークン送信部３４により送信された通信トークンＴ’を用いて、無線ＬＡＮ基地局１８および認証サーバ５０を介して所定のネットワーク１６の利用を試みる。利用可通知部５４’は、通信トークン認証部４４により通信トークンＴ’の正当性が認証された場合、無線ＬＡＮ基地局１８を介してＰＣ２０へ所定のネットワーク１６の利用を認める通知Ｍ’を送信する。この結果、携帯電話器１０は無線ＬＡＮ１７を介して所定のネットワーク１６の利用を行うことができる。区分課金部６２は、実施例１と同様に、通信事業者側サーバ１４から送信された所定の期間（例えば、1ヶ月間）におけるユーザ所有の携帯電話器１０のデータ通信に対する料金（＝Ａ）から、当該所定の期間における通信トークン料金送信部３６により送信された通信トークンＴ’の料金（＝所定のネットワーク１６の利用料＋無線ＬＡＮ１７の回線使用料金＝Ｂ’）を控除した額（＝Ａ－Ｂ’）を携帯電話器１０側の請求先（携帯電話器１０の所有者または利用者であるユーザ）に課金し、当該通信トークンＴ’の料金（＝Ｂ’）を他の請求先（上記ユーザに対して所定の関係を有する側、例えば雇用者側）に課金することができる。従って、ユーザが業務上、ホットスポットにおいて臨時的にインターネット（所定のネットワーク１６の一例）上のサーバへアクセスする場合であっても、上述した通信トークンＴ’を用いることにより、実施例１と同様に即時に公私分計することができる。

【実施例３】

【００５８】

上述した実施例１および２の各データ通信料金課金システム１および２において、所定のネットワーク１６への接続が認証を必要とする場合のために、ウェブサーバ３０は当該認証（ユーザ認証）を行うウェブサーバ側認証部（ウェブサーバ側認証手段。不図示）をさらに備えることができる。所定のネットワーク１６が企業内ネットワーク等である場合、当該企業内ネットワーク等へログインするためにはユーザ認証を必要とする。あるいは、接続料金定額サービスの場合、通信時間またはパケット量の測定をしないケースもあるため、接続料金定額サービスを利用する場合にはユーザ認証を必要とする。本実施例３によれば、ウェブサーバ３０はユーザ認証を行うウェブサーバ側認証部を備えているため、所定のネットワーク１６への接続が認証を必要とする場合、当該認証を行うことができる。

【００５９】

実施例３のデータ通信料金課金方法は、上述した実施例１または２の各データ通信料金課金方法において、ウェブサーバ側識別子送信ステップ（ステップＳ３２）に先立ち、ウェブサーバ３０が上記認証を行うウェブサーバ側認証ステップ（不図示）をさらに備えればよい。他の処理は図２に示される実施例１の処理、上述した実施例２の処理と同様であるため説明は省略する。

【実施例４】
【００６０】
本実施例４では、上述した各実施例において通信トークンの生成の際に暗号化を用いる場合について説明する。暗号化以外については上述した各実施例と同様である。以下では、図１を適宜引用して説明する。
【００６１】
通信トークン送信部４２は、ウェブサーバ側識別子送信部３２により送信された識別子ＩＤと所定の鍵（秘密鍵等）Ｋと所定の乱数Ｒとに基づき通信トークンＴ＊（暗号化されたことを上付＊で示す。）を生成する。生成した通信トークンＴ＊をウェブサーバ３０へ送信する。通信トークン送信部４２は携帯電話器１０の識別子ＩＤと所定の乱数Ｒとを関連付け（紐付け）した状態で記録しておく。所定の鍵Ｋは携帯電話器１０によらず一定の鍵としておけばよいが、所定の鍵Ｋも識別子ＩＤと関連付けて記録しておいてもよいことは勿論である。通信トークン認証部４４は、識別子・通信トークン送信部５２により送信された識別子ＩＤおよび通信トークンＴ＊と、所定の鍵Ｋと、通信トークン送信部４２により識別子ＩＤと関連付けて記録された所定の乱数Ｒとに基づき、通信トークンＴ＊の正当性を認証する。従前に通信トークン送信部４２により通信トークンＴ＊（従前）が生成された際、携帯電話器１０の識別子ＩＤ（従前）および所定の乱数Ｒとは紐付けされた状態で記録されている。このため、識別子・通信トークン送信部５２により送信された識別子ＩＤと同じ値の識別子ＩＤ（従前）を検索し、当該識別子ＩＤ（従前）に紐付けされている所定の乱数Ｒを求め、この所定の乱数Ｒと所定の鍵Ｋと識別子ＩＤとから通信トークンＴ＊（従前）を求める。この通信トークンＴ＊（従前）と識別子・通信トークン送信部５２により送信された通信トークンＴ＊とが一致した場合、通信トークン認証部４４は、従前に携帯電話コンテンツ用ネットワーク１５を介して通信トークンＴ＊（従前）を購入する際に用いられた携帯電話器１０と、現在所定のネットワーク１６の利用を試みようとしている際に用いられている携帯電話器１０とが同一であると認証することができる。
【００６２】
以上より、本発明の実施例４によれば、上述した各実施例で説明した機能に加えて、暗号化された通信トークンＴ＊を用いることができる。この結果、通信トークンＴ＊がコピーされていた場合、ＰＣ２０からのログイン要求を拒否することができる。この結果、上述した各実施例の効果に加えて、通信トークンＴ＊をコピーされないようにすることができるセキュリティ機能を有するデータ通信料金課金システムを構築することができる。
【実施例５】
【００６３】
上述したデータ通信料金課金システム１等では、携帯電話器１０の識別子は１つであることを想定していた。本実施例５では、携帯電話器１０は１つ以上の識別子を有し、上述した他の請求先も当該１つ以上の識別子に対応して１つ以上ある場合について説明する。
【００６４】
移動情報端末９０および課金サーバ６０は携帯電話器１０の１以上の識別子と当該１以上の識別子に各々対応する他の請求先との対応表１００（後述する図４参照）をさらに備えている。対応表１００は、例えばＰＣ２０および課金サーバ６０の記録装置７８ａ（図４参照）に記録されている。ＰＣ２０側では、識別子送信部２３’’（不図示）は、通信トークンの購入に際し対応表１００に基づき携帯電話器１０の１以上の識別子の内の一つの識別子をウェブサーバ３０へ送信する。ウェブサーバ３０側では、通信トークン料金送信部３６’’（不図示）は、課金サーバ６０へウェブサーバ側通信トークン送信部３４により送信された通信トークンの料金と識別子送信部２３’’により送信された識別子とを送信する。課金サーバ６０側では、区分課金部６２’’は、通信事業者側サーバ１４から送信された所定の期間における携帯電話器１０のデータ通信に対する料金から、当該所定の期間における通信トークン料金送信部３６’’により送信された通信トークンの料金を控除した額を携帯電話器１０側の請求先に課金し、上記通信トークンの料金を通信トークン料金送信部３６’’により送信された識別子に対応する対応表１００中の他の請求先に

課金する。

【００６５】

以上により、本発明の実施例５によれば、移動情報端末９０および課金サーバ６０は携帯電話器１０の１以上の識別子と当該１以上の識別子に各々対応する他の請求先との対応表１００をさらに備えている。識別子送信部２３’’は、通信トークンの購入に際し対応表１００に基づき携帯電話器１０の１以上の識別子の内の一つの識別子をウェブサーバ３０へ送信する。通信トークン料金送信部３６’’は、課金サーバ６０へウェブサーバ側通信トークン送信部３４により送信された通信トークンの料金と識別子送信部２３’’により送信された識別子とを送信する。区分課金部６２’’は、通信事業者側サーバ１４から送信された所定の期間における携帯電話器１０のデータ通信に対する料金から、当該所定の期間における通信トークン料金送信部３６’’により送信された通信トークンの料金を控除した額を携帯電話器１０側の請求先に課金し、上記通信トークンの料金を通信トークン料金送信部３６’’により送信された識別子に対応する対応表１００中の他の請求先に課金する。この結果、携帯電話器１０は複数の識別子を使い分けることにより、通信トークンの料金を複数の他の請求先へ課金させることができる。

【実施例６】

【００６６】

図４は、上述した各実施例を実現するための本発明のコンピュータ・プログラムを実行するＰＣ２０、ウェブサーバ３０、通信トークン発行サーバ４０、認証サーバ５０および課金サーバ６０のコンピュータの内部回路７０を示すブロック図である。図４に示されるように、ＣＰＵ７１、ＲＯＭ７２、ＲＡＭ７３、画像制御部７６、コントローラ７７、入力制御部７９、無線ＬＡＮ１７とのインタフェース機能を有する通信メディアインタフェース（Ｉ／Ｆ）部８１および入出力Ｉ／Ｆ部８２はバス８３に接続されている。図４において、上述の本発明のコンピュータ・プログラム（ＰＣ２０側のプログラム、課金サーバ６０側のプログラム等）は、ＲＯＭ７２、ＨＤ等の記録装置７８ａ、またはＤＶＤ若しくはＣＤ－ＲＯＭ７８ｎ等の記録媒体（脱着可能な記録媒体を含む）に記録されている。本発明のコンピュータ・プログラムは、ＲＯＭ７２からバス８３を介し、あるいは記録装置７８ａまたはＤＶＤ若しくはＣＤ－ＲＯＭ７８ｎ等の記録媒体からコントローラ７７を経由してバス８３を介しＲＡＭ７３へロードされる。内部回路７０がＰＣ２０および課金サーバ６０の場合、図４に示されるように記録装置７８ａには対応表１００が記録されている。入力制御部７９は、マウス、テンキー等の入力操作部８０と接続され入力制御等を行う。画像メモリであるＶＲＡＭ７５はＰＣ２０の表示部７４の少なくとも一画面分のデータ容量に相当する容量を有しており、画像制御部７６はＶＲＡＭ７５のデータを画像データへ変換して表示部７４へ送出する機能を有している。入出力Ｉ／Ｆ部８２は入出力インタフェース機能を有しており、ＵＳＢケーブル１１等により携帯電話器１０の入出力Ｉ／Ｆ部（不図示）と接続されている。

【００６７】

上述のようにＣＰＵ７１が本発明のコンピュータ・プログラムを実行することにより、本発明の目的を達成することができる。当該コンピュータ・プログラムは上述のようにＤＶＤまたはＣＤ－ＲＯＭ７８ｎ等の記録媒体の形態でコンピュータＣＰＵ７１に供給することができ、当該コンピュータ・プログラムを記録したＤＶＤまたはＣＤ－ＲＯＭ７８ｎ等の記録媒体も同様に本発明を構成することになる。当該コンピュータ・プログラムを記録した記録媒体としては上述された記録媒体の他に、例えばメモリ・カード、メモリ・スティック、光ディスク、ＦＤ等を用いることができる。

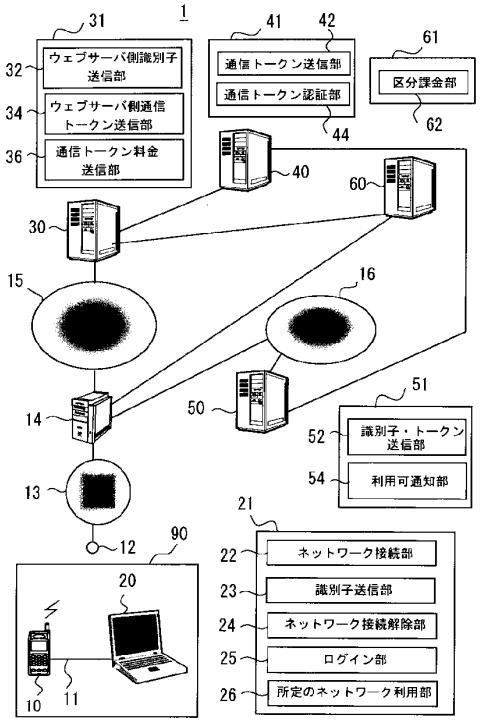
【産業上の利用可能性】

【００６８】

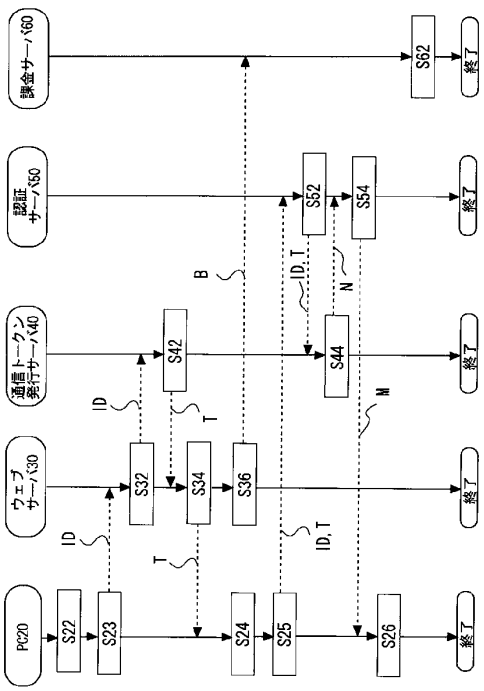
本発明の活用例として、上述のように公私分計を即時に行うことができるため、会社所有のＰＣおよび携帯電話器を用いた所定のネットワーク１６の利用に対する従来の会社側との割引契約に、個人所有のＰＣおよび携帯電話器を用いた場合における所定のネットワーク１６の利用に対しても即時に割引を適用するシステムへの応用が挙げられる。

【図面の簡単な説明】
【００６９】
【図１】本発明の実施例１におけるデータ通信料金課金システム１を示す図である。
【図２】データ通信料金課金システム１の構成要素であるＰＣ２０、ウェブサーバ３０、通信トークン発行サーバ４０、認証サーバ５０、課金サーバ６０で実行される各プログラムの流れまたはデータ通信料金課金方法を示すフローチャートである。
【図３】本発明の実施例２におけるデータ通信料金課金システム２を示す図である。
【図４】上述した各実施例を実現するための本発明のコンピュータ・プログラムを実行するＰＣ２０、ウェブサーバ３０、通信トークン発行サーバ４０、認証サーバ５０および課金サーバ６０のコンピュータの内部回路７０を示すブロック図である。
【符号の説明】
【００７０】
１、２　データ通信料金課金システム、　１０　携帯電話器、　１１　ＵＳＢケーブル、　１２　基地局、　１３　移動体通信網、　１４　通信事業者側サーバ、　１５　携帯電話コンテンツ用ネットワーク、　１６　所定のネットワーク、　１７　無線ＬＡＮ、　１８　無線ＬＡＮ基地局、　２０　ＰＣ、　２１、３１、４１、５１、６１　機能ブロック、　２２　ネットワーク接続部、　２３　識別子送信部、　２４　ネットワーク接続解除部、　２５、２５’　ログイン部、　２６　所定のネットワーク利用部、　３０　ウェブサーバ、　３２　ウェブサーバ側識別子送信部、　３４　ウェブサーバ側通信トークン送信部、　３６　通信トークン料金送信部、　４０　通信トークン発行サーバ、　４２　通信トークン送信部、　４４　通信トークン認証部、　５０　認証サーバ、　５２　識別子・通信トークン送信部、　５４、５４’　利用可通知部、　６０　課金サーバ、　６２　区分課金部、　７０　内部ブロック、　７１　ＣＰＵ、　７２　ＲＯＭ、　７３　ＲＡＭ、　７４　表示部、　７５　ＶＲＡＭ、　７６　画像制御部、　７７　コントローラ、　７８ａ　記録装置、　７８ｎ　記録媒体、　７９　入力制御部、　８０　入力操作部、　８１　通信メディアＩ／Ｆ部、　８２　入出力Ｉ／Ｆ部、　８３　バス、　９０　移動情報端末、　１００　対応表。

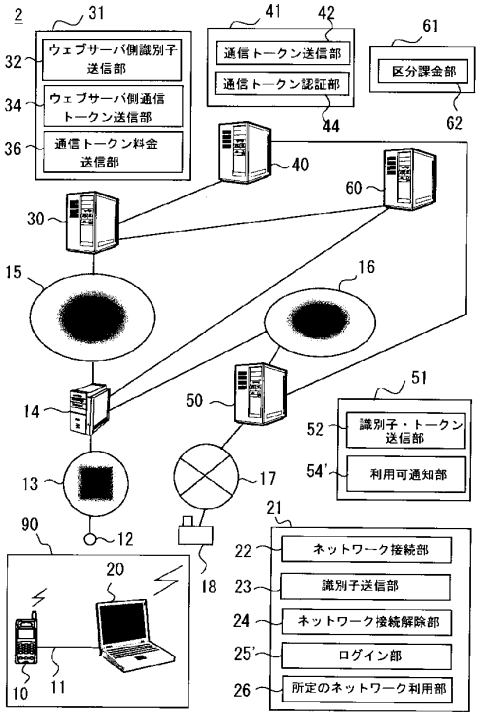
【図１】


1
31
ウェブサーバ側識別子送信部
32
ウェブサーバ側通信トークン送信部
34
通信トークン料金送信部
36
41
42
通信トークン送信部
通信トークン認証部
44
61
区分課金部
62
40
60
30
15
16
14
50
51
52
識別子・トークン送信部
54
利用可通知部
13
12
90
21
22
ネットワーク接続部
23
識別子送信部
24
ネットワーク接続解除部
25
ログイン部
26
所定のネットワーク利用部
20
10
11

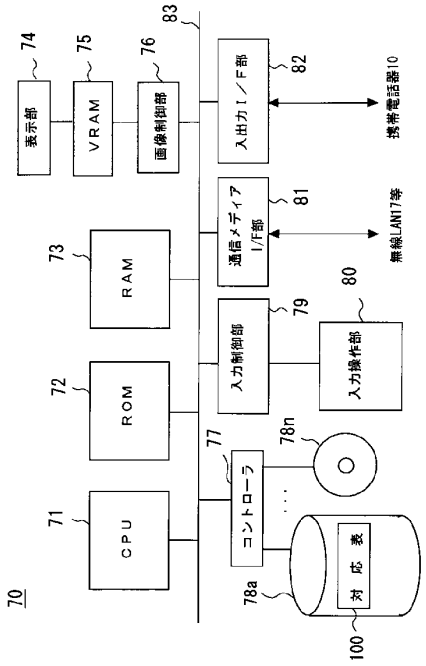
【図２】


課金サーバ60
認証サーバ50
通信トークン発行サーバ40
ウェブサーバ30
PC20
S22
S23
S24
S25
S26
S32
S34
S36
S42
S44
S52
S54
S62
終了
ID
T
ID,T
B
N
M

【図３】


2
31
ウェブサーバ側識別子送信部
32
ウェブサーバ側通信トークン送信部
34
通信トークン料金送信部
36
41
42
通信トークン送信部
通信トークン認証部
44
61
区分課金部
62
40
60
30
15
16
14
50
51
52
識別子・トークン送信部
54'
利用可通知部
13
17
90
12
21
22
ネットワーク接続部
23
識別子送信部
24
ネットワーク接続解除部
25'
ログイン部
26
所定のネットワーク利用部
18
20
10
11

【図４】


70
CPU
71
RAM
73
ROM
72
74
表示部
75
VRAM
76
画像制御部
77
コントローラ
78a
78n
対応表
100
79
入力制御部
80
入力操作部
81
通信メディアI/F部
82
入出力I/F部
83
携帯電話器10
無線LAN17等

フロントページの続き

Ｆターム(参考) 5K201 AA05 AA09 BD05 CB13 DC02 EA07 EC06 ED06 FA07

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
2 February 2006 (02.02.2006)

PCT

(10) International Publication Number
WO 2006/012610 A2

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

(21) International Application Number: PCT/US2005/026296

(22) International Filing Date: 22 July 2005 (22.07.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/590837	23 July 2004 (23.07.2004)	US
60/601431	13 August 2004 (13.08.2004)	US
60/607420	3 September 2004 (03.09.2004)	US
60/608814	10 September 2004 (10.09.2004)	US

(71) Applicant *(for all designated States except US)*: **CITRIX SYSTEMS, INC.** [US/GB]; 851 West Cypress Creek Road, Fort Lauderdale, FL 33309 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **RAO, Goutham, P.** [US/US]; 6963 Starling Valley Drive, San Jose, CA 95120 (US). **BRUEGGEMANN, Eric** [US/US]; 5642 Stevens Creek Blvd., no.606, Cupertino, CA 95014 (US). **RODRIGUEZ, Robert** [US/US]; 5647 Wells Court, San Jose, CA 95123 (US).

(74) Agents: **LANZA, John, D.** et al.; Lahive & Cockfield, LLP, 28 State Street, Boston, MA 02109 (US).

(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, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, 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) 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, 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).

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:** SYSTEMS AND METHODS FOR OPTIMIZING COMMUNICATIONS BETWEEN NETWORK NODES

(57) **Abstract:** The present invention is generally directed towards a remote access architecture for providing peer-to-peer communications and remote access connectivity. In one embodiment, the remote access architecture of the present provides a method for establishing a direct connection between peer computing devices via a third computing device, such as a gateway. Additionally, the present invention provides the following techniques to optimize peer-to-peer communications: 1) false acknowledgement of receipt of network packets allowing communications via a lossless protocol of packets constructed for transmission via a lossy protocol, 2) payload shifting of network packets allowing communications via a lossless protocol of packets constructed for transmission via a lossy protocol, 3) reduction of packet fragmentation by adjusting the maximum transmission unit (MTU) parameter, accounting for overhead due to encryption, 4) application-aware prioritization of client-side network communications, and 5) network disruption shielding for reliable and persistent network connectivity and access.

WO 2006/012610 A2

SYSTEMS AND METHODS FOR OPTIMIZING COMMUNICATIONS BETWEEN NETWORK NODES

Related Applications

This present application claims priority to U.S. Provisional Patent Application Number 60/590,837, entitled "Ad Hoc Distributed Networks And Remote Access Architecture", filed July 23, 2004, and U.S. Provisional Patent Application Number 60/601,431, entitled "System And Method For Assuring Redundancy In Remote Access Solution", filed August 13, 2004, and U.S. Provisional Patent Application Number 60/607,420, entitled "Virtual Network Bridging", filed September 3, 2004, and U.S. Provisional Patent Application Number 60/608,814, entitled "System And Method For Assuring Redundancy In Remote Access Solution", filed September 10, 2004, all of which are incorporated herein by reference.

Technical Field

The invention generally relates to optimizing network communications between nodes on a network.

Background Information

A Virtual Private Network (VPN) is a private data network that makes use of the public telecommunication infrastructure, such as the Internet, to maintain privacy through the use of tunneling and security mechanisms. As such, a VPN provides for data encryption and security for corporate data traversing the public network. In addition to addressing secure access to corporate data via a public network, VPNs are also directed towards routing network traffic from two disconnected, otherwise non-routable networks. For example, a first private network with private internet protocol addresses in the range 10.0.0.0 – 10.255.255.255 may communicate via a VPN with a second private network with private internet protocol addresses in the range 192.168.0.0 – 192.168.255.255. The VPN allows a remote machine on the first private network to communicate with an internal machine on the second private network by tunneling network traffic from the remote machine and making the network traffic appear on the second private network. This may work well for client-server protocols where a remote computer is transacting with an enterprise server located on a remote network.

However, traditional VPNs may not work well in the case where two remote computers tunnel via a VPN gateway to communicate directly with each other, such as in peer-to-peer protocols. The VPN achieves this peer-to-peer computing by flattening the disjoint private network address spaces in which the two remote computers tunnel all peer-to-peer communications via the VPN gateway. As a result, network traffic from one of the peers flows through the VPN gateway and switches tunnels on the intranet to flow back out on the internet to the peer computer. The network traffic between the peer computers may travel longer and less optimal routes event though the peer computers may have a shorter direct path between then. It would be useful to allow remote computers to benefit from the security afforded by VPNs without incurring the drawback of longer data paths routes.

Other inefficiencies exist with direct communications over a network between two computers. For example, the network connection is susceptible to breakdown. For instance, a wireless connection between a client and a server is often unreliable. In other cases, the network connection is intermittent. A connection can be lost when one enters an elevator or tunnel and may only be restored following one's exit from the elevator or tunnel. In another example, a connection can be disrupted when a mobile computing device moves from network access point to network access point, such as in a wireless network topology.

If an established communication session between the client and the server computer abnormally terminates, the client generally has to re-establish the connection by starting a new communication session. To begin the new communication session, the user typically has to retransmit the authentication credentials, such as a login/password pair, to the server computer so that the server computer can authorize the user for the new communication session. This retransmission of the authentication credentials of a user across multiple communication sessions repeatedly exposes the authentication credentials of that user to potential attackers, thereby decreasing the level of security of the authentication credentials. In addition, this often is a slow process that also results in user frustration and inefficiency. Furthermore, in establishing a new communication session, the network may require the client obtains a new network identifier, such as an internet protocol address. The applications or programs on the client may need to be restarted because of the change in the client's network identifier. Thus, it would be desirable to shield the computing devices from network disruptions.

Another inefficiency associated with direct communication between peer computing devices is that the protocol used for communications may not be as efficient or secure as desired. As an example, the network communications may include real-time data communications such as voice over IP (VoIP) communications. The real-time data communications may be communicated via an unreliable protocol such as the user datagram protocol in order to reduce latency in the telephone call. However, the VoIP communication may traverse a TCP/IP network or secure SSL gateway, which provides a reliable protocol to the VoIP communications. This may increase the latency in the telephone call that the unreliable protocol was intended to reduce. Techniques are needed for transmitting data via a lossless protocol that is intended for communication using a lossy protocol.

Another inefficiency in direct communication result from the use of encryption. Encryption, such as SSL, may be used to provide secure network communications. Although the communication is secure, the encryption of the network traffic increases the size of the network packets, which can cause the packet payload to become too large for a single packet. This can result in packet fragmentation, causing more overhead for communication processing. Techniques for adjusting the maximum size of a packet to account for encryption overhead would be useful.

Another inefficiency result from the fact that a client typically sends network communications as they are generated by the activity of the user and applications of the client, and processes incoming network communications as they are received. For example, in one case, although an application is running in the foreground and currently in active use by the user, a network packet generated or received for an application running in the background may be processed ahead of a network packet generated or received for the application running in the foreground. In another example, the client may be running a VoIP application to provide a telephone call to a remote computing device. One or more other applications on the client may be running that are not related to the real-time data communication of VoIP. The network packets for these applications may be processed ahead of the real-time network packets of the VoIP telephone call thereby increasing the latency and reducing the quality of the voice communication. It is desirable to provide application-aware, client-specific prioritization of packet traffic.

Summary of the Invention

The present invention is generally directed towards a remote access architecture for providing peer-to-peer communications and remote access connectivity. In one embodiment, the remote access architecture of the present invention provides a method for establishing a direct connection between peer computing devices via a third computing device, such as a gateway. Additionally, the present invention provides various techniques for optimizing peer-to-peer communications, including real-time communications such as voice over internet protocol (VoIP) signaling and media, video, and other real-time data applications such as web collaboration, screen or desktop sharing, and instant messaging. The present invention provides the following peer to peer optimization techniques: 1) false acknowledgement of receipt of network packets allowing communications via a lossless protocol of packets constructed for transmission via a lossy protocol, 2) payload shifting of network packets allowing communications via a lossless protocol of packets constructed for transmission via a lossy protocol, 3) reduction of packet fragmentation by adjusting the maximum transmission unit (MTU) parameter, accounting for overhead due to encryption, 4) application-aware prioritization of client-side network communications, and 5) network disruption shielding for reliable and persistent network connectivity and access, such as for mobile computing.

In one aspect, the present invention relates to a method for establishing a peer-to-peer communication session between a first computing device on a first network and a second computing device on a second network. The first network may be disconnected from and not routable to the second network. The method includes establishing, by the first computing device, a first tunneling session with a third computing device, and establishing, by the second computing device, a second tunneling session with the third computing device. The third computing device may be a gateway, such as an SSL VPN gateway. The first computing device initiates a communication session to the second computing device via the third computing device, such as via a signaling protocol. A server receives a signal to establish the initiated communication session, and the server communicates to the first computing device a first network address comprising a network address of the second computing device associated with the second tunneling session. The first computing device communicates a request to initiate a connection with the second computing device using the first network address. The method further

includes intercepting, by the third computing device, the request, and providing the first computing device a second network address for the second computing device. The second network address identifies a public network address associated with the second computing device. The third computing device communicates a request to the second computing device to allow a connection from the first computing device using the second network address, such as via a swimmer session traversing a firewall.

In one embodiment of the present invention, the first tunneling session or the second tunneling session is established using a Secure Socket Layer or a virtual private network The third computing device may be a remote access gateway. In another embodiment, the second computing device is located behind a firewall associated with the second network address.

In another embodiment, the method of the present invention includes providing, by the third computing device, the second network address to the first computing device by communicating an out of band signal to the first computing device via the first tunneling session. In an additional embodiment, the method of includes providing, by the second computing device, a forward hole in a firewall for the first computing device to communicate to the second computing device using the second network address.

In a further embodiment of the present invention, the third computing device communicates a key to the first computing device and the second computing device. The first computing device and the second computing device may exchange keys. Additionally, the first and second computing device may check that the key received from the other computing device matches before transmitting data to the other computing device.

In some embodiments of the present invention, the method associates a first telecommunication device with the first computing device, and associates a second telecommunication device with the second computing device. The first telecommunication device or the second telecommunication device may include a software component or a hardware component, such as a hard or soft VoIP telephone. In one embodiment, the method of the present invention includes establishing a telecommunication session between the first telecommunication device and the second telecommunication device via the connection between the first and second computing devices. The first telecommunication device and the second telecommunication device

may communicate over the telecommunication session without traversing the third computing device.

In another embodiment of the present invention, the method communicates a remote display protocol via the connection between the first computing device and the second computing device. The remote desktop protocol may include the Independent Computing Architecture protocol or the Remote Desktop Protocol. In yet a further embodiment, the method may include sharing a screen view or screen data of the first computing device with the second computing device via the connection.

In one aspect, the present invention relates to a method performed in a gateway for establishing a peer-to-peer communication session between a first computing device on a first network and a second computing device on a second network. The first network may be disconnected from and not routable to the second network. The method includes establishing a first tunneling session with the first computing device on a first network, and establishing a second tunneling session with the second computing device on the second network. The gateway receives a request by the first computing device to initiate a communication session with the second computing device. The first computing device provides a first network address for contacting the second computing device. The first network address identifies a network address of the second computing device associated with the second tunneling session. The gateway receives a request by the first computing device to initiate a connection with the second computing device using the first network address, intercepts the request to initiate the connection, and provides the first computing device a second network address for the second computing device. The second network address identifies a public network address associated with the second computing device. The gateway communicates to the second computing device a request to allow the connection from the first computing device to the second computing device using the second network address, such as via a swimmer session traversing a firewall.

In one embodiment, the first tunneling session or the second tunneling session via the gateway includes a Secure Socket Layer or a virtual private network. In another embodiment, the second computing device is located behind a firewall associated with the second network address. In a further embodiment, the method of the present invention provides the second network address to the first computing device by communicating an out of band signal to the first computing device via the first tunneling

session. Additionally, the gateway may communicate a key to the first computing device and to the second computing device.

In another aspect, the present invention is related to a system for establishing a peer-to-peer communication session between a first computing device on a first network and a second computing device on a second network via a third computing device. The first network may be disconnected from and not routable to the second network. The system includes a first computing device on the first network, and a second computing device on the second network. A third computing device establishes a first tunneling session with the first computing device and a second tunneling session with the second computing device. The system also includes a server accessible via the third computing device. In operation of the system, the server communicates via the third computing device to the first computing device a first network address identifying a network address of the second computing device associated with the second tunneling session. The first computing device communicates via the third computing device a first request to initiate a connection with the second computing device using the first network address. The third computing device intercepts the first request, and provides the first computing device a second network address for the second computing device. The second network address identifies a public network address associated with the second computing device. The third computing device communicates a second request to the second computing device to allow a connection from the first computing device using the second network address.

In one embodiment of the system, the first tunneling session or the second tunneling session includes a Secure Socket Layer or a virtual private network. Furthermore, the third computing device may be a remote access gateway, such as an SSL VPN gateway. In another embodiment of the system, the second computing device is located behind a firewall associated with the second network address.

In an additional embodiment of the present invention, the third computing device provides the second network address to the first computing device by communicating an out of band signal via the first tunneling session, such as via an out of band TLS session. In one embodiment, the second computing device provides a forward hole in a firewall for the first computing device to communicate to the second computing device using the second network address.

In a further embodiment of the system of the present invention, the third computing device communicates a key to the first computing device and the second computing device. The first computing device and the second computing device may exchange keys. Additionally, the first and second computing device may check that the key received from the other computing device matches before transmitting data.

In some embodiments of the present invention, the system includes a first telecommunication device associated with the first computing device, and a second telecommunication device associated with the second computing device. The first telecommunication device or the second telecommunication device may include a software component or a hardware component, such as a hard or soft VoIP telephone. In one embodiment, the system of the present invention includes establishing a telecommunication session between the first telecommunication device and the second telecommunication device via the connection between the first and second computing devices. The first telecommunication device and the second telecommunication device may communicate over the telecommunication session without traversing the third computing device.

In another embodiment of the present invention, the first computing device and the second computing device communicate a remote display protocol via the connection. The remote desktop protocol may include the Independent Computing Architecture protocol or the Remote Desktop Protocol. In yet a further embodiment, the first computing device may share a screen view or screen data with the second computing device via the connection.

In another aspect, the present invention is related to a method for communicating via a lossless protocol a packet constructed to be transmitted via a lossy protocol. The method may be performed in one or more electronic devices, such as in a system, and by any suitable means and mechanisms. The method includes establishing a connection between a first computing device and a second computing device via a lossless protocol. In some embodiments, the second computing device may be a gateway, such as an SSL VPN gateway. The first computing device detects a lossless protocol packet comprising a payload having one or more packets constructed in accordance with a lossy protocol. The first computing device communicates a false acknowledgement of receipt of the lossless protocol packet to the first computing device and/or the second computing device. The false acknowledgement of receipt of the lossless protocol packet prevents

employing the reliability algorithms and mechanisms of the lossless protocol. The first computing device communicates the lossless protocol packet to the second computing device. In some embodiments, the false acknowledgement of receipt of the lossless protocol packet is communicated prior to communicating the lossless protocol packet.

In one embodiment, the method of the present invention includes encrypting, by the first computing device, the one or more packets using a key. In some embodiments, the encryption key may be provided to the first computing device via an out of band transport security layer session between the first computing device and the second computing device. In a further embodiment, the method encrypts the one or more packets on a packet by packet basis.

In another embodiment of the method of the present invention, in response to receiving the false acknowledgement of receipt of the lossless protocol packet by the first computing device and/or the second computing, the first computing device and/or the second computing prevents executing an operation associated with providing a lossless characteristic of the lossless protocol. In one embodiment, the lossless protocol is a transport control protocol.

In a further embodiment, the method of the present invention prevents the network stack of the first computing device and/or the second computing device from executing one or more of the following in connection with the lossless protocol: 1) a retransmit, 2) an ordering, 3) a flow control algorithm, 4) a naple's algorithm, and 5) a sliding window algorithm.

In one embodiment, the lossy protocol includes a user datagram protocol. In another embodiment, the method includes communicating, by the first computing device, the
lossless protocol packet via a secure socket layer or a transport security layer tunnel to the second computing device.

In another embodiment, the one or more packets of the payload comprises a real-time protocol. In an additional embodiment, the method includes communicating by the first computing device one of real-time voice, audio, or data to the second computing device via the one or more packets.

In one aspect, the present invention relates to a method for transmitting packets from an application using an unreliable transport protocol over a TCP connection. The method includes receiving, at a first device, a first packet to be transmitted using an unreliable

transport protocol, and creating a first TCP packet including a first payload of the received first packet and a first TCP header of information associated with a TCP connection established between the first device and a second device. The first device transmits the first TCP packet to the second device. The method further includes receiving, at the first device, a second packet to be transmitted using an unreliable transport protocol, and creating a second TCP packet including a second payload of the received second packet and the first TCP header information. Before receipt of an acknowledgement of the receipt of the first payload from the second device, the first device transmits the second TCP packet to the second device.

In one embodiment, the method of the present invention establishes the TCP connection with a port number associated with the unreliable transport protocol. In another embodiment, the method includes dynamically determining, by the first device, the first TCP packet and second TCP packet comprise an unreliable transport protocol. In some embodiments, the unreliable transport protocol is UDP.

In an additional embodiment, the method includes receiving the first TCP packet and second TCP packet on the first device by intercepting the first TCP packet and second TCP packet using a packet capturing mechanism. In some embodiments, the method establishes by the first device, the TCP connection with a VPN gateway device. In other embodiments, the method includes establishing peer-to-peer communications between the first device and the second device via the TCP connection. In another embodiment of the present invention, the method includes encrypting, by the first device, the first and second TCP packets, and decrypting, by the second device, the encrypted first and second TCP packets.

In another aspect, the present invention relates to a method for transmitting packets from an application using an unreliable transport protocol over a TCP connection. The method includes intercepting, at a second device, a first TCP packet created on a first device and received on the second device. The first TCP packet includes a first payload of a first packet generated by an application using an unreliable protocol and a first TCP header of information associated with a TCP connection established between the first device and the second device. The intercepting of the method occurs before the first TCP packet is provided to a TCP stack on the second device. The method includes identifying, responsive to the TCP header of information, that the first payload is a packet generated by an application using an unreliable

transport protocol, stripping the TCP header of information from the first TCP packet, and forwarding the first payload to an application using the unreliable data protocol.

In one embodiment, the unreliable protocol is UDP. In another embodiment, the step of identifying comprises identifying that the TCP header information includes a port number associated with the unreliable transport protocol. In some embodiments, the method includes intercepting, by the second device, the first TCP packet using a packet capture driver.

In some embodiments, the first device is a client device and the second device is a VPN gateway. Additionally, the method of the present invention includes performing Network Address Translation (NAT) on the second device prior to forwarding the first payload to the application.

In a further aspect, the present invention relates to a system for transmitting packets from an application using an unreliable transport protocol over a TCP connection. The system includes a first device and a second device. The first device has an application that generates a first and second packet. The first and second packet are intended to be transmitted using an unreliable transport protocol. The first device also has a filter process and a tunneling process. The filter process intercepts the first and second packets from the application and forwards the intercepted packets to the tunnel process. The tunnel process requests the opening of a TCP connection between the first device and a second device. The request to open the TCP connection indicates to the first and second device that the TCP connection will transport packets intended to be transmitted with an unreliable transport protocol. The tunnel process forwards the first and second packets as payloads in a first and second TCP packet to the second device. The tunnel process sends the second TCP packet after sending the first TCP packet and prior to receiving an acknowledgement for the first TCP packet.

The second device of the system of the present invention is in communication with the first device. The second device has second filter process and tunneling process. The second tunnel process opens the TCP connection requested by the first device, and identifies and forwards the source address of the TCP connection to the second filter process. The second filter process intercepts packets from the application received at the second device with the TCP connection source address in a header. The second filter process strips the TCP header from the received packets and forwards the stripped

packets to an intended destination, and circumventing the TCP/IP stack on the second device.

In one embodiment of the system of the present invention, the filter process on the first device and/or the second filter process of the second device is a packet capture driver. In some embodiments, the first device is a client device and the second device is a VPN gateway device. In one embodiment, the unreliable data protocol is UDP.

In another embodiment, the system also includes a third device to which the stripped packets are transmitted. Additionally, the second device may further include a Network Address Translation (NAT) table used to perform network address translation prior to transmitting the stripped packets to the third device.

In a further aspect, the present invention is related to a method for adjusting the maximum transmission unit of a secure network communication to reduce network fragmentation. The method may be performed in one or more electronic devices, such as in a system, and by any suitable means and mechanisms. The method includes establishing a session between a first computing device and a second computing device. The session may established by an agent of the first computing device. The first computing device has a first network stack. The method detects, by the first computing device, a network packet having an encrypted payload, and determines a setting for a maximum transmission unit parameter of the first network stack to reduce the maximum transmission unit size by at least a size associated with the encrypted portion of the payload. The method alters the maximum transmission unit (MTU) parameter of the first network stack to the determined setting. As such, the reported MTU parameter is reduced to account for the encryption.

In one embodiment, the method of the present invention includes communicating the network packet via a secure socket layer or a transport layer security tunnel to the second computing device. The second computing device may be a gateway, such as an SSL VPN gateway. In another embodiment, the payload comprises a real-time protocol.

Additionally, in one embodiment, the method may further comprise altering the maximum transmission unit parameter via a network driver interface specification (NDIS) level mechanism of the first network stack In another embodiment, the method determines the setting of the maximum transmission unit parameter dynamically per session between the first computing device and the second computing device. In one embodiment, the agent of the first computing device communicates via an IOCTL

application programming interface to the first network stack to alter the maximum transmission unit parameter to the determined setting.

In some embodiments, the method of the present invention establishes the session between the first computing device and the second computing device via a gateway. In other embodiments, the method communicates by the first computing device real-time voice, audio, or data to the second computing device via the payload of the network packet. In yet another embodiment, the method may include communicating a false acknowledgement of receipt of the network packet to the first computing device and/or the second computing device before communicating the network packet. In one embodiment, the network packet comprises a lossless protocol packet, such as a transport control protocol. In another embodiment, the payload comprises a lossy protocol packet, such as a user datagram protocol.

In an additional aspect, the present invention is related to a method for a client to prioritize network communications of the client associated with an application of the client. The method includes intercepting, by the client, one or more network packets associated with one or more applications of the client, and storing the one or more network packets to a queue. The client determines the queued one or more network packets is associated with a first application of the client. The client indicates a priority for the determined one or more network packets to place the determined one or more network packets ahead of at least one network packet in the queue associated with a second application of the client. The client
provides the prioritized one or more network packets for communications via a network stack of the client.

In one embodiment, the method of the present invention includes determining, by the client, the queued one or more networks packets of the first application comprises real-time data. The real-time data may include one of the following: 1) a real-time protocol, 2) a user datagram protocol, and 3) a representation of voice or audio.

In another embodiment, the method includes preventing, by the client, at least one network packet of the second application from being communicated via the network stack ahead of the one or more network packets of the first application. In a further embodiment, the method includes holding, by the client, in the queue a network packet associated with the second application, and releasing the held network packet upon

communication of the one or more network packets associated with the first application prioritized ahead of the held network packet.

In yet another embodiment of the present invention, the method includes intercepting, by the client, the one or more network packets transparently to the one or more applications on the client. In some embodiments, the first application is running in the foreground, and the second application is running in the background.

In one embodiment of the present invention, the method includes associating a priority with the first application higher than a priority associated with the second application. In another embodiment, a user may specify the priority of the first application or the second application. In a further embodiment, the client receives the one or more network packets from a computing device. Also, the one or more applications may provide the one or more network packets for communicating from the client to a computing device.

In another aspect, the present invention is related to a client for prioritizing network communications of the client associated with an application of the client. The client includes a mechanism for intercepting one or more network packets of the client associated with one or more applications of the client. The client also includes a network driver for storing the one or more networks packets to a queue and communicating the one or more network packets via a network stack of the client. The client further includes an agent for determining the one or more network packets is associated with a first application of the client, and indicating to the network driver a priority of the one or more network packets to place the determined one or more network packets ahead of at least one network packet in the queue associated with a second application of the client.

In one embodiment, the agent of the present invention determines the one or more networks packets of the first application comprises real-time data. The real-time data comprises one of the following: 1) a real-time protocol, 2) a user datagram protocol, and a 3) representation of voice or audio.

In a further embodiment, the agent or the network driver of the present invention prevents at least one network packet of the second application from being communicated via the network stack ahead of the one or more network packets of the first application. In one embodiment, the network driver holds in the queue a network packet associated with the second application, and releases the held network packet upon communication

of the one or more network packets associated with the first application prioritized ahead of the held network packet.

In another embodiment, the present invention, via the mechanism, intercepts the one or more network packets transparently to the one or more applications on the client. In some embodiments, the first application is running in the foreground, and the second application is running in the background. Also, the first application may have a priority higher than the second application of the client. Furthermore, the client may include a configuration mechanism for a user to specify the priority. In some embodiments, the client receives the one or more network packets from a computing device. In other embodiments, the one or more applications provides the one or more network packets for communicating from the client to a computing device.

In an additional embodiment, the network driver includes a Network Driver Interface Specification (NDIS) driver. Also, the network driver may operate in kernel-mode of an operating system of the client. In some cases, the agent operates in user-mode of an operating system of the client. Furthermore, the agent or the network driver includes the mechanism for intercepting one or more network packets of the client.

In yet another aspect, the present invention is related to a method for shielding from a network disruption a session established via a first protocol. The method includes the steps of establishing, via an agent of a client, a session via a first protocol over a network connection between the client and a device. The network connection is associated with a network stack. A first portion of the network stack has one or more layers of the network stack below the layer of the first protocol, and a second portion of the network stack includes a layer for the first protocol and one or more layers of the network stack above the first protocol. The method includes detecting a disruption in the network connection causing the second portion of the network stack to be disestablished, and maintaining, by the agent, the session and the second portion of the network stack during the disruption. The method further includes re-establishing the first portion of the network stack and the network connection while maintaining the session and the second portion of the network stack.

In one embodiment, the method includes continuing the session with the maintained second portion of the network stack and the re-established first portion of the network stack.

In some embodiments, the method also includes dropping, by the first and/or second portion of the network stack, any network packets received during the disruption.

In another embodiment, the device comprises a remote access gateway or another computing device. In some cases, the method includes establishing the session via the first protocol of one of the following: 1) secure socket layer (SSL) protocol, 2) a transport layer security (TLS) protocol, and 3) a tunneling protocol. Additionally, the method of the present invention may include communicating, by the agent, real-time data via the session between the client and the device. The real-time data may include a real-time protocol or the real-time data may represent voice or audio.

In some embodiments, the agent operates in user-mode of an operating system of the client. In one embodiment, the first portion of the network comprises one of a transport control protocol or an internet protocol. In another embodiment, the second portion of the network stack comprises one of 1) an internet protocol, 2) a user datagram protocol, or 3) a voice over internet protocol. Additionally, the client may communicate with the device via a remote display protocol. The remote display protocol may be an Independent Computing Architecture (ICA) protocol or a Remote Desktop Protocol (RDP).

In another embodiment, the method of the present invention is performed transparently to an application of the client communicating via the network connection. In one embodiment, the method includes intercepting, by the agent, transparently to an application of the client one or more network packets associated with the application. In one embodiment, the method includes intercepting, by a network driver associated with the first portion of the stack, transparently to the application on the client one or more network packets associated with the application.

In an additional aspect, the present invention is related to a system for shielding from a network disruption a session established via a first protocol. The system has an agent of a client establishing a session between the client and a device over a network connection via a first protocol. The system includes a network stack having a first portion and a second portion, such as the network stack of the client. The second portion of the network stack comprises a layer for the first protocol and one or more layers of the network stack above the first protocol, and a first portion of the network stack comprises one or more layers of the network stack below the layer of the first protocol. The system includes a detector for detecting a disruption in the network

connection causing the first portion of the network stack to be disestablished. In operation of the system and upon detection of the disruption by the detector, the agent maintains the session and the second portion of the network stack during the disruption. The client re-establishes the first portion of the network stack and the network connection while the agent maintains the session and the second portion of the network stack.

In one embodiment of the system of the present invention, the agent continues the session with the maintained second portion of the network stack and the re-established first portion of the network stack. In some embodiments, the first and/or second portion of the network stack drops any network packets received during the disruption.

In one embodiment, the device of the system is a remote access gateway or another computing device The first protocol used by the system of the present invention may include one of the following: 1) secure socket layer (SSL) protocol, 2) a transport layer security (TLS) protocol, and 3) a tunneling protocol. In another embodiment, the agent of the present invention communicates real-time data via the session between the client and the device. The real-time data may include a real-time protocol, or a representation of voice or audio.

In some embodiments of the system, the agent operates in user-mode of an operating system of the client. In one system embodiment, the first portion of the network comprises a transport control protocol and/or or an internet protocol. In another embodiment, the second portion of the network stack includes one of 1) an internet protocol, 2) a user datagram protocol, or 3) a voice over internet protocol. Additionally, the client may communicate with the device via a remote display protocol, which may be an Independent Computing Architecture (ICA) protocol or a Remote Desktop Protocol (RDP).

In another embodiment, the system of the present invention maintains the second portion of the network stack and re-establishes the first portion of the network stack transparently to an application of the client communicating via the network connection. In one embodiment, the agent intercepts network packets transparently to an application of the client one or more network packets associated with the application. In one embodiment, the system also includes intercepting, by a network driver associated with

the second portion of the stack, transparently to the application on the client one or more network packets associated with the application.

The details of various embodiments of the invention are set forth in the accompanying drawings and the description below.

Brief Description of the Drawings

The foregoing and other objects, aspects, features, and advantages of the invention will become more apparent and may be better understood by referring to the following description taken in conjunction with the accompanying drawings, in which:

Figure 1A is a block diagram depicting an embodiment for practicing the operations of the present invention via a gateway in a network environment;

Figure 1B is a block diagram depicting another embodiment for practicing the operations of the present invention in a peer-to-peer network environment;

Figure 1C is a block diagram depicting an embodiment of a remote access client of the present invention for network communications;

Figures 1D and 1E are block diagrams depicting embodiments of a computing device useful in practicing an embodiment of the present invention;

Figure 2A is a block diagram depicting an embodiment of a peer-to-peer network environment for practicing an embodiment of the technique of the present invention for establishing a peer-to-peer communication route;

Figure 2B is a flow diagram depicting an embodiment of the steps performed to optimize peer-to-peer route optimization technique of the present invention;

Figure 3A is a block diagram depicting an embodiment of network stacks of any of the computing devices of illustrative environments depicted in Figures 1A-1C;

Figure 3B is a flow diagram depicting an embodiment of the steps performed to use a false acknowledgement of receipt of network packets to communicate via a lossless protocol packets constructed for transmission via a lossy protocol;

Figure 3C is a flow diagram depicting an embodiment of the steps performed to communicate via a lossless protocol packets constructed for transmission via a lossy protocol;

Figure 4 is a flow diagram depicting one embodiment of steps performed for adjusting the maximum transmission unit parameter;

Figure 5A is a block diagram depicting an environment of a client for providing client-side application-aware prioritization techniques;

Figure 5B is a flow diagram depicting one embodiment of the steps performed to provide client-side application-aware prioritization;

Figure 6A is a block diagram depicting an environment of an apparatus for shielding a network disruption from a device; and

Figure 6B is a flow diagram depicting one embodiment of the steps performed in to shield network disruption from a device.

Description

Certain illustrative embodiments of the present invention are described below. It is, however, expressly noted that the present invention is not limited to these embodiments, but rather the intention is that additions and modifications to what is expressly described herein also are included within the scope of the invention. Moreover, it is to be understood that the features of the various embodiments described herein are not mutually exclusive and can exist in various combinations and permutations, even if such combinations or permutations are not expressly made herein, without departing from the spirit and scope of the invention.

The illustrative embodiments of the present invention are generally directed towards a remote access architecture for providing peer-to-peer communications and remote access connectivity. In one illustrative embodiment, the remote access architecture of the present provides a method for establishing a direct connection between peer computing devices via a third computing device, such as a gateway. The present invention also provides various techniques for optimizing the peer-to-peer communications established with or without the gateway. The peer-to-peer communications may include real-time communications such as voice over internet protocol (VoIP) signaling and media, video, and other real-time data applications such as web collaboration, screen or desktop sharing, and instant messaging. In addition to establishing a peer-to-peer connection via gateway, the present invention also provides the following techniques to optimize peer-to-peer communications: 1) false acknowledgement of receipt of network packets allowing communications via a lossless protocol packets constructed for transmission via a lossy protocol, 2) payload shifting of

network packets allowing communications via a lossless protocol of packets constructed for transmission via a lossy protocol, 3) reduction of packet fragmentation by adjusting the maximum transmission unit (MTU) parameter, accounting for overhead due to encryption, 4) application-aware prioritization of client-side network communications, and 5) network disruption shielding for reliable and persistent network connectivity and access, such as for mobile clients. These techniques may be practiced in peer-to-peer communications between two clients in some embodiments, or in other embodiments, in communications between a client and a gateway or between one computing device via a gateway to another computing device, such as via an SSL VPN gateway of an illustrative embodiment of the present invention.

In the illustrative embodiments of the present invention, the peer-to-peer route optimization technique determines a more optimal route to a resource a client may be trying to access via a gateway. The client and the resource accessed by the client, such as a server or a peer computer, may have a more direct route than via the gateway. For example, the client and the server may be located near each other but distant from the gateway, and thus, are closer to each other than via the gateway. Furthermore, using a gateway causes at least one additional hop in the end-to-end network communications between the client and the server. Instead of the client and server communicating via the gateway using their virtual private network (VPN) assigned internet protocol (IP) network addresses, the gateway and remote access architecture of the present invention facilitates the client and server communicating to each other via a direct route in a peer-to-peer fashion without using the gateway. In some cases, however, the client and server may not have a direct path between each other as either the client and/or server may be behind a firewall, such as a Network Address Translation (NAT) firewall. The peer-to-peer route optimization techniques and remote access architecture of the present invention also provide techniques for the client and server to communicate directly via traversal of the firewall. As such, the peer-to-peer route optimization techniques of the present invention provides a shorter more optimal route between peer computers than via the gateway.

In the illustrative embodiments of the present invention, the false acknowledgement technique of an embodiment of the present invention enables a packet constructed to be transmitted via a lossy protocol to be communicated via lossless protocol. For example, a real time protocol (RTP) may be implemented over a user

datagram protocol (UDP) for voice over IP (VoIP) communications. A lossy or unreliable protocol, such as UDP, may be used for voice communications because, in some real-time voice applications, it may be more important to get network packets to a recipient on time rather than getting the network packets in order or guaranteeing the delivery of network packets. However, by way of virtual private network and remote access solutions using a secure communication and/or tunneling protocol, such as Secure Socket Layer (SSL) or Transport Layer Security (TLS), a real-time application data constructed to be transmitted via a lossy protocol, such as UDP, may be communicated via a lossless or reliable protocol such as a transport control protocol (TCP). The techniques of the present invention allow a lossy protocol, such as RTP over UDP, to be communicated via a lossless protocol such as TCP, while avoiding one or more of the lossless characteristics of the lossless protocol from being applied to the communication. In the illustrative embodiment of the present invention, this technique communicates a false acknowledgement of receipt of the lossless protocol network packet to the corresponding network stacks to prevent the lossless protocol from executing algorithms that provide for reliability of the protocol. Using this technique, the lossy protocol can be communicated over a lossless protocol, such as via TCP, SSL or via a tunneling protocol of a gateway, for example, to make the communication secure, and have the lossy protocol network packets get to the recipient on time rather than getting to the recipient reliably. In one embodiment, this technique can be used to securely communicate real-time data communications such as VoIP over SSL or TLS between peers or via a gateway.

The illustrative embodiments of the present invention also provide another technique of payload shifting that enables a packet constructed to be transmitted via a lossy protocol to be communicated via lossless protocol. A first computing device receives a first packet to be transmitted using an unreliable transport protocol, and creates a first TCP packet including a first payload of the received first packet. The first TCP packet is created with a TCP header having information associated with a TCP connection established between the first and a second computing device. The first TCP packet is transmitted to the second computing device. A second packet to be transmitted using an unreliable transport protocol is received by the first computing, which in turn creates a second TCP packet including the payload of the received second packet but with the TCP header information of the first TCP packet. The second TCP packet is

transmitted to the second computing device before receiving an acknowledgement of the receipt of the first TCP packet from the second device. As such, the payload shifting technique communicates multiple unreliable transport protocol payloads under a TCP header until an acknowledgement of receipt is received.

In the illustrative embodiments of the present invention, the maximum transmission unit adjustment technique reduces the reported size of the maximum transmission unit (MTU) parameter of a network stack of a client to take into consideration the effect of the network packet size due to encryption of a payload. Encryption of the payload of a network packet increases the size of the network packet communicated to or by the client, and may cause a network packet to be fragmented. For example, a server may communicate to the client a network packet via an SSL gateway to the client. Although the server sends a network packet that should meet the MTU size the network stack of the client can handle, the encryption provided by the gateway increases the size of the network packet before it reaches the client. This may cause the network packet communicated from the server to the client via the gateway to be fragmented as the increased packet size from encryption may be too large for the MTU size of the client. The technique of the present invention adjusts the client's reported MTU size to report a smaller size to take in account for the overhead of the encryption. This technique reduces network fragmentation or otherwise prevents non-optimal fragmentation.

In the illustrative embodiments of the present invention, the prioritization technique provides for client-side and application-aware prioritization of network communications. That is, the remote access client of the present invention manages and controls network communication prioritizations on the client. The prioritizations are based on priorities of the application on the client. The remote access client transparently intercepts network communications associated with applications executing on the client, detects the network communication is associated with an application, and determines priorities for the network communications based on a priority for the application. For example, an application on the client may be communicating real-time data communications, such as VoIP, to a peer client or via a gateway. The remote access client may intercept a network packet, and detect, for example, the network packet contains real-time data or is from a VoIP application. The remote access client may indicate a priority for this network packet such that the network packet may be

communicated ahead of non-real-time data communications or ahead of network communications from other applications. As such, the prioritization techniques of the present invention may improve or increase the performance, operational characteristics, and user experience on the client based on the applications running on the client.

In the illustrative embodiments of the present invention, the network disruption shielding technique provides a persistent and reliable connection of a client to a network, such as a peer-to-peer communication session or a connection to a gateway. For example, a mobile client, such as a laptop with a software based IP telephone, may connect to a network for VoIP communications. A temporary disruption in a network connection may occur when the mobile client roams between different access points in the same network, or when the client switches between networks (*e.g.*, from a wired network to a wireless network). This disrupts the network service to the client and may drop the VoIP telephone call. Additionally, as the mobile client moves between access points, the mobile client may obtain a different IP network address, such as from a new Dynamic Host Configuration Protocol (DHCP) lease. This can also cause network connectivity and VoIP telephone communication disruption. The techniques of the present invention detects a disruption in the network and shields a portion of the network stack from the network disruption. The shielded portion of the network stack is maintained while the other portion of the network stack is reestablished and reconnected to the network. Once the network is available, the present invention continues with the client's network communications. In some embodiments, the network communications are queued during the network disruption and transmitted once the network is available. In other embodiments, such as for real-time data communications, network packets are dropped during the disruption to prevent the queuing of network packets that may cause latency in the real-time communication, such as VoIP telephone call.

Although the illustrative embodiments of the present invention may be generally described in connection with an internet protocol (IP) based protocol, such as a transport control protocol (TCP) or user datagram protocol (UDP), the techniques of the present invention may be used in any other types of networking environments with other networking protocols, such as any Internetwork Packet Exchange (IPX) protocol based networks using a Sequenced Packet Exchange (SPX) protocol. Also, although a lossy or unreliable protocol such as UDP and a lossless or reliable protocol such as TCP may be used for illustrating an embodiment of the present invention, any lossless/reliable and

lossy/unreliable protocol as known to those ordinarily skilled in the art may be used in practicing the operations of the present invention described herein. Furthermore, although some of the illustrative embodiments of the present invention may be described below in relation to real-time data communications, such as VoIP, the techniques of the present invention may be applied for non-real-time data communications as one ordinarily skilled in the art will also recognize and appreciate.

Additionally, at times, the illustrative embodiments of the present invention may be described in regards to peer-to-peer communications. In one aspect, a peer-to-peer model comprises a type of network in which any computer can act as both a server by providing access to its resources to other computers, and can act as a client by accessing shared resources from other computers. Although in another aspect, a peer-to-peer model may not comprise a notion of a client and a server, a client and a server may provide peer-to-peer communications as well as client to client, server to server, or a client/server to a computing device such as a gateway. In an additional aspect, peer-to-peer communications comprises a process whereby computers can exchange information between each other directly without the assistance of a third party network or a device, such as a gateway. Although peer-to-peer communications may be generally described as direct communication between computers, there may be other network elements between the computing devices to facilitate the transmission and/or communication, such as for example, a network hub.

Furthermore, although the illustrative embodiments of the present invention may be described peer-to-peer, point-to-point, client to server, or otherwise, one ordinarily skilled in the art will recognize and appreciate that the present invention may be practiced between computing devices in any manner via any network topology, and that any reference to peer-to-peer, client/server, or otherwise is not intended to limit the present invention in any way.

In one aspect, the present invention is related to a remote access architecture having a remote access client for communicating to a network via a gateway or peer-to-peer to another remote access client or another computing device. The remote access architecture of the present invention provides systems and methods for securely communicating network traffic transmitted between a private network behind a gateway to a client on an external network, such as public network. The remote access architecture of the present invention enables separation of the client from the private

network by providing network address translation (NAT) functionality on the gateway. A VPN gateway that uses Network Address Translation (NAT(provides masquerading of IP addresses of a client to shield the private network from direct layer-2 access by the client.

Referring now to Figure 1A, the environment 180 depicts a system for deploying the remote access architecture in an illustrative embodiment of the present invention. In brief overview, the environment 180 includes multiple computing devices 102a-102c (herein also referred to as clients 105a-105c) connected to a network 104 via one or more network connections 341a-341n. One or more of the clients 105a-105n may connect to a server 102a, a server farm 102e, or a peer computing devices 102d via a gateway 350.

Each client 105a-105n includes a remote access client 120a-120c, which will be described in more details in connection with Figure 1C, and one or more applications 338a-338n. Each of the clients 105a-105n communicate over the network 104 to the gateway 340 via a tunneling or gateway connections 341a-341n using any type and/or form of suitable tunneling or gateway protocols. In some embodiments, the gateway connections 341a-341n may be used for communicating securely, such as via encapsulating and encryption, or otherwise may use any other protocols, such as any real-time, lossless, or lossy protocol. In other embodiments, the gateway 340 provides a virtual private network connection between one or more of the clients 105a-105n and any of the computing devices 102d-102n.

The client 105 can be any type and/or form of computing device 102 that can run one or more applications 338 that access a network, such as network 104. The application 338 can be any type and/or form of application such as any type and/or form of web browser, web-based client, client-server application, a thin-client computing client, an ActiveX control, or a Java applet, or any other type and/or form of executable instructions capable of executing on client 105 or communicating via a network 104. The application 338 can use any type of protocol and it can be, for example, an HTTP client, an FTP client, an Oscar client, or a Telnet client. In some embodiments, the application 338 uses a remote display or presentation level protocol. In one embodiment, the application 338 is an ICA client, developed by Citrix Systems, Inc. of Fort Lauderdale, Florida. In other embodiments, the application 338 includes a Remote Desktop (RDP) client, developed by Microsoft Corporation of Redmond, Washington.

In other embodiments, the application 338 comprises any type of software related to VoIP communications, such as a soft IP telephone. In further embodiments, the application 338 comprises any application related to real-time data communications, such as applications for streaming video and/or audio.

The clients 105a-105n may access any of the resources provided via computing devices 102d-102n which may be on the same network 104, or which may be on a separate network, such as a private network. In some embodiments, computing devices 102a-102n may be on a network disconnected and not routable from the network 104 of the clients 105a-105n. In one embodiment, any of the clients 105a-105n may communicate with a peer computing device 102d having a remote access client 102n and application 338d. For example, the application 338d may comprise a portion of a client/server or distributed application corresponding to any of the applications 338a-338c on clients 105a-105n. In some embodiments, any of the remote access clients 120a-120n may communicate with the remote access client 120n via the gateway 340.

In another embodiment, any of the clients 105a may communicate via the gateway 340 to a server 102e running an application 338e, which for example, may be an application server providing email services such as Microsoft Exchange manufactured by the Microsoft Corporation of Redmond, Washington, a web or Internet server, or a desktop sharing server, or a collaboration server. In some embodiments, any of the application 338e may comprise any type of hosted service, such as GoToMeeting.com provided by Citrix Systems, Inc. of Ft. Lauderdale, Florida, WebEx.com provided by WebEx, Inc. of Santa Clara, California, or LiveMeeting.com provided by Microsoft Corporation of Redmond, Washington.

In another embodiment, any of the clients 105a may communicate via the gateway 340 to a server farm 102n or server network, which is a logical group of one or more servers that are administered as a single entity. The server farm 102n may be running one or more applications 338N, such as an application 338f providing a thin-client computing or remote display presentation application. In one embodiment, the server 102e or server farm 102n executes as an application 338e-338n, any portion of the Citrix Access Suite™ by Citrix Systems, Inc., such as the MetaFrame or Citrix Presentation Server™, and/or any of the Microsoft Windows Terminal Services manufactured by the Microsoft Corporation.

Still referring to Figure 1A, the gateway 340 may comprise any type and/or form of gateway, such as a remote access server, that may be used to connect one or more computing devices on one network to other networks. In another aspect, the gateway 340 may be used to provide a virtual private network connection to give a client 105a-105c access to a private network. In a further aspect, the gateway 340 may be a hardware or software set-up that translates between two dissimilar protocols or disjoint or disconnected networks or systems. The gateway 340 may comprise a specialized hardware or networking device, or may be a computing device configured to act as a gateway. As such, the gateway 340 may comprise software, hardware, or any combination of software and hardware. In one embodiment, the client 105 and the gateway 340 communicate via any type and/or form of gateway or tunneling protocol 341a-341n, such as SSL or TLS, or the Citrix Gateway Protocol manufactured by Citrix Systems, Inc. of Ft. Lauderdale, Florida.

In some embodiments, the gateway 340 may decrypt encrypted packets received from a client 105a-105c, and may encrypt packets communicated to a client 105a-105n. The gateway 340 may be used to protect a private network, such as network 104. In some embodiments, the gateway 340 associates a client 105a-105c with a private IP address or an IP address of the private network. In one of these embodiments, when the gateway 340 receives a packet from the client 105a-105c, the gateway 340 transforms the IP address of the packet to the IP address associated with the client 105a-105c for the private network. In some embodiments, the gateway 340 may apply access control policies to network traffic to and/or from a client 105a-105c. For example, access controls policies may be applied to a packet received from the client prior to routing the packet to a final destination.

In one embodiment of the gateway 340, once a frame enters the gateway 340 via an SSL tunnel, the packet and its payload are dispatched via callbacks into a handlers executing in user mode, which provide functionality for SSL decryption. In another embodiment, openSSL may be used. In other embodiments, a hardware accelerator is used. In a further embodiment, the gateway 340 comprises one or more blades for providing remote access. Once the packet is decrypted, it is injected into an HTTP network stack where headers are assembled and passed on to the remote access blade. In a remote access blade, a packet is classified by the type of data contained within the packet. In one embodiment, the packet contains an HTTP header requesting login and

registration. In another embodiment, the packet seeks TCP/UDP/RAW/OTHER connection establishment. In still another embodiment, the packet contains connection-specific data. In yet another embodiment, the packet contains a special feature request such as collaboration with other users, fetching of user directory and presence or requesting telephony functionality such as conferencing and web cast. The remote access module dispatches the packet appropriately to the corresponding sub handler. For example, the client 105 may request that a connection be set up to a specific machine on the private network behind the gateway 340. The remote access module may consult with the access control module and if a positive response is returned, the remote access module may grant the request. In some embodiments, the remote access module 120 may grant the request by injecting subsequent frames on the private network using a frame forwarding module utilizing NAT/PAT to correlate incoming frames to corresponding SSL tunnels 341a-341n to a client 105a-105c.

The network 104 as illustrated in Figure 1A can be any type of network. The network 104 can be a local-area network (LAN), such as a company Intranet, a metropolitan area network (MAN), or a wide area network (WAN), such as the Internet or the World Wide Web. The topology of the network 104 may be a bus, star, or ring network topology. The network 104 and network topology may be of any such network or network topology capable of supporting the operations of the present invention described herein. The client 108 and gateway 340 can connect to one or more networks 104 through a variety of connections including standard telephone lines, LAN or WAN links (e.g., T1, T3, 56 kb, X.25, SNA, DECNET), broadband connections (ISDN, Frame Relay, ATM, Gigabit Ethernet, Ethernet-over-SONET), and wireless connections or any combination thereof. Connections can be established using a variety of communication protocols (e.g., TCP/IP, IPX, SPX, NetBIOS, Ethernet, ARCNET, Fiber Distributed Data Interface (FDDI), RS232, IEEE 802.11, IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, and direct asynchronous connections).

In one embodiment of the present invention, the gateway 340 illustrated in Figure 1A is used to facilitate a direct peer-to-peer connection between computing devices 102a-102n. For example, client 105a may establish a tunneling session with the gateway 340 to access the peer computing device 102d. The gateway 340 negotiates with the remote access client 120a of client 105a and the remote access client 120n of computing device 102d to enable the client 105a to directly connect to the computing

device 102d without traversing the gateway 340. Once the network connection between the client 105a and computing device 102d is established, the client 105a can communicate in a peer-to-peer manner with computing device 102d. The gateway 340 of the present invention can facilitate a direct peer-to-peer connection between any of the computing devices 102a-102n illustrated in the environment 180. In one embodiment, the gateway 340 can facilitate a peer-to-peer connection between any of the clients 105a-105n, for example between client 105a and client 105b or between client 105b and client 105c. In another embodiment, the gateway 340 facilitates a peer-to-peer connection between computing devices 102d-120n, for example, between computing device 102d and server 102e or server farm 102n. In other embodiments, the gateway 340 facilitates a peer-to-peer connection between one of the clients 105a-105n and one of the computing devices 102d-102n. The techniques of facilitating a peer-to-peer connection via the gateway 340 will be discussed in more detail below in conjunction with Figures 2A and 2B.

Referring now to Figure 1B, the remote access client 120 of the present invention may be used in an illustrative embodiment of a peer-to-peer connection without a gateway 304. For example, the gateway 340 may facilitate a peer-to-peer connection between any of the computing device 102a-102n illustrated in Figure 1, and thereafter the computing devices 102a-102n communicate directly to each other in a peer-to-peer manner. In other embodiments, any computing device 102a may communicate directly to another computing device 102b or 102c via a network 104 without a gateway 340 facilitating the connection.

In brief overview of Figure 1B, the remote access client 120a may be deployed on a client 102a running one or more application 338a. The computing device 102a may connect over the network 104 to computing device 102b and/or computing device 102c. Computing device 102b may be a peer or client computing device also comprising a remote access client 120b. In some embodiments, remote access client 120a and 120b may communicate with each other via network 104, and may work in conjunction with each other for application 338a to communicate to application 338b, such as for a web-based or client/server application. In other embodiments, the remote access client 120a may communicate with computing device 120c which may be a server that does not execute a remote access client 120.

Figure 1C depicts a block diagram illustrating a system having a remote access client 120 for routing network packets from a client 105 to a network 104. In brief overview, the system includes a computing device102 (herein also referred to as a client 105) having an operating system that includes a user mode 332, also referred to as an application or user space, and a kernel-mode 334, which may be also referred to as the kernel or system level space. The client 105 runs an agent 326 that in one embodiment, may run in user-mode 332. The client 105 also runs a filter 322, which may, in one embodiment, execute in kernel-mode or the kernel space 334. In one embodiment, the filter 322 and the agent 326 form the remote access client 120 for routing packets via a network, or for otherwise providing remote access connectivity in accordance with the operations of the present invention described herein. The remote access client 120, or any portion thereof, such as the agent 326 or the filter 322, may execute in user-mode 332 or kernel-mode 334.

The client 105 may also have a network stack 310, which may comprise one or more network layers, such as any networks layers of the Open Systems Interconnection (OSI) communications model as those skilled in the art will recognize and appreciate. The network stack 310 may comprise one or more protocols, such as the TCP/IP protocol over Ethernet or a wireless protocol, such as IEEE 802.11, as those skilled in the art will recognize and appreciate. Furthermore, the network stack 310 may include one or more network drivers supporting the one or more layers, such as a TCP driver or a network layer driver. The network drivers may be included as part of the operating system of the computing device 102 or as part of any network interface cards or other network access components of the computing device 102. Additionally, any of the network drivers of the network stack 310 may be customized, modified or adapted to provide a custom or modified portion of the network stack 310 in support of any of the techniques of the present invention described herein. Additionally, some portions of the network stack 310 may operate in kernel-mode 334 while other portions run in user-mode 332, such as an application layer of the network stack 310.

The filter 322 may include a packet capturing mechanism 365, and the filter 322 and/or packet capturing mechanism 365 may comprise a network driver, such as a network driver operating at any layer, or portion thereof, of a network stack 310 of the client 105. The filter 322 and/or the packet capture mechanism 365 may comprise a driver complying with the Network Driver Interface Specification (NDIS), or a NDIS

driver. In another embodiment, the filter 322 and/or the packet capture mechanism 365 may comprise a min-filter or a mini-port driver. The packet capture mechanism 365 may also in some embodiments operate in kernel mode 334. Although the packet capture mechanism 365 is illustrated as part of the filter 322, the packet capture mechanism 365 may be separate from the filter 322. Additionally, the filter 322 and the packet capture mechanism 365 may operate at different layers, or portions thereof, of a network stack of the client 105.

The filter 322 may use a filter table for filtering packets. The filtering table is used to determine what action to take against packets, such as packets intercepted by the packet capture mechanism 365. The filter 322 can inspect the contents of the packets, such as routing information, to determine the action to take based on the filtering table. In some embodiments, the filter 322 may drop or accept the network packets depending on their content. In other embodiments, the filter 322 may route the network packets to the agent 326 based on the packets content and/or the filtering table. The filter table may also be used to ensure that unwanted packets are discarded. The filter 322 may be used to deny access to particular protocols or to prevent unauthorized access from remote computers by discarding packets to specified destination addresses.

In some embodiments, the filtering table includes information about a private network. In other embodiments, a filter 322 on a client computing device 102 receives the filtering table. In one of these embodiments, the filter 322 receives the filtering table from an application 338 or an agent 326 on the computing device 102. In another of these embodiments, the filter 322 receives configuration settings from the agent 326 and stores the configuration settings in a filtering table.

The packet capture mechanism 365 may intercept any of the network traffic of the client 105, such as network packets associated with the application 338. In some embodiments, the packet capture mechanism 365 intercepts network traffic transparently to the application 338, the agent 326, the gateway 340, or to any portion of the network stack 310 of the client 105, such as any other driver or layer operating at a layer above or below the layer the packet capture mechanism 365 operates. In this manner, the present invention can be used with and support any of the techniques described herein and for any application and any protocol used by the application. In one embodiment, the packet capture mechanism 365 intercepts outbound packet traffic, such as any network traffic communicated via network 104 and/or gateway 340. The packet capture

mechanism 365 may forward the packets to the agent 325 or a frame monitor mechanism 360 of the agent 326. In some embodiments, the filter 322 communicates with the agent 326 via asynchronous I/O control messages. In one of these embodiments, the packet capture mechanism 365 may forward packets addressed to a private network behind a gateway 340 via asynchronous I/O control messages. In other embodiments, the filter 322 communicates with the agent 326 running in the user space 334 via UDP packets. In one embodiment, the filter 322 receives configuration settings from the agent 326 driver via asynchronous I/O control messages. The configuration settings may include information regarding which networks, protocols, or types of packets to filter. In one embodiment, the filter 322 stores the configuration settings in a filtering table. In another embodiment, the filter 322 receives a filtering table including the configuration settings.

In one embodiment, the filter 322 intercepts all outbound packets of the client 105 for inspection. For example, in some embodiments, the filter intercepts a packet generated by an application 338 executing in user-mode 332 for transmission by the client 105. If the packet satisfies a condition listed in the filtering table, the filter 322 may transmit the packet to the agent 326 and not to the original destination of the packet. The filter 322 may use an asynchronous I/O control message to forward the packet to the agent 326. The filter 322 may transmit the packet to the agent 326 in accordance with or responsive to a routing table .

In some embodiments, the agent 326 and the filter 322 communicate via an IOCTL application programming interface (API), such as any IOCTL libraries and function calls provided by the Microsoft Windows family of operating systems. In other embodiments, the IOCTL based interface between the agent 326 and the filter 322 may be provided by any portion of the operating system running on the client 105. Although discussed in terms of I/O control message and the IOCTL interface, the agent 326 and the filter 322 may communicate via any suitable mechanism and/or means.

The kernel 334 of client 105 may include an NDIS interface. In some embodiments, the NDIS interface includes a plurality of intermediate filters. In one embodiment, a packet passes through the NDIS interface and may be inspected by the plurality of intermediate filters. Although the filter 322 may be provided as an NDIS driver, the filter 322 may also be a process or other set or type of executable instructions executing in the kernel 334.

The agent 326 of the present invention may execute in the application space 332 or user-mode on the client 105. In other embodiments, the agent 326 operates in kernel-mode 334. In some embodiments, the agent 326 provides functionality for receiving packets from the filter 322. In other embodiments, the agent 326 provides functionality for applying a policy to a received packet. In still other embodiments, the agent 326 provides functionality for managing an SSL tunnel to the gateway 340. In yet other embodiments, the agent 326 provides functionality for encrypting and transmitting a packet to the gateway 340. The agent 326 may include frame monitor mechanism 360. The frame monitor 360 may include policies and logic for applying a policy to a received packet. The agent 326 may transmit a packet to a gateway 340 responsive to a policy-based determination made by the frame monitor 360.

In some embodiments, the frame monitor 360 may apply a policy to determine a condition of the client 105, or endpoint, at the time of transmission of the packet. In other embodiments, the frame monitor 360 may identify an application 338 that generated the packet. In some of these embodiments, the frame monitor 360 may make a policy-based determination to transmit the packet to the gateway 340 responsive to the identified application 338. In another embodiment, the frame monitor 360 may perform a checksum on the packet to verify that the identified application actually generated the packet.

In other embodiments, the packet capture mechanism 365 may be included in the agent 326 instead of or in addition to the filter 322. As such, the agent 326 may intercept network traffic. The packet capture mechanism 365 may use any hooking application programming interface (API) to intercept, hook, or otherwise obtain inbound and/or outbound packets of the client 105, such as the network traffic associated with application 338.

In one embodiment, a TCP connection is initiated by an application 338 executing on the client 105 for transmission of IP packets to a target computing device, such as computing device 102c of Figure 1B or the gateway 340 in Figure 1A. The remote access client 120 may intercept or capture the IP packets generated by the application 338. The remote access client 120 may send a TCP acknowledgement packet to the application 338 and terminate the TCP connection initiated by the application 338. Then, the remote access client 120 creates a second TCP connection to the second computing device 102c or the gateway 340 and transmits the captured IP

packets via the second TCP connection. In some embodiments, the remote access client 120 may store a captured IP packet in a buffer. In these embodiments, the remote access client 120 may transmit the buffered IP packets via the second TCP connection to the second computing device 102c. Storing the captured IP packets in a buffer enables preservation of the packets in the event of a disruption in the network connection.

In one embodiment, upon receipt of the captured IP packets, the gateway 340 may create a third TCP connection between the gateway 340 and the targeted computing device 102d, such as in Figure 1A. The gateway 340 may maintain a port-mapped Network Address Translation (NAT) table, enabling the gateway 340 to transmit response packets from the target computing device 102d to the port monitored by the application 338 that originally generated the IP packet on the client 105. Because the client 105 communicates only with a public network address of the gateway 3400, the client 105 is unaware of the network address of the target computing device 102d, increasing security to the network on which the target computing device 102d resides. Similarly, since the gateway 340 originates the TCP connection to the target computing device 102d, the target computing device 102d does not receive the address information of the client 105, protecting the client 105 and the network on which it resides. Additionally, since the gateway 340 receives the IP packets, the gateway 340 may make a determination responsive to a policy or security check as to whether or not to transmit the IP packets to the target computing device 102d, further increasing protection to the network on which the target computing device 102d resides.

In one embodiment, the present invention provides a method for securing a packet transmitted from a private, secured network behind a gateway 340 to a client 105 on an external network 104. The invention enables separation of the client 105 from the private network by providing network address translation (NAT) functionality on the gateway 340. A VPN gateway that uses NAT provides masquerading of IP addresses of a client 105 to shield the private network from direct layer-2 access by the client 105.

In one aspect, any portion of the remote access client 120, such as the agent 326, frame monitor 360, the filter 322, and packet capture mechanism 365, or any portion thereof may comprise software, hardware, such as an ASIC or an FPGA, or any

combination of software and/or hardware. In some embodiments, portions of the remote access client 120 may be provided via one or more blades on the client 105.

Although the remote access client 120 is illustrated with multiple components, such as an agent 326 and a filter 322, one ordinarily skilled in the art will recognize and appreciate that the operations and functionality of the remote access client 120 described herein may be practiced in a single mechanism or single component. For example, in some embodiments, the operations and functionality of the remote access client 120 may be included within an application 338. In one embodiment for example, the functionality and operations of the remote access client 120 may be provided just as an agent 326, and in another embodiment, just as a network driver, such as the filter 322.

In some embodiments, the remote access client 120, or any portion thereof, such as the agent 326, frame monitor 360, the filter 322, and packet capture mechanism 365 may comprise an application, module, service, computer program, software component, web service, web component, library, function, process, task, thread, or any other type and/or form of executable instruction which is designed to and capable of executing the functionality of the present invention as described herein, and which may operate in any portion or combination of user-mode 332 and/or kernel-mode 334.

As illustrated in Figures 1A-1C, the remote access client 120 of the present invention may be deployed and used in a variety of ways to communicate and provided remote access over a network to other computing devices, such as via a gateway 340 or directly between peer computing devices. In these variety of environments, the remote access client 120 may be used to practice one or more of the optimization techniques of the present invention as described in more detail below. For example, the remote access client 120 may be used for optimizing any real-time data communications, such as VoIP, desktop sharing, or web conferencing in any of the illustrative environments of Figures 1A-1C.

In the illustrative embodiments of Figures 1A-1C, the computing devices 102a-120n, such as for any of the clients 105, server, or the gateway 340, may be provided as any type and/or form of computing device such as a personal computer or computer server of the sort manufactured by the Hewlett-Packard Corporation of Palo Alto, California or the Dell Corporation of Round Rock, TX. Figures 1D and 1E depict block diagrams of a computing device 102 useful for practicing an embodiment of the present invention. As shown in Figures 1D and 1E, each computing device 102 includes a

central processing unit 102, and a main memory unit 104. As shown in Figure 1D, a typical computing device 102 may include a visual display device 124, a keyboard 126 and/or a pointing device 127, such as a mouse. Each computing device 102 may also include additional optional elements, such as one or more input/output devices 130a-130b (generally referred to using reference numeral 130), and a cache memory 140 in communication with the central processing unit 102.

The central processing unit 102 is any logic circuitry that responds to and processes instructions fetched from the main memory unit 104. In many embodiments, the central processing unit is provided by a microprocessor unit, such as: the 8088, the 80286, the 80386, the 80486, the Pentium, Pentium Pro, the Pentium II, the Celeron, or the Xeon processor, all of which are manufactured by Intel Corporation of Mountain View, California; the 68000, the 68010, the 68020, the 68030, the 68040, the PowerPC 601, the PowerPC604, the PowerPC604e, the MPC603e, the MPC603ei, the MPC603ev, the MPC603r, the MPC603p, the MPC740, the MPC745, the MPC750, the MPC755, the MPC7400, the MPC7410, the MPC7441, the MPC7445, the MPC7447, the MPC7450, the MPC7451, the MPC7455, or the MPC7457 processor, all of which are manufactured by Motorola Corporation of Schaumburg, Illinois; the Crusoe TM5800, the Crusoe TM5600, the Crusoe TM5500, the Crusoe TM5400, the Efficeon TM8600, the Efficeon TM8300, or the Efficeon TM8620 processor, manufactured by Transmeta Corporation of Santa Clara, California; the RS/6000 processor, the RS64, the RS 64 II, the P2SC, the POWER3, the RS64 III, the POWER3-II, the RS 64 IV, the POWER4, the POWER4+, the POWER5, or the POWER6 processor, all of which are manufactured by International Business Machines of White Plains, New York; or the AMD Opteron, the AMD Athlon 64 FX, the AMD Athlon, or the AMD Duron processor, manufactured by Advanced Micro Devices of Sunnyvale, California. The computing device 102 may be based on any of the above described processors, or any other processor capable of operating as described herein.

Main memory unit 104 may be one or more memory chips capable of storing data and allowing any storage location to be directly accessed by the microprocessor 100, such as Static random access memory (SRAM), Burst SRAM or SynchBurst SRAM (BSRAM), Dynamic random access memory (DRAM), Fast Page Mode DRAM (FPM DRAM), Enhanced DRAM (EDRAM), Extended Data Output RAM (EDO RAM), Extended Data Output DRAM (EDO DRAM), Burst Extended Data Output

DRAM (BEDO DRAM), Enhanced DRAM (EDRAM), synchronous DRAM (SDRAM), JEDEC SRAM, PC100 SDRAM, Double Data Rate SDRAM (DDR SDRAM), Enhanced SDRAM (ESDRAM), SyncLink DRAM (SLDRAM), Direct Rambus DRAM (DRDRAM), or Ferroelectric RAM (FRAM). The main memory 104 may be based on any of the above described memory chips, or any other available memory chips capable of operating as described herein. In the embodiment shown in Figure 1E, the processor 100 communicates with main memory 104 via a system bus 150 (described in more detail below). Figure 1E depicts an embodiment of a computing device 102 in which the processor communicates directly with main memory 104 via a memory port 103. For example, in Figure 1E the main memory 104 may be DRDRAM.

Figures 1D and 1E depict embodiments in which the main processor 100 communicates directly with cache memory 140 via a secondary bus, sometimes referred to as a backside bus. In other embodiments, the main processor 100 communicates with cache memory 140 using the system bus 150. Cache memory 140 typically has a faster response time than main memory 104 and is typically provided by SRAM, BSRAM, or EDRAM.

In the embodiment shown in Figure 1D, the processor 100 communicates with various I/O devices 130 via a local system bus 150. Various busses may be used to connect the central processing unit 102 to any of the I/O devices 130, including a VESA VL bus, an ISA bus, an EISA bus, a MicroChannel Architecture (MCA) bus, a PCI bus, a PCI-X bus, a PCI-Express bus, or a NuBus. For embodiments in which the I/O device is a video display 124, the processor 100 may use an Advanced Graphics Port (AGP) to communicate with the display 124. Figure 1E depicts an embodiment of a computer 102 in which the main processor 100 communicates directly with I/O device 130b via HyperTransport, Rapid I/O, or InfiniBand. Figure 1E also depicts an embodiment in which local busses and direct communication are mixed: the processor 100 communicates with I/O device 130a using a local interconnect bus while communicating with I/O device 130b directly.

The computing device 102 may support any suitable installation device 116, such as a floppy disk drive for receiving floppy disks such as 3.5-inch, 5.25-inch disks or ZIP disks, a CD-ROM drive, a CD-R/RW drive, a DVD-ROM drive, tape drives of various formats, USB device, hard-drive or any other device suitable for installing software and programs such as the remote access client software 120 related to the present invention.

The computing device 102 may further comprise a storage device 128, such as one or more hard disk drives or redundant arrays of independent disks, for storing an operating system and other related software, and for storing application software programs such as any program related to the remote access client 120 of the present invention. Optionally, any of the installation devices 118 could also be used as the storage device 128. Additionally, the operating system and the proxy software 120 can be run from a bootable medium, for example, a bootable CD, such as KNOPPIX®, a bootable CD for GNU/Linux that is available as a GNU/Linux distribution from knoppix.net.

Furthermore, the computing device 102 may include a network interface 118 to interface to a Local Area Network (LAN), Wide Area Network (WAN) or the Internet through a variety of connections including, but not limited to, standard telephone lines, LAN or WAN links (*e.g.*, 802.11, T1, T3, 56kb, X.25), broadband connections (*e.g.*, ISDN, Frame Relay, ATM), wireless connections, or some combination of any or all of the above. The network interface 118 may comprise a built-in network adapter, network interface card, PCMCIA network card, card bus network adapter, wireless network adapter, USB network adapter, modem or any other device suitable for interfacing the computing device 102 to any type of network capable of communication and performing the operations described herein.

A wide variety of I/O devices 130a-130n may be present in the computing device 102. Input devices include keyboards, mice, trackpads, trackballs, microphones, and drawing tablets. Output devices include video displays, speakers, inkjet printers, laser printers, and dye-sublimation printers. The I/O devices may be controlled by an I/O controller 123 as shown in Figure 1D. The I/O controller may control one or more I/O devices such as a keyboard 126 and a pointing device 127, e.g., a mouse or optical pen. Furthermore, an I/O device may also provide storage 128 and/or an installation medium 118 for the computing device 102. In still other embodiments, the computing device 102 may provide USB connections to receive handheld USB storage devices such as the USB Flash Drive line of devices manufactured by Twintech Industry, Inc. of Los Alamitos, California.

In further embodiments, an I/O device 130 may be a bridge 170 between the system bus 150 and an external communication bus, such as a USB bus, an Apple Desktop Bus, an RS-232 serial connection, a SCSI bus, a FireWire bus, a FireWire 800

bus, an Ethernet bus, an AppleTalk bus, a Gigabit Ethernet bus, an Asynchronous Transfer Mode bus, a HIPPI bus, a Super HIPPI bus, a SerialPlus bus, a SCI/LAMP bus, a FibreChannel bus, or a Serial Attached small computer system interface bus.

A computing device 102 of the sort depicted in Figures 1D and 1E typically operate under the control of operating systems, which control scheduling of tasks and access to system resources. The computing device 102 can be running any operating system such as any of the versions of the Microsoft® Windows operating systems, the different releases of the Unix and Linux operating systems, any version of the MacOS® for Macintosh computers, any embedded operating system, any real-time operating system, any open source operating system, any proprietary operating system, any operating systems for mobile computing devices, or any other operating system capable of running on the computing device and performing the operations described herein. Typical operating systems include: WINDOWS 3.x, WINDOWS 95, WINDOWS 98, WINDOWS 2000, WINDOWS NT 3.51, WINDOWS NT 4.0, WINDOWS CE, and WINDOWS XP, all of which are manufactured by Microsoft Corporation of Redmond, Washington; MacOS, manufactured by Apple Computer of Cupertino, California; OS/2, manufactured by International Business Machines of Armonk, New York; and Linux, a freely-available operating system distributed by Caldera Corp. of Salt Lake City, Utah, Java or Unix, among others.

In other embodiments, the computing device 102 may have different processors, operating systems, and input devices consistent with the device. For example, in one embodiment the computer 102 is a Zire 71 personal digital assistant manufactured by Palm, Inc. In this embodiment, the Zire 71 operated under the control of the PalmOS operating system and includes a stylus input device as well as a five-way navigator device.

Moreover, the computing device 102 can be any workstation, desktop computer, laptop or notebook computer, server, handheld computer, mobile telephone, any other computer, or other form of computing or telecommunications device that is capable of communication and that has sufficient processor power and memory capacity to perform the operations described herein.

In one aspect, the present invention is related to providing various techniques for optimizing communications between computing devices, such as depicted in any of the illustrative environments Figures 1A-1C. The present invention provides the following

techniques, which may be practiced stand-alone or in any combination: 1) peer-to-peer route optimization, 2) communications via a lossless protocol of packets constructed for transmission via a lossy protocol, 3) reducing network fragmentation by adjusting maximum transmission unit (MTU) adjustment to account for encryption, 4) client-side application-aware network communication prioritization, and 5) shielding a device from network disruption. The peer-to-peer route optimization technique will be discussed in conjunction with Figures 2A and 2B, techniques for communications via a lossless protocol of packets constructed for transmission via a lossy protocol are discussed in conjunction with Figures 3A and 3B, the MTU adjustment technique in conjunction with Figure 4, the client-side application-aware prioritization technique in conjunction with Figures 5A and 5B, and the network disruption shielding in conjunction with Figures 6A and 6B.

In one aspect, the present invention is related to providing a peer-to-peer route optimization technique between a first computing device accessing a second computing device via a gateway, such as the gateway 340 illustrated in Figure 1A. The peer-to-peer routing techniques provides a more optimal and direct communication between computing devices establishing or attempting to establish a communication session via a gateway. The illustrative method 260 of an embodiment of the present invention will be discussed in view of the illustrative environment 200 of Figure 2A. In brief overview, the environment 200 includes a gateway 340 providing remote access connectivity to a private network, such as a network with IP address ranges 10.10.10.XXX. The gateway 340 in association with the private network may have assigned an IP address of 10.10.10.2 for communications on the private network. This private network may include a server 102c. Also, the private network comprises a telecommunication device 210c, such as any type and/or form of VoIP telephone. The telecommunication device 210c is assigned IP address 10.10.10.100 on the private network.

In one embodiment, the server 102 comprises a signaling server, which may provide any type and/or form of signaling services for establishing a communication session between computing devices, such as a first computing device 102a and a second computing device 102b. In one embodiment, the server 102c supports a Session Initiation Protocol, SIP, which is an Internet Engineering Task Force (IETF) standard protocol for initiating an interactive user session that involves multimedia elements such as video, voice, chat, gaming, and virtual reality. In one embodiment, SIP works in the

application layer of the Open Systems Interconnection (OSI) communications model. In some embodiments, the first computing device 102a initiates a session via signaling, such as via the SIP protocol, to the signaling server 102c via signaling path 220. In one embodiment, the signaling server 102c in conjunction with the gateway 340 is used for establishing a media path 225 between the first computing device 102a and the second computing device 102b, such as for a VoIP telecommunication session between telephones 210a and 210b.

The first computing device 102a of environment 200 may be part of a network, private or public, accessing the gateway 340 via network 104 over the connection 341a and traversing the firewall 205a. The firewall 205a provides access to and traversal of a public network, and has assigned the IP address of 24.24.24.100. The first computing device 102a may be in communication with, or interfaced or coupled to a telecommunication device 210a, such as a VoIP communication device, or any other real-time data communication device. The second computing device 102b may be part of a private network and have assigned the IP address of 192.168.20.20. Additionally, the second computing device 102b may include a software based telecommunication device 210b, such as software-based VoIP telecommunication device or program. The second computing device 102b may access the gateway 340 via network 104 over connection 341b and traversing firewall 205b having a public network IP address of 216.216.10.10. The firewalls 205a and 205b may be any type and/or form of firewall as known to those ordinarily skilled in the art, such as a NAT firewall.

The first computing device 102a and second computing device 102b of Figure 2A includes and uses the remote access client 120 of the present invention to provide an ad-hoc peer-to-peer virtual network connectivity in the environment 200. In addition to maintaining a tunnel and virtual private connection, such as an SSL VPN connection, to the gateway 340, the remote access client 120 of the present invention also has logic, functionality, and operations to establish a direct ad-hoc connection, such as an SSL VPN connection, to a peer it is trying to reach. In view of Figure 2A, the illustrative method 260 of Figure 2B will be used to discuss how a peer-to-peer secure communication session is established for the media path 225 in one illustrative embodiment of the present invention. The peer-to-peer routing technique of the present invention as illustrated by method 260 provides better voice quality and reduces latency related to VoIP communications as well as other real-time data communications.

In brief overview of illustrative method 260, at step 262, the computing devices 102a and 102b establish tunneling sessions with the gateway 340. At step 264, the first computing device 102a initiates a session to second computing device 102b via gateway 340 using signaling protocol via the signaling path 220 to signaling server 102b. The session may be initiated by the telecommunication device 102a in communication with the first computing device 102a. At step 266, a signaling server 102c sets up the telecommunication session, and at step 268, provides the first computing device 102a with a first network identifier of the second computing device 102b. The first network identifier comprises the network address, such as a host name or IP address, of the second computing device 102b based on its IP address established via the tunnel 341b with the gateway 340. At step 270, the first computing device 102a communicates to the second computing device 102b using the first network identifier to establish a connection or communication session.

In further overview, at step 272, the gateway 340 intercepts the communications by the first computing device 102a and provides the first computing device 102a a second network identifier for the second computing device 102b. The second network identifier comprises an IP address or host name of the second computing device 102a directly or publicly accessible by the first computing device 102a, such as the last known public IP address of the second computing device 102b. At step 274, in one embodiment, the gateway 340 communicates to the second computing device 102b to request the second computing device 102b establish a swimmer session for first computing device 102a to connect to the second computing device 102b via firewall 205b. In some embodiments, the gateway 340, at step 276, may negotiate or otherwise provide encryptions keys for the first computing device 102a and second computing device 102b. At step 278, the first computing device 102a establishes a direct connection, communication session, or media path 225 to the second computing device 102b. In other embodiments, at step 280, the first computing device 102a and/or second computing device 102b match encryption keys received by the other computing device before allowing communications.

In some embodiments of illustrative step 262, the computing device 102a and 102b may establish a connection with the gateway 340 by any suitable means and/or mechanisms, such as by any type and/or form of tunneling or gateway protocol. In some embodiments, the connections 341a and 341b to the gateway 340 may form a virtual

private network connection, and in other embodiments, may use SSL or TLS to provide secure communications to the private network, such as the private network identified by the IP range 10.10.10.XXX in illustrative Figure 2A. In one embodiment, the computing devices 102a and 102b connect to the gateway 340 by traversing a firewall 205a-205b via a public network, while, in other embodiments, the computing devices 102a and 102b may connect to the gateway 340 via a private network, and may not traverse a firewall 205a-205b. One ordinarily skilled in the art will recognize and appreciate the variety of ways the computing devices 102a-102b may connect to and communicate with the gateway 340.

At illustrative step 264, in one embodiment, the telecommunication device 210a, such as a hard IP phone, initiates a telecommunication session, such as a telephone call, to the telecommunication device 210b, such as a soft IP phone. In some embodiments, the telecommunication device 210a initiates the telephone call by indicating the extension of the telecommunication device 210b. When the telecommunication device 210a initiates the telecommunication session, this initiation, indication, or request to establish a telecommunication session or media session may be sent to the signaling server 102a via SIP protocol, a proprietary signaling protocol, or any other type of protocol suitable for signaling. The signals are communicated via signaling path 220 via the tunneling session 341a to the gateway 230 and reach the signaling server 102c via the intranet routes of the private network behind the gateway 340.

Although the illustrative embodiment of method 260 is discussed in view of VoIP or telecommunication signaling and sessions, one ordinarily skilled in the art will recognize and appreciate that the present invention may be used for initiating any type and/or form of communication session, real-time or otherwise, such as an interactive user session that involves multimedia elements such as video, voice, chat, gaming, and virtual reality. As such, the telecommunication devices 210a-210b, signaling/signal path 220, and signaling server 120a may accordingly and suitably comprise the type and/or form of device, signaling, protocols, and communications corresponding to the type and/or form of communication session.

In some embodiments of illustrative step 266, the signal server 102c may set up, negotiate, or establish any type and/or form of communication session, and in one embodiment the signaling server 102c sets up a telecommunication session, such as the VoIP telephone call initiated by the telecommunication device 210a. When setting up

the telecommunication or other media session, the signaling server 102c, at step 270, instructs, requests, signals or otherwise communicates to the initiating telecommunication device 210a and/or first computing device 102a to contact, signal, connect, or otherwise communicate to the peer telecommunication device 210b via a certain network address. In some embodiments, the network address provided by the signaling server 102c to the initiating telecommunication device 210a comprises the network address for the computing device 102b on the private network, i.e., 10.10.10.XXX, behind the gateway 340. In one embodiment, the network address for the peer telecommunication device 210b may comprise an enterprise private network address.

At this point, instead of contacting the peer telecommunication device 210b via its VPN private IP address, the illustrative method of 260, via the remote access client 120 facilities the telecommunication device 210a and/or the first computing device 102a to directly contact the peer or target telecommunication device 210b or the second computing device 102b. The techniques of the present invention is not specific to any VoIP protocol, and may be applied to any other protocols, such as any peer-to-peer protocol between computing devices. The techniques of the present invention makes decisions by way of the IP address of the resource a client is trying to connect with.

At step 270, when the telecommunication device 210a initiates a data connection to the telecommunication device 210b with the first network address provided by the signaling server 120c at step 268, such as the VPN private IP address of the soft IP phone, the gateway 340 intercepts the communication to provide the telecommunication device 210 and/or first computing device 102b with a second network address for contacting the telecommunication device 210b. In one embodiment, the gateway 340 intervenes and sends an out of band signal over the same established VPN tunnel 341a to the first computing device 102a that is facilitating traffic for the hard IP phone 210a. One ordinarily skilled in the art will recognize and appreciate that the gateway 340 may communicate to the telecommunication device 210 and/or computing device 102a that network address for contacting the computing device 102b and/or telecommunication device 210b directly by any suitable means and/or mechanisms. For example, the gateway 340 may communicate the second network address to the first computing device 102a via a second tunneling session.

In some embodiments, the gateway indicates to the first computing device 102a of the last known public IP address that the second computing device 102b which is running the soft IP phone 210b used to contact the gateway 340. In other embodiments, this public IP may not be the actual IP address of the second computing device but may be the IP address of the firewall 205b that the second computing device 102b is behind. If the computing device 210a contacts the public IP address of the firewall 205b directly, packets may be rejected by the firewall 205b. In these embodiments, the gateway 340 instructs the computing device 102b to establish what is known to those skilled in art as a swimmer session to the first computing device 102a. A forward hole is punched in the firewall 205b via which the first computing device 102a can traverse or get back in. In other embodiments, any suitable means and/or mechanism may be used to allow the first computing device 102a to traverse the firewall 205b to connect and communicate with the second computing device 102b.

Although illustrative method 260 is discussed in conjunction with environment 200 of Figure 2A having the second computing device 102n behind a firewall 205a, as one ordinarily skilled in the art will recognize and appreciate, the illustrative method 260 can be used in environments where the second computing device 102b is directly accessible without traversing a firewall 205a. As such, the illustrative method 260 may not need to at step 274 instruct the second computing device 102b to provide a swimmer session or other mechanism for the first computing device 102a to connect to the second computing device 102b.

In some embodiments, the gateway 340, at step 276, may negotiate a secret key between the computing devices 102a-103b for secure communications. The remote access client 120 on the computing devices 102a-102b may use this key for secure and encrypted communicates, and/or to authenticate or authorize the other computing device. In other embodiments, to ensure that malicious computing devices do not take advantage of this open hole, the gateway 340 at step 276 negotiates a secret key between the two computing devices 102a and 102b and the respective remote access clients 120 ensure that the keys match before allowing data communication. For example, in the embodiment of establishing a swimmer session, this key ensures that the packets coming in the open hole are from the computing device that the swimmer session was meant for.

In other embodiments, the gateway 340 does not perform step 276 to provide a secure mechanism of peer-to-peer communication sessions between the computing

devices 102a-102b. For example, the computing devices 102a-102b may be in the same private enterprise network and therefore, may be trusted. In further embodiments, instead of the gateway 340 negotiating a secret key, the computing devices 102a-102b use any suitable means and/or mechanism for authenticating and/or authorizing the other computing device for peer-to-peer communications. In some embodiments, the computing devices 102a-102b may authenticate and/or authorize via the gateway tunneling sessions, such as via path 341a, or at step 280, via the media path 225 established at step 278. For example, the remote access clients 120 of each computing device 102a-102b may check for matching keys over established media path 225 before allowing any data to be communication over the connection 225.

At step 278, the direct media path 224 for any type and/or form of communications is established between the computing devices 102a-102b without traversing the gateway 340, and, in some embodiments, not using the respective VPN assigned IP addresses of the computing devices 102a-102b but instead their public IP address or the IP address assigned to them by their resident network. Using the techniques of the present invention, the respective remote access client 120 of computing devices 102a-102b act as temporary peer-to-peer SSL gateways to each other, decrypting each other's SSL session directly without communicating via the gateway 340. The direct peer-to-peer communication session via path 225 avoids the extra-hop via the gateway 340. This will reduce any latency due to taking a longer route via the gateway 340, and will improve the quality, performance, and experience of real-time data communications, such as the VoIP communications illustrated in Figure 2A.

In some embodiments, the gateway 340 may be configured to automatically perform the techniques of illustrative method 260 every time a computing device 102 is trying to establish a peer-to-peer communication session or otherwise access a resource via the gateway 340. In other embodiments, the gateway 340 may be configured to automatically perform the techniques of the illustrative method 260 only for a certain IP address range either for a source IP address, a destination IP address, or any combinations thereof. In further embodiments, the gateway 340 may perform this technique based on the type of application and/or resource being accessed via the gateway 340. For example, in one embodiment, the gateway 340 may automatically perform this technique for any type of desktop or screen sharing application sharing screen data via the gateway 340. In other embodiments, the gateway 340 may determine

to perform this technique based on any type and/or form of business rules, access control policies, or other configuration, algorithm, and statistics. For example, the gateway 340 may perform this technique based on ping-based timing statistics between peer computing devices. If the peer computing devices are closer to each other than the gateway 340, the gateway performs the peer-to-peer routing technique. One ordinarily skilled in the art will recognize and appreciate the various ways the gateway of the present invention may be adapted or otherwise configured to perform the peer-to-peer routing technique of the present invention.

In one aspect, the present invention is related to allowing communications via a lossless protocol packets constructed for transmission via a lossy protocol. In one technique illustrated in Figure 3B, the present invention use a false acknowledgement technique when communicating a lossy or unreliable protocol via a lossless or reliable protocol, such as, for example, communicating RTP over UDP via a TCP or SSL/TCP connection. In another technique illustrated in Figure 3C, the present invention uses payload shifting to communicate via a lossless protocol packets constructed for transmission via a lossy protocol. In some embodiments, these techniques of the present invention helps achieve Transport Layer Security (TLS) at a UDP level as one ordinarily skilled in the art will recognize and appreciate in view of the description below.

The illustrative method 360 of the embodiment of the present invention for practicing the false acknowledgement technique will be discussed in view of the illustrative environment 300 of Figure 3A and additionally in view of Figures 1A-1E. In brief overview, the environment 300 comprises a client 105a of computing device 102a in communications with a peer client 105b of computing device 102b or alternatively, the gateway 340 via network 104. In some embodiments, the client 105a may traverse IP routers 305a-305b or the network 104 may have IP routers 305a-305b. Although, in other embodiments, the computing devices 102a-102b and gateway 340 may be on the same network 104. Additionally, a telecommunication device 210a may be associated with client 105a and a second telecommunication device 210b may be associated with the peer client 105b or the gateway 340.

Client 105a may comprise a first network stack 310a, and the client 105 or gateway 340 may comprise a second network stack 310b. The network stacks 3201a-310a may comprise one or more network layers, such as any networks layers of Open Systems Interconnection (OSI) communications model. For example, as illustrated in

Figure 3A, the network stacks 310a-310b comprises a TCP/IP 343a-343 communication layer communication on top of the frame layer that is suitable as known to those skilled in art for a TCP/IP based network 104. The TCP layer 343a-343b comprises an illustrative embodiments of a reliable or lossless protocol. For example, in TCP 343a-343b as known to those ordinarily skilled in the art, the network stack 310a-310b or any drivers or mechanisms thereof, such as a TCP driver, may perform algorithms and operations, and comprise logic or functionality to provide one or more of the lossless or reliable characteristics of the protocol. For example, to support TCP 343a-343b, the network stack 310a-320b may perform packet ordering, packet retransmission, acknowledgements of receipt of packet, a flow control algorithm, a sliding window algorithm, and/or a nagle's algorithm, and any other reliability related operations and algorithms as one ordinarily skilled in the art will recognize and appreciate in view of TCP 343a-343b or any other lossless protocol.

Additionally, the networks stacks 310a-310b may comprise an SSL 341a-341b layer for supporting SSL or SSL VPN communications. For example, the SSL layer 341a-341b may be used for a gateway or tunneling session between remote access clients 120 or between a remote access client 120 and a gateway 340. As illustrated in Figure 3A, the network stacks 310a-310b may also provides a layer for a lossy protocol 342a-342b, such as UDP, to be communicated over the lossless protocol 343a-343b, such as TCP. In some embodiments, the lossy or unreliable protocol 342a-342b may comprises Real Time Protocol (RTP) over UDP, and may comprise a payload have any type and/or form of real-time data, such any representation of voice or audio. In other embodiments, the lossy protocol 342a-342b may carry the VoIP over communications to and from the client 105a in an established VoIP session, such as a session established via illustrative method 260 discussed above in connection with Figures 2A and 2B. A lossless protocol, such as UDP 342a-342b may be chosen for real-time applications like voice, because it may be more important to get packets to the recipient, such as peer client 105b, on time rather than getting the packets in a reliable manner, such as via a lossless protocol.

The network stacks 310a-310b also include a shim 322a-322b of the remote access client 120 of the present invention. The shim 322a-322b may comprise any portion of the remote access client 120, and in some embodiments, comprises a network driver, network driver interface, or other network layer related mechanism for providing

the false acknowledgement technique of the present invention as described herein. The shim 322a-322b may comprise software, hardware, or any combination of software and hardware. In one embodiment, the shim 322a-322b may operate at the IP layer of the network stack prior to a network packet reaching the TCP layer 343a. In other embodiments, the shim 322a-322b may operate at the TCP layer 343a-343b. One ordinarily skilled in the art will recognize and appreciate that the shim 322a-322b may operate in any manner associated with the layer of operations of the lossless protocol in the network stack 310a-310b, including in or adjacent to the layer of the lossless protocol.

The false acknowledgement technique of the present invention as illustrated by method 360 of Figure 3B allows a lossy protocol, such as UDP 342a-343b, to be communicated via a lossless protocol, such as TCP 343a-343b. By the shim 322a-322b issuing a false acknowledgement of receipt of a TCP packet, the technique of the present inventions prevents or avoid the reliability mechanisms, operations and algorithms of the lossless protocol, such as in the example of TCP 343a-343b, any of the packet ordering, packet retransmission, a flow control algorithm, a sliding window algorithm, and/or a nagle's algorithm. As such, the lossy protocol 342a-342b can be communicated over a lossless protocol 343a-343b but maintain its lossy or unreliable characteristics which may be desired such as in real-time data communications. This technique also enables the lossy protocol to be communicated securely, or traverse a gateway via a tunneling protocol, or simply via TCP/IP while not applying the lossless characteristics of the lossless protocol to the lossy protocol communications.

In brief overview of illustrative method 360, at step 365, the computing devices 102a and 102b or the gateway 340 establish a lossless protocol based connection, such as a TCP connection, by which lossless protocol packets are communicated. At step 370, the remote access client 120 of the present invention may detect that the payload of a lossless protocol packet comprises a lossy protocol, such as RTP or UDP, or otherwise comprises real-time data. In one embodiment, at step 375, the illustrative method 360 may encrypt the payload with a key, such as a key provided via an out of band TLS or SSL session of step 367. At step 380, a false acknowledgement of receipt of the lossless protocol packet may be communicated or otherwise provided to the network stacks 310a-310b, such as by the shim 322a-322b. In response to the receipt of the false acknowledgement of receipt of the lossless protocol packet, at step 385, the respective

network stacks 310a-310b do not execute one or more, or all of the algorithms and operations that provide the reliable or lossless characteristics of the lossless protocol. At step 390, the lossless protocol packet with the lossy protocol payload is communicated between the network stacks 310a-310b.

At step 365 of illustrative method 360, the lossless protocol connection may be established via any suitable means and/or mechanisms using an type and/or form of lossless protocol. In one embodiment, the network stack 310a of a client 105a establishes a lossless protocol connection, such as TCP, to a peer client 105a having network stack 310b. In another embodiment, the network stack 310a of client 105a establishes a lossless protocol connection to a gateway 340 having network stack 310b. Additionally, the lossless protocol connection of step 365 may be established in a secured manner, such as SSL, or as a virtual private connection. Although the network stacks 310a-310b are illustrated as having the same network layers, one ordinarily skilled in the art will recognize and appreciate that the network stacks may have corresponding layers, which may be of different versions or associated with different operating systems and/or drivers, and that each network stack 310a-310b may have additional layers, less layers or different layers.

At illustrative step 360, in one embodiment, the remote access client 120 intercepts a network packet, such as via the packet capture mechanism 365, and inspects the network packet by any suitable means and/or mechanisms to determine the type of the protocol used in the payload of the network packet, or the type of contents in the payload of the network packet. In some embodiments, the shim 322a-322b of the remote access client 120 may be used for intercepting and inspecting the network packet. In one embodiment, the remote access client 120 may intercept a network packet and determine if the network packet comprises any lossless protocol or a specific lossless protocol, such as TCP. If the network packet is a lossless protocol, the remote access client 120 checks the payload to determine the type of protocol and/or the type of data. In one embodiment, the remote access client 120 may determine by any suitable fields of the payload of the network packet, such as any portion of header of the lossy protocol representing the payload, that the payload has a lossy protocol content. In another embodiment, the remote access client 120 may determine by any data of the payload, if the payload comprises a lossy protocol or comprises real-time data.

In one embodiment, the remote access client 120 determines that a TCP packet comprises a payload of RTP or UDP, and applies an encryption of the payload. The remote access client 120 may encrypt the payload of the network packet using any type and/or form of encryption with a key provided in any suitable manner. In some embodiments, the key or cipher is negotiated via an out of band TLS session between the clients 105a-105b or the client 105a and gateway as shown in Figure 3A as opposed to, in other embodiments, a traditional TLS session where the session is first negotiated and the same socket is used for data communication. In some embodiments, the encryption at step 375 is performed on a packet by packet basis. In another embodiment, encryption is performed on multiple packets at a time.

At step 380 of illustrative method 360 of the present invention, a false acknowledgment of receipt of the network packet, e.g., the lossless protocol packet, is issued, communicated, or otherwise provided to the network stacks 310a-310b comprising the respective sending and receiving computing devices 102a-120b, or gateway 340. The shim 322a-322b, any portion of the remote access client 120, or any portion of the network stack 310a-310b may issue the false acknowledgment of receipt of the network packet. In one aspect, the false acknowledgement of receipt of the network packet is false in the sense that it is communicated not to acknowledge the actual receipt of a network packet but in order to prevent the lossless and reliable mechanisms of the lossless protocol associated with the network stacks 310a-310b. As such, the false acknowledgement of receipt of the network packet may comprise the same form and/or type as an actual acknowledgement of receipt of the network packet.

In some embodiments, the false acknowledgement of receipt is issued to the network stacks 310a-310b prior to communicating the network packet or packets. In other embodiments, the false acknowledgement of receipt is issued after communicating the network packet(s) but at a time or in a manner such as to prevent the lossless protocol mechanisms of the receiving network stack 310a-310b from being applied to the transmitted network packet. In one embodiment, the false acknowledgment of receipt of the network packet is issued for each network packet, and in another embodiment, may be issued once per communication session or lossless protocol connection. Furthermore, one ordinarily skilled in the art will recognize and appreciate the false acknowledgement of receipt may be performed in different places in the network stack 310a-310b for different operating systems. For example, in one

embodiment, the acknowledgement of receipt may be issued at the Network Driver Interface Specification (NDIS) driver level in the Microsoft Family of Windows Operating Systems.

At step 385 of illustrative method 360, the network stack 310a-310b receiving the false acknowledgment of receipt of the network packet from step 380 may in response to such receipt, may not execute, stop executing, or prevent from executing any one or more algorithms and operations providing one or more lossless characteristics of the lossless protocol. For example, in the embodiment of TCP as the lossless protocol, the network stack 310a-310b may not execute any one or more of the following with respect to the network packet, or the TCP connection: packet ordering, packet retransmission, a flow control algorithm, a sliding window algorithm, and/or a nagle's algorithm. In some embodiments, the false acknowledgment of receipt must be received on a packet by packet basis to prevent the lossless layer of the network stack 310a-310b from employing reliability algorithms. As such, the sending network stack 310a-310b can determine on a packet by packet basis which packets to apply the false acknowledgment techniques of the present invention to. There may be some lossless protocol network packets comprising the lossy protocol for which the reliability algorithms of the lossless protocol should be applied. In other embodiments, the false acknowledgment of receipt of the network packet may be received once for the lossless protocol connection to prevent employing reliability algorithms for any subsequent packets received during the lossless protocol session or connection.

At step 390, the illustrative method 360 communicates the lossless protocol packet having the lossless protocol payload via the network stacks 310a-310b. In one embodiment, the lossless protocol packet is communicated after step 385, or in other embodiments, before step 385. So, although the lossless protocol packet becomes lost in the network, no attempt is made to reclaim the packet as one would expect for a lossy protocol packet.

Although the illustrative embodiment of method 360 is discussed using a false acknowledgment of receipt of the network packet such as in TCP, any type and/or form of indication, request, or instruction may be communicated to the network stacks 310a-310b to prevent employing any reliability or lossless algorithms of the lossless protocol. In some embodiments, the lossless protocol layer of the network stack 310a-310b may be adapted or configured to have a configuration, flag, or instruction to not use the

reliability algorithms either on a packet by packet basis, or a session or connection basis. For example, the lossless protocol may have fields, such in a header of a lossless protocol packet, that indicates whether reliability should be discarded or avoided for the packet.

Referring now to Figure 3C, another embodiment of steps taken to transmit packets constructed according to a lossy protocol via a lossless protocol is shown by illustrative method 345, which may also be referred to as a payload shifting technique. In brief overview of illustrative method 345, at step 348, a first packet to be transmitted using an unreliable transport protocol is received by a first device, such as client 105. At step 350, the first device 105 creates a first TCP packet including a first payload of the received first packet and a first TCP header of information associated with a TCP connection established between the first device 105 and a second device. The first device 105 transmits the first TCP packet to the second device at step 352. At step 354, the first device 105 receives a second packet to be transmitted using an unreliable transport protocol, and at step 356, creates a second TCP packet including a second payload of the received second packet and the first TCP header information. At step 358, the first device transmits, before receipt of an acknowledgement of the receipt of the first payload from the second device, the second TCP packet to the second device.

Still referring to Figure 3C, and now in more detail, at step 348, a first packet to be transmitted using an unreliable transport protocol is received by a first device 105. In some embodiments, the packet is intended to be transmitted using a lossy protocol of UDP. In further embodiments, the packet comprises RDP over UDP. In other embodiments, the first packet is generated by an application program 338 executing in user mode 332. In some embodiments, the packet is generated by an application 338 executing in kernel mode 334. In other embodiments, the first packet is received by the first device 105 for retransmission. In still other embodiments, the first packet is intercepted by a filter process 322 before it reaches the network stack 310a-310b. The filter process 322 may execute in user mode 332 or in kernel mode 334. In some embodiments, the filter 322 is a mini-driver. In other embodiments, the filter 322 is an NDIS driver. In other embodiments, the filter 322 process uses application hooking to intercept the first packet. In further embodiments, the application hooking is implemented via an application programming interface (API). In one embodiment, the hooking of network packets occurs at the network layer of the network stack 310a-310n.

At step 350, the first device 105 creates a first TCP packet including a first payload of the received first packet and a first TCP header of information associated with a TCP connection established between the first device 105 and a second device. For example, the TCP connection may be established between the client 105 and a peer computing device 102b in one embodiment, and between the client 105 and the gateway 340 in another embodiment. In some embodiments, the first device 105 indicates that the TCP packet contains a payload of packets constructed to be transmitted via a lossy protocol by opening a specific TCP port. In other embodiments, the first device 105 indicates that the TCP packet contains a payload of packets constructed to be transmitted via a lossy protocol by setting a flag in the TCP header. The TCP header may include information regarding the source node, information regarding the destination node, or a sequence number particularly identifying the TCP packet.

At step 352, the first device 105 transmits the first TCP packet to the second device. In some embodiments, the second device may be a gateway 340. In other embodiments, the second device is a "peer" computing device 102b. The first TCP packet may be encrypted before transmission to the second device using, for example, SSL or TLS.

At step 354, the first device 105 receives a second packet to be transmitted using an unreliable transport protocol, such as UDP. The second packet may be received from the same application 338 that generated the first packet. At step 356, the first device 105 creates a second TCP packet including a second payload of the received second packet and the first TCP header information, as described above. At step 358, the first device 105 then transmits, before receipt of an acknowledgement of the receipt of the first payload from the second device, the second TCP packet to the second device. In some embodiments, when an acknowledgment is received from the second device, the first device 105 updates the TCP header information before transmitting the packet. In other embodiments, the first device 105 creates a third TCP packet with updated TCP header information and having the second payload. The first device then transmits the third TCP packet.

Upon receipt of the TCP packet, the second device decrypts it, if necessary, and determines that the payload is one or more packets constructed to be transmitted using a lossy protocol. The second device may determine this based on the port on which the

packet was received or by a flag in the TCP header information. Once determined, the second device strips the TCP header from the payload and delivers the payload.

In another aspect, the present invention is related to adjusting the reported maximum transmission unit (MTU) parameter to optimize network communications by reducing packet fragmentation for encrypted network packets. This technique may be applied on one or both network stacks 310a-310b of illustrative environment 300 of Figure 3A. Encrypting a payload of a network packet, such as any network packet processed according to the illustrative method 360 described above, may increase the size of the payload. That is, the size of the network packet may increase to account for the change in size of the unencrypted original payload to the encrypted payload.

Still referring to Figure 3A, the network stacks 310a-310b may comprise a maximum transmission unit 402a-402b (MTU) parameter to indicate the size of the largest unit of data that can be sent over a type of physical medium in a network, such as an Ethernet based network. In the embodiment of TCP/IP, the MTU 402a-402b indicates the largest datagram or packet than can be transmitted by an Internet Protocol (IP) layer interface, without the interface needing to br4eak down or fragment the datagram into smaller units. An MTU parameter 402a-402b may be associated with a communications interface such as a network interface card. The default MTU size for Ethernet is 1,500 bytes, and IEEE 802.3 is 1,492 bytes. As one ordinarily skilled in the art will recognize and appreciate, the default MTU size will be based on the networking technologies such as Token Ring, FDDI, X.25, etc.

Referring now to Figure 4, a flow diagram depicts an illustrative embodiment of the MTU adjustment method 400 of the present invention. In brief overview, at step 405, a session between computing devices is established, such as between a first computing device 102a and a second computing device 102b. At step 410, one of the computing devices 102, such as the first computing device 102a, detects a network packet having an encrypted payload. At step 415, the computing device 102a-120b determines a setting for the MTU 402a-402b parameter of the network stack 310a-310b to account for the size of the encrypted portion of the payload. At step 420, the MTU 402a-402b parameter is decreased to account for the encrypted portion. If the MTU 402a-402b is requested or reported, the MTU 402a-402b will indicate a size smaller than the MTU size associated with the physical layer, such as 1,500 for Ethernet.

Using this technique, any device on the network 104 may communicate network packets to the network stack 310a-310b according to the decreased MTU size that can be encrypted along the route to the network stack 310a-310b and not be fragmented. If the network packet is encrypted it should still fit in the actual MTU size of the physical network layer medium, such as Ethernet. For example, the MTU parameter 402a-402b may be set to the default MTU size of 1,500 for Ethernet and in accordance with the illustrative method 400 decreased by a determined number of bytes, for example 100, to account for encryption overhead. A network packet may be transmitted from a server resource to the client comprising a size equal to the reported MTU 402a-402b size of 1,400. The network packet may traverse the gateway 340 and get encrypted via the SSL tunnel, which in turns increases the network packet size to 1,475. Since this size fits into the MTU size of the Ethernet physical medium, the network packet will not be fragmented.

At step 405 of illustrative method 400, any type and/or form of communication session between a first computing device 102a and a second computing device 102b, such as client 105b or gateway 340 of Figure 2A, may be established. In some embodiments, the session is established using the remote access client 120 on a first computing device. In one embodiment, the remote access client 120 establishes a session with the gateway 340, such as an SSL VPN session, or to another remote access client 120 on a peer computing device 102b.

In some embodiments of step 410, the remote access client 120 detects a network packet having an encrypted payload. In one embodiment, the packet capture mechanism 365 intercepts network packets and the agent 326 determines if the packet is encrypted. However, any other portion of the remote access client 120, such as the filter 322 or frame monitor 360 may determine if the packet is encrypted. In one embodiment, the entire payload of the network packet is encrypted, while in other embodiments, a portion of the payload is encrypted. The present invention may use any type and/or form of means or mechanism for determining if a packet has encryption. For example, in some cases, the remote access client 120 may check for a flag or field of the network packet indicating the payload is encrypted. In other embodiments, the remote access client 120 may check whether any portion of the payload is unintelligible, because it contains random data or noise from encryption. Additionally, the encrypted payload may be

encrypted in association with any layer of the network stack 310a-310b, such as layer 2, 3, 6 or 7 encryption.

In some embodiments of step 415, the illustrative method 400 of the present invention determines the adjustment to the reported MTU 402a-402b size on a packet by packet basis, or in other embodiments, on a connection or session basis, and at step 420 adjusts the MTU 402a-402b accordingly. In one embodiment, the MTU 402a-402b is decreased exactly by the amount of encryption overhead for the network packet. In some cases, the illustrative method 400 determines the MTU 402a-402b size adjustment once for the entire session or connection and decreases the size of the MTU 402a-402b to a value to account for encryption overhead for the entire session. For example, although network packets may have varying encryption overhead, the adjustment accounts for the largest encryption overhead. In further embodiments, the MTU 402a-402b may be adjusted to take into consideration encryption that may occur when the network packet leaves the network stack 310a-310b, such as encryption by a gateway 340 that may occur in the end-to-end network traversal of the network packet .

Additionally, the MTU 402a-402b size may be adjusted for other network performance factors in addition to the encryption overhead. In some embodiments, although the MTU 402a-402b is decreased due to encryption overhead, it may be further decreased to account for other overhead and factors related to network communication, as well as increased in other cases. For example, the MTU 402a-402b may have been previously adjusted for a factor not related to encryption and after using the techniques of the present invention the MTU 402a-402b is decreased to take into account encryption overhead. One ordinarily skilled in the art will recognize and appreciate that there may be other factors and considerations for adjusting the MTU besides or in addition to adjusting for encryption overhead in accordance with the techniques of the present invention.

Referring now to Figures 5A and 5B, the present invention, in an additional aspect, is related to client-side application-aware network communication prioritization techniques. The remote access client 120 of the present invention provides for the intelligent and client centric prioritization of application network communications on a client based on the type and/or priority of an application. As depicted in the system 500 of Figure 5A, the remote access client 105 of computing device 102 is connected to network 104. The client 105 may execute one or more applications 338a-338n, which

access the network 104 via the agent 326 and filter 322 of the remote access client 120. In some embodiments, the applications 338a-338n provide one or more real-time data communications, such as VoIP. In other embodiments, one or more of the applications 338a-338 may provide email, collaboration, online meeting, and/or desktop sharing related services or functionality.

As illustrated in Figure 5A, the packet capture mechanism 365, 365' may be included in the filter 322 or the agent 326 of the remote access client 120, for intercepting network traffic of any of the applications 338a-338n of the client 105. The remote access client 120 may comprise any queues 540a-540n for queuing and prioritizing network communications of the client 105. In one embodiment, the queues 540a-540n may be included in a network driver, such as an NDIS driver for the filter 322, and in other embodiments, may be included with or accessible by the agent 326. The queues 540a-540n may comprise any type and/or form of suitable means and/or mechanisms for storing and/or arranging network packets, such as network packets intercepted by the packet capture mechanism 365. In some embodiments, the queues 540a-540n may be associated with or assigned to network packets related to applications 338a-338n of the client 105. In other embodiments, the queues 540a-540n may be organized by levels of priority, such as high, medium, low, or numerically such as priority 1...10. One ordinarily skilled in the art will recognize and appreciate that number of queues 540a-540n may be based on any desired granularity of prioritization, such as 3, 5 or 10 levels of priority. Additionally, some of the queues 540a-540n may be used for receiving and/or transmitting network packets prior to being placed into and/or taken out of a priority based queue 540a-540n.

The remote access client 120 may also have, access, or use a routing table 538 for determining how to route network packets of the client via the agent 326, such as onto the network 104 via a gateway 340. In one embodiment, the agent 326 establishes and maintains an SSL VPN connection to the gateway 340, such as illustrated in Figure 1A for example. In one embodiment, the routing table 538 comprise information about a source computing device and a destination computing device to identify a communication path or connection between a source and destination communication points. The routing table 538 may include a source IP address and source port, and an destination IP address and destination port to identify a communication path on the network 104. For example, the source IP address and source port may represent the IP

address of the client 105 and the port by which an application 338a-338n on the client 105 communicates on the network 105. The destination IP address may represent the IP address of a peer computing device to which the application 338a-338n communicates with via the destination port used by the peer device.

Additionally, the remote access client 120 may have one or more policies 520 for specifying client-side prioritization of network communications related to applications 338a-338n running on application. These policies 520 may be specified by any suitable means and/or mechanisms. In some embodiments, the policies 520 may be specified by the name of the application 338a-338n and/or the type of application 338a-338n. In other embodiments, the policies 520 may be specified in accordance to the type of one or more protocols used by the applications 338a-338n and/or the size of the payload of the network packet. In another embodiment, the policies 520 define prioritization based on whether an application is running in the foreground or the background of the client 105. In yet another embodiment, policies 520 may indicate prioritization based on the destination network address, such as host name or IP address, and/or destination port number. Additionally, the policies 520 may be specified hierarchically to account for multiple applications 338a-338n and/or multiple protocols that may be executed on the client 105 at any point. Furthermore, the policies 520 may be specified conditionally, such as if one application 338a is running, a second application 338b may have a higher or lower priority. One ordinarily skilled in the art will recognize and appreciate the multitude of ways to define client-side application priorities.

The policies 520 may be accessible by the agent 326, configured into the agent 326, or loaded by the agent 326. For example, the policies 520 may be provided by or downloaded via the gateway 340. The policies 520 may comprise any type and format of syntax and/or language for specifying a policy, and may be provided via any type and/or form of medium, such as electronically by one or more network packets or via a file, such as an XML file. The policies 520 may be configurable by a user by any suitable means and/or mechanism. For example, the agent 326 may provide a configuration mechanism such as a user interface, graphical or otherwise, design and constructed for configuring or specifying the policies 520.

In view of the system 500 of Figure 5A and Figures 1A-1C, the prioritization technique of the present invention illustrated by method 550 in Figure 5B will be described. In brief overview, at step 555 of the illustrative method 550, the client 105

intercepts one or more networks packets associated with an application 338a-338n on the client 105, and, at step 560, the network packets are stored to a queue 540a-540n. At step 565, a priority for the intercepted and queued network packet is determined based on the type and/or priority of the application 338a-338n. At step 570, the determined priority is indicated for the network packets, and, at step 575, the network packets are communicated according to the determined priority. As such, the outbound network packets generated by an application 338a-338n on the client 105 are prioritized by the client 105 prior to transmission based on the type and/or priority of the application 338a-338n. For example, the application 338a may generate real-time data of VoIP communications, such as RTP over UDP via a TCP/IP session of an SSL connection to the gateway 340. The client 105, using the techniques of the present invention, may prioritize the real-time data communications of application 338a ahead of other applications, such as non-real-time data communication applications. This technique may compliment Quality of Service (QOS) networks where network traffic prioritization occurs in intermediary network devices, such as switches and routers.

At step 555 of illustrative method 500, the client 105 may intercept network packets of one or more applications 338a-338n transparently to the application 338a-338n, the gateway 340, a peer computing device, and any of the network layers of a network stack. In this manner, the techniques of the present invention support any type of application 338a-338n on the client 105. In some embodiments, the network packets are intercepted by the packet capture mechanism 360 via agent 326 or filter 322. Any inbound and/or outbound network packets of an application 338a-338n may be intercepted by the remote access client 120 of the present invention.

At step 560, the network packets intercepted at step 555 may be stored in a queue 540a-540n. In one embodiment, the network packet is stored to a temporary queue 540a-540n prior to prioritizing the network packet at steps 565 and 570. In other embodiments, the network packet is stored to a determined priority queue 540a-540n or a queue 540a-540n associated with an application 338a-338n after the network packet is prioritized at steps 565 and/or step 570.

At step 565, the remote access client 120 of the present determines the association of network packets with applications 338a-338n in order to determine priorities and apply any priority based policies 520. The client 105, such as via agent 326, can associate network traffic with applications 338a-338n by any suitable means

and/or mechanisms. In some embodiments, the agent 326 identifies the network packet as generated from an application 338a-338n by any of the content of the network packet, such as any headers, fields, or the type and content of data in the payload of the network packet. In other embodiments, a network packet is associated with an application 338a-338n by matching information from the routing table 538, such as source and destination IP addresses and ports numbers with the IP addresses and ports numbers of the network packet. In some embodiments, the agent 326, such as via the frame monitor 360, may perform a checksum on the packet to verify that the identified application actually generated the packet.

Additionally, the remote access client 120 may determine whether the application 338a-338n associated with the network packet is running in the foreground or the background of the client 105. Furthermore, the remote access client 120 may determine any priorities, such as process task priority, assigned to the application 338a-338n by the operating system of the client 105. In other embodiments, the remote access client 120 may determine any other characteristics or statistics of the application 338a-338n such as size, memory usage, total execution time, and/or frequency of use. One ordinarily skilled in the art will recognize and appreciate the various characteristics of an application the present technique may use for providing client-side application-aware network communication prioritization.

At step 570, the remote access client 120 of the present invention indicates a priority for intercepted and queued network packets based on the application 338a-338n associated with the packet at step 565. In one embodiment, the agent 326 uses the policies 520 to apply a priority to network packets of applications 338a-338n in accordance with the prioritization rules specified or indicated by the policies 520. In some embodiments, the agent 326 may use characteristics of the application 338a-338n, such as running in the foreground or background, to indicate priority for a network packet of the application 338a-338n. In other embodiments, the agent 326 may use any combination of the policies 520 and characteristics of the application 338a-338n to indicate a priority for the network packets of the application 338a-338n.

In some embodiments, the agent 326 indicates the priority to the filter 322 for management of network packet queues 540a-540n to apply the indicated priorities. The agent 326 may communicate the priority of network packets to the filter 322 by any suitable means and/or mechanism such as via an application programming interface

(API), such an IOCTL interface, or any other type and/or form of interface known to those ordinarily skilled in the art. In one embodiment, the filter 322 is not aware of the application 338a-338n by name but can associate priorities to network packets of applications 338a-338n via the routing table 538. An application 338a-338n corresponding to a network packet can be identified by any combination of source and destination identifiers, such as IP addresses and port numbers. As such, in some embodiments, the agent 326 indicates priorities to the filter 322 by routing information instead of application name. In other embodiments, the agent 326 provides to the filter 322 a mapping between applications 338a-338n, such as by application name or process id, to the routing information in a routing table 538.

Based on the indicated priorities for applications 338a-338n, in some embodiments, the filter 322 may place, arrange, or coordinate network packets into queues 540a-540n in support of the priorities. In one embodiment, the filter 322 may move network packets from temporary queues 540a-540n or from memory or other storage to a queue 540a-540n associated with the application 338a-338n, a queue 540a-540n associated with a priority, or a queue 540a-540n associated with both an application and a priority. For example, in one embodiment, all high priority network traffic may be placed in a high priority queue 540a and arranged in order based on an order of priority of the application 338a-338n, such as real-time data applications 338a-338n prior to other applications 338a-338n. In some embodiments, the network packets may be arranged in order in a priority queue 540a-540n based on the time the network packet was intercepted by the packet capture mechanism 365, such as in a FIFO manner. In yet a further embodiment, one queue 540a-540n may be used for prioritization by the filter 322. Each network packet may be placed and arranged in a priority order respective to all other intercepted network packets to provide a packet by packet prioritization across all applications 338a-338n and intercepted network packets. One ordinarily skilled in the art will recognize and appreciate that the network packets may be arranged in various priority queues 540a-540n, such as high, medium, low, or by any other granularity, and be placed or arranged in the queue in any suitable manner in practicing the operations of the present invention described herein.

In one embodiment, all network packets for an application 338a-338n are placed in a queue 540a-540n associated with the application 540a-540n. For example, intercepted network packets for an application communicating to a first destination IP

address, and a first destination port may be placed in a first queue 540a. In another embodiment, all networks packets for a type of application 338a-338n, such as an email or voice application, or all network packets for a type of protocol used by the application 338a-338n, such as RTP or UDP, may be placed in a queue 540a-540n for prioritizing networks packets for one or more applications. For example, online collaboration related applications 338a-338n may be placed and prioritized in a first queue 540a for collaboration related applications. A second queue 540b may be used for email related applications 338a-338n. In another example, a queue 540a may be used for applications 338a-338n communicating real-time data or communicating using the RTP and/or UDP protocol. In a further example, a queue 540a may be used for applications 38a-338n communicating using a remote display protocol, such as ICA or RDP.

Within each application associated queue 540a-540n organized by specific application 338a-338n, type or category of application 338a-338n, or by protocol, the network packets may be further prioritized by the characteristic of the application 338a-338n generating them, e.g., a foreground application, the size of the network packet, or the time the network packet was intercepted. In some embodiments, one or more queues 540a-540n may be used for network packets intercepted but not prioritized because a policy 520 does not exist or apply to the network packet, or the policies 520 indicate to ignore or not process the network packet for prioritization. One ordinarily skilled in the art will recognize and appreciate the various ways network packets may be placed and arranged in a priority based manner in queues 540a-540n associated with the application 338a-338n, the type of application 338a-338n or the protocol used by the application 338a-338n, and that the priority may be based on the policies 520 specified for the client 105.

At step 575 of illustrative method 550, the network packets are communicated from the queues 540a-540n according to the determined priorities for the network packets. In some embodiments, the network packets are organized into priority queues 540a-540b so that the network packets of the highest priority queue 540a-540n are communicated first, and then the next highest priority queue 540a-540n second, and so on. In other embodiments, the queues 540a-540n are organized by application 338a-338n, and therefore, at step 575, the present invention communicates network packets from the queue 540a-540n based on the respective priorities of the applications 338a-338n. Regardless of the queue 540a-540n organization and management, one ordinarily

skilled in the art will recognize and appreciate that the remote access client of the present invention will communicate the network packets from the queues in a manner according to or consistent with the determined priorities, which in turn, may be based or derived from the policies 520 of the client.

In some embodiments, the remote access client 120 of the present invention considers other network factors in determining what network packets to communicate from what queue. For example, the remote access client 120 may receive an indication of network congestion, such as receiving a window size of zero for a TCP connection related to an application 338a-338n. In another example, the remote access client 120 may recognize a high number of retransmits to a particular destination. As such, in some embodiments, the remote access client 120 may throttle back or not communicate network packets related to other networks factors, such as congestion, even though the network packets may have a higher priority than other network packets in a queue 540a-540n. Thus, the client 105 controls and manages the prioritization of network communications of the client 105 on an application 338a-338n basis and in accordance with any policies 520 for the client 105 and in further view of any network statistics and other factors occurring on the network.

In yet a further aspect and referring now to Figures 6A and 6B, the present invention is related to providing a network disruption shielding technique for persistent and reliable connectivity. Figure 6A illustrates environment 300 as discussed above in conjunction with Figure 3A. The environment 300 illustrates network stacks 310a and 310b, which may represent network stacks of computing devices 102a-120b or gateway 340, such as any of the computing devices 102 and the gateway 340 illustrated in Figures 1A-1C, 2A, or 5A. Each network stack 310a-310b may comprise one or more networks layers, such as a TCP/IP network layer on top of the frame network layer as one ordinarily skilled in the art will recognize and appreciate. Although the network stacks 310a-310b are illustrated in environment 300 of Figure 6A with a certain set of network layers, one ordinarily skilled in the art will recognize and appreciate that the network stacks 310a-310b may have any type and/or form of network layers, in any suitable combination, and each of the network stacks 310a-310b may have different forms of each layer in relation to the other network stack.

The network stacks 310a-310b may be considered to have a first portion 605a-605b of the network stack, and a second portion 610a-610b of the network stack. As

illustrated in the example network stacks 310a-310b of Figure 6A, the first portion 605a-605b of the network stack comprises the network layers at and below the TCP network layer. The second portion 610a-610b may comprise those network layers above the TCP network layer, such as a UDP over SSL protocol layer. Although the first portion 605a-605b and the second portion 610a-610b are shown as portioned, segmented, or otherwise divided at the TCP layer, the first portion and second portion may be formed at a higher or lower dividing layer in practicing the network disruption shielding technique of the present invention as one ordinarily skilled in the art will recognize and appreciate.

The network stacks 310a-310b illustrated in Figure 6A may represent an application 338a-338n on client 105, such as the client depicted in Figure 5A, establishing a peer-to-peer SSL VPN connection to a second computing device 102b or, alternatively, a gateway 340. The client 105 may be a mobile client, such as a notebook, personal digital assistant (PDA), a smart phone, or any type of mobile computing or telecommunication device. The client 105 may communicate real-time data such as VoIP communication via the UDP protocol or RTP over UDP via the SSL session established to the peer device 102b or gateway 340. In one embodiment, the agent 326 of the remote access client 120 establishes and maintains the SSL or SSL VPN session to the gateway 340 or to peer computing device 102b. The agent 326 may operate in user-mode 332, and may handle any network layer and protocol processing related to the second portion 610a-610b of the network stack 310a-310b, along with any application layer protocols. As a TCP/IP based network 104, the UDP over SSL session of the second portion 610a-610b of the network stack 310a-310b may be communicated over a TCP/IP stack forming the first portion 605a-605b of the network stack 310a-310b. In view of the remote access client 120 of the present invention, such as illustrated in Figure 1A or 5A, the filter 322 may be a network driver operating in kernel-mode 332 within the first portion 605a-605b of the network stack 310a-310b.

The present invention uses a network disruption shielding technique as depicted by illustrative method 650 in Figure 6B to maintain the second portion 610a-610b of the network stack 310a-310b through a network level connection interruption, such as any type and/or form of network disruption to the first portion 605a-605b of the network stack 310a-310b. The network disruption shielding technique of the present invention may be performed transparently to an application 338a-338n of the client 105, a user of the client 105, any one or more network layers above the first portion

605a-605b, and the gateway 340 or peer computing device 102b, and any portion of their respective network stacks 310a-310b. In one embodiment, the network disruption is shielded without notification to the user of the client that the network was disrupted or a session was interrupted.

In brief overview of illustrative method 650, at step 665, a client 105 establishes a session via at least a first protocol over a network connection between the client and another device, such as a peer computing device or gateway. As such, a network stack 310a-310b is established or used on the client 105. The network stack 310a-310b has a first portion 605a-605b and a second portion 610a-610b. At step 660, a disruption in the network connection is detected causing the first portion 605a-605b of the network stack 310a-310b to be disestablished, or otherwise disrupted from being used or continued to be used. At step 665, the present invention maintains the second portion 610a-610b of the network stack 310a-310b during the disruption and maintaining a session, or sessions, associated with the network layers of the second portion 610a-610b.

During the disruption, at step 670, any network packets related to the second portion 610a-610b of the network stack 310a-310b may be queued. At step 675, the first portion 605a-605b of the network stack 310a-301b is reestablished or otherwise received from the network disruption. While the first portion 605a-605b of the network stack 310a-301b is reestablished, the present invention maintains the second portion 610a-610b, and sessions thereof, allowing at step 680, to continue with the session by linking or re-associating the second portion 610a-610b with the first portion 605a-605b of the network stack 310a-310b. The network connection and/or the session may automatically be re-authenticated at step 680. At step 685, the illustrative method may communicate any queued network packets and continue with the session transparently as if the network disruption did not occur.

In an embodiment of illustrative step 655, a first computing device 102a may establish a network connection with a second device, such as a peer computing device 102b or a gateway 340, by any suitable means and/or mechanism and using any type and/or form of connection based protocol. For example, the network connection may be established via a TCP connection on a TCP/IP network or by an SPX connection on an IPX/SPX network. In some embodiments, the network connection may be initiated by any of the applications 338a-338n on the client, such as any application illustrated in

Figure 5A. For example, a remote display client, such as an ICA client of Citrix Systems, Inc. or a Remote Display Client of Microsoft Corporation may initiate or establish the network connection. In other embodiments, the network connection of illustrative step 665 may be initiated and/or established via the agent 326, filter 322, or any other portion of the remote access client 120. In one embodiment, the establishing of the network connection forms the first portion 605a-605b of the network stack 310a-310b. In other embodiments, the first portion 605a-605b of the network stack 310a-310b, or portion thereof, is established via connection to a network 104 upon startup of the client 105.

In some embodiments, the second portion 610a-610b of the network stack 310a-310b is formed by establishing one more sessions, such as an SSL session, via any type and/or form of protocol over the network connection, such as a remote display protocol of ICA or RDP. The session may be established via any application 338a-338n or the remote access client 120 of the client. In one embodiment, the session may correspond to a tunneling or gateway session with a peer computing device 102b or a gateway 340. In another embodiment, the session may be any type of interactive session such as a media session established via a signaling protocol, SIP for example. For example, the session of the second portion 610a-610b of the network stack 310a-310b may comprise a VoIP communication session, such as one established by illustrative method 260 of Figure 2B. Additionally, there may be multiple sessions associated with the second portion 610a-610b of the network stack 310a-310b. For example, an SSL or SSL VPN session may form one session, while a second session, such as media session via RTP over UDP may form a second session. Additionally, at any application layer of the network stack 310a-310b one or more applications 338a-338n on the client 105 may establish an application level session with a peer computing device 102b. In one embodiment, the agent 326 of the remote access client 120 is responsible for establishing and maintaining the second portion 610a-610b of the network stack 310a-310b and one or more of the associated sessions.

At step 660 of the illustrative method 650 of the present invention, a disruption is network connection is detected. In one embodiment, the network disruption may be caused by a mobile client 105 roaming between networks and networks segments, which, in some embodiments, causes the client 105 to obtain a new network IP address and/or host name. In some embodiments, the disruption disrupts the first portion 605a-

605b of the network stack 310a-310b, such as, for example, causing a TCP or SPX connection to be disconnected. In one aspect, the disruption causes the first portion 605a-605b, or any portion thereof, of the network stack 310a-310b to be disestablished, or otherwise needing to be re-established, reconnected, reconfigured or rebuilt. For example, in some embodiments, the IP layer of the network stack may maintain intact while the TCP layer is reestablished. In one embodiment, any TCP related drivers may need to be re-started. In other embodiments, the TCP/IP layer be intact even though the network connection is disrupted, and only a new TCP connection needs to be established. In other embodiments, the TCP/IP layer is intact but needs to reconfigure itself for a new network or network segment, such as changing the IP address of the client 105. One ordinarily skilled in the art will recognize and appreciate the various ways a network connection may be disrupted and impact or affect a first portion of the network stack.

In some embodiments, the agent 326, or any other portion of the remote access client 120 may detect the network disruption by any suitable means and/or mechanisms. In one embodiment, the agent 326 may determine a network disruption by receiving an error message or failure upon calling or executing an API call to the first portion 605a-605b of the network stack 310a-310b. For example, the SSL session maintained by the agent 326 for the second portion 610a-610b relies or depends on the TCP connection of the first portion 605a-605b of the network stack 310a-310b. As the agent 326 transacts via the SSL session, the agent 326 may receive an error or failure message indicating a problem with the TCP connection. In other embodiments, the agent 326 may receive an event or message from any network layer of the first portion 605a-605b of the network stack 310a-310b indicating a network disruption. One ordinarily skilled in the art will recognize and appreciate the various ways the network disruption may be detected.

At illustrative step 665, in some embodiments, upon detection of the network disruption, the agent 326 or any other portion of the remote access client 120 of the present invention maintains the second portion 610a-601b of the network stack 310a-310b during the disruption. For example, although the SSL based session maintained by the agent 326 depends on an underlying TCP connection, the agent 326 keeps the SSL session open or active through the disruption to the TCP connection. As there may multiple sessions associated with one or more layers of the second portion 610a-610b of the network stack, the agent 326, in some embodiments, keeps one or more, or all, of the

multiple sessions open or active although the first portion 605a-605b of the network stack 310a-310b is disrupted.

At step 670 of illustrative method 650, the remote access client 120 of the present invention, in some embodiments, queues one or more network packets of any of the protocols related to the second portion 610a-610b of the network stack 310a-310b during the network disruption. The remote access client 120 may use any type and/or form of queuing mechanisms, such as any of the queues 540a-540n illustrated in Figure 5A. In other embodiments, the remote access client 120 may discard network packets during the disruption, such any packets related to a lossy protocol, such as RTP over UDP for voice communications. In some cases, it may be desirable to discard packets, such as UDP packets, to reduce latency and quality issues, such as in voice communications. In further embodiments, the remote access client 120 may queue some network packets and discard other network packets. In an additional embodiment, the remote access client 120 may queue the network packets, and discard some or all of the network packets after a predetermined period of time. The remote access client 120 may use the policies 520 to determine which network packets to queue and/or discard. For example, a network packet of a first application 338a may be queued while a network packet of a second application 338n is discarded. In other embodiments, the remote access client 120 may use any network statistics or any network traffic inspection techniques, for example stateful inspection, as known to those skilled in the art to determine whether to queue and/or discard network packets during the disruption.

At step 675 of illustrative method 650, the first portion 605a-605b of the network stack 310a-310b is reestablished while the second portion 610a-610b of the network stack 310a-310b is maintained along with maintaining any desired session or sessions of the second portion 610a-610b of the network stack 310a-310b. The first portion 605a-605b of the network stack 310a-310b may be reestablished by any suitable means and/or mechanisms. For example, the client 105 may reestablish the TCP/IP connection to the network 104, such as by logging into a new network for a roaming mobile client 105. In other embodiments, the remote access client 120, such as via the agent 326 or the filter 322, reestablishes the first portion 605a-605b of the network stack 310a-310b. For example, the agent 326 may initiate and establish a new TCP connection. Upon reestablishing the first portion 605a-605b, the second portion 610a-610b of the network stack 310a-310b is linked with, re-associated with or starts to use or continue to use the

first portion 605a-605b to reestablish the network stack 310a-310b. In some embodiments, the agent 326 may be notified by an event of any network layer that the first portion 605a-605b has been reestablished or in other embodiments, may poll by any predetermined frequency to determine the first portion 605a-605b is reestablished. For example, the agent 326 may check if the TCP connection is active or can be reconnected.

In some embodiments, at step 680, the remote access client 120, such as the agent 326, may automatically re-authenticate the client 105 or a user of the client 105 for the network connection, such as a TCP connection for the first portion 605a-605b of the network stack 610a-610b. For example, the remote access client 120 may automatically re-authenticate the client 105 to a network 104 using any network related credentials of a user of the client 105. Additionally, the remote access client 120 may automatically re-authenticate the client 105 or a user of the client 105 for any session associated with the second portion 610a-610b of the network stack 310a-310b. For example, the SSL session between the agent 326 and the gateway 340 or peer computing device 102c may be re-authenticated.

In another example, an application 338a may be accessing a host service, web server, or application server that uses authentication credentials for access. The agent 326 may automatically re-authenticate the application 338a to the corresponding service or server using application related authentication credentials. In some embodiments, the remote access client 120 may re-authenticate the client and/or user of the client 105 at multiple levels, such as for network access and/or TCP connection, SSL or SSL VPN session, and/or any application level sessions, such as a media interactive user session, for example, a VoIP telephone session. Furthermore, the remote access client 120 may re-authenticate at any time prior to step 685, during step 685, for example, after communicating queued network packets but before continuing other communications, or after step 865, in response to a request to authenticate from a peer computing device, such as a server or the gateway 340.

At step 685 of illustrative method 650, the remote access client 120 of the present invention continues to use the session or sessions of the second portion 610a-610b of the network stack. If any network packets have been queued or remain queued at step 670, the remote access client 120 communicates the queued network packets and continues communicating any network packets of the client 105, such as network

packets generated by or sent to the one more applications 338a-338n of the client 105. As such, the network disruption shielding technique of the present invention provides a seamless and transparent solution to nomadic mobile computing solutions and for generally providing reliable and persistent network connectivity and access.

In the example of a VoIP communications, the illustrative method 650 of the present invention will reduce the number of telephone call drops due to network disruptions and improve the usage of and experience with VoIP. A VoIP user will not need to reconnect the telephone call due to temporary network disruptions in network availability as the remote access client 120 of the present invention will automatically maintain the session and reconnect to the network. Additionally, the remote access client 120 of the present invention will automatically re-authenticate the connection and sessions for providing security after the network disruption. Furthermore, the network shielding technique of the present invention is useful for 1) continuing transactions, commands, or operations automatically through the network disruption, 2) maintaining session related context and cache through the network disruption, and 3) automatically handling change in network address of the client due to changes in the network.

By providing a reliable and persistent connection, the present invention also avoids interruptions to transactions, commands or operations as part of the functionality exercised between the a first computing device 102a and a second computing device 102b, such as client 105a and 105b in Figures 1C. For example, a file copy operation using Windows Explorer has not been designed to continue working after there is a disruption in a network connection. A user on the client 105 may use the file copy feature of Windows Explorer to copy a file from the client 105 to a server 102c. Because of the size of the file or files, this operation may take a relatively extended period of time to complete. If during the middle of the operation of the copy of the file to the server, there is an interruption in the network connection between the client 105 and the server, the file copy will fail. Once the network connection is re-established, the user will need to start another file copy operation from Windows Explorer to copy the file from the client 105 to the server. Under the present invention, the user would not need to start another file copy operation. The network connection would be re-established in accordance with the network disruption shielding technique of the present invention as illustrated in Figure 6B. As such, the file copy of Windows Explorer would not get notified of the interruption in the network connection and therefore, would not

fail. The remote access client 120 would re-establish any connections and transmits any queued data so that operation can continue without failure. The remote access client 120 would maintain a queue of the data related to the file copy operations that has not been transferred to the server because of the interruption in the network connection. Once the network connection is re-established, the remote access client 120 can transmit the queued data and then continue on with transferring the data related to the file copy operation in due course.

Although this aspect of the invention is described in terms of a file copy operation example, one ordinarily skilled in the art will recognize that any operation, transaction, command, function call, etc. transacted between a first computing device 102a and a second computing device 102b, can be maintained and continued without failure from the network connection disruption, and, furthermore, without the client 105 or user of the client 105 recognizing there was a disruption or having notice of the disruption. Additionally, the transaction or operation can be maintained and continued transparently to the application 338, the gateway 340, second computing device 102c, and any part of the second portion 610a-610b of the network stack 310a-310b.

By providing the client 105 with a reliable and persistent connection to a peer computing device 102b or gateway 340, the present invention avoids the process of opening a new user session with an application 338 on the peer, such as a host service on server, by maintaining the user session through network connection interruptions. For each user session between peer computing device, each computing device may maintain session specific context and caches, and other application specific mechanisms related to that instance of the user session. For each new user session established, these session specific context and caches need to be re-populated or re-established to reflect the new user session. For example, a user on the client 105 may have an http session with a server 102c having a web server or web application. The server 102c may keep context specific to providing this instance of the http session with the client 105. The context may be stored in the memory of the server, in files of the server, a database or other component related to providing the functionality of the server 102c. Also, the client 105 may have local context specific to the instance of the http session, such as a mechanism for keeping track of an outstanding request to the web server. This context may be stored in memory of the client 105, in files on the client 105, or other software component interfaced with the client 105. If the connection between the client 105 and

the server 102c is not persistent, then a new user session needs to be established with new session specific context on the server 102c and the client 105. The present invention maintains the session so that a new session, and therefore new specific session context, does not need to be re-established.

The present invention maintains the user session through network level connection interruptions and without notification to the user of the client that the session was interrupted. In operation of this aspect of the invention, the client 105 establishes the connection to the peer computing devices. Via the connection, a session between the client 105 and the server is established. The remote access client 120 can store and maintain any session related information such as authentication credentials, and client 105 and host server 102c context for the established session. Upon detection of a disruption in network connection, the remote access client 120 can re-establish the first portion 605a-605b of the network stack 310a-301b while maintaining the second portion 610a-610b of the network stack. The network connection disruption may cause an interruption to the underlying TCP/IP connection used by the session between the client 105 and the server 102c. However, since the second portion 610a-610b of the network stack 310a-310b is maintained, the session can be re-established and/or continued after the network connection is re-established without the user on the client 105 having notification that the session was interrupted. Thus, the interruption of the session caused by the network connection disruption is effectively hidden from the user using the network disruption shielding techniques of the present invention.

Furthermore, by providing a reliable and persistent connection, the present invention also enables a client 105 to traverse through different network topologies without re-starting a session or an application 338 on the client 105. For example, the client 105 may be a computer notebook with a wireless network connection. As the client 105 moves from a first wireless network to a second wireless network, the client's network connection may be temporarily disrupted from the first wireless network as a network connection is established with the second wireless network. The second wireless network may assign a new network identifier, such as a host name or internet protocol address, to the client 105. This new network identifier may be different than the network identifier assigned to the client 105 by the first wireless network. In another example, the client 105 may be physically connected through an Ethernet cable to a port on the network. The physical connection may be unplugged and the client 105 moved to

another location to plug into a different port on the network. This would cause a disruption into the network connection and possibly a change in the assigned network identifier. Without the present invention, any sessions between peer computing devices may need to be restarted due to the change in the network topology, the disruption to the network connection, and/or the change in the assigned network identifier. By the method and systems described herein, the remote access client 120 of the present invention maintains the network connection for the client and automatically re-established the client's 105 network connection including handling changes in the network topology and network identifier. The client 105, and any applications or sessions on the client 105, can continue to operate as if there was not a network connection disruption or a change in the network identifier. Furthermore, the user on the client 105 may not recognize there were any interruptions or changes, and the client 105 may not receive any notice of such interruptions.

In an additional aspect, any of the techniques of the present invention, such as the illustrative methods of Figures 2B, 3B, 3C, 4, 5B and 6B, can be practiced in one or more combinations with each other. In one embodiment, the peer-to-peer routing technique may be practiced with the false acknowledgement and/or MTU adjustment techniques. This would provide a client communicating real-time data, such as VoIP, to connect to the peer via a more optimal and direct route and to communicate the real-time data via UDP over a secure SSL/TCP/IP connection, while avoiding any latency due to any reliability mechanism of TCP and reduce fragmentation due to the encryption overhead. Additionally, this embodiment may be further combined with the client-side application-aware prioritization technique and/or the network disruption shielding technique. As such, the secure real-time data communications can be communicated from the client at higher priorities than other applications of the client to improve the quality of the real-time experience, such as VoIP. The network disruption technique would allow a mobile VoIP phone, such as a soft phone of a notebook, roam between network access points and automatically continue with the session.

The techniques of the present invention are complimentary to each other for network communication optimizations, such as for example in VoIP communications over a SSL VPN gateway. As such, each of the 1) peer-to-peer routing technique, 2) the false acknowledgement technique, 3) payload shifting technique, 4) the MTU adjustment technique, 5) the client-side application-aware technique, and 5) the network

disruption shielding technique of the present invention may be practiced with one or more of the following techniques and optimization of the present invention: 1) the peer-to-peer routing technique, 2) the false acknowledgement technique, 3) payload shifting technique, 4) the MTU adjustment technique, 5) the client-side application-aware technique, and/or 5) the network disruption shielding technique.

In one further illustrative example of the present invention, an online meeting, collaboration and/or desktop sharing service, such as the hosted service of GoToMeeting.com, WebEx.com,or LiveMeeting.com may use the techniques of the present invention in one or more combinations. The host service may use a gateway 340, and the techniques of illustrative method 260 to facilitate a peer-to-peer connection between a first computing device of a meeting presenter and a second computing device of a meeting attendee. The computing devices of the meeting presenter and attendees may download via the host service the remote access client 120, or any portions thereof. Once the meeting presenter and the meeting attendee establish a peer-to-peer connection, the peer computing devices may use any of the optimization techniques of the present invention to optimize their communications, such as the MTU adjustment technique, client-side application aware technique, or the network disruption shielding technique. Along with the peer-to-peer routing, the optimization techniques of the present invention, will improve the performance, efficiency and user experience of the online meeting, collaboration, or desktop sharing.

In yet a further aspect and in view of Figure 2A, for example, the remote access client 120 of the present invention can distribute Dynamic Host Configuration Protocol (DHCP) IP addresses of the client 105 or the publicly visible IP addresses to the telecommunication device 210a-210b, such as either a hardware or software based VoIP telephone. The gateway 340 of the present invention facilitates the discovery of the public IP addresses of the client, such as client 105b illustrated in Figure 2A. As such, the techniques of the present invention enables protocols that communicate their IP address over the protocol to continue to function.

Many alterations and modifications may be made by those having ordinary skill in the art without departing from the spirit and scope of the invention. Therefore, it must be expressly understood that the illustrated embodiments have been shown only for the purposes of example and should not be taken as limiting the invention, which is defined by the following claims. These claims are to be read as including what they set forth

literally and also those equivalent elements which are insubstantially different, even though not identical in other respects to what is shown and described in the above illustrations.

We claim:

1. A method for establishing a peer to peer communication session between a first computing device on a first network and a second computing device on a second network, the first network disconnected from and not routable to the second network, the method comprising the steps of:

(a) establishing, by the first computing device, a first tunneling session with a third computing device, and establishing, by the second computing device, a second tunneling session with the third computing device;

(b) initiating, by the first computing device, a communication session to the second computing device via the third computing device;

(c) receiving, by a server, a signal to establish the communication session;

(d) communicating, by the server, to the first computing device a first network address comprising a network address of the second computing device associated with the second tunneling session;

(e) communicating, by the first computing device, a request to initiate a connection with the second computing device using the first network address;

(f) intercepting, by the third computing device, the request, and providing the first computing device a second network address for the second computing device, the second network address comprising a public network address associated with the second computing device; and

(g) communicating, by the third computing device, a request to the second computing device to allow a connection from the first computing device using the second network address.

2. The method of claim 1, wherein at least a portion of one of the first tunneling session or the second tunneling session comprises one of a Secure Socket Layer or a virtual private network

3. The method of claim 1, wherein the third computing device comprises a remote access gateway.

4. The method of claim 1, wherein the second computing device is located behind a firewall associated with the second network address.

5. The method of claim 1, comprising providing, by the third computing device, the second network address to the first computing device by communicating an out of band signal to the first computing device via the first tunneling session.

6. The method of claim 1, comprising providing, by the second computing device, a forward hole in a firewall for the first computing device to communicate to the second computing device using the second network address.

7. The method of claim 1, comprising communicating, by the third computing device, a key to the first computing device and the second computing device.

8. The method of claim 7, comprising communicating, by the first computing device, the key to the second computing device.

9. The method of claim 8, comprising checking, by the first computing device, that the key received from the second computing device matches the key of the first computing device before transmitting data to the second computing device.

10. The method of claim 7, comprising communicating, by the second computing device, the key to the first computing device.

11. The method of claim 10, comprising checking, by the second computing device, that the key received from the first computing device matches the key of the second computing device before transmitting data to the second computing device.

12. The method of claim 1, associating a first telecommunication device with the first computing device, and associating a second telecommunication device with the second computing device.

13. The method of claim 12, wherein one of the first telecommunication device or the second telecommunication device comprises one of a software component or a hardware component.

14. The method of claim 12, comprising establishing a telecommunication session between the first telecommunication device and the second telecommunication device via the connection.

15. The method of claim 15, comprising communicating between the first telecommunication device and the second telecommunication device over the telecommunication session without traversing the to the first computing device

16. The method of claim 1, comprising communicating a remote display protocol via the connection between the first computing device and the second computing device.

17. The method of claim 16, wherein the remote desktop protocol comprises one of an Independent Computing Architecture protocol or a Remote Desktop Protocol.

18. The method of claim 1, comprising sharing a screen view of the first computing device with the second computing device via the connection.

19. In a gateway, a method for establishing a peer to peer communication session between a first computing device on a first network and a second computing device on a second network, the first network disconnected from and not routable to the second network, the method comprising the steps of:

(a) establishing a first tunneling session with the first computing device on a first network;

(b) establishing a second tunneling session with the second computing device on the second network;

(c) receiving a request by the first computing device to initiate a communication session with the second computing device;

(d) providing to the first computing device a first network address for contacting the second computing device, the first network address comprising a network address of the second computing device associated with the second tunneling session;

(e) receiving a request by the first computing device to initiate a connection with the second computing device using the first network address;

(f) intercepting the request to initiate the connection, and providing the first computing device a second network address for the second computing device, the second network address comprising a public network address associated with the second computing device; and

(g) communicating to the second computing device a request to allow the connection from the first computing device to the second computing device using the second network address.

20. The method of claim 19, wherein at least a portion of one of the first tunneling session or the second tunneling session comprises one of a Secure Socket Layer or a virtual private network.

21. The method of claim 19, wherein the second computing device is located behind a firewall associated with the second network address.

22. The method of claim 19, comprising providing the second network address to the first computing device by communicating an out of band signal to the first computing device via the first tunneling session.

23. The method of claim 19, comprising communicating a key to the first computing device.

24. The method of claim 19, comprising communicating a key to the second computing device.

25. A system for establishing a peer to peer communication session between a first computing device on a first network and a second computing device on a second network via a third computing device, the first network disconnected from and not routable to the second network, the system comprising:

a first computing device on the first network;

a second computing device on the second network;

a third computing device establishing a first tunneling session with the first computing device and a second tunneling session with the second computing device;

a server accessible via the third computing device;

wherein:

the server communicates via the third computing device to the first computing device a first network address comprising a network address of the second computing device associated with the second tunneling session;

the first computing device communicates via the third computing device a first request to initiate a connection with the second computing device using the first network address;

the third computing device intercepts the first request, and provides the first computing device a second network address for the second computing device, the second network address comprising a public network address associated with the second computing device; and

the third computing device communicates a second request to the second computing device to allow a connection from the first computing device using the second network address.

26. The system of claim 25, wherein at least a portion of one of the first tunneling session or the second tunneling session comprises one of a Secure Socket Layer or a virtual private network.

27. The system of claim 25, wherein the third computing device comprises a remote access gateway.

28. The system of claim 25, wherein the second computing device is located behind a firewall associated with the second network address.

29. The system of claim 25, wherein the third computing device provides the second network address to the first computing device by communicating an out of band signal via the first tunneling session.

30. The system of claim 25, wherein the second computing device provides a forward hole in a firewall for the first computing device to communicate to the second computing device using the second network address.

31. The system of claim 25, wherein the third computing device communicates a key to the first computing device and the second computing device.

32. The system of claim 31, wherein the first computing device communicates the key to the second computing device.

33. The system of claim 32, wherein the first computing device checks that the key received from the second computing device matches the key of the first computing device before transmitting data to the second computing device.

34. The system of claim 31, wherein the second computing device communicates the key to the first computing device.

35. The system of claim 34, wherein the second computing device checks that the key received from the first computing devices matches the key of the second computing device before transmitting data to the second computing device.

36. The system of claim 25, comprising a first telecommunication device associated with the first computing device, and a second telecommunication associated with the second computing device.

37. The system of claim 36, wherein one of the first telecommunication device or the second telecommunication device comprises one of a software component or a hardware component.

38. The system of claim 37, wherein the first telecommunication device establishes a telecommunication session with the second telecommunication device via the connection.

39. The system of claim 38, wherein the first telecommunication device communicates with the second telecommunication device over the telecommunication session without traversing the third computing device.

40. The system of claim 25, wherein the first computing device and the second computing device communicate a remote display protocol via the connection.

41. The system of claim 25, wherein the remote desktop protocol comprises one of an Independent Computing Architecture protocol or a Remote Desktop Protocol.

42. The system of claim 25, wherein the first computing device shares a screen view with the second computing device via the connection.

43. A gateway for establishing a peer to peer communication session between a first computing device on a first network and a second computing device on a second network, the first network disconnected from and not routable to the second network, the gateway comprising:

a means for establishing a first tunneling session with the first computing device on a first network;

a means for establishing a second tunneling session with the second computing device on the second network;

a means for receiving a request by the first computing device to initiate a communication session with the second computing device;

a means for providing to the first computing device a first network address for contacting the second computing device, the first network address comprising a network address of the second computing device associated with the second tunneling session;

a means for receiving a request by the first computing device to initiate a connection with the second computing device using the first network address;

a means for intercepting the request to initiate the connection, and providing the first computing device a second network address for the second computing device, the second network address comprising a public network address associated with the second computing device; and

a means for communicating to the second computing device a request to allow the connection from the first computing device to the second computing device using the second network address.

44. The system of claim 43, wherein at least a portion of one of the first tunneling session or the second tunneling session comprises one of a Secure Socket Layer or a virtual private network.

45. The system of claim 43, wherein the second computing device is located behind a firewall associated with the second network address.

46. The system of claim 43, comprising a means for providing the second network address to the first computing device by communicating an out of band signal to the first computing device via the first tunneling session.

47. The system of claim 43, comprising a means for communicating a key to the first computing device.

48. The system of claim 43, comprising a means for communicating a key to the second computing device.

49. A method for communicating via a lossless protocol a packet constructed for transmissions via a lossy protocol, the method comprising the steps of:

(a) establishing a connection between a first computing device and a second computing device via a lossless protocol;

(b) detecting, by the first computing device, a lossless protocol packet comprising a payload having one or more packets constructed in accordance with a lossy protocol;

(c) communicating, by the first computing device, a false acknowledgement of receipt of
the lossless protocol packet to one of the first computing device or the second computing device; and

(d) communicating, by the first computing device, the lossless protocol packet to the second computing device.

50. The method of claim 49, comprising encrypting, by the first computing device, the one or more packets using a key.

51. The method of claim 50, comprising providing the encryption key to the first computing device via an out of band transport security layer session between the first computing device and the second computing device.

52. The method of claim 49, comprising encrypting the one or more packets on a packet by packet basis.

53. The method of claim 49, further comprising performing step (c) before step (d).

54. The method of claim 49, wherein the second computing device is a gateway.

55. The method of claim 49, comprising, in response to receiving the false acknowledgement of receipt of the lossless protocol packet by one of the first computing device or the second computing, preventing a network stack of one of the first computing device or the second computing from executing an operation associated with providing a lossless characteristic of the lossless protocol.

56. The method of claim 49, wherein the lossless protocol comprises a transport control protocol.

57. The method of claim 56, comprising preventing the network stack of one of the first computing device or the second computing device from executing one or more of the following in connection with the lossless protocol: a retransmit, an ordering, a flow control algorithm, a naple's algorithm, and a sliding window algorithm.

58. The method of claim 49, wherein the lossy protocol comprises a user datagram protocol.

59. The method of claim 49, comprising communicating, by the first computing device, the
lossless protocol packet via one of a secure socket layer or a transport security layer tunnel to
the second computing device.

60. The method of claim 49, wherein the one or more packets comprises a real-time protocol.

61. The method of claim 49, comprising communicating by the first computing device one of
real-time voice, audio, or data to the second computing device via the one or more packets.

62. A system for communicating via a lossless protocol a packet constructed for transmissions via a lossy protocol, the system comprising:

a means for establishing a connection between a first computing device and a second computing device via a lossless protocol;

a means for detecting, by the first computing device, a lossless protocol packet comprising a payload having one or more packets constructed in accordance with a lossy protocol;

a means for communicating, by the first computing device, a false acknowledgement of receipt of the lossless protocol packet to one of the first computing device or the second computing device; and

a means for communicating, by the first computing device, the lossless protocol packet to the second computing device.

63. The system of claim 62, comprising a means for encrypting, by the first computing device, the one or more packets using a key.

64. The system of claim 63, comprising a means for providing the encryption key to the first computing device via an out of band transport security layer session between the first computing device and the second computing device.

65. The system of claim 63, comprising a means for encrypting the one or more protocol packets on a packet by packet basis.

66. The system of claim 62, further comprising a means for communicating the false acknowledgement of receipt of the lossless protocol packet before communicating the

lossless protocol packet.

67. The system of claim 62, wherein the second computing device is a gateway.

68. The system of claim 62, comprising a means, in response to receiving the false acknowledgement of receipt of the lossless protocol packet by one of the first computing device or the second computing, for preventing a network stack of one of the first computing device or the second computing from executing an operation associated with providing a lossless characteristic of the lossless protocol.

69. The system of claim 62, wherein the lossless protocol comprises a transport control protocol.

70. The system of claim 69, comprising a means for preventing the network stack of one of the first computing device or the second computing device from executing one or more of the following in connection with the lossless protocol: a retransmit, an ordering, and a flow control algorithm.

71. The system of claim 62, wherein the lossy protocol comprises a user datagram protocol.

72. The system of claim 62, comprising a means for communicating, by the first computing device, the lossless protocol packet via one of a secure socket layer or a transport security layer tunnel to the second computing device.

73. The system of claim 62, wherein the one or more packets comprises a real-time protocol.

74. The system of claim 62, comprising a means for communicating by the first computing device one of real-time voice, audio, or data to the second computing device via the one or more packets.

75. A method for transmitting packets from an application using an unreliable

transport protocol over a TCP connection, comprising:

receiving, at a first device, a first packet to be transmitted using an unreliable transport protocol;

creating a first TCP packet including a first payload of the received first packet and a first TCP header of information associated with a TCP connection established between the first device and a second device;

transmitting, by the first device, the first TCP packet to the second device;

receiving, at the first device, a second packet to be transmitted using an unreliable transport protocol;

creating a second TCP packet including a second payload of the received second packet and the first TCP header information; and

transmitting, by the first device, before receipt of an acknowledgement of the receipt of the first payload from the second device, the second TCP packet to the second device.

76. The method of claim 75, comprising establishing the TCP connection with a port number associated with the unreliable transport protocol.

77. The method of claim 75, comprising dynamically determining, by the first device, the first TCP packet and second TCP packet comprise an unreliable transport protocol.

78. The method of claim 75, wherein the unreliable transport protocol is UDP.

79. The method of claim 75, comprising further:

receiving the first TCP packet and second TCP packet on the first device by intercepting the first TCP packet and second TCP packet using a packet capturing mechanism.

80. The method of claim 75, comprising establishing, by the first device, the TCP connection with a VPN gateway device.

81. The method of claim 75, comprising establishing peer-to-peer communications between the first device and the second device via the TCP connection.

82. The method of claim 75, comprising encrypting, by the first device, the first and second TCP packets, and decrypting, by the second device, the encrypted first and second TCP packets.

83. A method for transmitting packets from an application using an unreliable transport protocol over a TCP connection, comprising:

intercepting, at a second device, a first TCP packet created on a first device and received on the second device, the first TCP packet including a first payload of a first packet generated by an application using an unreliable protocol and a first TCP header of information associated with a TCP connection established between the first device and the second device, the intercepting occurring before the first TCP packet is provides to a TCP stack on the second device;

identifying, responsive to the TCP header of information, that the first payload is a packet generated by an application using an unreliable transport protocol;

stripping the TCP header of information from the first TCP packet; and

forwarding the first payload to an application using the unreliable data protocol.

84. The method of claim 83, wherein the unreliable protocol is UDP.

85. The method of claim 83, wherein the step of identifying comprises identifying the TCP header information includes a port number associated with the unreliable transport protocol.

86. The method of claim 83, comprising further:

intercepting, by the second device, the first TCP packet using a packet capture driver.

87. The method of claim 83, wherein the first device is a client device and the

second device is a VPN gateway.

88. The method of claim 87, comprising further:
performing Network Address Translation (NAT) on the second device prior to forwarding the first payload to the application.

89. A system for transmitting packets from an application using an unreliable transport protocol over a TCP connection, the system comprising:
a first device, the first device comprising:
an application generating a first and second packet, the first and second packet intended to be transmitted using an unreliable transport protocol;
a filter process, the filter process intercepting the first and second packets from the application and forwarding the intercepted packets to a tunnel process; and
a tunnel process, the tunnel process requesting the opening of a TCP connection between the first device and a second device, the request to open the TCP connection indicating to the first and second device that the TCP connection will transport packets intended to be transmitted with an unreliable transport protocol, the tunnel process forwarding the first and second packets as payloads in a first and second TCP packet to the second device, the tunnel process sending the second TCP packet after sending the first TCP packet and prior to receiving an acknowledgement for the first TCP packet ; and
a second device in communication with the first device, the second device comprising:
a second tunnel process opening the TCP connection requested by the first device, the second tunnel process identifying and forwarding the source address of the TCP connection to a second filter process; and
the second filter process, the second filter process intercepting packets from the application received at the second device with the TCP connection source address in a header, the second filter process stripping the TCP header from the received packets and forwarding the stripped packets,

circumventing the TCP/IP stack on the second device, to an intended destination.

90. The system of claim 89, wherein the filter process on the first device comprises a packet capture driver.

91. The system of claim 89, wherein the second filter process on the second device comprises a packet capture driver.

92. The system of claim 89, wherein the first device is a client device and the second device is a VPN gateway device.

93. The system of claim 89, further comprising:
a third device to which the stripped packets are transmitted.

94. The system of claim 93, wherein the second device comprises further:
a Network Address Translation (NAT) table used to perform network address translation prior to transmitting the stripped packets to a third device.

95. The system of claim 89, wherein the unreliable data protocol is UDP.

96. A method for adjusting the maximum transmission unit of a secure network communication to reduce network fragmentation, the method comprising the steps of:

(a) establishing a session between a first computing device and a second computing device, the first computing device having a first network stack;

(b) detecting, by the first computing device, a network packet having an encrypted payload;

(c) determining, by the first computing device, a setting for a maximum transmission unit parameter of the first network stack to reduce the maximum transmission unit size by at least a size associated with the encrypted portion of the payload; and

(d) altering the maximum transmission unit parameter of the first network stack to the determined setting.

97. The method of claim 96, comprising communicating the network packet via one of a secure socket layer or a transport layer security tunnel to the second computing device.

98. The method of claim 96, wherein the payload comprises a real-time protocol.

99. The method of claim 96, further comprising altering the maximum transmission unit parameter via a network driver interface specification level mechanism of the first network stack

100. The method of claim 96, further comprising determining the setting of the maximum transmission unit parameter dynamically per session between the first computing device and the second computing device.

101. The method of claim 96, comprising establishing the session between the first computing device and the second computing device via a gateway.

102. The method of claim 96, communicating by the first computing device one of real-time voice, audio, or data to the second computing device via the payload of the network packet.

103. The method of claim 96, comprising communicating a false acknowledgement of receipt of the network packet to one of the first computing device or the second computing device before communicating the network packet.

104. The method of claim 96, further comprising establishing the session between the first computing device and the second computing device via an agent of the first computing device.

105. The method of claim 104, comprising communicating, by the agent, via an IOCTL application programming interface to the first network stack to alter the

maximum transmission unit parameter to the determined setting.

106. A system for adjusting the maximum transmission unit of a secure network communication to reduce network fragmentation, the system comprising:

a means for establishing a session between a first computing device and a second computing device, the first computing device having a first network stack;

a means for detecting, by the first computing device, a network packet having an encrypted payload;

a means for determining, by the first computing device, a setting for a maximum transmission unit parameter of the first network stack to reduce the maximum transmission unit size by at least a size associated with the encrypted portion of the payload; and

a means for altering the maximum transmission unit parameter of the first network stack to the determined setting.

107. The system of claim 106, comprising a means for communicating the network packet via one of a secure socket layer or a transport layer security tunnel to the second computing device.

108. The system of claim 106, wherein the payload comprises a real-time protocol.

109. The system of claim 106, wherein the payload comprises a representation of one of real-time voice, audio, or data.

110. The system of claim 106, further comprising a means for altering the maximum transmission unit parameter of the first computing device via a network driver interface specification level mechanism of the first network stack

111. The system of claim 106, further comprising a means for determining the setting of the maximum transmission unit parameter dynamically per session between the first computing device and the second computing device.

112. The system of claim 106, comprising a means for establishing the session

between the first computing device and the second computing device via a gateway.

113. The system of claim 106, comprising a means for communicating by the first computing device one of real-time voice, audio, or data to the second computing device via the payload of the network packet.

114. The system of claim 106, comprising a means for communicating a false acknowledgement of receipt of the network packet to one of the first computing device or the second computing device before communicating the network packet.

115. The system of claim 106, wherein the network packet comprises a lossless protocol packet.

116. The system of claim 115, wherein the lossless protocol packet comprises a transport control protocol.

117. The system of claim 106, wherein the payload comprises a lossy protocol packet.

118. The system of claim 117, wherein the lossy protocol packet comprises a user datagram protocol.

119. The system of claim 106, comprising an agent of the first computing device for establishing the session between the first computing device and the second computing device.

120. The system of claim 119, wherein the agent communicates via an IOCTL application programming interface to the first network stack to alter the maximum transmission unit parameter to the determined setting.

121. A method for a client to prioritize network communications of the client associated with an application of the client, the method comprising the steps of:

(a) intercepting, by the client, one or more network packets associated with one or more applications of the client;

(b) storing, by the client, the one or more network packets to a queue;

(c) determining, by the client, the queued one or more network packets is associated with a first application of the client;

(d) indicating, by the client, a priority for the determined one or more network packets to place the determined one or more network packets ahead of at least one network packet in the queue associated with a second application of the client; and

(e) providing the prioritized one or more network packets for communications via a network stack of the client.

122. The method of claim 121, wherein the step of determining, by the client, further comprises determining the queued one or more networks packets of the first application comprises real-time data.

123. The method of claim 122, wherein the real-time data comprises one of the following: a real-time protocol, a user datagram protocol, and a representation of one of voice or audio.

124. The method of claim 121, comprising preventing, by the client, at least one network packet of the second application from being communicated via the network stack ahead of the one or more network packets of the first application.

125. The method of claim 121, comprising holding, by the client, in the queue a network packet associated with the second application, and releasing the held network packet upon communication of the one or more network packets associated with the first application prioritized ahead of the held network packet.

126. The method of claim 121, comprising intercepting, by the client, the one or more network packets transparently to the one or more applications on the client.

127. The method of claim 121, comprising running the first application in the foreground, and the second application in the background.

128. The method of claim 121, comprising associating a priority with the first

application higher than a priority associated with the second application.

129. The method of claim 128, comprising specifying, by a user, the priority of one of the first application or the second application.

130. The method of claim 121, comprising receiving, by the client, the one or more network packets from a computing device.

131. The method of claim 121, comprising providing, by the one or more applications, the one or more network packets for communicating from the client to a computing device.

132. A client for prioritizing network communications of the client associated with an application of the client, the client comprising:

a mechanism for intercepting one or more network packets of the client associated with one or more applications of the client, and

a network driver for storing the one or more networks packets to a queue and communicating the one or more network packets via a network stack of the client; and

an agent for determining the one or more network packets is associated with a first application of the client, and indicating to the network driver a priority of the one or more network packets to place the determined one or more network packets ahead of at least one network packet in the queue associated with a second application of the client.

133. The client of claim 132, wherein the agent determines the one or more networks packets of the first application comprises real-time data.

134. The client of claim 132, wherein the real-time data comprises one of the following: a real-time protocol, a user datagram protocol, and a representation of one of voice or audio.

135. The client of claim 132, wherein one of the agent or the network driver prevents at least one network packet of the second application from being communicated via the network stack ahead of the one or more network packets of the first application.

136. The client of claim 132, wherein the network driver holds in the queue a network packet associated with the second application, and releasing the held network packet upon communication of the one or more network packets associated with the first application prioritized ahead of the held network packet.

137. The client of claim 132, wherein the mechanism intercepts the one or more network packets transparently to the one or more applications on the client.

138. The client of claim 132, wherein the first application is running in the foreground, and the second application is running in the background.

139. The client of claim 132, wherein the first application has a priority higher than the second application of the client.

140. The client of claim 132, comprising a configuration mechanism for a user to specify the priority.

141. The client of claim 132, wherein the client receives the one or more network packets from a computing device.

142. The client of claim 132, wherein the one or more applications provides the one or more network packets for communicating from the client to a computing device.

143. The client of claim 132, wherein the network driver comprises a Network Driver Interface Specification (NDIS) driver.

144. The client of claim 132, wherein the network driver operates in kernel-mode of an operating system of the client.

145. The client of claim 132, wherein the agent operates in user-mode of an operating system of the client.

146. The client of claim 132, wherein one of the agent or the network driver comprises the mechanism for intercepting one or more network packets of the client.

147. A method for shielding from a network disruption a session established via a first protocol, the method comprising the steps of:

(a) establishing, via an agent of a client, a session via a first protocol over a network connection between the client and a device, the network connection associated with a network stack, a first portion of the network stack comprises one or more layers of the network stack below the layer of the first protocol, and a second portion of the network stack comprises a layer for the first protocol and one or more layers of the network stack above the first protocol;

(b) detecting a disruption in the network connection causing the first portion of the network stack to be disestablished;

(c) maintaining, by the agent, the session and the second portion of the network stack during the disruption; and

(d) re-establishing the second portion of the network stack and the network connection while maintaining the session and the second portion of the network stack.

148. The method of claim 147, comprising the step of:

(e) continuing the session with the maintained second portion of the network stack and the re-established first portion of the network stack.

149. The method of claim 147, comprising the step of

(e) dropping, by the second portion of the network stack, any network packets received

during the disruption.

150. The method of claim 147, wherein the device comprises one of a remote access gateway or a computing device.

151. The method of claim 147, further comprising establishing the session via the first protocol of one of the following: secure socket layer (SSL) protocol, a transport layer security (TLS) protocol, and a tunneling protocol.

152. The method of claim 147, comprising communicating, by the agent, real-time data via the session between the client and the device.

153. The method of claim 152, wherein the real-time data comprises a real-time protocol.

154. The method of claim 152, wherein the real-time data comprises a representation of one of voice or audio.

155. The method of claim 147, comprising operating the agent in user-mode of an operating system of the client.

156. The method of claim 147, wherein the first portion of the network comprises one of a transport control protocol or an internet protocol.

157. The method of claim 147, wherein the second portion of the network stack comprises one of an internet protocol, a user datagram protocol, or a voice over internet protocol.

158. The method of claim 147, comprising the client communicating with the device via a remote display protocol.

159. The method of claim 158, wherein the remote display protocol comprises one of an Independent Computing Architecture protocol or a Remote Desktop protocol.

160. The method of claim 147, comprising performing one of steps (b), (c) and (d) transparently to an application of the client communicating via the network connection.

161. The method of claim 147, comprising intercepting, by the agent, transparently to an application of the client one or more network packets associated with the application.

162. The method of claim 147, comprising intercepting, by a network driver

associated with the second portion of the stack, transparently to the application on the client one or more network packets associated with the application.

163. A system for shielding from a network disruption a session established via a first protocol, the system comprising

an agent of a client establishing a session between the client and a device over a network connection via a first protocol;

a network stack having a first portion and a second portion, the first portion of the network stack comprising one or more layers of the network stack below the layer of the first protocol, and the second portion of the network stack comprising a layer for the first protocol and one or more layers of the network stack above the first protocol; and

a detector for detecting a disruption in the network connection causing the second portion of the network stack to be disestablished;

wherein:

upon detection of the disruption by the detector, the agent maintains the session and the second portion of the network stack during the disruption; and

the client re-establishes the first portion of the network stack and the network connection while the agent maintains the session and the second portion of the network stack.

164. The system of claim 163, wherein the agent continues the session with the maintained second portion of the network stack and the re-established first portion of the network stack.

165. The system of claim 163, wherein one of the first portion or the second portion of the network stack drops any network packets received during the disruption.

166. The system of claim 163, wherein the device comprises one of a remote access gateway or a computing device.

167. The system of claim 163, wherein the first protocol comprises one of the following: secure socket layer (SSL) protocol, a transport layer security (TLS) protocol, and a tunneling protocol.

168. The system of claim 163, wherein the agent communicates real-time data via the session between the client and the device.

169. The system of claim 168, wherein the real-time data comprises one of a real-time protocol.

170. The system of claim 168, wherein the real-time data comprises a representation of one of voice or audio.

171. The system of claim 163, wherein the agent operates in user-mode of an operating system of the client.

172. The system of claim 163, wherein the first portion of the network stack comprises one of a transport control protocol or an internet protocol.

173. The system of claim 163, wherein the second portion of the network stack comprises one of an internet protocol, a user datagram protocol, or a voice over internet protocol.

174. The system of claim 163, wherein the first protocol comprises a remote display protocol.

175. The system of claim 174, wherein the remote display protocol comprises one of an Independent Computing Architecture protocol or a Remote Desktop protocol.

176. The system of claim 163, wherein the agent intercepts one or more network packets of an application of the client transparently to the application.

177. The system of claim 163, comprising a network driver associated with the second portion of the network stack, the network driver intercepts one or more network packets of an application of the client transparently to the application, and provides the one or more packets to the agent to communicate via the session.

178. The system of claim 177, wherein the network driver comprises a Network Driver Interface Specification (NDIS) driver.

179. The system of claim 177, wherein the network driver operates in kernel-mode of an operating system of the client.

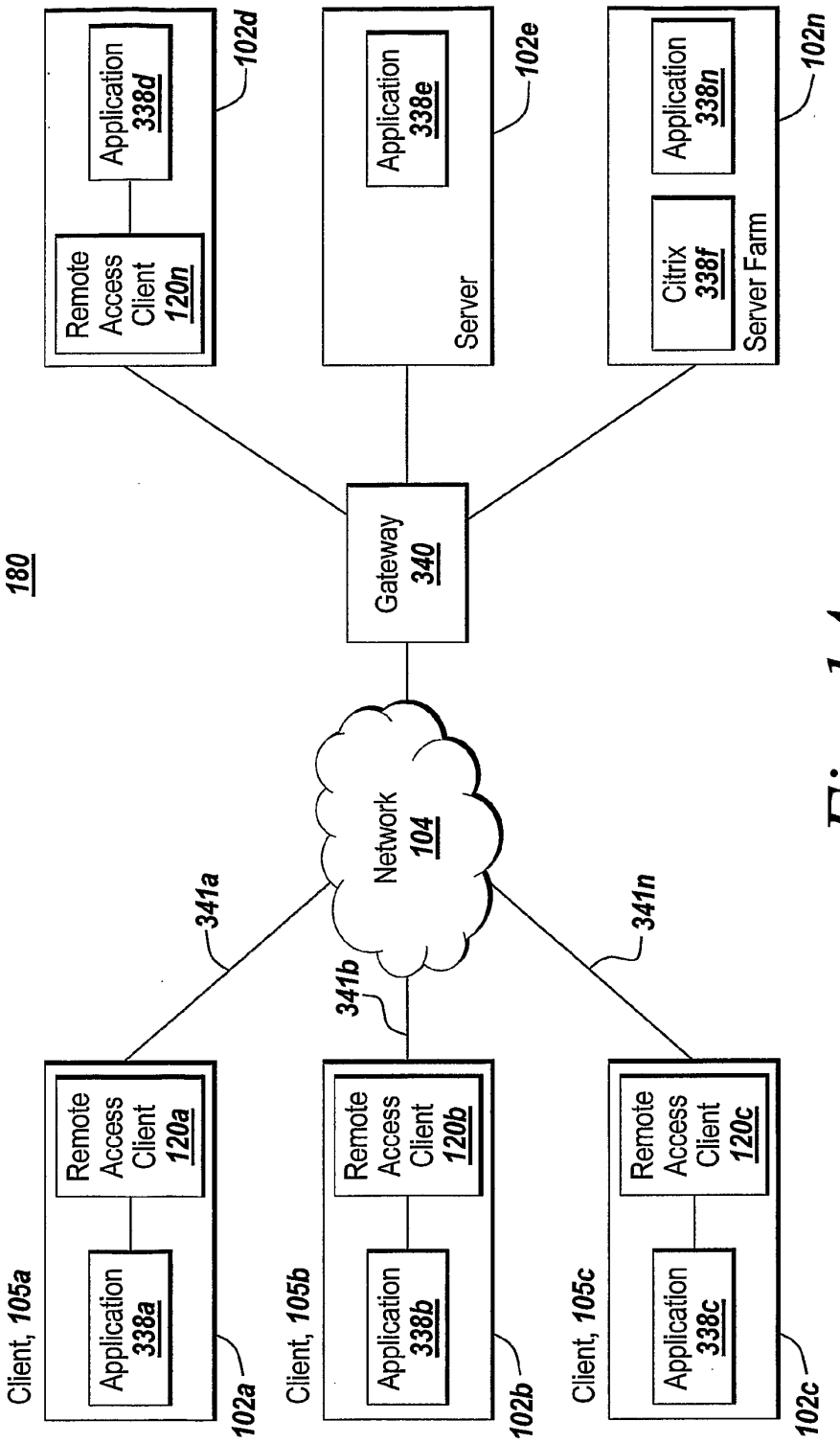

180
Client, 105a
Application 338a
Remote Access Client 120a
102a
341a
Client, 105b
Application 338b
Remote Access Client 120b
102b
341b
Client, 105c
Application 338c
Remote Access Client 120c
102c
341n
Network 104
Gateway 340
Remote Access Client 120n
Application 338d
102d
Server
Application 338e
102e
Server Farm
Citrix 338f
Application 338n
102n

Fig. 1A

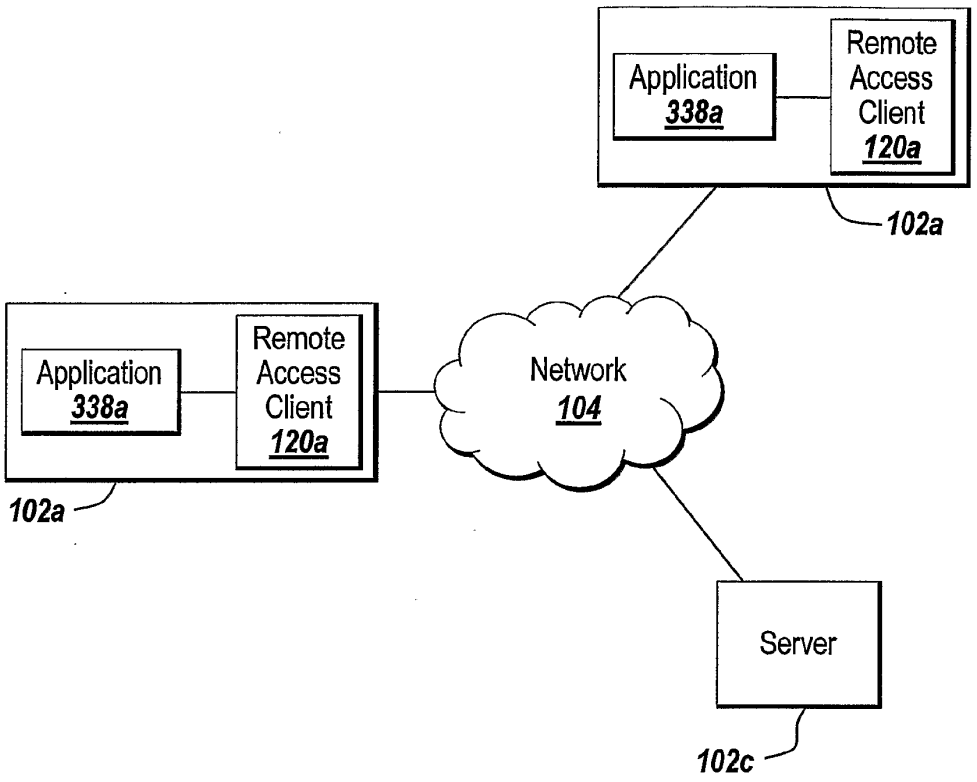

Application
338a
Remote
Access
Client
120a
102a
Application
338a
Remote
Access
Client
120a
102a
Network
104
Server
102c

Fig. 1B

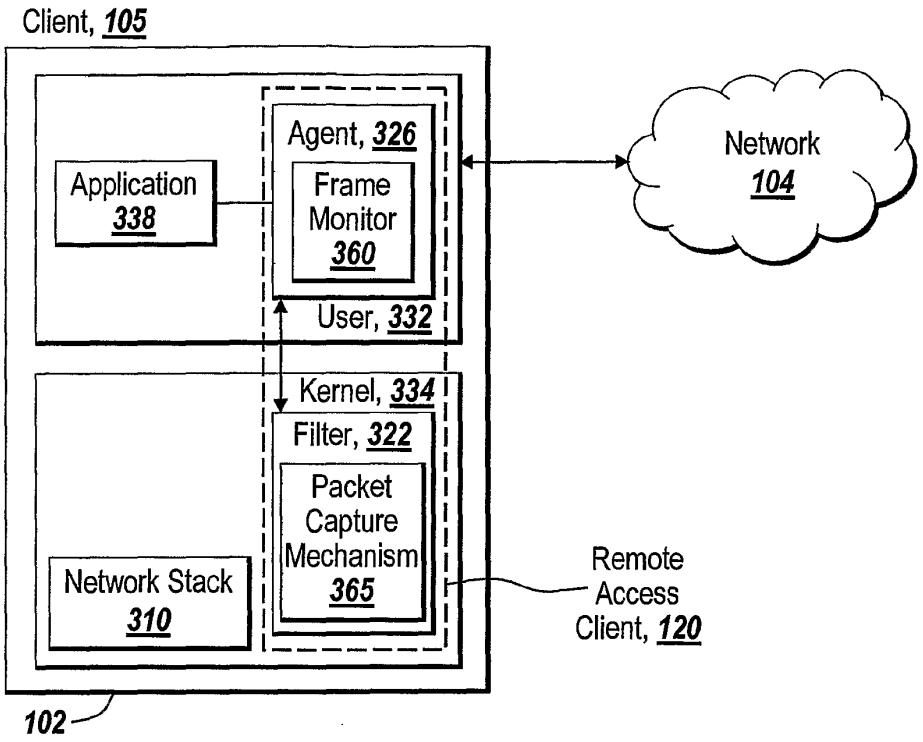

Client, 105
Agent, 326
Application 338
Frame Monitor 360
User, 332
Kernel, 334
Filter, 322
Packet Capture Mechanism 365
Network Stack 310
Network 104
Remote Access Client, 120
102

Fig. 1C

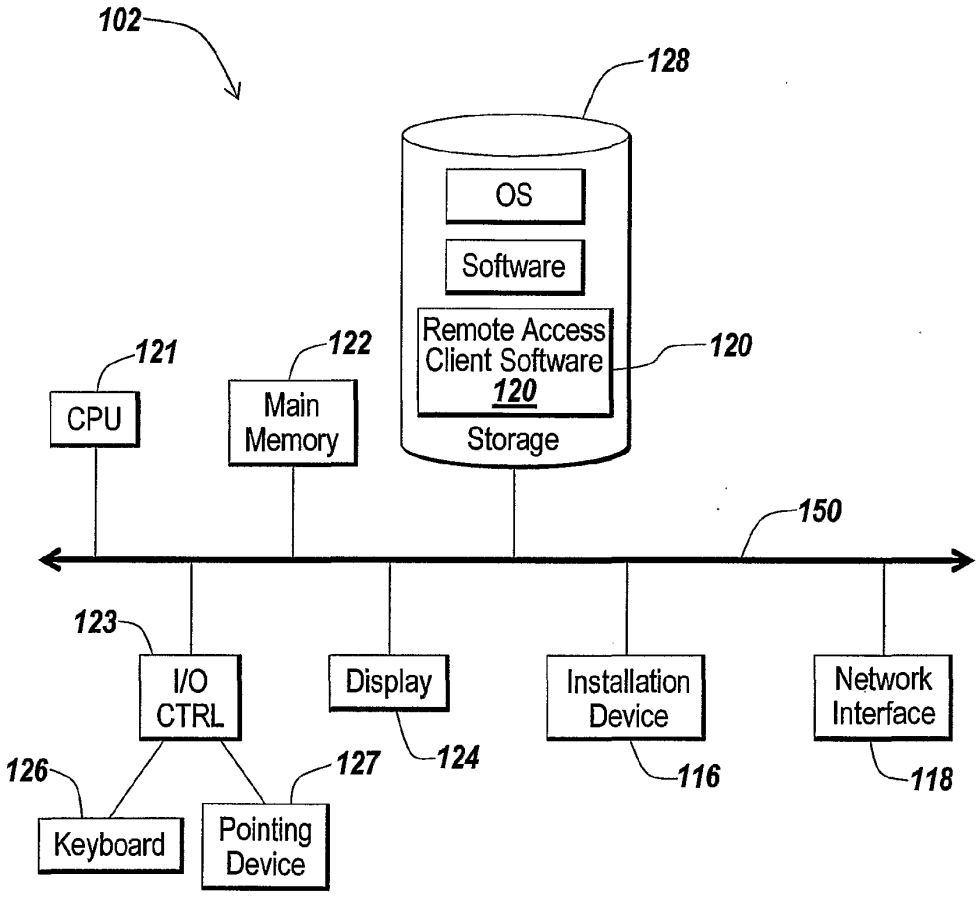

102
128
OS
Software
Remote Access Client Software
120
120
Storage
121
CPU
122
Main Memory
150
123
I/O CTRL
Display
124
Installation Device
116
Network Interface
118
126
Keyboard
127
Pointing Device

Fig. 1D

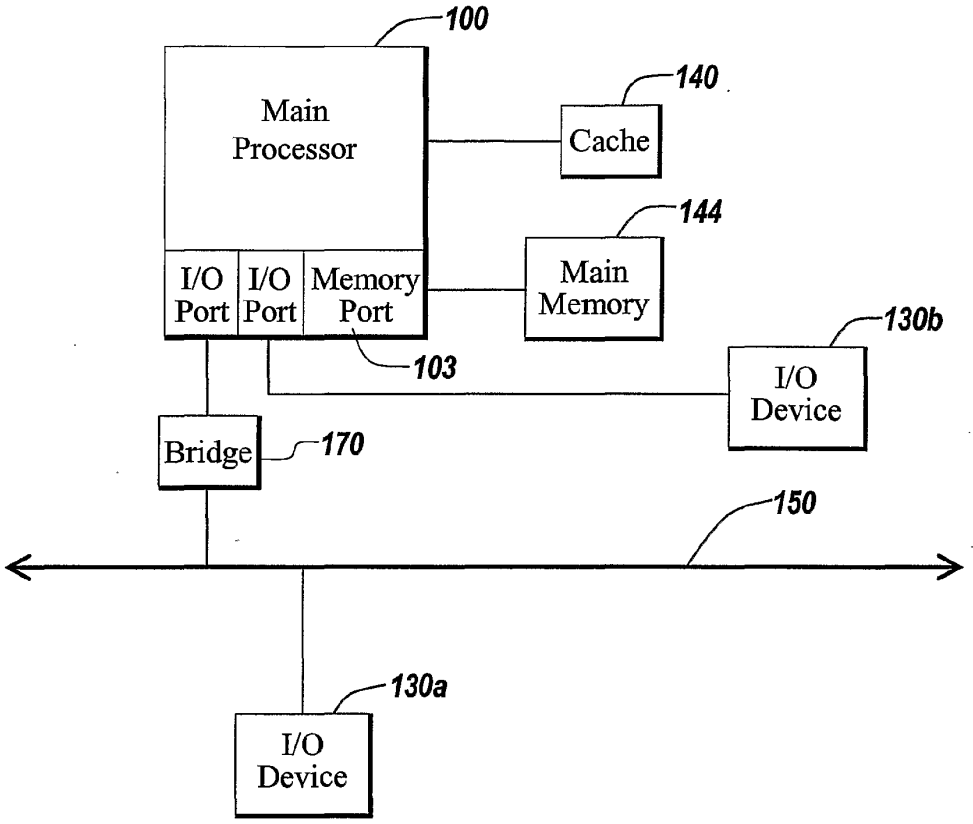

100
Main Processor
140
Cache
144
Main Memory
I/O Port
I/O Port
Memory Port
103
130b
I/O Device
Bridge
170
150
130a
I/O Device

Fig. 1E

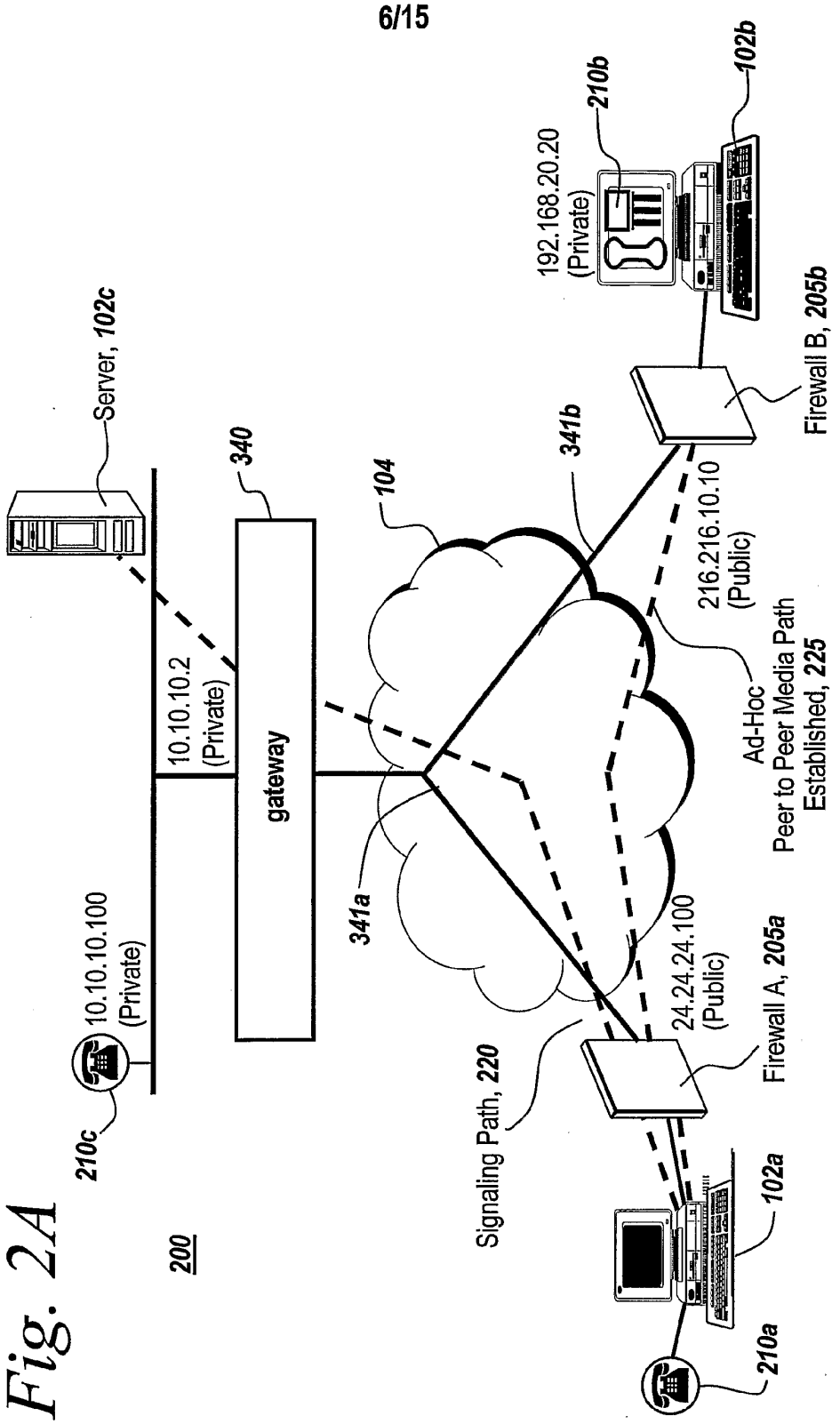

Server, 102c
340
104
341b
192.168.20.20
(Private)
210b
102b
10.10.10.2
(Private)
gateway
216.216.10.10
(Public)
Ad-Hoc
Peer to Peer Media Path
Established, 225
Firewall B, 205b
10.10.10.100
(Private)
341a
24.24.24.100
(Public)
Signaling Path, 220
Firewall A, 205a
210c
200
102a
210a

Fig. 2A

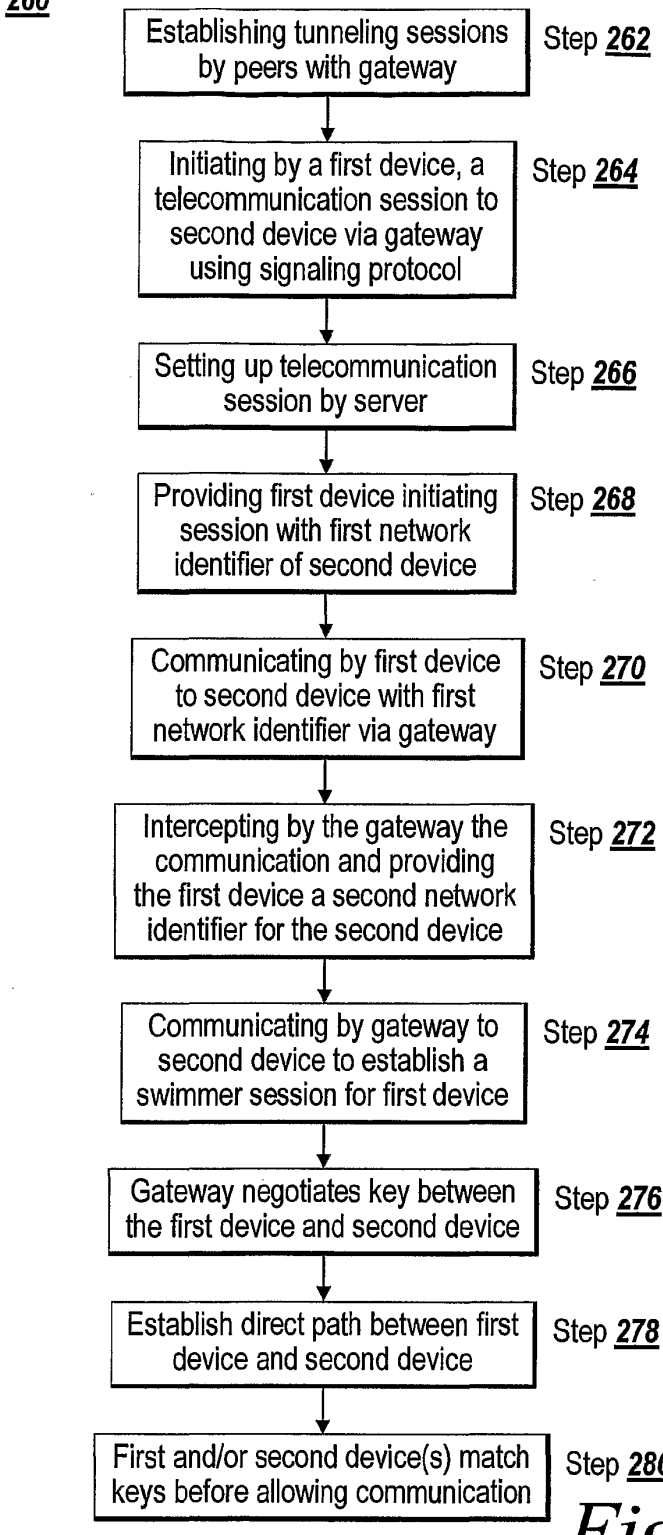

260
Establishing tunneling sessions by peers with gateway
Step 262
Initiating by a first device, a telecommunication session to second device via gateway using signaling protocol
Step 264
Setting up telecommunication session by server
Step 266
Providing first device initiating session with first network identifier of second device
Step 268
Communicating by first device to second device with first network identifier via gateway
Step 270
Intercepting by the gateway the communication and providing the first device a second network identifier for the second device
Step 272
Communicating by gateway to second device to establish a swimmer session for first device
Step 274
Gateway negotiates key between the first device and second device
Step 276
Establish direct path between first device and second device
Step 278
First and/or second device(s) match keys before allowing communication
Step 280

Fig. 2B

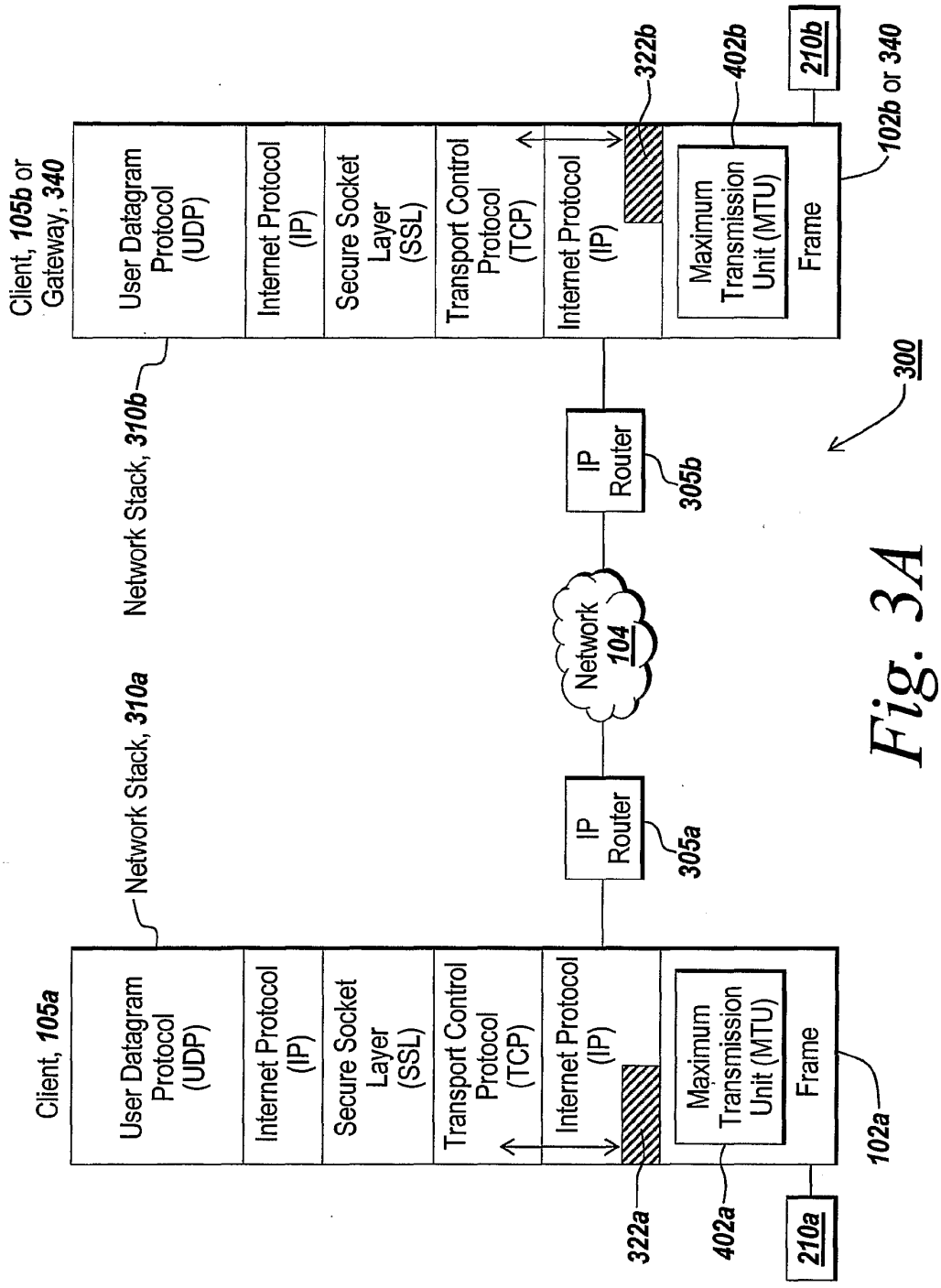

Client, 105a
User Datagram Protocol (UDP)
Internet Protocol (IP)
Secure Socket Layer (SSL)
Transport Control Protocol (TCP)
Internet Protocol (IP)
Maximum Transmission Unit (MTU)
Frame
Network Stack, 310a
Network Stack, 310b
Client, 105b or Gateway, 340
User Datagram Protocol (UDP)
Internet Protocol (IP)
Secure Socket Layer (SSL)
Transport Control Protocol (TCP)
Internet Protocol (IP)
Maximum Transmission Unit (MTU)
Frame
IP Router
305a
IP Router
305b
Network 104
300
322a
402a
210a
102a
322b
402b
210b
102b or 340

Fig. 3A

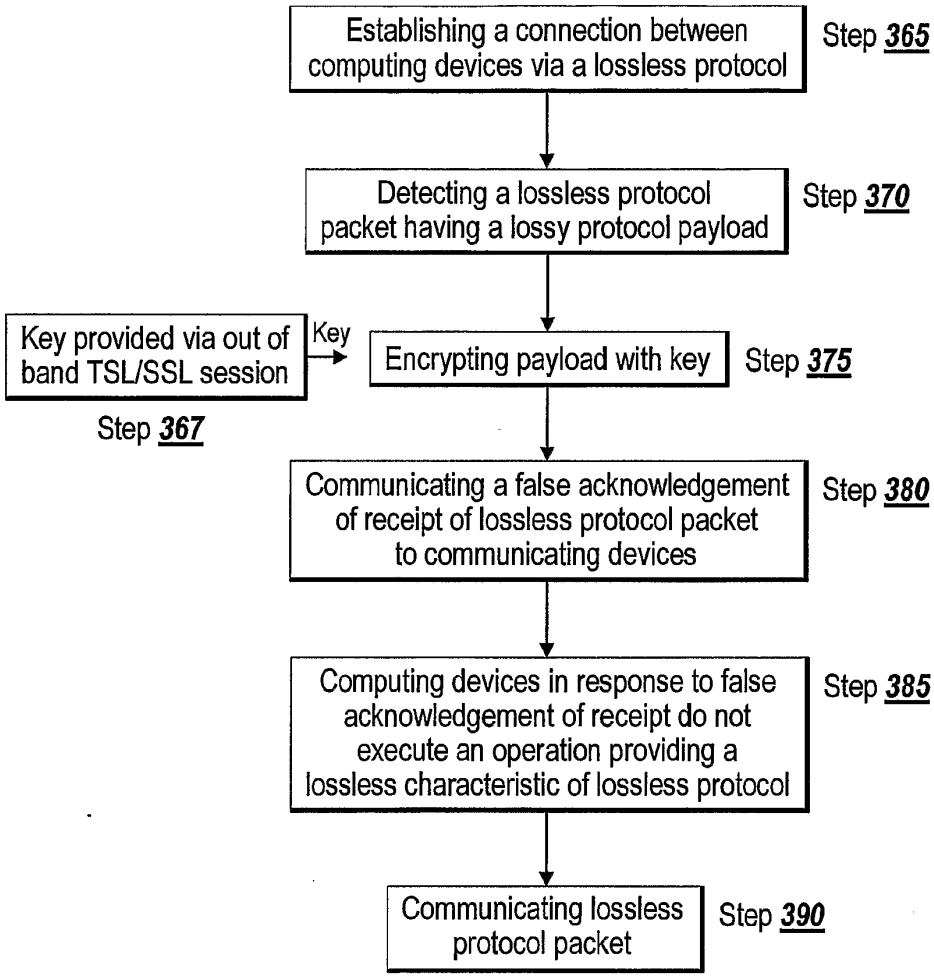

Establishing a connection between computing devices via a lossless protocol
Step 365
Detecting a lossless protocol packet having a lossy protocol payload
Step 370
Key provided via out of band TSL/SSL session
Key
Encrypting payload with key
Step 375
Step 367
Communicating a false acknowledgement of receipt of lossless protocol packet to communicating devices
Step 380
Computing devices in response to false acknowledgement of receipt do not execute an operation providing a lossless characteristic of lossless protocol
Step 385
Communicating lossless protocol packet
Step 390

Fig. 3B

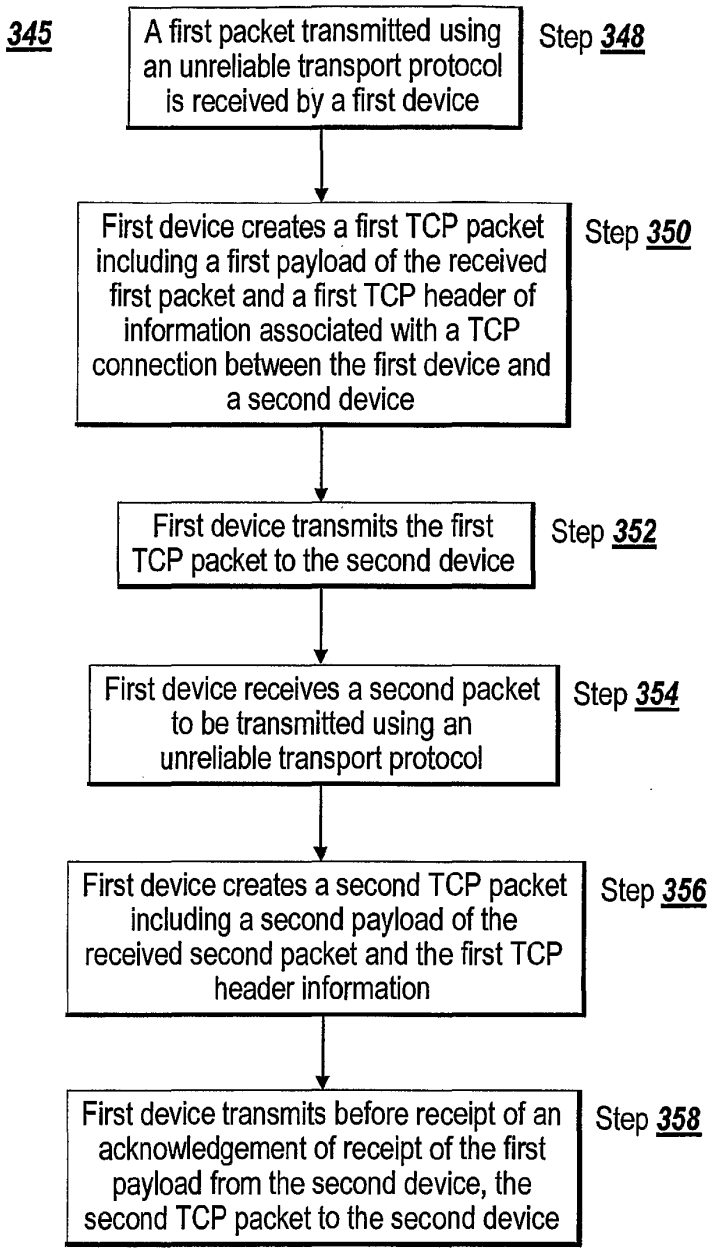

345
A first packet transmitted using an unreliable transport protocol is received by a first device
Step 348
First device creates a first TCP packet including a first payload of the received first packet and a first TCP header of information associated with a TCP connection between the first device and a second device
Step 350
First device transmits the first TCP packet to the second device
Step 352
First device receives a second packet to be transmitted using an unreliable transport protocol
Step 354
First device creates a second TCP packet including a second payload of the received second packet and the first TCP header information
Step 356
First device transmits before receipt of an acknowledgement of receipt of the first payload from the second device, the second TCP packet to the second device
Step 358

Fig. 3C

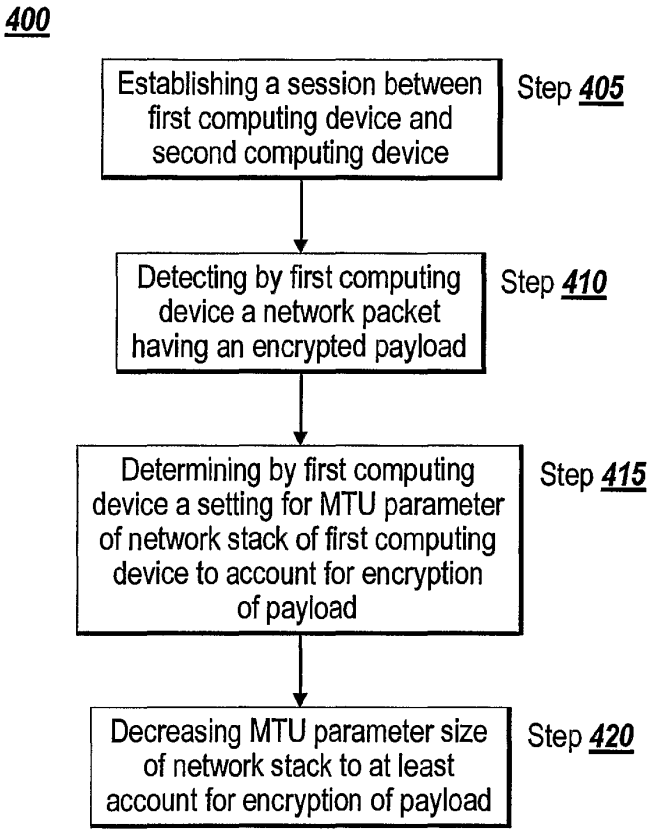

400
Establishing a session between first computing device and second computing device
Step 405
Detecting by first computing device a network packet having an encrypted payload
Step 410
Determining by first computing device a setting for MTU parameter of network stack of first computing device to account for encryption of payload
Step 415
Decreasing MTU parameter size of network stack to at least account for encryption of payload
Step 420

Fig. 4

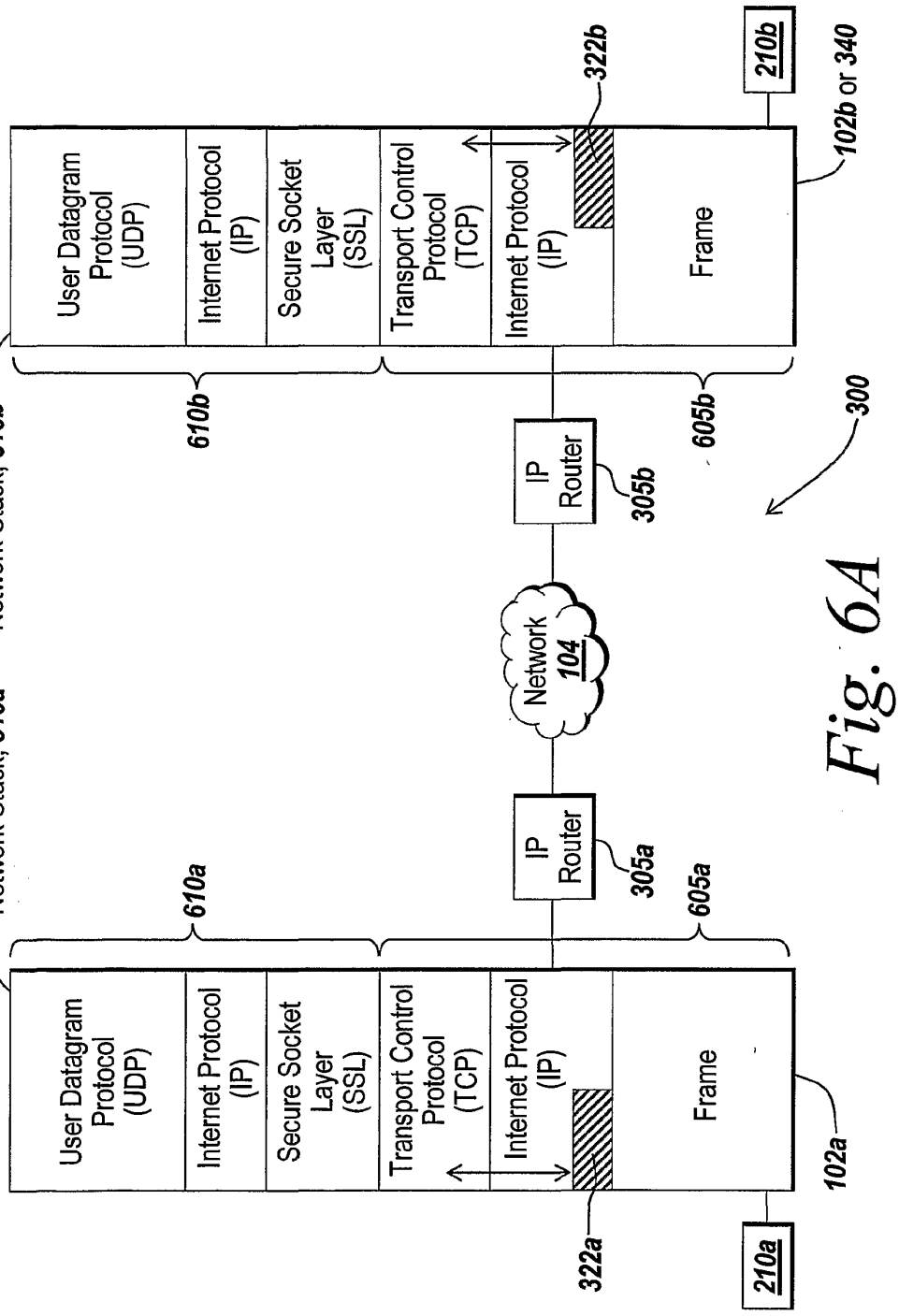

Network Stack, 310b
Network Stack, 310a
User Datagram Protocol (UDP)
Internet Protocol (IP)
Secure Socket Layer (SSL)
Transport Control Protocol (TCP)
Internet Protocol (IP)
Frame
610b
610a
605b
605a
IP Router
305b
IP Router
305a
Network 104
322b
322a
210b
210a
102b or 340
102a
300

Fig. 6A

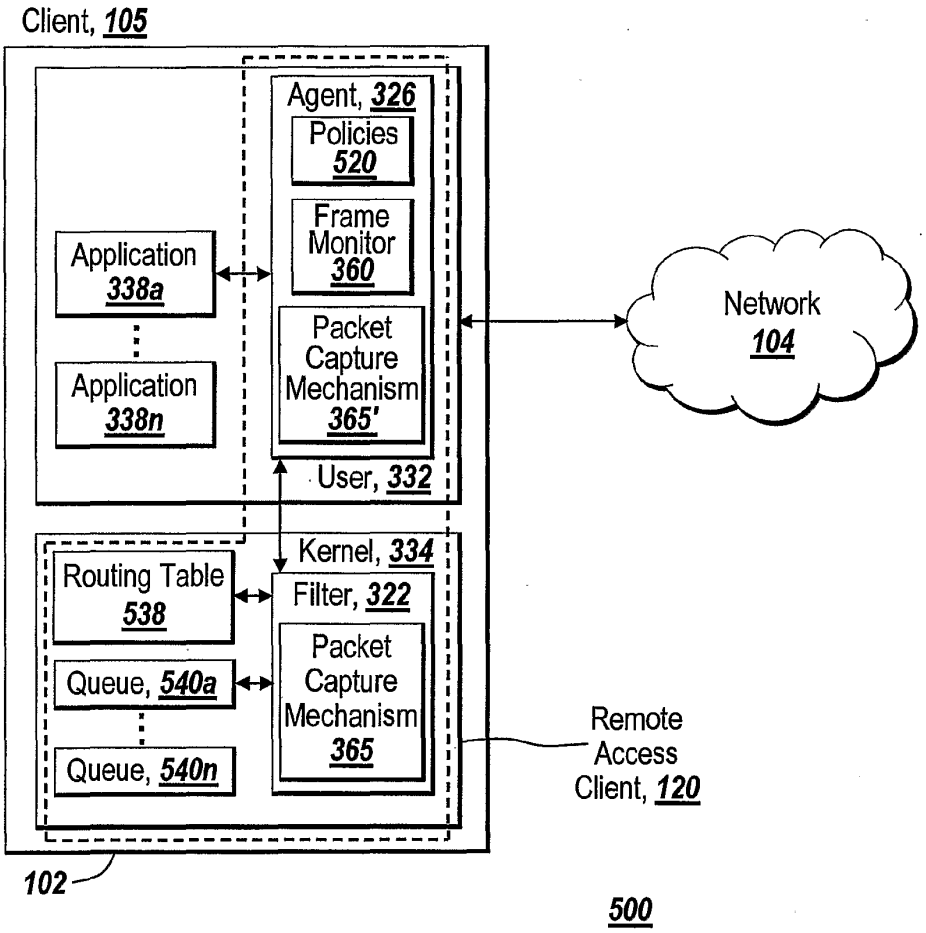

Client, 105
Agent, 326
Policies 520
Frame Monitor 360
Application 338a
Application 338n
Packet Capture Mechanism 365'
Network 104
User, 332
Kernel, 334
Routing Table 538
Filter, 322
Queue, 540a
Queue, 540n
Packet Capture Mechanism 365
Remote Access Client, 120
102
500

Fig. 5A

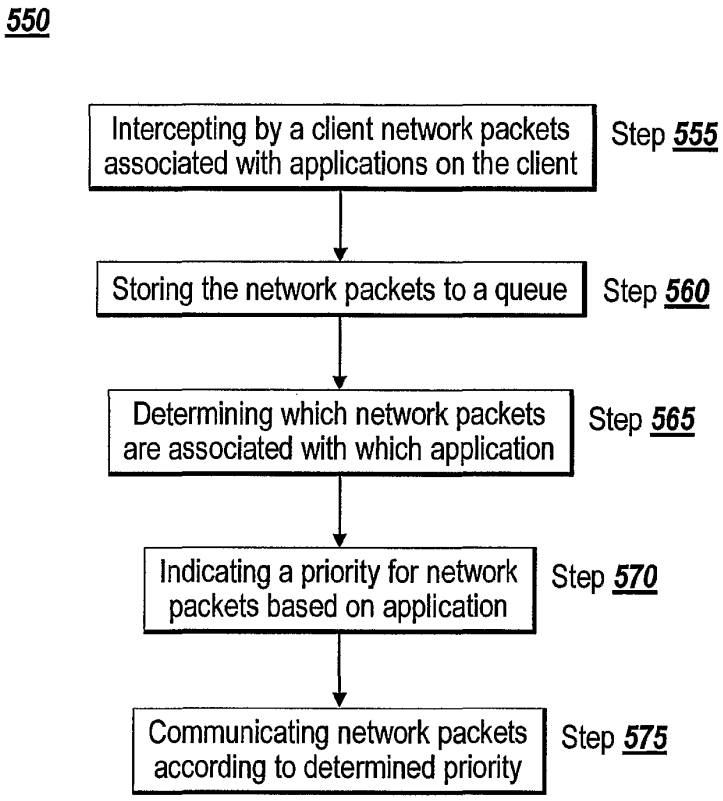

550
Intercepting by a client network packets associated with applications on the client
Step 555
Storing the network packets to a queue
Step 560
Determining which network packets are associated with which application
Step 565
Indicating a priority for network packets based on application
Step 570
Communicating network packets according to determined priority
Step 575

Fig. 5B

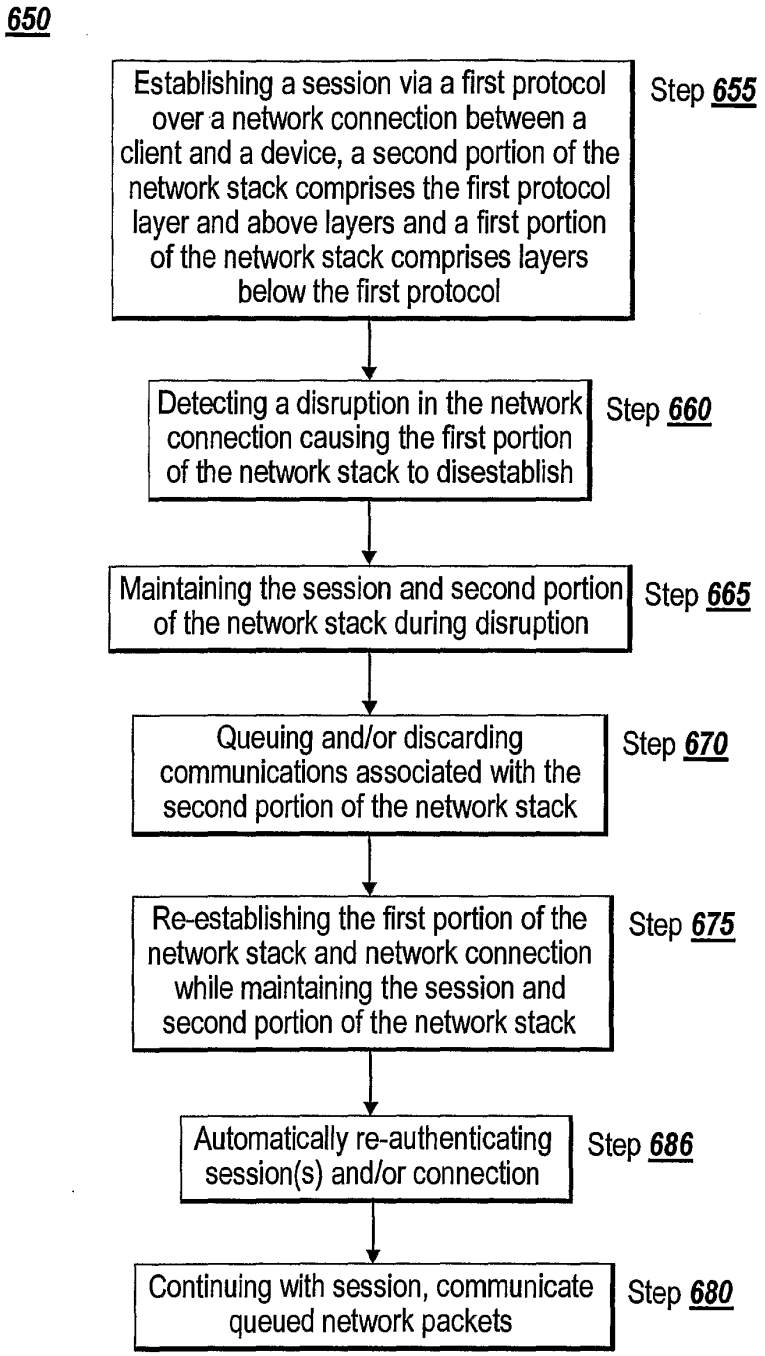

650
Establishing a session via a first protocol over a network connection between a client and a device, a second portion of the network stack comprises the first protocol layer and above layers and a first portion of the network stack comprises layers below the first protocol
Step 655
Detecting a disruption in the network connection causing the first portion of the network stack to disestablish
Step 660
Maintaining the session and second portion of the network stack during disruption
Step 665
Queuing and/or discarding communications associated with the second portion of the network stack
Step 670
Re-establishing the first portion of the network stack and network connection while maintaining the session and second portion of the network stack
Step 675
Automatically re-authenticating session(s) and/or connection
Step 686
Continuing with session, communicate queued network packets
Step 680

Fig. 6B

[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
G06F 17/60

[12] 发明专利申请公开说明书

[21] 申请号 02156671.2

[43] 公开日 2004 年 6 月 30 日

[11] 公开号 CN 1508734A

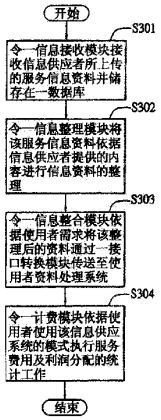
[22] 申请日 2002.12.13 [21] 申请号 02156671.2
[71] 申请人 华人创意股份有限公司
地址 台湾省台北市
[72] 发明人 温世仁 吴鸿祺

[74] 专利代理机构 北京三幸商标专利事务所
代理人 刘激扬
权利要求书 3 页 说明书 10 页 附图 3 页

[54] 发明名称 用以支持中小企业营运发展的信息供应方法以及系统

[57] 摘要

一种用以支持中小企业营运发展的信息供应方法以及系统，令一信息接收模块接收信息供应者上传的服务信息资料并储存在数据库中；令一信息整理模块将该服务信息资料依据信息供应者提供的内容进行相关资料的整理；令一信息整合模块依据使用者输入的需求将该整理后且符合该需求的资料，通过一接口转换模块传送至使用者数据处理系统；最后，令一计费模块依据使用者使用系统的模式，执行服务费用的统计工作。 通过该使用本发明，能够提供个人工作室、住家办公室及中小企业的经营者及其从业人员使用者通过单一网站即可获得所需的信息服务。



ISSN1008-4274

1. 一种用以支持中小企业营运发展的信息供应方法，用以提供使用者借由一数据处理系统通过一网络通讯系统取得所需要的信息服务，其特征在于，该用以支持中小企业营运发展的信息供应方法包括：

令一信息接收模块接收信息供应者上传的服务信息资料并储存在一数据库中；

令一信息整理模块将该服务信息资料依据信息供应者所提供的内容进行信息资料的整理；

令一信息整合模块依据使用者所输入的需求，将该整理后且符合该需求的资料通过一接口转换模块传送至使用者数据处理系统；以及

令一计费模块依据使用者使用该用以支持中小企业营运发展的信息供应系统的模式，执行服务费用的统计与利润分配工作。

2. 如权利要求 1 所述的方法，其特征在于，该信息供应者上传的服务信息资料可以是文字资料、图像数据、声音资料、影像资料、以超级链接方式所提供的网络协议地址及统一资源寻址器地址资料其中的一种。

3. 如权利要求 1 所述的方法，其特征在于，该信息供应者上传的服务信息资料可以是商业情报、商业机会、专业服务、专业规划、业务连接、行政程序及增值服务中的一种。

4. 如权利要求 1 所述的方法，其特征在于，该信息资料的整理步骤还包括将同一信息供应者及不同信息供应者其中任一者提供的相同、相似及不同信息的其中任一种信息，加以分类、归纳及结合的数据处理过程。

5. 如权利要求 1 所述的方法，其特征在于，该信息整合形式可以是数据库信息的搜寻、信息服务提供者网络资源的连接及提供线上实时的信息请求与响应中的任一种。

6. 如权利要求 1 所述的方法，其特征在于，该接口转换模块转换的通讯协议可以是国际互联网协议及无线应用软件协议中的任一种。

7. 如权利要求 1 所述的方法，其特征在于，使用该用以支持中小企业营运发展的信息供应系统的模式可以是使用者连接该网站的层次、连接的时间及信息服务的内容中的任一种。

8. 如权利要求 1 所述的方法，其特征在于，该数据处理系统可以是服务器、工作站、个人计算机、笔记本型计算机、掌上型计算机、

个人数字助理以及移动电话中的任一种。

9. 如权利要求 1 所述的方法，其特征在于，该网络通讯系统可以是国际互联网、企业内部互联网以及企业间互联网中的任一种。

10. 如权利要求 1 所述的方法，其特征在于，该网络通讯系统可以是有线通讯系统以及无线通讯系统中的任一种。

11. 如权利要求 1 所述的方法，其特征在于，该数据库是一关系型数据库。

12. 如权利要求 1 所述的方法，其特征在于，该信息接收模块、信息整理模块、信息整合模块、接口转换模块及计费模块是一软件程序。

13. 如权利要求 1 所述的方法，其特征在于，该使用者可以是个人工作室、住家办公室及中小企业的经营者及其从业人员中的任一种。

14. 一种用以支持中小企业营运发展的信息供应系统，用以提供使用者借由一数据处理系统通过一网络通讯系统取得所需要的信息服务，其特征在于，该用以支持中小企业营运发展的信息供应系统包括：

一数据库，用以储存至少包括信息提供者所提供的信息、信息整理的相关资料、信息需求者的信息资料、信息需求者及信息供应者间信息服务整合的资料以及服务费用资料；

一信息接收模块，用以接收信息提供者通过网络通讯系统提供的信息；

一信息整理模块，用以整合该信息接收模块接收该信息提供者所提供的信息内容；

一信息整合模块，用以将该信息整理模块所整理的信息与使用者所提出的信息需求作一连接互通；

一接口转换模块，用以依据不同的客户端数据处理系统提供符合该系统的资料传送、存取的规格；以及

一计费模块，用以依据使用者使用资源服务的模式计算其所需支付的服务费用，以及信息供应者与用以支持中小企业营运发展的信息供应系统管理者的利润分配。

15. 如权利要求 14 所述的系统，其特征在于，该信息供应者提供的信息可以是文字资料、图像数据、声音资料、影像资料、以超级链接方式提供的网络协议地址及统一资源寻址器地址资料中的任一种。

16. 如权利要求 14 所述的系统，其特征在于，该信息供应者上传的服务信息资料可以是商业情报、商业机会、专业服务、专业规划、业务连接、行政程序及增值服务中的任一种。

17. 如权利要求 14 所述的系统，其特征在于，该信息整理模块是将同一信息供应者及不同信息供应者中任一者提供的相同、相似及不同的信息中的任一种信息，加以分类、归纳及结合的数据处理过程。

18. 如权利要求 14 所述的系统，其特征在于，该信息整合模块的整合形式可以是数据库信息的搜寻、信息服务者网络资源的连接及提供线上实时的信息请求与响应中的任一种。

19. 如权利要求 14 所述的系统，其特征在于，该接口转换模块转换的通讯协议可以是国际互联网协议及无线应用软件协议中的任一种。

20. 如权利要求 14 所述的系统，其特征在于，使用该用以支持中小企业营运发展的信息供应系统的模式可以是使用者连接该网站的层次、连接的时间及信息服务的内容中的任一种。

21. 如权利要求 14 所述的系统，其特征在于，该数据处理系统可以是服务器、工作站、个人计算机、笔记本型计算机、掌上型计算机、个人数字助理以及移动电话中的任一种。

22. 如权利要求 14 所述的系统，其特征在于，该网络通讯系统可以是国际互联网、企业内部互联网以及企业间互联网中的任一种。

23. 如权利要求 14 所述的系统，其特征在于，该网络通讯系统可以是有线通讯系统以及无线通讯系统中的任一种。

24. 如权利要求 14 所述的系统，其特征在于，该数据库是一关系型数据库。

25. 如权利要求 14 所述的系统，其特征在于，该信息接收模块、信息整理模块、信息整合模块、接口转换模块及计费模块是一软件程序。

26. 如权利要求 14 所述的系统，其特征在于，该使用者可以是个人工作室、住家办公室及中小企业的经营者及其从业人员中的任一种。

用以支持中小企业营运发展的信息供应方法以及系统

技术领域

本发明是关于一种用以支持中小企业营运发展的信息供应方法以及系统，特别是关于一种整合信息以提供使用者通过单一网站获取该整合信息的信息供应方法与系统。

背景技术

随着电子信息科技的蓬勃发展，诸如个人计算机、笔记本型计算机、平板计算机、掌上型计算机、个人数字助理乃至移动电话等具有数据处理功能的电子装置或系统，其在功能上愈来愈强大，除单纯进行数据处理外，这些设备已经能够提供使用者上网浏览、信息的上传或下载、听音乐、编辑、播放影像信息等多元化的多媒体服务，来获取所需要的信息。另一方面由于有线及无线网络通讯技术的日益成熟，再加上这些电子装置或系统的体积愈来愈轻薄短小，便于使用者在行动中进行信息的取得。基于上述种种客观环境，使用者主观上也更乐意通过该具有网络连接与数据传输功能的电子装置或系统进行信息的搜寻及取得。

但是当愈来愈多的使用者不再通过报纸、杂志，甚至广播电视等传统的媒体来取得信息，而是选择通过具有实时性的网络通讯系统来取得所需的信息时，网络信息供应商势必要考虑如何能够充分利用网络通讯系统的特性，提供有别于传统媒体所能够提供的信息。

现有通过网络通讯系统提供使用者信息的方法不一般是以下方法：由使用者通过浏览器联接门户网站，输入要搜寻信息的关键词等搜寻条件，通过该门户网站提供的搜寻引擎进行与该关键词相符及/或近似的网页资料，由使用者通过输入网址或借由超级链接的方式与该网址进行联接，通过浏览器进行资料的浏览或传输。

这种现有的信息搜寻方法，对于缺乏网络搜寻经验或是搜寻条件等相关信息不是十分充分的使用者而言，信息的寻找、取得有时就如同大海捞针。此外，若使用者要同时搜寻许多具有实质关联性、却不具有形式关联性的网站时，上述的搜寻方式恐怕无法有效解决使用者的需要。此时，使用者仍须通过一次次的搜寻才有可能找到所需要的

信息。即令使用者已经搜寻到所有的相关信息，但若缺乏有效率的资料筛选，则所搜集到的信息对于使用者而言不但无法有效的解决自身的需要，有时反而会成为庞大的负担。

另一方面，使用者在通过付费网站获取信息方面，通常所采用的方法有固定费率制，也就是缴纳一定的费用取得在一定期间内无限次的使用权；储值制，也就是购买一定的点数，再从所使用的信息对应的点数中加以扣除。除上述两种以外，再一种方法就是依据服务提供商所开列的价格，通过信用卡或转帐的方式支付费用。上述服务费用的支付方法均是依据固定的服务价目表收费，并不能够将使用者登录或连接的等级、范围甚或是服务内容作为服务费率调整的依据。

综上所述，如何能够为使用者提供一套具有整合多元信息、并能够更合理地保证信息服务提供商与信息需求方利益的方法，是亟需解决的问题。

发明内容

为克服现有技术的缺点，本发明的主要目的在于提供一种用以支持中小企业营运发展的信息供应方法以及系统，它能够提供一信息供应网站，让信息供应者通过该信息供应网站提供信息服务。

本发明的另一目的在于提供一种用以支持中小企业营运发展的信息供应方法以及系统，它能对信息供应者提供的信息进行有效的整合，提高使用者查找所需信息的效率。

本发明的又一目的在于提供一种用以支持中小企业营运发展的信息供应方法以及系统，它能够提供使用者通过一信息服务整合的机制与信息供应者进行信息服务的交易。

本发明的再一目的在于提供一种用以支持中小企业营运发展的信息供应方法以及系统，它能够提供一计费机制，让信息供应者依据使用者使用信息服务的模式，进行服务费用的计算。

本发明的又再一目的在于提供一种用以支持中小企业营运发展的信息供应方法以及系统，它能够提供一接口转换机制，用以提供客户端的使用者可以借由不同类型的数据处理系统通过本发明获得信息服务。

为达成上述目的，本发明之用以支持中小企业营运发展的信息供应系统包括：一数据库，用以储存至少包括信息提供者所提供的信息、信息整理的相关资料、信息需求者的信息资料、信息需求者及信息供应者间信息服务整合的资料以及服务费用资料；一信息接收模块，用

以接收信息提供者通过网络通讯系统提供的信息；一信息整理模块，用以整合该信息接收模块接收该信息提供者所提供的信息内容；一信息整合模块，用以将该信息整理模块所整理的信息与使用者所提出的信息需求作一连接互通；一接口转换模块，用以依据不同的客户端数据处理系统提供符合该系统的资料传送、存取的规格；以及一计费模块，用以依据使用者使用资源服务的模式计算其所需支付的服务费用，以及信息供应者与用以支持中小企业营运发展的信息供应系统管理者的利润分配。

通过该用以支持中小企业营运发展的信息供应系统，进行信息供应的方法是：令一信息接收模块接收信息供应者上传的服务信息资料并储存在一数据库中；令一信息整理模块将该服务信息资料依据信息供应者所提供的内容进行信息资料的整理；令一信息整合模块依据使用者所输入的需求，将该整理后且符合该需求的资料通过一接口转换模块传送至使用者数据处理系统；以及令一计费模块依据使用者使用该用以支持中小企业营运发展的信息供应系统的模式，执行服务费用的统计与利润分配工作。

与传统的信息供应方法以及系统比较，本发明通过整合信息供应者提供的信息机制、信息服务整合的机制、计费机制及接口转换机制，借由一信息供应网站以供信息供应者通过该信息供应网站提供信息服务，它能对信息供应者提供的信息进行有效的整合，提高使用者查找所需信息的效率；同时能够提供使用者通过一信息服务整合的机制与信息供应者进行信息服务的交易，它所提供一计费机制，让信息供应者依据使用者使用信息服务的模式，进行服务费用的计算及收取。本发明提供的接口转换机制，能够让客户端的使用者可以借由不同类型的数据处理系统通过本发明获得其所需的信息服务。

附图说明

图 1 为一应用架构方块示意图，用以显示本发明之用以支持中小企业营运发展的信息供应系统的应用架构；

图 2 为一系统架构方块示意图，用以显示本发明之用以支持中小企业营运发展的信息供应系统的系统架构；以及

图 3 为流程图，用以显示本发明之用以支持中小企业营运发展的信息供应方法的流程步骤。

具体实施方式

实施例

在以下实施例中，本发明用以支持中小企业营运发展的信息供应方法以及系统中所提供的信息包括文字资料、图像数据、影音资料以及其它无法由人类通过感官直接辨识的电磁记录资料，实际上能够通过本发明的用以支持中小企业营运发展的信息供应方法以及系统提供信息供应服务的，均适用于本发明的用以支持中小企业营运发展的信息供应方法以及系统。

请参阅图 1，如图所示，在本实施例中，本发明的用以支持中小企业营运发展的信息供应系统 100，是应用在现有的主从架构网络通讯系统 200 中，又该用以支持中小企业营运发展的信息供应系统 100 是建构在该网络通讯系统 200 的伺服端，用以提供具有网络连接功能的网络终端装置 300 及网络终端装置 400 的客户端使用者，借由一浏览器应用程序通过该网络通讯系统 200，与建构在该伺服端的用以支持中小企业营运发展的信息供应系统 100 相互连接，进行包括程序或资料的上传或下载、资料储存及数据管理等工作。其中，该网络通讯系统 200 可以是一国际互联网(Internet)、企业内部互联网(Intranet)或企业间互联网(Extranet)；该网络终端装置 300 及网络终端装置 400 可以是个人计算机(PC)、笔记本型计算机(NB)、工作站(Workstation)或其它具有数据处理功能的装置或系统；该浏览器应用程序可以是微软的网络探险家(Internet Explorer)或是网景的领航员(Netscape Navigator)等。上述的主从架构网络通讯系统 200、该网络终端装置及该浏览器应用程序均为现有的软、硬件架构，故在此不重复说明。

请参阅图 2，它显示了本发明的用以支持中小企业营运发展的信息供应系统 100 的系统架构，如图所示，该用以支持中小企业营运发展的信息供应系统 100 搭配至一网络服务器 210，该网络服务器 210 是提供该用以支持中小企业营运发展的信息供应系统 100，通过该网络通讯系统 200 与网络终端装置 300 及网络终端装置 400 相互连接，并提供该网络终端装置 300 及网络终端装置 400 响应使用者的指令或其它需求以进行资料存取之用。在本实施例中，该网络终端装置 300 及网络终端装置 400，是利用各该网络终端装置上的网络浏览器应用程序，如上述的微软的 IE 或是网景的 Navigator，通过网络通讯系统 200 经由该网络服务器 210，与该用以支持中小企业营运发展的信息供应系统 100 相互连接，以进行档案管理相关的工作。需特别说明的是，该用以支持中小企业营运发展的信息供应系统 100 还可以与一防火墙(Firewall)系统联接(未图标)，用以保护该用以支持中小企业营运发展的信息供应

系统 100。该用以支持中小企业营运发展的信息供应系统 100 包括：一数据库 220、一信息接收模块 230、一信息整理模块 240、一信息整合模块 250、一接口转换模块 260 以及一计费模块 270。

该数据库 220 是用来储存至少包括信息提供者所提供的信息、信息整合的相关资料、信息需求者的信息资料、信息需求者及信息供应者之间信息服务整合的资料以及服务费用等资料表。在本实施例中，为增加资料查询及检索的效率，该数据库 220 可以是一关系型数据库。其中，该信息提供者所提供的信息资料表，用来储存至少包括信息提供者所提供的文字资料、图像数据、影音资料以及其它能够以储存在该数据库的任何形式的资料等数据区位；该信息整合的相关资料表，用以储存至少包括信息类别资料、信息内容相互关系资料以及信息整合资料等数据区位；该信息需求者的信息资料表，用以储存至少包括使用者基本身分、使用者使用信息的权限以及使用者使用资源的记录等数据区位；该信息需求者及信息供应者之间信息服务整合的资料表，用以储存至少包括有信息服务整合类别资料以及信息服务整合历史记录资料等数据区位；该服务费用资料表，则用以储存至少包括信息供应者的收费模式、信息供应者所提供的信息被使用的计量以及信息供应者与该用以支持中小企业营运发展的信息供应系统管理者之间利润分配基础等数据区位。

通过这种关系型数据库的建立，当使用者输入上述任一种资料时，该用以支持中小企业营运发展的信息供应系统 100 即可快速的寻找到其对应的资料。需特别说明的是，上述的各该数据区位及其所属的资料表仅为举例而已，在实际情况下，其内容应更为明确详细。此外，各该数据区位的内容也有可能包括有其它的数据区位或是资料表，只是由于篇幅所限，以及为陈述上的简洁，仅显示与本发明的用以支持中小企业营运发展的信息供应方法以及系统有关的部分资料。另一方面，该关系型数据库的系统架构也有多种，应视使用者的需要加以建构，故也不再重复说明。

该信息接收模块 230 是用来接收信息提供者通过网络通讯系统 200 所提供的信息。在本实施例中，信息提供者可以是顾问咨询服务、专业规划服务、生活增值服务、知识增值服务、业务连接服务，甚至包括法人组织或政府机关的行政单位或对外服务窗口等任何自然人或法人构成的信息提供主体。该信息提供者可借由该网络终端装置通过该网络通讯系统 200，将提供的信息服务内容上传至该网络服务器 210，该信息接收模块 230 随即将接收到的信息服务相关资料加以储存至该

数据库 220 中。

需特别说明的是，信息提供者与该用以支持中小企业营运发展的信息供应系统 100 的管理者之间应建立一资料传送的协议，如以特定的识别号码或文字定义的特定的信息种类，当该信息接收模块 230 接收到具有该识别号码或文字的信息相关资料时，则应依据该识别号码或文字将该相关信息储存至该数据库 220 中对应的信息资料储存字段。

该信息整理模块 240 是对该信息接收模块 230 接受该信息提供者提供的信息内容，按照一定的规则进行整理。在本实施例中，由于信息提供者所提供的信息内容包罗万象，内容可能包括各个领域中不同层次的内容，可能是民间企业或是政府机关。但是通常一种业务的处理流程可能包括许多不同的信息供应者才能完成。如专利的申请，其流程可能包括寻找专业的专利事务所讨论专利申请的相关信息，委托其办理如专利说明书的撰写或专利申请程序的代办，当完成专利说明书的撰写后，还必须送交专利局进行专利审查，最后再经由相关的作业程序才能确定是否获得专利权。

该信息整理模块 240 能够将与专利申请相关的信息服务内容作一整理，当使用者欲搜寻与专利申请相关的信息服务时，即可获取一连串有用且相关的信息服务。在整理手段上，可以通过上述由信息供应者与用以支持中小企业营运发展的信息供应系统管理者之间的协议，借由特定的识别号码或文字加以分类，以将前阶段由民间专利事务所提供的服务，与后阶段由政府机关的专利局提供的行政程序服务等加以连接。也就是当信息供应者提供的信息通过该信息接收模块 230 储存至该数据库 220 时，该信息整理模块 240 能够将该特定相关的信息加以整理，并以特定的关键内容如“专利申请”等储存至该数据库 220 中的特定数据区位中，以供该用以支持中小企业营运发展的信息供应系统 100 进行资料的存取。

该信息整合模块 250 用来将该信息整理模块 240 所整理出的信息与使用者所提出的信息需求作一个连接互通。在本实施例中，当使用者借由网络终端装置通过该网络通讯系统 200，与建构有该用以支持中小企业营运发展的信息供应系统 100 的网站相互连接时，该网站会提供一信息服务相关的搜寻机制，如请求使用者输入使用者基本身分、使用者使用信息的权限等个人识别资料，以及特定的信息搜寻关键识别号码或文字等，通过该信息整合模块 250 的搜寻功能，即能够将信息需求者所需的信息服务与该用以支持中小企业营运发展的信息供应系统 100 中所能够提供的相关信息服务相互结合。其结合方式包括提

供使用者以超级链接的方式与该信息供应者相互连接、以提供如统一资源寻址器(URL)等网络资源的连接及/或提供如线上实时视频会议(Net-Meeting)等线上实时的信息请求及响应。

该接口转换模块 260 会依据不同客户端的网络终端装置提供符合该系统资料传送存取的资料规格。在本实施例中，该网络终端装置 300 及 400 并不限定为现有的个人计算机或笔记本型计算机，还可包括任何能够通过网络通讯系统 200 连接至架构有该用以支持中小企业营运发展的信息供应系统 100 网站的系统或装置，如移动电话所适用的无线应用软件协议(WAP)等其它网页浏览格式。该接口转换模块 260 是为使用不同资料浏览或存取协议的系统或装置提供转换接口，使其均可连接到架构有该用以支持中小企业营运发展的信息供应系统 100 的网站，供使用不同浏览或存取协议的网络终端装置进行信息的搜寻或接受信息供应者所提供各种形式的信息服务。

该计费模块 270 是用以依据使用者使用资源服务的模式，计算其所应支付的服务费用。在本实施例中，该计费模块 270 除了依据信息供应者或该用以支持中小企业营运发展的信息供应系统 100 的管理者所确定的信息服务价目表，计算使用者所使用的信息服务内容所应支付的总服务费用外。还能够依据使用者使用该用以支持中小企业营运发展的信息供应系统 100 的模式及其历史记录，作为计算服务费用的标准。以上述的“专利申请”流程为例，使用者自搜寻相关专利事务所或专利局的信息时，该计费模块 270 随即开始记录使用者使用该网站的使用时间、点选次数或下载档案的资料量等行为模式、并加以记录，若该使用者与其中一家具有专利代理经验的信息供应者相互联系，并且双方进行了如线上实时咨询等信息服务时，该计费模块 270 随即记录使用者与该信息供应者之间服务与被服务的信息，若使用者再通过该网站与专利局进行信息需求与供应的服务时，该计费模块 270 仍会记录他们之间的有关信息。通过上述追踪记录使用者的行为模式、并加以记录的方式，能够以依据使用者利用该网站的不同层次(Level)作为计算服务费用的标准。

请参阅图 3，它显示通过上述的用以支持中小企业营运发展的信息供应系统 100，在实施该用以支持中小企业营运发展的信息供应方法的步骤是。

在步骤 S301 中，令该信息接收模块 230 接收信息供应者上传的服务信息资料并储存在该数据库 220 中。通过该信息接收模块 230 能够接收资料供应者所传送的信息资料，以超级链接的方式所提供的网络

协议地址及／或统一资源寻址器地址等资料。

承前所述，该信息提供者与该用以支持中小企业营运发展的信息供应系统 100 的管理者之间得建立一资料传送的协议，如以特定的识别号码或文字定义特定的信息种类，当该信息接收模块 230 接收到具有该识别号码或文字的信息等相关资料时，则能够依据该识别号码或文字将该相关信息储存至该数据库 220 中对应的信息资料储存字段中。

在本实施例中，若一专利事务所欲通过该用以支持中小企业营运发展的信息供应系统 100 作为一专利信息供应者，则其能够借由网络终端装置通过该网络通讯系统 200，将其所能提供的信息资料传送至该网络服务器 210，其中该传送的资料包括文字或影像信息资料，以超级链接方式所提供的网络协议地址及／或统一资源寻址器地址等资料。此外，还包括特定的识别号码或文字，如“0001”与“专利服务”等，该信息接收模块 230 在该网络服务器 210 接收到上述的资料时，随即将该资料储存至该数据库 220 中符合该识别号码“0001”与识别文字“专利服务”的数据区位中，接着进行步骤 S302。

在步骤 S302 中，令该信息整理模块 240 将该服务信息资料依据信息供应者所提供的内容进行相关资料的归纳、整理。其过程包括将同一信息供应者或不同信息供应者所提供的相同、相似或不同的信息加以分类、归纳或结合等。

承前所述，除该专利服务的信息供应者能够传送相关信息资料外，设架构有该用以支持中小企业营运发展的信息供应系统 100 的网站还能够与政府机关、如上述的专利局等相互合作，提供诸如线上专利申请或咨询等服务。由于一专利的申请流程可能需通过包括专利事务所与专利局等信息服务提供者的协助才能顺利完成。则该信息整理模块 240 则应将专利事务所及专利局所提供的信息服务作一信息归类，当使用者登录架构有该用以支持中小企业营运发展的信息供应系统 100 的网站，且欲请求该网站提供“专利申请”的信息服务时，则能够轻易的搜寻到上述经归纳后的该专利事务所及专利局所提供的信息服务，接着进行步骤 S303。

在步骤 S303 中，令一信息整合模块 250 依据使用者输入的需求，将该整理后且符合该需求的资料通过一接口转换模块 260 传送至客户端网络终端装置。其整合的模式包括数据库 220 信息的搜寻、信息服务提供者网络资源的连接及/或提供线上实时的信息请求及响应等。

承前所述，当有“专利服务”信息需求的使用者登录该网站后，该网站能够提供使用者一输入该使用者相关信息的功能，如要输入使

用者的基本身分、使用者使用信息的权限等个人识别资料，以及特定的信息搜寻关键识别号码或文字，如识别号码“0001”与识别文字“专利服务”等，通过该信息整合模块 250 的搜寻功能，即能够将信息需求者所需要的“专利服务”的相关信息服务，与该用以支持中小企业营运发展的信息供应系统 100 中所能够提供的、经整合后的该专利事务所及专利局所提供的信息服务相互结合。

在本实施例中，使用者进行数据库 220 中相关资料的搜寻、与该专利事务所进行网络视频会议及上述假设的专利局线上的专利申请作业流程等信息服务，接着进行步骤 S304。

在步骤 S304 中，令一计费模块 270 依据使用者使用该用以支持中小企业营运发展的信息供应系统 100 的模式，执行服务费用的统计工作。它是依据使用者使用信息的模式，计算所需支付的费用以及信息供应者之间的利润分配。

承前所述，在使用者通过上述的信息整合模块 250 取得该用以支持中小企业营运发展的信息供应系统 100 所提供的服务信息的过程中，该计费模块 270 会记录使用者与该信息供应者整合的信息，若使用者再通过该网站与专利局进行信息需求与供应的联系时，该计费模块 270 仍会记录其信息。

在本实施例中，以上述的“专利申请”流程为例，使用者自搜寻相关专利事务所或专利局的信息时，该计费模块 270 随即开始记录使用者使用该网站的使用时间、点选次数或下载档案的资料量等行为模式并加以记录，若该使用者与其中一具有专利代理经验的信息供应者相互联系，双方进行如线上实时咨询等信息服务时，该计费模块 270 随即记录使用者与该信息供应者之间的相关信息，若使用者再通过该网站与专利局进行信息需求与供应的联系时，该计费模块 270 仍会记录其有关信息。通过上述的信息记录，该计费模块 270 能够依据所记录该使用者连接该网站的层次、连接的时间及/或信息服务的内容等，计算出相对应的服务费用，其中，该服务费用的计算基准应视实际情况加以制定。此外，该计费模块 270 还能够依据信息提供者与该用以支持中小企业营运发展的信息供应系统 100 的管理者对于信息提供的利润分配基准，进行利润分配的计算。

综上所述，本发明之用以支持中小企业营运发展的信息供应方法以及系统，能够通过整合信息服务供应者所提供的信息服务供应机制、信息服务整合的机制、计费机制及接口转换机制，借由一信息供应网站以供信息服务供应者通过该信息供应网站提供信息服务。

本发明的用以支持中小企业营运发展的信息供应方法以及系统能够协助个人工作室、住家办公室及中小企业的经营者及其从业人员，在接取订单、增创营收、善用外部资源、进行委外服务、增加经营弹性、减少聘雇人员及办公室空间的需求、节省营运成本、降低创业门槛等方面提供帮助，进而达到解决失业问题及调整产业结构的目的。

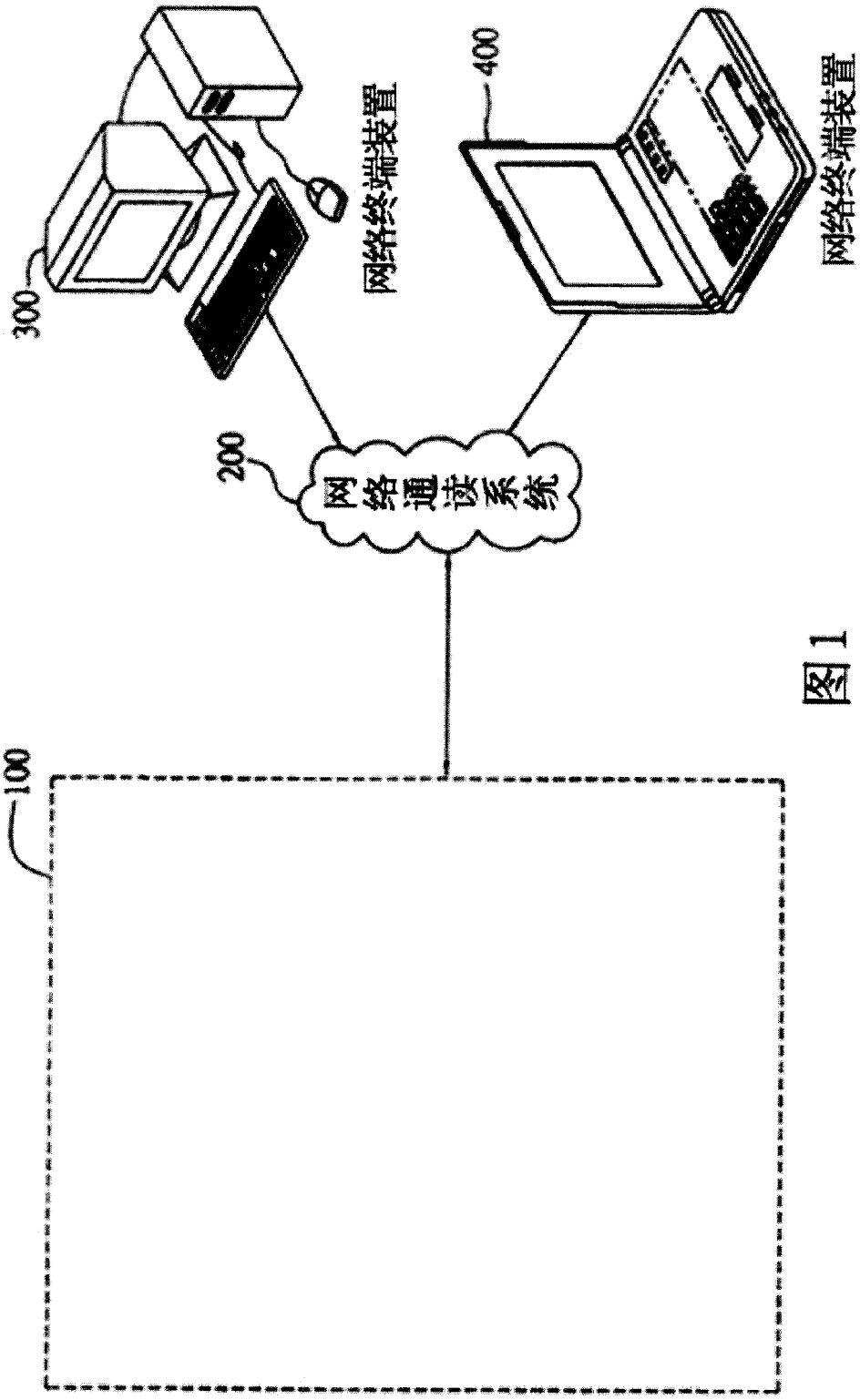


图 1

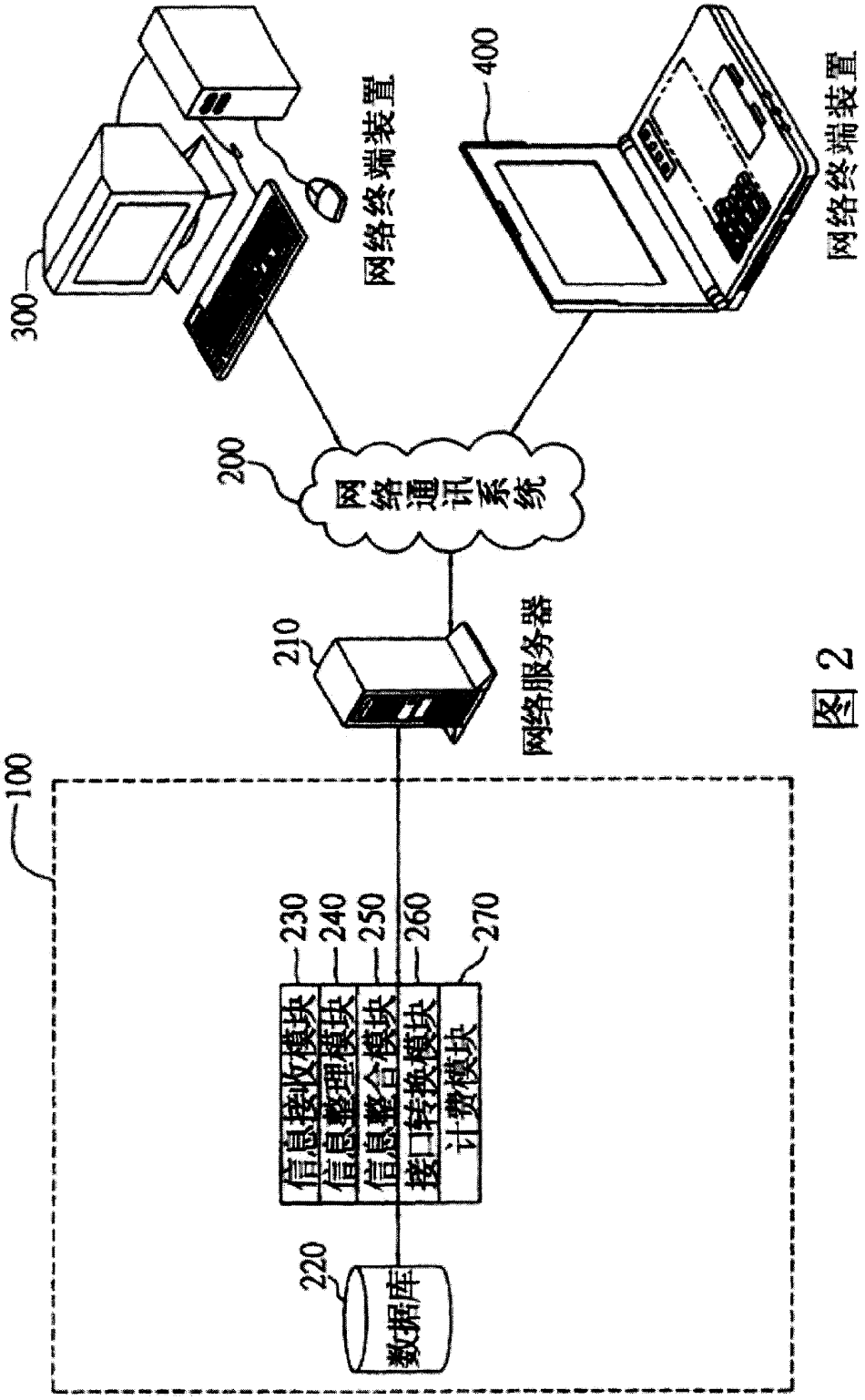

300
网络终端装置
400
网络终端装置
200
网络通讯系统
210
网络服务器
100
230
240
250
260
270
信息接收模块
信息整理模块
信息整合模块
接口转换模块
计费模块
220
数据库

图 2

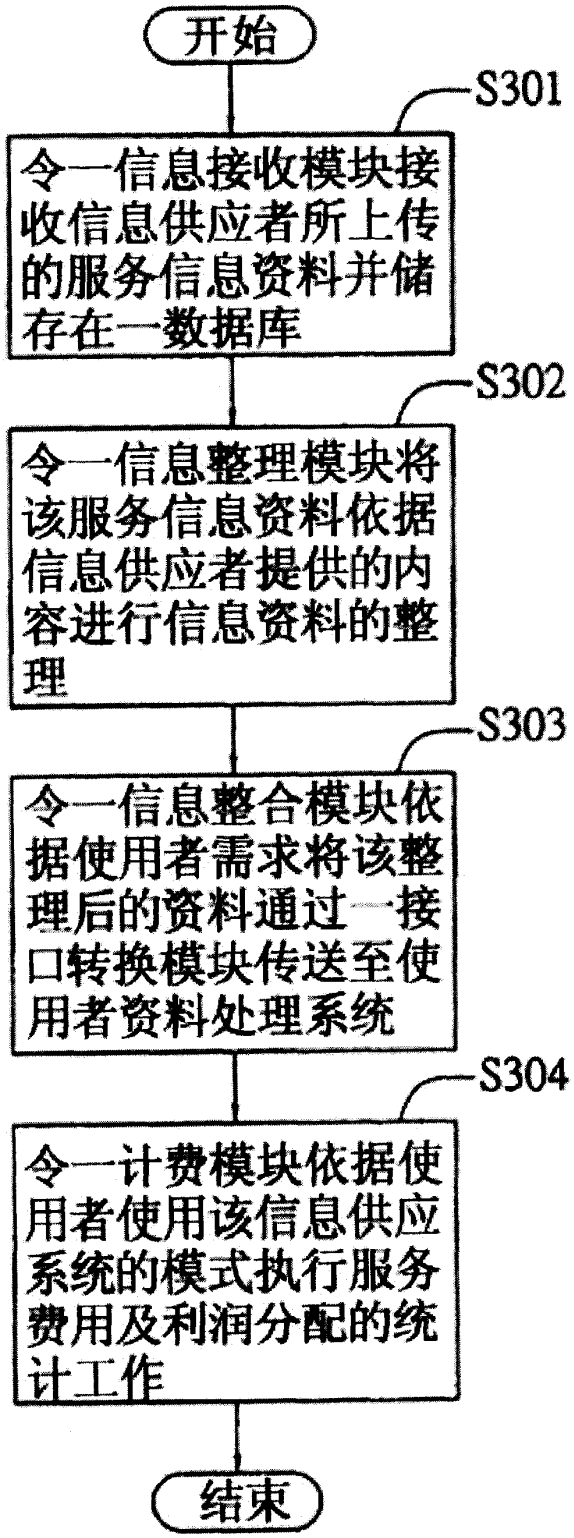

开始
S301
令一信息接收模块接收信息供应者所上传的服务信息资料并储存在一数据库
S302
令一信息整理模块将该服务信息资料依据信息供应者提供的内容进行信息资料的整理
S303
令一信息整合模块依据使用者需求将该整理后的资料通过一接口转换模块传送至使用者资料处理系统
S304
令一计费模块依据使用者使用该信息供应系统的模式执行服务费用及利润分配的统计工作
结束

图 3

Annie

Patents English Chinese Find prior art Discuss this application View PDF Download PDF

Method and system for providing information for supporting operation development of small-medium enterprises

CN 1508734 A

Publication number	CN1508734 A
Publication type	Application
Application number	CN 02156671
Publication date	Jun 30, 2004
Filing date	Dec 13, 2002
Priority date	Dec 13, 2002
Inventors	温世仁, 吴鸿祺
Applicant	华人创意股份有限公司
Export Citation	BiBTeX, EndNote, RefMan

Legal Events (3)

External Links: SIPO, Espacenet

ABSTRACT

The invention is a kind of information supplying method and the system for supporting small and medium-sided enterprise development. A information receiving model receives the service information data uploaded by supplier and stores them in the databank; a information arranging model carries on the arrangement of relative data according to the content supplied by the supplier; a information integrating model transmits the proper data to the user data processing system through a interface converting model, finally, a charge calculating model calculates the charge according to the mode used by the user.

DESCRIPTION translated from Chinese

Supply methods to support the development of SMEs as well as operating system

Technical Field

The present invention relates to an operation to support the development of SMEs information provision method and system, especially with regard to an integrated information to provide users to access information through a single Web site that integrated information provision method and system.

Background

With the rapid development of electronic information technology, such as personal computers, notebook computers, tablet computers, palmtop computers, personal digital assistants and even mobile phones and other electronic devices or systems having a data processing function, its increasingly powerful in function, In addition to simple data processing, these devices have been able to provide users with Internet browsing, upload or download information, music, editing and playback of multimedia video information and other diversified services to get the information they need. On the other hand due to the wired and wireless network communications technologies become more sophisticated, the volume plus these electronic devices or systems increasingly compact size, ease of access to information in the user performs actions. Based on all these objective circumstances, users are more willing subjective electronic device or system that has a network connection and data transmission capabilities to search and access to information.

But when more and more users are no longer to obtain information through traditional media, newspapers, magazines and even radio and television, choosing instead to obtain the necessary information through the network communication system with real-time, online information provider bound to consider how to take full advantage of the characteristics of the network communications system, providing different from traditional media to provide information.

Existing methods provide user information through the network communication system is not generally the following methods: by the user through a browser connection portal, enter search keywords and other search criteria information

CLAIMS (26) translated from Chinese

An information provision method to support SME Business Development, to provide users with a data processing system by means of the information required to obtain services through a network communication system, wherein the means for support of the SME Business Supply method development include: make an information receiving module receives the information service provider information uploaded and stored in a database; make an information consolidation module based on the content of the service information provided by the information provider of information materials finishing; make an information integration module based on the needs of the user input, the finishing and meet the needs of data through a user interface conversion module is transferred to the data processing system; and to make a billing module according to the user to use the use to support the development of SMEs operating mode of information supply system, the implementation of service fees and profit distribution statistics work.

2. The method according to claim 1, characterized in that the information service provider information may be uploaded text data, image data, audio data, image data, network protocol address provided by hyperlinks and unified address information resource addressing one of them.

3. The method according to claim 1, characterized in that the service information This information can be uploaded provider of business intelligence, business opportunities, professional services, professional planning, business connections, administrative procedures and value-added services in one .

4. The method according to claim 1, characterized in that the finishing step also includes the same information will be different from the same information provider and wherein any one of the information provider provides, any of which is similar to and different information information, classify, summarize and combine the data processing.

5. The method according to claim 1, characterized in that the integration of information and forms can be connected to provide search and information services provider of database information online real-time network resource information request and response in

provided through the portal, and the search engine Keywords consistent and / or similar web information input by the user through the website or by way of hyperlinks connecting with the site, browse or transfer data through the browser.

This existing information search method, for lack of experience, or search Web search and related information is not very full of users, the information search, obtain sometimes like needle in a haystack. In addition, if the user to simultaneously search a number of substantive relevance, is not associated with a form of site, said search means could not be effectively addressed the needs of users. In this case, the user must still search through time and time again possible to find the information they need. And even if the user has to find all the relevant information, but if the lack of effective screening information, then the information gathered for the user not only can not effectively solve their own needs, sometimes it will become a huge burden.

On the other hand, users get to information through pay sites, typically used a fixed rate system, which is to pay a fee to obtain unlimited times within a certain period the right to use; stored value system, which is to buy a certain points, and then be deducted from the corresponding point information used in the. In addition to the two outside, then one approach is based on the service provider listed price, pay by credit card or debit way. The method of payment of the above services are based on a fixed fee service price list, the user is not able to log on or connect the level, the scope of services or even service rates as the basis for the adjustment.

In summary, how can we provide users with a set of integrated pluralistic information and the ability to more reasonable assurance that the information service provider and information needs of Fangli Yi approach is needed to solve problems.

DISCLOSURE

To overcome the disadvantages of the prior art, the main object of the present invention is to provide a support operation for the development of SMEs information provision method and system capable of providing an information provider website information provider to provide information so that the information supplied by website services.

Another object of the present invention is to provide a support operation for the development of SMEs information provision method and system that can provide information on the information provider for effective integration, improve the efficiency of users to find the information.

A further object of the present invention is to provide a support for the development of the SME Business information provision method and system, which can provide a user through an information service integration mechanisms and information provider of information services deals.

A further object of the present invention is to provide a support operation for the development of SMEs information provision method and system, which can provide an accounting mechanism to allow information providers to use information service based on user model to calculate the cost of services .

Again object of the present invention is to provide an operation to support the development of SMEs information provision method and system, which can provide an interface conversion mechanism for providing client user can borrow from the different types of data processing systems The present invention is to obtain information services.

To achieve the above objects, the present invention in order to support the development of SMEs operating information supply system comprising: a database for storing information providers including at least the information provided, the relevant data and information collated, the information needs of those information, information and data as well as those who need services cost any one.

The method according to claim 6, wherein the interface conversion module converts the communication protocol may be Internet Protocol and wireless application protocol either.

7. The method according to claim 1, characterized in that, using this to support the development of SMEs operating mode information supply system may be a content level of the site's users to connect, the connection time and information services in the either.

8. The method according to claim 1, characterized in that the data processing system may be a server, workstations, personal computers, notebook computers, handheld computers, personal digital assistants and mobile phones either.

9. The method according to claim 1, characterized in that the network may be the Internet communication system between the Internet and corporate intranets any one.

10. The method according to claim 1, characterized in that the network communication system may be a wired communication systems and wireless communication system of any one.

11. The method according to claim 1, characterized in that the database is a relational database.

12. The method according to claim 1, characterized in that the message receiving module, information sorting module, information integration module, the interface conversion module and a billing module is a software program.

13. The method according to claim 1, characterized in that the user may be operators and their employees personal studio, home office and SME any one.

14. A method for supporting the development of the SME Business information supply system to provide users with borrowed by a data processing system to obtain the required information and services through a network communication system, wherein the means for support of the SME Business development of information supply system comprising: a database for storing at least include the information provided by those who provide information, relevant data and information collated, the information needs of those information, information needs and information providers who integrate data and information services Service cost information; an information receiving module for receiving information provider provides information through a network communication system; an information consolidation module to integrate the information receiving module receives information about the content of the information provided by the provider; an information integration module to the information needs of information consolidation module collated information submitted by the user to make a connection interworking; an interface converter module for different clients according to the data processing system to provide data transmission in line with the system, access specifications; and a billing module for computing services they need to pay the costs, as well as information provider and distribution of profits to support the development of SMEs operating information providing system administrators use of resources based on user-service model.

15. The system according to claim 14, characterized in that the information provider provides information may be text data, image data, audio data, image data, addresses in hyperlinks network protocol and provide uniform resource addressing address data in either.

16. The system of claim 14, wherein the service information provider uploaded the information may be business intelligence, business

data integration between information provider of information services; an information receiving module for receiving information provider provides information through a network communication system; an information consolidation module to integrate the information receiving module an information integration module to the information needs of information consolidation module collated information and user make a connection the proposed exchange;; an interface converter module for different customers based on the content of the information provided by the information provider end data processing system provides data transmission in line with the system specifications access; and a billing module for computing services they need to pay the costs, as well as information service providers based on user patterns and the use of resources to support SME Business Development Supply system administrator profit distribution.

The method by which to support the development of SMEs operating information supply system for the supply of information is: make an information receiving module receives information on the service provider information uploaded and stored in a database; an information consolidation module makes the service information provided in accordance with the content of the information provider to collate information; and make an information integration module based on the needs of the user input, the finishing and meet the needs of data transmission via an interface conversion module to the user data processing systems; and to make a billing module according to the user to use the development of SMEs to support operations information supply system mode, performing a service fee of statistical work and the distribution of profits.

Compared with the traditional supply methods and information systems, information mechanism of the present invention to provide by integrating information provider, the information service integration mechanisms, billing mechanism and interface conversion mechanism, through information supplied by a website to provide information by the information provider Supply website provides information services, information providers can provide information for effective integration, improve the efficiency of users to find the information required; at the same time be able to provide users with information and services through an integrated mechanism and information provider of information services transaction, it provides a billing mechanism, so that information providers use information service based on user patterns, calculate and charge for the services. Interface conversion mechanism of the present invention provides, allows the client user can borrow from the different types of data processing systems and services to get the information they need by the present invention.

Brief Description

Figure 1 is a block diagram of the application architecture, application architecture to show support for the operation of the present invention the development of SMEs information supply system; Figure 2 is a block diagram of the system architecture, the present invention is used to show support for SMEs operation and development of information systems architecture supply system; and Figure 3 is a flow chart, the process steps for information provision method of the present invention to support the development of SMEs operating display.

opportunities, professional services, professional planning, business connections, administrative procedures and any value-added services species.

17. The system according to claim 14, characterized in that the module is the same as information of the same sort of information providers and different information provider provided by any one, any one of similar and different information in the information, classify, summarize and combine the data processing.

18. The system according to claim 14, characterized in that the form of the integration of information integration module may search a database of information, and providing on-line information services connected by network resources and real-time information request in response to any one of species.

19. The system of claim 14, wherein the interface conversion module converts the communication protocol may be Internet Protocol and wireless application protocol either.

20. The system of claim 14, characterized in that, using this to support the development of SMEs operating mode information supply system may be a content level of the site's users to connect, the connection time and information services in the either.

21. The system of claim 14, wherein the data processing system may be a server, workstations, personal computers, notebook computers, handheld computers, personal digital assistants and mobile phones either.

22. The system of claim 14 claim, characterized in that the network may be the Internet communication system between the Internet and corporate intranets any one.

23. The system of claim 14 claim, wherein the network communication system may be wired communication systems and wireless communications systems in any one.

24. The system according to claim 14, characterized in that the database is a relational database.

25. The system according to claim 14, characterized in that the message receiving module, information sorting module, information integration module, the interface conversion module and a billing module is a software program.

26. The system of claim 14 claim, characterized in that the user may be operators and their employees personal studio, home office and small and medium enterprises of any kind.

DETAILED DESCRIPTION

Example In the following examples, the present invention is to support the development of SMEs operating information supply method and an information system is provided including text data, image data, audio and video data as well as by other human senses can not be recorded by the direct identification of electromagnetic data actually able to provide information supply services through information provision method and system to support the operation and development of SMEs in the present invention are useful in the present invention, an information provision method and system to support the operation and development of SMEs.

See Figure 1, as shown in this embodiment, in order to support the operation and development of SMEs in the information supply system 100 of the invention, is used in the existing master-slave architecture network communication system 200, versus a to support the operation and development of SMEs in the information supply system 100 is constructed on the

servo end of the network communication system 200 for providing network terminal device has a network connection function client user network terminal device 300 and 400, made by a browser application 200, 100 interconnected with the construction of the servo end to support the operation and development of SMEs in the information supply system via the network communication system for including a program or data upload or download, data storage and data management. Wherein the network communication system 200 may be a Internet (Internet), intranet (Intranet) or enterprises Internet (Extranet); the network terminal device 300 and a network terminal device 400 may be a personal computer (PC), notebook computer (NB), workstation (Workstation) or other device or system with data processing capabilities; the browser application may be Microsoft's Internet Explorer (Internet Explorer) or Netscape Navigator (Netscape Navigator) and so on. Said main are existing software and hardware architecture from architecture network communication system 200, the network terminal device and the browser application, so this will not be repeated.

See Figure 2, which shows the operation to support the development of SMEs information systems architecture supply system 100 of the invention, as shown in the operation to support the development of SMEs with information supply system 100 to a network server 210, the network server 210 is provided to support the operation and development of SMEs in the information supply system 100 through the network communication system 200 and the network terminal device 300 and a network terminal device 400 connected to each other, and to provide the network terminal device 300 and network the terminal apparatus 400 in response to user commands or other requirements for use of data access. In this embodiment, the network terminal device 300 and a network terminal device 400 is using a web browser application on each of the network terminal device, such as Microsoft's IE or Netscape Navigator as described above, through the network communication system 200 210, 100 connected to each other via the network server to support the development of SMEs operating information supply system for records management-related work. In particular, and it noted that the operation to support the development of SMEs information supply system 100 also may be a firewall (Firewall) system connections (not shown) to protect the operation to support the development of SMEs information supply system 100 . The operation to support the development of SMEs information supply system 100 includes: a database 220, an information receiving module 230, an information consolidation module 240, an information integration module 250, an interface conversion module 260, and a billing module 270.

The database is used to store at least 220, including information provided by the information provided, the information related to the integration of data, information, information needs of those, who between information needs and information providers of information services and integrated information service expense sheet . In the present embodiment, in order to increase the efficiency of data query and retrieval, the database 220 may be a relational database. Among them, the information sheet provided by the information provider, used to store text data including at least provided information provider, image data, video and audio information and other data can be stored in any form of the databases and other data area bits; information integration related information table for storing information including at least category, information content and information integration relationship information data such as location information; the information needs of those information table for storing includes at least the basic user identity, user permission to use information and recording user data such as resource use location; the information needs of persons between information providers and information services to integrate the data sheet, including an information service for storing at least types of information integration and data information services into history data such as location; the service cost data tables, including at least information provider to store the charging mode, metering and information provider information provider the information provided is used to support the operation and development of SMEs Supply Profit distribution between basic data such as location system administrator.

Through this relationship database when a user enters any of the above information, which is used to support 100 to quickly find the information corresponding to its SME Business Development Supply System. In particular, and it noted that all the data and information on the location of the above table belongs only way of example only, in reality, its contents should be more clearly detailed. In addition, the contents of each bit of the data area may also include other data or information table location, but due to limited space, as well as a succinct statement on the show only to the present invention supports SME Business Development Supply methods and some of the information system related. On the other hand, the relational database system architecture also has many, depending on the needs of users should be construction, it is also not repeated.

The message receiving module 230 is used to receive network information provider through the communication system 200 to provide information. In this embodiment, the information provider may be consulting services, professional planning services, life value-added services, value-added knowledge services, business connectivity services, and even any natural or legal person or legal entity government administrative units or foreign service window, etc. Information provided constituted body. This information is provided by the network may, by the terminal device 200 via the network communication system, the information services to be provided to upload to the network server 210, the information receiving module 230 then the received information service related information to be saved to the database 220.

Need of special note is the establishment between information providers and managers to support the operation and development of the SME information supply system 100 a data transfer protocol, the particular type of information, such as specific identification number or text definition When 230 receives information related information having the identification

number or character of the information receiving module should be based on the identification number or text to the relevant information stored in the database 220 corresponding information storage field.

This information consolidation module 240 is receiving module 230 accepts the information content of the information providers, in accordance with certain rules finishing. In this embodiment, since the information content provided by the information provider all-inclusive, the content may include various fields at different levels of content, may be private companies or government agencies. But usually a business process flow may include a number of different information provider to complete. As a patent application, the process may include professional patent search firm to discuss patent applications related information for the execution of programs written or patent application as the patent specification of the charge d'affaires, after the completion of drafting patent specification must also be sent to the Patent patent examination Board, and finally by the relevant operating procedures in order to determine whether the franchise.

This information consolidation module 240 can be related applications and patent information services as a consolidation, when the user wants to search and patent applications related to information services, you can get a series of useful and related information services. On finishing means, said by agreement by the information provider and to support the development of SMEs operating information supply system between managers, to be borrowed by a particular identification number or text classification, to the front stage by private patent matters services provided, to be connected with the later stages of the administrative service provided by government agencies and other offices. That is when the information provider of information provided by the information receiving module 230 to 220 stored in the database, the information sorting module 240 can be related to the specific information received, and in particular the key elements as "patent application" and storage to the database 220 of location-specific data in order for the operation to support the development of SMEs information supply system 100 access data.

The information integration module 250 to the information needs of information consolidation module 240 to sort out information and users are asked to make a connection exchange. In this embodiment, when the user by the network terminal device 200 via the network communication systems, and construction has to support the operation and development of SMEs in the information supply system 100 is connected to each other at the site, the site will provide an information service relevant search mechanism, such as requesting the user to enter a personal identification data basic user identity, user permission to use the information, as well as specific information search key identification number, or text and so on, through the information integration module search function 250, that can The information requirements are needed for information services and related information services to support the operation and development of the SME information supply system 100 can offer combined with each other. Its combination of methods include providing users with hyperlinks connected to each other and the information provider to provide a unified resource addressing connector device (URL) and other network resources, and / or provide such as on-line real-time video conferencing (Net-Meeting) and other online real-time information requests and responses.

The interface conversion module 260 will be based on network unit to provide different clients in line with the specifications of the information system data transmission access. In this embodiment, the network terminal device 300 and 400 is not limited to existing personal computer or notebook computer, it may also include any communication system 200 connected via a network to have the infrastructure to support SME Business Development system or device information supply system 100 sites, such as mobile phones applies wireless applications protocol (WAP) and other browser formats. The interface conversion module 260 is to use a different browser or system or device data access protocol conversion interface is provided, it can be connected to architecture has to support the operation and development of SMEs in the information supply system 100 sites for different use Browse or access protocol network terminal devices to search for information or receive information providers are providing various forms of information services.

The billing module 270 is for the use of resources based on user mode services, computing services, they should pay the costs. In this embodiment, the billing module 270, in conformity with the information provider or manager to support the development of SMEs operating information providing system 100 of the determined price list information services, information services used to calculate the user Total service charges to be paid outside. It can also be based on the user to use the operation to support the development of SMEs information supply system model and its history of 100, as a standard computing service costs. In the aforementioned "patent application" process, for example, when a user from searching for relevant patent office or patent offices of information, the billing module 270 begins recording the user to use the site of use, click on the number or download files The amount of data and other behavior patterns, and recorded, if the user with one of the information provider has experienced patent agents interrelated, and both sides were as real-time online information and consulting service, the billing module 270 immediately recorded use between those and the information provider services and information to be served, if the user then the demand and supply of information services through the site with the Patent Office, the billing module 270 will still record information between them. It is recorded by the above-mentioned track record of user behavior patterns and the way the user can take advantage of different levels according to the website (Level) as a standard to calculate the cost of services.

See Figure 3, which shows through the above-mentioned operation to support the development of SMEs information supply system 100, the procedures described in the information supply method to support the operation and development

of SMEs in yes.

In step S301, so that the information service information receiving module 230 receives information provider uploaded and stored in the database 220. Information received by the information provider module 230 is capable of receiving data transmitted, the network protocol address provided by way of hyperlinks and / or uniform resource addressing address and other information.

Cheng said before, the information provider to support the operation and development of SMEs in the information supply system was set up a data transfer protocol between the 100 managers, such as a specific identification number or text to define specific types of information, when The information receiving module 230 receives the information and other related information with that identification number or text, it is possible according to the identification numbers or letters to the relevant information stored in the database 220 corresponding information storage field.

In this embodiment, if a patent office by the desire to support the operation and development of SMEs in the information supply system 100 as a provider of patent information, it can borrow from the network terminal device 200 via the network communication system, which It can provide information sent to the network server 210, wherein the transmission of data, including text or image information, network protocol addresses to hyperlinks provided and / or uniform resource addressing address and other information. Moreover, further comprising a specific identification number or text, such as "0001" and "Patent services", the information receiving module 230 at the network server 210 receives the information, then the information stored in the database 220 to meet the The identification number "0001" and recognized character "Patent Services" data location, followed by step S302.

In step S302, so that the information received from the service module 240 on the basis of information provided by the content information provider summarize the relevant information and organize. The process includes the same information the same provider or different information provided by suppliers, similar or different information to be classified, or a combination of induction and the like.

Cheng said before, in addition to the patent information service providers can communicate the relevant information, provided the architecture has to support the development of SMEs operating site information providing system 100 also with government agencies, such as the above-mentioned patent offices and other mutual cooperate in providing such as online and other patent applications or consulting services. Because of a patent application process may include assistance and other needs by the patent office and patent office information service providers in order to successfully complete. Then this information should be finishing module 240 information services Patent Office and the Patent Office provided information to make a classification, when the user logs architecture has to support the operation and development of the SME information supply system 100 sites, and wants When requesting the site to provide "patent application" of information services, it is possible to easily find the information and services that the patent office and summarized by the Patent Office after the above offer, followed by step S303.

In step S303, so that an information integration module 250 in accordance with the needs of the user input, the finishing and meet the needs of data through an interface conversion module 260 is transmitted to the client network terminal devices. Its integrated model includes a connection search, information services provider database 220 information network resources and / or provide real-time online information request and response and so on.

Before the bearing, when the "Patent Services" users log on to the information needs of the site, the site can provide users with an input of the user information related functions, such as the identity of the user to enter basic user usage information permissions and other personally identifiable information, as well as specific information search key identification number or character, such as the identification number "0001" and recognition of the word "patent services" through which information integration module search function 250, that person can demand the required information "patent" of related information services, and information services to support the operation and development of the SME information supply system 100 can be provided by the Patent Office and the Patent Office provided consolidated combined with each other.

In this embodiment, the user searches the database 220 relevant information, and the patent office video conferencing and network of offices above assumptions online patent application processes and other information services, followed by step S304.

In step S304, so that a billing module 270 according to the user to use this information to support the development of SMEs operating mode supply system 100, performing a service fee of statistics. It is based on the user using the information mode, calculate the required fees paid profits and the distribution of information between providers.

The front bearing, when the user 250 acquires service information to support the operation and development of the SME information supply system 100 is provided by the above process of information integration module, the billing module 270 will record the information supply Aggregated information, if the user further information contact the demand and supply through the site with the Patent Office, the billing module 270 will still record its information.

In this embodiment, the above-mentioned "patent application" process, for example, when users search for relevant patent office or patent offices of information from the billing module 270 begins recording the user to use the site of use, point When the selected frequency or amount of data downloaded file to record patterns of behavior and, if the user and the information provider which patent agency experience having contact with each other, the two sides as online real-time information and consulting services, the billing module 270 then record the relevant information and the user information between suppliers, if the user further information contact the demand and supply through the site with the Patent Office, the billing module 270 will continue to record their information. By the above information recording, the billing module 270 can connect the user based on the recorded level of the site, the connection time and / or information services and other content, calculate the corresponding service charges, which the service fees calculation basis should be developed as practicable. In addition, the billing module 270 can also provide the basis for information and managers to support the operation and development of SMEs in the information supply system 100 is provided baseline information for profit distribution, the calculated distribution of profits.

In summary, the present invention in order to support the development of the SME Business information provision method and system capable of information services through the integration of information mechanism provided by the service provider, information service integration mechanisms, billing mechanism and interface conversion mechanism , by the information supplied by a website to provide information and services provider to provide information services through the information provider sites.

Information provision method and system to support the operation and development of SMEs in the present invention can assist individuals studio, home office and SME managers and employees, in the next to take orders, to create revenue, use of external resources, conduct outsourcing services and increase business flexibility, reduce demand and office space, hiring staff, to save operating costs, reduce business barriers, such as providing help, and then to solve the unemployment problem and the purpose of the adjustment of industrial structure.

LEGAL EVENTS

Date	Code	Event	Description
Jun 30, 2004	C06	Publication	
Sep 8, 2004	C10	Request of examination as to substance	
Mar 21, 2007	C02	Deemed withdrawal of patent application after publication (patent law 2001)	

Google Home - Sitemap - USPTO Bulk Downloads - Privacy Policy - Terms of Service - About Google Patents - Send Feedback

Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2688553 A1 2008/12/04

(21) 2 688 553

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(86) Date de dépôt PCT/PCT Filing Date: 2008/06/01
(87) Date publication PCT/PCT Publication Date: 2008/12/04
(85) Entrée phase nationale/National Entry: 2009/11/26
(86) N° demande PCT/PCT Application No.: IL 2008/000740
(87) N° publication PCT/PCT Publication No.: 2008/146296
(30) Priorité/Priority: 2007/05/30 (US60/940,882)

(51) Cl.Int./Int.Cl. *G06F 21/24* (2006.01)
(71) Demandeur/Applicant:
YOGGIE SECURITY SYSTEMS, LTD., IL
(72) Inventeur/Inventor:
TOUBOUL, SHLOMO, IL
(74) Agent: HICKS INTELLECTUAL PROPERTY LAW

(54) Titre : SYSTEME ET PROCEDE POUR FOURNIR A UN DISPOSITIF UNE PROTECTION PARE-FEU POUR RESEAU ET ORDINATEUR AVEC ISOLEMENT D'ADRESSE DYNAMIQUE

(54) Title: SYSTEM AND METHOD FOR PROVIDING NETWORK AND COMPUTER FIREWALL PROTECTION WITH DYNAMIC ADDRESS ISOLATION TO A DEVICE

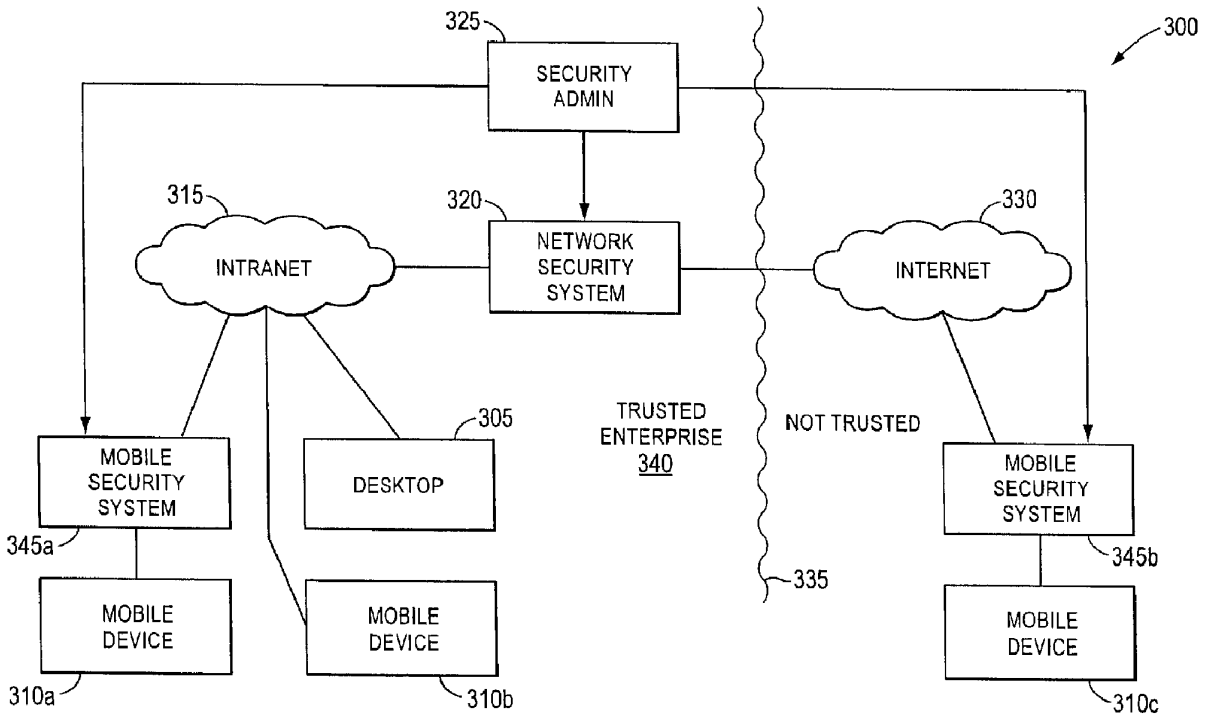


FIG. 3

(57) Abrégé/Abstract:
A computer performs dynamic address isolation. The computer comprises an application associated with an application address, a network interface coupled to receive incoming data packets from and transmit outgoing data packets to an external network, a

(21) 2 688 553

(13) A1

(57) Abrégé(suite)/Abstract(continued):
network address translation engine configured to translate between the application address and a public address, and a driver for automatically forwarding the outgoing data packets to the network address translation engine to translate the application address to the public address, and for automatically forwarding the incoming data packets to the network address translation engine to translate the public address to the application address. The computer may communicate with a firewall configured to handle both network-level security and application-level security.

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 December 2008 (04.12.2008)

PCT

(10) International Publication Number
WO 2008/146296 A2

(51) International Patent Classification:
G06F 21/24 (2006.01)

(21) International Application Number:
PCT/IL2008/000740

(22) International Filing Date: 1 June 2008 (01.06.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/940,882 30 May 2007 (30.05.2007) US

(71) Applicant *(for all designated States except US)*: **YOGGIE SECURITY SYSTEMS, LTD.** [IL/IL]; 42870 Beit Halevy (IL).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **TOUBOUL, Shlomo** [IL/IL]; 6 Main Street, 42945 Kefar Haim (IL).

(74) Agent: **SANFORD T. COLB & CO.**; P.O. Box 2273, 76122 Rehovot (IL).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(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, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

(54) Title: SYSTEM AND METHOD FOR PROVIDING NETWORK AND COMPUTER FIREWALL PROTECTION WITH DYNAMIC ADDRESS ISOLATION TO A DEVICE

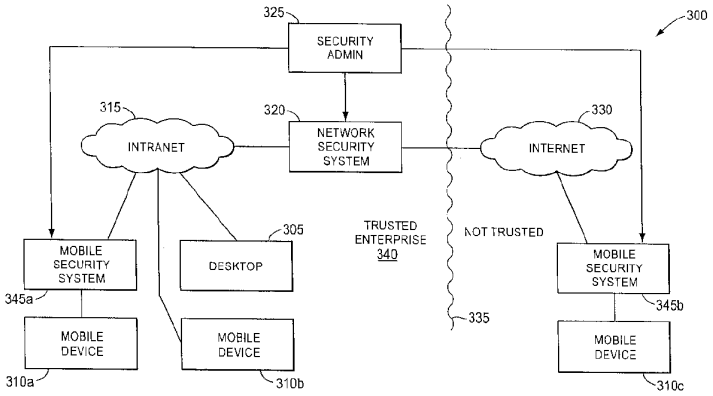


FIG. 3

(57) Abstract: A computer performs dynamic address isolation. The computer comprises an application associated with an application address, a network interface coupled to receive incoming data packets from and transmit outgoing data packets to an external network, a network address translation engine configured to translate between the application address and a public address, and a driver for automatically forwarding the outgoing data packets to the network address translation engine to translate the application address to the public address, and for automatically forwarding the incoming data packets to the network address translation engine to translate the public address to the application address. The computer may communicate with a firewall configured to handle both network-level security and application-level security.

WO 2008/146296 A2

SYSTEM AND METHOD FOR PROVIDING NETWORK AND COMPUTER FIREWALL PROTECTION WITH DYNAMIC ADDRESS ISOLATION TO A DEVICE

PRIORITY CLAIM

This application claims benefit of U.S. provisional patent application serial no. 60/940,882, which is hereby incorporated by reference.

TECHNICAL FIELD

This invention relates generally to computer security, and more particularly provides a system and method for providing data and device security between external and host devices.

BACKGROUND

The internet is an interconnection of millions of individual computer networks owned by governments, universities, nonprofit groups, companies and individuals. While the internet is a great source of valuable information and entertainment, the internet has also become a major source of system damaging and system fatal application code, such as "viruses," "spyware," "adware," "worms," "Trojan horses," and other malicious code.

To protect users, programmers design computer and computer-network security systems for blocking malicious code from attacking both individual and network computers. On the most part, network security systems have been relatively successful. A computer that connects to the internet from within an enterprise's network typically has two lines of defense. The first line of defense includes a network security system, which may be part of the network gateway, that includes firewalls, antivirus, antispyware and content filtering. The second line of defense includes individual security software on individual machines, which is not typically as secure as the network security system and is thus more vulnerable to attacks. In combination, the first and second lines of defense together provide pretty good security protection. However, when a device connects to the internet without the intervening network security system, the device loses

its first line of defense. Thus, mobile devices (e.g., laptops, desktops, PDAs such as RIM's Blackberry, cell phones, any wireless device that connects to the internet, etc.) when traveling outside the enterprise network are more vulnerable to attacks.

Figure 1 illustrates an example network system 100 of the prior art. Network system 100 includes a desktop 105 and a mobile device 110, each coupled to an enterprise's intranet 115. The intranet 115 is coupled via a network security system 120 (which may be a part of the enterprise's gateway) to the untrusted internet 130. Accordingly, the desktop 105 and mobile device 110 access the internet 130 via the network security system 120. A security administrator 125 typically manages the network security system 120 to assure that it includes the most current security protection and thus that the desktop 105 and mobile device 110 are protected from malicious code. Demarcation 135 divides the trusted enterprise 140 and the untrusted public internet 130. Because the desktop 105 and the mobile device 110 are connected to the internet 130 via the network security system 120, both have two lines of defense (namely, the network security system 120 and the security software resident on the device itself) against malicious code from the internet 130. Of course, although trusted, the intranet 115 can also be a source of malicious code.

Figure 2 illustrates an example network system 200 of the prior art, when the mobile device 110 has traveled outside the trusted enterprise 140 and reconnected to the untrusted internet 130. This could occur perhaps when the user takes mobile device 110 on travel and connects to the internet 130 at a cybercafé, at a hotel, or via any untrusted wired or wireless connection. Accordingly, as shown, the mobile device 110 is no longer protected by the first line of defense (by the network security system 120) and thus has increased its risk of receiving malicious code. Further, by physically bringing the mobile device 110 back into the trusted enterprise 140 and reconnecting from within, the mobile device 110 risks transferring any malicious code received to the intranet 115.

As the number of mobile devices and the number of attacks grow, mobile security is becoming increasingly important. The problem was emphasized in the recent Info-Security

Conference in New York on December 7-8, 2005. However, no complete solutions were presented.

Similarly, when a host device is connected to an external device such as a USB flash drive, iPod, external hard drive, etc., both devices are vulnerable to receipt of malicious code or transfer of private data. Figure 11 illustrates an example prior art data exchange system 1100 that includes a host computer (host) 1105 and an external device 1110. The host 1105 includes a external device (ED) port 1115, such as a USB port, for receiving the external device 1110. The host 1105 also includes ED drivers 1120 for performing enumeration and enabling communications between the external device 1110 and the host 1105. The external device 1110 includes an ED plug, such as a USB plug, for communicating with the ED port 1115. Both of the host 1105 and external device 1110 are vulnerable to receipt of malicious code or transfer of private data.

Accordingly, there is a need for a system and method of providing security to host and external devices.

SUMMARY

In one embodiment, the present invention provides a computer comprising an application associated with an application address; a network interface coupled to receive incoming data packets from and transmit outgoing data packets to an external network; a network address translation engine configured to translate between the application address and a public address; and a driver for automatically forwarding the outgoing data packets to the network address translation engine to translate the application address to the public address, and for automatically forwarding the incoming data packets to the network address translation engine to translate the public address to the application address. The network address translation engine may be part of the driver or part of a firewall. The firewall may be located on a mobile security system. The network address translation engine may be configured to use Dynamic Host Configuration Protocol. The computer may be configured to send data packets identifying the application to a firewall, and the firewall may be configured to handle both network-level security and application-level security.

In one embodiment, the present invention provides a system comprising a network interface; a firewall in communication with the network interface configured to handle both network-level security and application-level security; and a computer in communication with the firewall, having one or more applications, and being configured to send data packets identifying the one or more applications to the firewall. Each data may be is associated with one of the one or more applications. Each data packet may comprise data identifying the application associated with the data packet. The firewall may be configured to use the data identifying the application associated with the data packet to handle application-level security, to create a data packet subset by removing the data identifying the application from the data packet, and to send the data packet subset to an external network. The network interface may be configured to receive incoming data from an external network, and to route the incoming data to the firewall. Each application may be associated with at least one address. The firewall may be configured to dynamically isolate the address from an external network. The firewall may be configured to dynamically isolate the address from the external network through the use of Dynamic Host Configuration Protocol.

In one embodiment, the present invention provides a method within a personal computer of processing incoming data associated with a public address, the method comprising receiving the data from an external network; translating the public address into an internal address associated with an application; analyzing the data for malicious code; and routing the data to the application if the data does not comprise malicious code. The analyzing step may comprise analyzing the data for malicious code at both the network level and the application level. The translating step may use Dynamic Host Configuration Protocol.

In one embodiment, the present invention provides a method within a computer of processing outgoing data, the method comprising receiving outgoing data from an application, the application being associated with an internal address; translating the internal address into a public address; and routing at least a subset of the outgoing data to an external network using the public address, thereby dynamically isolating the internal address from the external network. The translating step may use Dynamic Host Configuration Protocol. The method may further comprise configuring the outgoing data into one or more data packets; associating each of the one or more data packets with the application; and embedding application-identifying data in each of the one or more data packets. The method may further comprise creating one or more data packet subsets by removing the application-identifying data from each of the one or more data packets, wherein the routing step comprises routing the one or more data packet subsets to the external network.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a block diagram of a prior art network system in a first state.

Figure 2 is a block diagram of a prior art network system in a second state.

Figure 3 is a block diagram of a network system in accordance with an embodiment of the present invention.

Figure 4 is a block diagram illustrating details of a computer system in accordance with an embodiment of the present invention.

Figure 5 is a block diagram illustrating details of the mobile security system in accordance with an embodiment of the present invention.

Figure 6 is a block diagram illustrating details of the mobile security system in accordance with a Microsoft Window's embodiment.

Figures 7 is a block diagram illustrating details of a smart policy updating system in accordance with an embodiment of the present invention.

Figure 8 is a block diagram illustrating details of network security measures relative to the OSI layers.

Figure 9 is a block diagram illustrating details of the communication technique for spreading security code to the mobile security systems.

Figures 10A-10C are block diagrams illustrating various architectures for connecting a mobile device to a mobile security system, in accordance with various embodiments of the present invention.

Figure 11 is a block diagram illustrating a prior art data exchange system.

Figure 12 is a block diagram illustrating a secure data exchange system, in accordance with an embodiment of the present invention.

Figure 13 is a block diagram illustrating details of a security device, in accordance with an embodiment of the present invention.

Figure 14 is a block diagram illustrating details of a security system, in accordance with an embodiment of the present invention.

Figure 15 is a block diagram illustrating a secure data exchange system, in accordance with another embodiment of the present invention.

Figure 16 is a flowchart illustrating a method of secure data exchange between a host and an external device, in accordance with an embodiment of the present invention.

Figure 17 is a block diagram illustrating a prior art network system having a hardware-based firewall.

Figure 18 is a block diagram illustrating a prior art network system having a software-based firewall.

Figure 19 is a block diagram illustrating a network system that performs dynamic address isolation, in accordance with an embodiment of the present invention.

Figure 20 is a block diagram illustrating a prior art network system having separate network and personal firewalls.

Figure 21 is a block diagram of a network system comprising a hybrid firewall in accordance with an embodiment of the present invention.

Figure 22 is a block diagram illustrating a network system comprising a hybrid firewall and configured according to the embodiment of the present invention shown in Figure 10A.

Figure 23 is a flowchart of a method of routing a data communication from an external network to an application, in accordance with an embodiment of the present invention.

Figure 24 is a flowchart of a method of routing a data communication from an application to an external network, in accordance with an embodiment of the present invention.

Figure 25 is a flowchart of a method of routing a data communication from an external network to an application, in accordance with an embodiment of the present invention.

Figure 26 is a flowchart of a method of routing a data communication from an application to an external network, in accordance with an embodiment of the present invention.

DETAILED DESCRIPTION

The following description is provided to enable any person skilled in the art to make and use the invention, and is provided in the context of a particular application and its requirements. Various modifications to the embodiments may be possible to those skilled in the art, and the generic principles defined herein may be applied to these and other embodiments and applications without departing from the spirit and scope of the invention. Thus, the present invention is not intended to be limited to the embodiments shown, but is to be accorded the widest scope consistent with the principles, features and teachings disclosed herein.

An embodiment of the present invention uses a small piece of hardware that connects to a mobile device and filters out attacks and malicious code. The piece of hardware may be referred to as a "mobile security system" or "personal security appliance." Using the mobile security system, a mobile device can be protected by greater security and possibly by the same level of security offered by its associated corporation/enterprise.

Figure 3 illustrates a network system 300 in accordance with an embodiment of the present invention. Network system 300 includes a desktop 305, a first mobile device 310a, and a second mobile device 310b. The first mobile device 310a is illustrated as within the enterprise network 340 at this time and is coupled via a mobile security system 345a to the enterprise's intranet 315. The desktop 305 and second mobile device 310b are also within the enterprise network 340 but in this embodiment are coupled to the intranet 315 without an intervening mobile security system 345 such as mobile security system 345b. The intranet 315 is coupled via a network security system 320 (which may be part of the enterprise's gateway) to the untrusted internet 330. Accordingly, the first mobile device 310a, the second mobile device 310b and the desktop 305 access the untrusted internet 330 via the network security system 320. Each may also be protected by a personal security system resident thereon (not shown). A third mobile device 310c is currently outside the enterprise network 340 and is coupled via a mobile security system 345b to the untrusted internet 330. The third mobile device 310 may be in use by an employee of the trusted enterprise 340 who is currently on travel. A security administrator 325 manages the mobile security system 345a, the mobile security system 345b, and the network

security system 320 to assure that they include the most current security protection. One skilled in the art will recognize that the same security administrator need not manage the various devices. Further, the security administrator could be the user and need not be within the trusted enterprise 340.

Demarcation 335 divides the trusted enterprise 340 and the untrusted publicly accessible internet 330. Each of mobile device 310a, 310b and 310c may be referred to generically as mobile device 310, although they need not be identical. Each mobile security system 345a and 345b may be referred to generically as mobile security system 345, although they need not be identical.

As shown, although the mobile device 310c has traveled outside the trusted enterprise 340, the mobile device 310c connects to the untrusted internet 330 via the mobile security system 345b and thus retains two lines of defense (namely, the mobile security system 345b and the security software resident on the device itself). In this embodiment, the mobile security system 345 effectively acts as a mobile internet gateway on behalf of the mobile device 310c. In an embodiment, the mobile security system 345 may be a device dedicated to network security. In an embodiment, each mobile security system 345 may support multiple mobile devices 310, and possibly only registered mobile devices 310, e.g., those belonging to enterprise 340.

Each mobile security system 345 (e.g., 345a, 345b) may be a miniature server, based on commercial hardware (with Intel's Xscale as the core), Linux OS and network services, and open-source firewall, IDS/IPS and antivirus protection. The mobile security system 345 may be based on a hardened embedded Linux 2.6.

In this embodiment, because the security administrator 325 is capable of remotely communicating with the mobile security system 345b, IT can monitor and/or update the security policies/data/engines implemented on the mobile security system 345b. The security administrator 325 can centrally manage all enterprise devices, remotely or directly. Further, the security administrator 325 and mobile security systems 345 can interact to automatically translate enterprise security policies into mobile security policies and configure mobile security

systems 345 accordingly. Because the mobile security system 345 may be generated from the relevant security policies of the enterprise 340, the mobile device 310c currently traveling may have the same level of protection as the devices 305/310 within the trusted enterprise 340.

The mobile security system 345 may be designed as an add-on to existing software security or to replace all security hardware and software on a traveling mobile device. These security applications will preferably operate on different OSI layers to provide maximum security and malicious code detection, as shown in the example system illustrated in Figure 8. Operating on the lower OSI layers and doing TCP/IP packets analysis only (by screening firewall or router packets) would miss virus and/or worm behavior. Also, many modern viruses use mobile code implemented on a "higher" level than the 7th OSI layer (Application – HTTP, FTP, etc.) and therefore cannot be interpreted at the packet layer nor at the application layer. For example, applying antivirus analysis only at the session or transport layer on a malicious Java Script (that is included in an HTML page), trying to match the signature with packets and without understanding the content type (Java Script), will not detect the malicious nature of the Java Script. To offer greater protection, the mobile security system 345 may act as corporate class security appliance and engage different security applications based on the content type and the appropriate OSI layers, (or even a "higher" level if content is encapsulated in the application layer). The mobile security system 345 may be configured to perform content analysis at different OSI layers, e.g., from the packet level to the application level. It will be appreciated that performing deep inspection at the application level is critical to detect malicious content behavior and improve detection of viruses, worms, spyware, Trojan horses, etc. The following software packages may be implemented on the mobile security system 345:

- Firewall and VPN – including stateful and stateless firewalls, NAT, packet filtering and manipulation, DOS/DDOS, netfilter, isolate user mobile devices from the internet and run VPN program on the device, etc.
- Optional web accelerator and bandwidth/cache management based on Squid.
- IDS/IPS – Intrusion detection and prevention system based on Snort. Snort is an open source network intrusion prevention and detection system utilizing a rule-driven language, which combines the benefits of signature, protocol- and anomaly-based inspections.

- Antivirus and antispyware based on ClamAV; additional AV and AS engines, e.g., McAfee, Kaspersky, Pandamay, may be offered for additional subscription fees.
- Malicious Content Detection – on the fly heuristics that perform content analysis to detect malicious content before having signatures. This will be based on a rule base and updated rules and will be content dependent scanning.
- URL Categorization Filtering – based on a commercial engine, such as Surfcontrol, Smart Filters or Websense. May provide around 70 categories of URLs such as gambling, adult content, news, webmail, etc. The mobile device 345 may apply different security policies based on the URL category, e.g., higher restriction and heuristics for Gambling or Adult content web sites, etc.

FIG. 4 is a block diagram illustrating details of an example computer system 400, of which each desktop 305, mobile device 310, network security system 320, mobile security system 345, and security administrator 325 may be an instance. Computer system 400 includes a processor 405, such as an Intel Pentium® microprocessor or a Motorola Power PC® microprocessor, coupled to a communications channel 410. The computer system 400 further includes an input device 415 such as a keyboard or mouse, an output device 420 such as a cathode ray tube display, a communications device 425, a data storage device 430 such as a magnetic disk, and memory 435 such as Random-Access Memory (RAM), each coupled to the communications channel 410. The communications interface 425 may be coupled directly or via a mobile security system 345 to a network such as the internet. One skilled in the art will recognize that, although the data storage device 430 and memory 435 are illustrated as different units, the data storage device 430 and memory 435 can be parts of the same unit, distributed units, virtual memory, etc.

The data storage device 430 and/or memory 435 may store an operating system 440 such as the Microsoft Windows XP, the IBM OS/2 operating system, the MAC OS, UNIX OS, LINUX OS and/or other programs 445. It will be appreciated that a preferred embodiment may also be implemented on platforms and operating systems other than those mentioned. An embodiment may be written using JAVA, C, and/or C++ language, or other programming languages, possibly using object oriented programming methodology.

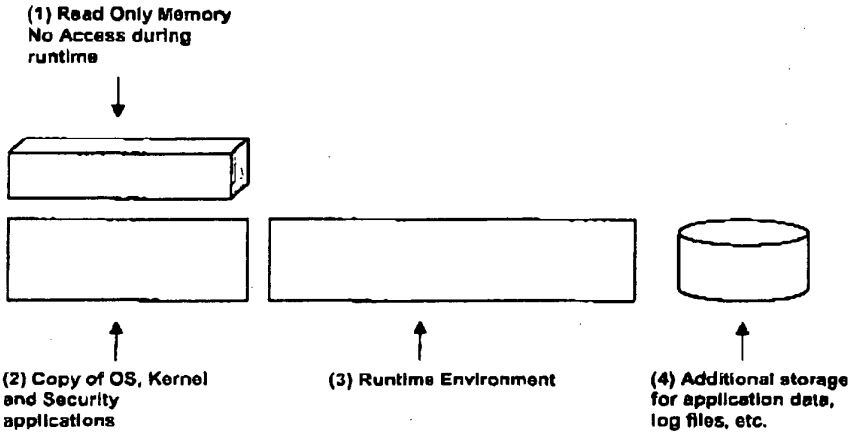
One skilled in the art will recognize that the computer system 400 may also include additional information, such as network connections, additional memory, additional processors, LANs, input/output lines for transferring information across a hardware channel, the internet or an intranet, etc. One skilled in the art will also recognize that the programs and data may be received by and stored in the system in alternative ways. For example, a computer-readable storage medium (CRSM) reader 450 such as a magnetic disk drive, hard disk drive, magneto-optical reader, CPU, etc. may be coupled to the communications bus 410 for reading a computer-readable storage medium (CRSM) 455 such as a magnetic disk, a hard disk, a magneto-optical disk, RAM, etc. Accordingly, the computer system 400 may receive programs and/or data via the CRSM reader 450. Further, it will be appreciated that the term "memory" herein is intended to cover all data storage media whether permanent or temporary.

Figure 5 is a block diagram illustrating details of the mobile security system 345 in accordance with an embodiment of the present invention. Mobile security system 345 includes adapters/ports/drivers 505, memory 510, a processor 515, a preboot flash/ROM memory module 520 storing a secure version of the mobile security system's operating system and other applications, network connection module 525, security engines 530, security policies 535, security data 540, remote management module 550, distribution module 555, and backup module 560. Although these modules are illustrated as within the mobile security system 345, one skilled in the art will recognize that many of them could be located elsewhere, e.g., on the security administrator 325 or on third-party systems in communication with the mobile security system 345. The mobile security system 345 may be in a pocket-size, handheld-size or key-chain size housing, or possibly smaller. Further, the mobile security system 345 may be incorporated within the mobile device 310.

The adapters/ports/drivers 505 include connection mechanisms (including software, e.g., drivers) for USB, Ethernet, WiFi, WiMAX, GSM, CDMA, BlueTooth, PCMCIA and/or other connection data ports on the mobile security system 345. In one embodiment, the adapters/ports/drivers 505 may be capable of connection to multiple devices 310 to provide network security to the multiple devices 310.

Memory 510 and processor 515 execute the operating system and applications on the mobile security system 345. In this example, the preboot flash 520 stores the operating system and applications. At boot time, the operating system and applications are loaded from the preboot flash 520 into memory 510 for execution. Since the operating system and applications are stored in the preboot flash 520, which cannot be accessed during runtime by the user, the operating system and applications in the preboot flash 520 are not corruptible. Should the copy of the operating system and applications in memory 510 be corrupted, e.g., by malicious code, the operating system and applications may be reloaded into the memory 510 from the preboot flash 520, e.g., upon restart. Although described as stored within the preboot flash 520, the OS and applications can be securely stored within other read-only memory devices, such as ROM, PROM, EEPROM, etc.

Memory (including memory 510 and preboot flash 520) on the mobile security system 345 may be divided into zones as follows:



Upon each "hard" restart, the boot loader (resident at area 1) of the mobile security system 345 copies the kernel and security applications (a fresh unchanged copy) from area 1 to 2. This causes a clean version of the OS and applications to be loaded into area 2 each time. That way, if a special mobile security system 345 attack is developed, the attack will be unable to infect the

system, since the OS and applications are precluded from accessing memory area 1 during runtime. Further, any attack that does reach memory 510 will be able to run only once and will disappear upon a hard restart. A triggering mechanism may be available to restart the mobile security system 345 automatically upon infection detection.

The network connection module 525 enables network connection, e.g., to the internet 330 or the intranet 315 via network communication hardware/software including WiFi, WiMAX, CDMA, GSM, GPRS, Ethernet, modem, etc. For example, if the mobile device 310 wishes to connect to the internet 330 via a WiFi connection, the adapters/ports/drivers 505 may be connected to the PCI port, USB port or PCMCIA port of the mobile device 310, and the network connection module 525 of the mobile security system 345 may include a WiFi network interface card for connecting to wireless access points. Using the network connection module 425, the mobile security system 345 may communicate with the network as a secure gateway for the mobile device 310. Other connection architectures are described in Figures 10A-10C.

The security engines 530 execute security programs based on the security policies 535 and on security data 540, both of which may be developed by IT managers. Security engines 530 may include firewalls, VPN, IPS/IDS, antivirus, antispyware, malicious content filtering, multilayered security monitors, Java and bytecode monitors, etc. Each security engine 530 may have dedicated security policies 535 and security data 540 to indicate which procedures, content, URLs, system calls, etc. the engines 530 may or may not allow. The security engines 530, security policies 535 and security data 540 may be the same as, a subset of, and/or developed from the engines, policies and data on the network security system 320.

To provide a higher security level provided by antivirus and antispyware software, the security engines 530 on each mobile security system 345 may implement content analysis and risk assessment algorithms. Operating for example at OSI Layer 7 and above (mobile code encapsulated within Layer 7), these algorithms may be executed by dedicated High Risk Content Filtering (HRCF) that can be controlled by a rules engine and rule updates. The HRCF will be based on a powerful detection library that can perform deep content analysis to verify real content types. This is because many attacks are hidden within wrong mime types and/or may use

sophisticated tricks to present a text file type to a dangerous active script or ActiveX content type. The HRCF may integrate with a URL categorization security engine 530 for automatic rule adjustment based on the URL category. In one embodiment, when the risk level increases (using the described mechanism) the mobile security system 345 may automatically adjust and increase filtering to remove more active content from the traffic. For example, if greater risk is determined, every piece of mobile code, e.g., Java script, VB script, etc. may be stripped out.

Three aspects for integration with corporate policy server legacy systems include rules, LDAP and active directory, and logging and reporting as discussed below. In one embodiment, a policy import agent running on the security administrator 325 will access the rule base of Checkpoint Firewall-1 and Cisco PIX Firewalls and import them into a local copy. A rule analysis module will process the important rules and will offer out-of-the-box rules and policies for mobile security systems 345. This proposed policy will offer all mobile security systems 345 a best fit of rules that conform the firewall policy of the enterprise 340. The agent will run periodically to reflect any changes and generate updates for mobile security system 345 policies 535. The LDAP and Active Directory may be integrated with the directory service to maintain mobile security system 345 security policies 535 that respond to the enterprise's directory definitions. For example, a corporate policy for LDAP user Group "G" may automatically propagate to all mobile security systems 345 in "G" group. Mobile security system 345 local logs and audit trails may be sent in accordance to a logging and reporting policy to a central log stored at the security administrator 325. Using a web interface, IT may be able to generate reports and audit views related to all mobile device 310 users, their internet experiences, and attempts to bring infected devices back to the enterprise 340. IT will be able to forward events and log records into legacy management systems via SYSLOG and SNMP Traps.

The security engines 530 may perform weighted risk analysis. For example, the security engine 530 may analyze HTTP, FTP, SMTP, POP3, IM, P2P, etc. including any traffic arriving from the internet 330. The security engine 530 may assign a weight and rank for every object based on its type, complexity, richness in abilities, source of the object, etc. The security engine 530 may assign weight based on the source using a list of known dangerous or known safe sources. The security engine 530 may assign weight to objects based on the category of the

source, e.g., a gambling source, an adult content source, a news source, a reputable company source, a banking source, etc. The security engine 530 may calculate the weight, and based on the result determine whether to allow or disallow access to the content, the script to run, the system modification to occur, etc. The security engine 530 may "learn" user content (by analyzing for a predetermined period of time the general content that the user accesses) and accordingly may create personal content profiles. The personal content profile may be used to calibrate the weight assigned to content during runtime analysis to improve accuracy and tailor weighted risk analysis for specific user characteristics.

In some embodiments, the security engines 530, security policies 535 and security data 540 may enable bypassing the mobile security system 345. The security policy 535, set by the security administrator 325, may include a special attribute to force network connection through the mobile security system 325 when outside the trusted enterprise 340. Thus, if this attribute is set "on," when a mobile device 310 attempts to connect to the internet 330 without the mobile security system 345 and not from within the trusted enterprise 340, all data transfer connections including LAN connection, USB-net, modem, Bluetooth, WiFi, etc. may be closed. The mobile device 310 may be totally isolated and unable to connect to any network, including the internet 330.

In one embodiment, to enable this, when first connecting the mobile security system 345 to the mobile device 310 using for example the USB cable (for both power and USB connection creation), the USB plug & play device driver will be sent into the mobile device 310. The installed driver may be "Linux.inf" which allows a USB-net connection for the mobile security system 345. This connection allows the mobile security system 345 to access the internet 330 via the USB port and using the mobile device 310 network connection plus additional code ("the connection client"). In a Windows example, the connection client may be installed at the NDIS level of the mobile device 310 above all the network interface cards of every network connection as shown in Figure 6. The implementation will be as an NDIS Intermediate (IM) Driver or NDIS-Hooking Filter Driver. Both implementations may be at the kernel level, so that an end user cannot stop or remove it. When starting the mobile device 310, the connection client may attempt to connect to the security administrator 325 or the network security system 320 locally

within the trusted enterprise 340. If the node is not found (finding via VPN is considered as not found in local LAN), the connection client will assume it is working from outside the trusted enterprise 340 and expects to find the mobile security system 345 connected, e.g., via USB-net or other connection mechanism. If the mobile security system 345 is not found, the connection client may avoid any communication to any network connection. By a policy definition, this behavior can be modified to allow communication to the enterprise 340 via VPN installed in the mobile device 310. Similarly, in case of a mobile device system 345 failure, all traffic may be disabled, except for the VPN connection into the enterprise 340.

It will be appreciated that NDIS is one possible implementation of intercepting traffic at the kernel level. For example, in another embodiment, the system may hook Winsock or apply other ways that may be in future Windows versions.

In an embodiment where the mobile security system 345 supports multiple mobile devices 310, the security engines 530, security policies 535 and security data 540 may be different for each mobile device 310 (e.g., based on for example user preferences or IT decision). Alternatively, it can apply the same engines 530, policies 535 and data 540 for all connected devices 310.

The remote management module 550 enables communication with security administrator 325 (and/or other security administrators), and enables local updating of security engines 530, security policies 535, security data 540 including signatures and other applications. In one embodiment, modification to the security policies 535 and data 540 can be done by the security administrator 325 only. The remote management module 550 of the mobile security system 345 may receive updates from an update authorities device (UAD), e.g., on the security administrator 325 via a secured connection. A UAD may operate on an update server at a customer IT center located on the internet 330 to forward updates to mobile security systems 345 that possibly do not belong to an enterprise 540 in charge of managing updates. A UAD may operate on a mobile security system 345. Security engine 530 updates may modify the antivirus engine DLL, etc. OS and security application updates may be implemented only from within the enterprise 540

while connecting to the security administrator 325 and via an encrypted and authenticated connection.

The security administrator 325 can modify URL black and white lists for remote support to traveling users. In case of false positives, the security administrator 325 may allow access to certain URLs, by bypassing the proactive heuristics security but still monitoring by firewall, antivirus, IPS/IDS, etc. Additional remote device-management features may enable the security administrator 325 to perform remote diagnostics, access local logs, change configuration parameters, etc. on the mobile security system 345. The security administrator 325 may delegate tasks to a helpdesk for support.

The remote management module 550 may communicate with a wizard (e.g., wizard 745), which may be on the security administrator 325, as illustrated in Figure 7, or on another system. Details of the wizard 745 and details of the communication schemes between the remote management module 550 and the wizard 745 are described below with reference to Figure 7.

The distribution module 555 enables distribution of updates, e.g., security policy 535 updates including rule updates, security data 540 updates including signature updates, security engine 530 updates, application/OS updates, etc. by the mobile security system 345 to N other mobile security systems 345. A routing table identifying the N other mobile security systems 345 to whom to forward the updates may be provided to the distribution module 555 to enable system 345 to system 345 communication. Updates may be implemented according to policies set by the security administrator 325. When forwarding updates, the distribution module 555 acts as a UAD.

Each mobile security system 345 may obtain its routing table with security information updates, periodically, at predetermined times, upon login, etc. The routing tables may be maintained on a server, e.g., the security administrator 325 or another mobile security system 345. In one embodiment, the mobile security systems 345 may contact the server to retrieve the routing tables. Alternatively, the server may push the routing tables to the mobile security systems 345.

The distribution module 555 may enable rapid updates as shown in Figure 9. Currently, all commercial antivirus products available do not update devices faster than viruses spread. To assure that a new virus attack does not spread faster than for example signature updates, each mobile security system 345 may be an active UAD. In one embodiment, as shown in Figure 9, each mobile security system 345 is responsible for forwarding the signature updates to four other devices 345. As one skilled in the art will recognize, all devices 345 need to forward to the same number of other devices 345. Multiple devices 345 may be responsible for forwarding to the same device 345. When necessary, offline devices 345 being activated may poll the server, e.g., the security administrator 325, for routing table updates. Many other updating techniques are also possible.

The backup module 560 may constantly backup image and changes of the boot sector and system files of the mobile device 310 into the flash memory 520 or into another persistent memory device. That way, in case of major failure, including a loss of the system or boot sector of the mobile device 310, the mobile security system 345 may be identified as a CD-ROM during reboot and may launch the backup module (or separate program) to restore the boot sector and system files on the mobile device 310, thereby recovering the mobile device 310 without the need for IT support. In an embodiment where the network security system 345 supports multiple mobile devices 310, the backup module 560 may contain separate boot sector and system files for each of the mobile devices 310, if different.

Figure 7 is a block diagram illustrating details of a smart policy updating system 700 in accordance with an embodiment of the present invention. System 700 includes the security administrator 325 coupled to the network security system 320 and to the mobile security system 345. The network security system 320 includes security engines 705, including an antivirus engine 715, an IPS/IDS engine 720, a firewall engine 725, and other security engines. The network security system 320 also includes security policies and data 710, including antivirus policies and data 730, IPS/IDS policies and data 735, firewall policies and data 740, and other policies and data. Similarly, the mobile security system 345 includes an antivirus engine 755, an IPS/IDS engine 760, a firewall engine 765, and other engines. The mobile security system 345

also includes security policies and data 535/540, including antivirus security policies and data 770, IPS/IDS security policies and data 775, firewall security policies and data 780, and other security policies and data.

The security administrator 325 includes a wizard 745 for enabling substantially automatic initial and possibly dynamic setup of the security engines 530, security policies 535 and security data 540 on the mobile security system 345. In one embodiment, the wizard 745 may automatically load all security engines 705 and policies and data 710 of the network security system 320 as the security engines 530 and policies and data 535/540 on the mobile security system 345. In another embodiment, the wizard 745 may include all security engines 705 and policies and data 710 except those known to be irrelevant, e.g., those related to billing software used by accounting, those relating to web software running only on the web servers, etc. In another embodiment, the engines 530 would need to be loaded by an IT manager, and would not be loaded automatically by the wizard 745.

In one embodiment, the wizard 745 may determine whether the mobile security system 345 requires a particular security engine 530, e.g., an antivirus engine 755, IPS/IDS engine 760, firewall engine 765, etc. If so determined, then the wizard 745 would load the engine 530 onto the mobile security system 345. The wizard 745 would then determine which policies and data sets, e.g., some for antivirus engine 755, some for the IPS/IDS engine 760, some for the firewall engine 765, etc. are important to the mobile security system 345. The wizard 745 will then determine which of the antivirus policies and data 730 on the network security system 320 are relevant to the antivirus policies and data 770 on the mobile security system 345, which of the IPS/IDS policies and data 735 on the network security system 320 are relevant to the IPS/IDS policies and data 775 on the mobile security system 345, which of the firewall policies and data 740 on the network security system 320 are relevant to the firewall policies and data 780 on the mobile security system 345, and which of the other policies and data on the network security system 320 are relevant to the policies and data on the mobile security system 345. As stated above, the wizard 745 may determine that all security engines 705 or just a subset are needed on the mobile security system 345. The wizard 745 may determine that all policies and data 710 for a given engine type or just a subset should be forwarded. The wizard 745 may determine which

relevant policies and data 710 should be forwarded to the mobile security system 345 based on rules developed by an IT manager, based on item-by-item selection during the setup procedure, etc. Alternative to the wizard 745, an IT manager can setup the engines 530 and policies and data 535/540 on the mobile security system 345 without the wizard 745.

The security administrator 325 may also include an update authorities device 750. The update authorities device 750 may obtain security system updates (e.g., signature updates) and may send the updates to the network security system 320 and to the mobile security system 345. One skilled in the art will recognize that the updates to the network security system 320 and the updates to the mobile security system 345 need not be the same. Further, the update authorities device 750 may obtain the updates from security managers, security engine developers, antivirus specialists, etc. The update authorities device 750 may forward the updates to all network security systems 320 and all mobile security systems 345, or may forward routing tables to all mobile security systems 345 and the updates only to an initial set of mobile security systems 345. The initial set of mobile security systems 345 may forward the updates to the mobile security systems 345 identified in the routing tables in a P2P manner, similar to the process illustrated in Figure 9. As stated above, each mobile security system 345 operating to forward updates is itself acting as an update authorities device 750.

Other applications may be included on the mobile security system 345. For example, add-on applications for recurring revenue from existing customers may include general email, anti-spam, direct and secured email delivery, information vaults, safe skype and other instant messaging services, etc.

- Email Security and Anti-spam – implementation of mail relay on mobile security systems 345 (including the web security engine above) and a local spam quarantine (based on SendMail or similar process) may implement a complete mail security suite (SMTP and POP3) including anti-spam with real time indexing (via online web spam quarries). Users may have access to the quarantine to review spam messages, release messages, modify and custom spam rules, etc., via a web interface.
- Direct and Secured Email Delivery based on mail relay will allow the mobile security system 345 to send user email directly from one mobile security system 345 to another

mobile security system 345 without using in route mail servers. This allows corporate users to send emails that need not travel in the internet, thus leaving trace and duplicates on different unknown mail servers in route. This combined with the ability to use a secured pipe between two mobile security systems is valuable to corporations. Without such methodology, people could trace emails exchange without accessing to the enterprise's mail server, by tracking down copies in intermediate mail servers that were used to deliver the messages.

- Information Vault – Application to encrypt and store end user information on the mobile security system 345 may be available only to authorized users via a web interface and a web server implemented on every mobile security system 345 (e.g., BOA, Apache, etc.)
- Safe Skype and Other IM – implementing an instant messaging client on the mobile security system 345 can guarantee that the instant messaging system or P2P application has no access to data on the mobile device 310. Adding a chipset of AC/97 to provide a sound interface on the mobile security system 325 could allow users to talk and receive calls directly from/to the mobile security system 325.

Although not shown, a small battery may be included with the mobile security system 345. This battery may be charged by the USB connection during runtime or using the power adapter at any time. The battery may guarantee proper shutdown, e.g., when user disconnects the USB cable from the mobile security system 345. It will be signaled by the system which will launch applications and system shutdown. This will ensure a proper state of the file system and flashing open files buffers.

A multi-layered defense and detection abilities is required. This may be done by a special code that is constantly monitoring the scanning result by different systems (antivirus, IDS/IPS, firewall, antispyware, URL category, etc.) and at different levels to build a puzzle and identify an attack even if its not recognized by each of the individual subsystems. By doing this, the mobile security system 345 will maintain and in some cases even improve the security level provided within the enterprise 540.

One available benefit of the mobile security system 345 is its ability to enforce the policy of the enterprise 540 on the end user while they are traveling or working from home. Since the mobile security system 345 uses similar security engines and policy as when connected from within the enterprise 540 and since the end user cannot access the internet 330 without it (except via VPN connection into the enterprise 540), IT may be capable of enforcing its security policy beyond the boundaries of the enterprise 540. The OS may be under the entire supervision of IT, while the mobile security system 345 OS acts as an end user OS under his control. This resolves the problems of who controls what and how security and productivity face minimal compromise.

A standalone version of the mobile security system 345 may offer the same functionality, and may provide a local management interface via web browser. Attractive to home users and small offices that lack an IT department, the mobile security system 345 enables the end user to launch a browser, connect to the mobile security system 345, set the different policies (update policy, security rules, etc.) including modifying the white and black URL lists, etc. There is also an opportunity to provide end users with a service of remote management of the mobile security systems 345 by subscription.

Figures 10A, 10B and 10C illustrate three example architectures of connecting a mobile security system 345 to a mobile device 310, in accordance with various embodiments of the present invention. In Figure 10A, the mobile device 310 is coupled to the mobile security system 345 via USB connections 1015 and 1020 and is coupled to the internet 330 via a NIC card 1005. The mobile device 310 receives internet traffic from the internet 330 via its NIC card 1005. A kernel-level redirector 1010 (e.g., via NDIS, Winsock, etc.) on the mobile device 310 automatically redirects the internet traffic via the USB connections 1015 and 1020 to the mobile security system 345, which scans, cleans and returns the cleaned internet traffic to the mobile device 310 via the USB connections 1015 and 1020. In Figure 10B, the mobile device 310 is coupled to the mobile security system 345 via USB connections 1025 and 1030. The mobile security system 345 includes a NIC card 1035 for receiving internet traffic from the internet 330. The mobile security system 345 scans, cleans and forwards the internet traffic via the USB connections 1025 and 1030 to the mobile device 310. In Figure 10C, the mobile device 310 is coupled to the mobile security system 345 via NIC cards 1040 and 1045. The mobile security

system 345 receives internet traffic from the internet 330 via its NIC card 1045. The mobile security system 345 scans, cleans and forwards the internet traffic wirelessly via the NIC cards 1040 and 1045 to the mobile device 310. Other connection architectures are also possible.

Figure 12 is a block diagram illustrating a secure data exchange system 1200, in accordance with an embodiment of the present invention. The secure data exchange system 1200 includes a host computer (host) 1205 coupled via a security device 1210 to an external device 1110. The host 1205 may include a laptop, desktop, PDA, mobile phone, or other processor-based device. The external device 1110 may be any external device with memory such as a USB drive, external hard drive, PDA, music player, cell phone, etc. The security device 1210 is communicatively coupled to the host 1205 via an ED port 1225 (USB, serial, parallel, Firewire, Ethernet, WiFi, WiMAX, GSM, CDMA, BlueTooth, PCMCIA and/or other connection) and an ED plug 1230 (USB, serial, parallel, Firewire, Ethernet, WiFi, WiMAX, GSM, CDMA, BlueTooth, PCMCIA and/or other connection). The external device 1110 is communicatively coupled to the security device 1210 via an ED port 1235 (USB, serial, parallel, Firewire, Ethernet, WiFi, WiMAX, GSM, CDMA, BlueTooth, PCMCIA and/or other connection) and ED plug 1120 (USB, serial, parallel, Firewire, Ethernet, WiFi, WiMAX, GSM, CDMA, BlueTooth, PCMCIA and/or other connection). The connector type of the ED port 1225 and ED plug 1230 combination may be different that the connector type of the ED port 1235 and ED plug 1120 combination. In one embodiment, all ports 1225/1235 and plugs 1230/1120 are USB. Although the plugs 1120/1230 are illustrated as male and ports 1225/1235 are shown as female, one skilled in the art will recognize that the opposite is possible (plugs 1120/1230 may be female and ports 1225/1235 may be male).

The host 1205 includes ED drivers 1220 for performing enumeration and enabling communication with the security device 1210. Similarly, the security device 1210 includes ED drivers 1245 for performing enumeration and enabling communication with the external device 1110.

In one embodiment, the security device 1210 includes a programmable hardware appliance capable of enforcing security policies to protect against malicious code such as viruses,

spyware, adware, Trojan Horses, etc. and to protect against transfer of private data. In one embodiment, the security device 1210 is configured to protect both the host 1205 and the external device 1215. In one embodiment, the security device 1210 is configured to protect only one of the external device 1110 or the host 1205. Additional details of the security device 1210 are provided with reference to Figures 13 and 14.

Figure 13 is a block diagram illustrating details of the security device 1210, in accordance with an embodiment of the present invention. The security device 1210 include a processor 1305, such as an Intel Pentium® microprocessor or a Motorola Power PC® microprocessor, coupled to a communications channel 1315. The security device 1210 further includes an ED plug 1230, an ED port 1235, a communications interface 1310, storage 1320 such as an EEPROM, and memory 1325 such as Random-Access Memory (RAM) or Read Only Memory (ROM), each coupled to the communications channel 1315. The communications interface 1310 may be coupled to a network such as the internet. One skilled in the art will recognize that, although the storage 1320 and memory 1325 are illustrated as different units, the data storage device 1320 and memory 1325 can be parts of the same unit, distributed units, virtual memory, etc. The term "memory" herein is intended to cover all data storage media whether permanent or temporary. One skilled in the art will recognize that the security device 1210 may include additional components, such as network connections, additional memory, additional processors, LANs, input/output lines for transferring information across a hardware channel, the internet or an intranet, etc.

As shown, memory 1325 stores an operating system 1330 such as the Microsoft Windows XP, the IBM OS/2 operating system, the MAC OS, Unix OS, Linux OS, etc. It will be appreciated that a preferred embodiment may also be implemented on platforms and operating systems other than those mentioned. An embodiment may be written using JAVA, C, and/or C++ language, or other programming languages, possibly using object oriented programming methodology. The memory 1325 also stores ED drivers 1245 and a security system 1335. The ED drivers 1245 may include standard drivers for standard external devices 1110 and proprietary drivers for proprietary external devices 1110. The ED drivers 1245 may be transferred onto the

memory 1325 via ED plug 1230. The security system 1335 includes code for enforcing security policies on data transfer actions between the host 1205 and external device 1110.

Figure 14 is a block diagram illustrating details of a security system 1335, in accordance with an embodiment of the present invention. The security system 1335 includes a security manager 1405, security engines 1410, security policies 1415, and security data 1420.

In one embodiment, the security manager 1405 includes code for performing enumeration, namely, to identify the external device 1110 or external device 1110 type and to identify the corresponding ED driver 1245 capable of establishing communication between the security device 1210 and the external device 1110. The security manager 1405 also includes code to control execution of the various security engines 1410 based on the security policies 1415 and security data 1420 to evaluate data transfer requests or other device requests. Further, the security manager 1405 includes code to communicate with the host 1205, which will be the source of the data transfer and/or other requests.

In one embodiment, the security engines 1410 includes code for securing the transfer of data between the host 1205 and the external device 1110 based on the security policies 1415 and security data 1420. The security engines 1410 may include firewalls, antivirus, antispyware, malicious content filtering, multilayered security monitors, Java and bytecode monitors, etc. The security engines 1410 may also include data privacy modules to enforce data privacy policies 1415. Each security engine 1410 may have dedicated security policies 1415 and security data 1420 to indicate which procedures, URLs, system calls, content, ID, etc. the data requested for transfer may contain or whether the data requested for transfer is considered nontransferable (or nontransferable without additional security measure such as a password and ID).

To provide a higher security level, the security engines 1410 may implement content analysis and risk assessment algorithms. In one embodiment, a security engine 1410 assigns a weight and rank for every transfer object based on its type, complexity, richness in abilities, source, etc. The security engine 1410 may assign weight based on the source using a list of known dangerous or known safe sources. The security engine 1410 may assign weight to objects

based on the category of the source, e.g., a gambling source, an adult content source, a news source, a reputable company source, a banking source, etc. The security engine 1410 may calculate the weight, and based on the result determine whether to allow or disallow access to the content, the script to run, the system modification to occur, etc. The security engine 1410 may "learn" user content (by analyzing for a predetermined period of time the general content that the user accesses) and accordingly may create personal content profiles. The personal content profile may be used to calibrate the weight assigned to content during runtime analysis to improve accuracy and tailor weighted risk analysis for specific user characteristics.

Thus, upon receiving a data transfer and/or other request from the host 1205, the security manager 1405 will launch the appropriate security engines 1410 based on the security policies 1415. For example, the security policies 1415 may be configured not to allow specific ActiveX controls to be loaded from the host 1205 onto the external device 1110. The security policies 1415 may be configured not to allow data transfer from private folders on the host 1205 to the external device 1110. The security manager 1405 will launch the appropriate security engines 1410 to assure that these example security policies 1415 are met. Further, the security engines 1410 may use security data 1420, which may include definition files of malicious ActiveX controls, locations of private folders, etc.

Although not shown, the security system 1335 may include additional components such as the preboot flash 520 with OS and applications, the remote management module 550, the distribution module 555, and the backup module 560 discussed above with reference to Figure 5. Other components are also possible.

Figure 15 is a block diagram illustrating a secure data exchange system 1500, in accordance with another embodiment of the present invention. The secure data exchange system 1500 includes a security device 1505 communicatively coupled to the host 1520 via an ED plug 1515 on the security device 1505 and a first ED port 1525 on the host 1520. The secure data exchange system 1500 also includes an external device 1110 communicatively coupled to the host 1520 via the ED plug 1120 on the external device 1110 and a second ED port 1535 on the host 1520.

Because the external device 1110 is not directly coupled to the security device 1505, the security device 1505 is not physically intercepting the data transfer requests between the external device 1110 and the host 1520. Accordingly, in this embodiment, the host 1520 includes a redirect driver 1530, which is configured to redirect data transfer requests between the external device 1110 and the host 1520 regardless of data transfer direction. In one embodiment, the security device 1505 may be configured to protect only one of the external device 1110 or the host 1520. Further, in one embodiment, the security device 1505 does not contain any ED drivers, e.g., ED drivers 1245.

In one embodiment, if the security device 1505 is not coupled to the host 1520, the host 1520 uses the ED drivers 1540 to communicate with the external device 1110. In one embodiment, the host 1520 is configured not to communicate with the external device 1110 until the security device 1505 is coupled to the host 1520. In one embodiment, the host 1520 uses the ED drivers 1540 to communicate with the external device 1110 only if additional security measures are taken, such as receipt of a password and ID, or until the security device 1505 is coupled to the host 1520.

In one embodiment, the host 1520 may conduct enumeration of the security device 1505 upon connection of the security device 1505 to the ED port 1525. Upon identifying the security device 1505 or security device 1505 type, the host 1520 may initiate the redirect driver 1530 to redirect all data transfer requests or other external device 1110 requests from all other ED ports 1535 to the security device 1505. In one embodiment, the redirect driver 1530 only accepts data transfer requests from the security device 1505, which presents the requests of the external device 1110 as a proxy. In one embodiment, the redirect driver 1530 performs data transfer requests received from the external device 1110 only after the security device 1505 has conducted its check and given its authorization. Other protocols are also possible.

Figure 16 is a flowchart illustrating a method 1600 of secure data exchange between a host and an external device, in accordance with an embodiment of the present invention. The method 1600 begins in step 1605 with the security device 1505 being connected to the first ED

port 1525 of the host 1520. The external device 1110 in step 1610 is connected to the second ED port 1535 of the host 1520. The host 1505 in step 1615 performs enumeration techniques to identify the security device 1505 and the external device 1110 and to install the appropriate drivers 1530/1540 to enable communication with the security device 1505 and the external device 1110. The redirect driver 1530 in step 1620 receives a data transfer request from either the host 1505 to the external device 1110 or from the external device 1110 to the host 1505. The redirect driver 1530 in step 1625 redirects the data transfer request to the security device 1505, which in step 1630 enforces its security policies (antivirus, antispyware, anti-adware, data privacy, etc.) on the data transfer request. The security device 1505 in step 1635 determines whether the data transfer request passes the security policies. If so, then the security device 1505 in step 1640 authorizes the data transfer request and the host 1520 in step 1645 performs the data transfer request. If not, then the security device 1505 in step 1650 rejects the data transfer request. Method 1600 then ends.

It will be appreciated that, in one embodiment, the security device 1210/1505 may be implemented as part of the host 1205/1520, e.g., within the housing of the host 1205/1520 and/or as a security procedure executed by the host 1205/1520.

Dynamic Isolation

Figure 17 shows a prior art network system 1700 having a hardware-based firewall. The network system 1700 includes internal computers 1705a and 1705b, a first network interface card (NIC) 1710, a hardware-based firewall 1715 that performs network address translation (NAT), a second NIC 1720, an external network 1725 (such as the Internet), and external computers 1730a and 1730b.

The firewall 1715 is a hardware-based firewall, such as Check Point FW-1 or Cisco PIX. The firewall uses two different network ports (the first NIC 1720 and the second NIC 1720) to separate and isolate the internal computers 1705a and 1705b from the external network 1720. The firewall 1715 uses network address translation (NAT) to translate the Internet Protocol (IP) address of the internal computer 1705a (denoted as IP address x) and the IP address of the

internal computer 1705b (denoted as IP address y) into a public IP address z, thus hiding the IP addresses of the internal computers 1705a and 1705b. The firewall 1715 performs a similar translation on the Media Access Control (MAC) addresses of the internal computers 1705a and 1705b.

The network system 1700 provides a higher level of security than PC software-based firewalls (such as Microsoft Windows Personal Firewall and Check Point ZoneAlarm) running on the internal computers 1705a and 1705b themselves, since PC software-based firewalls do not hide the IP and MAC addresses of the internal computers.

Figure 18 shows a prior art network system 1800 having a software-based firewall. The network system 1800 includes an external network 1805 (such as the Internet), one or more NICs 1810 (denoted as 1810a, 1810b, ... 1810n), a Network Driver Interface Specification (NDIS) driver 1815 that acts as an interface between layer 2 (the data link layer) and layer 3 (the network layer), an intermediate driver 1820 (such as MINIPort in the Microsoft Windows operating system), a software-based firewall 1825, an operating system 1830, and one or more applications 1835 (denoted as 1835a, 1835b, ... 1835m). The operating system 1830 contains a TCP/IP protocol suite 1840.

In operation, the intermediate driver 1820 directs traffic arriving from the NICs 1810 and NDIS driver 1815 to the software-based firewall 1825. The software-based firewall 1825 decides what to do with the traffic (allow, deny, or reject) and permits only the allowed traffic to proceed to the operating system 1830.

The network system 1800 does not use a hardware-based firewall. Only one of the NICs 1810 needs to be used at any given time. However, the IP and MAC addresses of the NICs 1810 (which are visible to the external network 1805) are the same IP and MAC addresses that are viewed and used by the applications 1835 (i.e., there is no address isolation between the applications 1835 and the external network 1805).

Figure 19 shows a network system 1900 that performs dynamic address isolation, in accordance with an embodiment of the present invention. The network system 1900 includes an external network 1905 (such as the Internet), one or more NICs 1910 (denoted as 1910a, 1910b, ... 1910n), an NDIS driver 1915 that acts as an interface between layer 2 (the data link layer) and layer 3 (the network layer), an intermediate driver 1920, a software-based or hardware-based firewall 1925, an operating system 1930, and one or more applications 1935 (denoted as 1935a, 1935b, ... 1935m). The operating system 1930 contains the TCP/IP protocol suite 1940. The intermediate driver 1920 includes a NAT engine 1945, which contains a translations table for IP and MAC addresses.

The NICs 1910, NDIS driver 1915, intermediate driver 1920, firewall 1925, operating system 1930, and applications 1935 may be installed in a mobile device 310. The firewall 1925 may be an external firewall 1925 connected to the intermediate driver 1920 by a Universal Serial Bus (USB) connection, a wireless connection, or another network wire connection. For example, the firewall 1925 may be part of the mobile security system 345.

In operation, the intermediate driver 1920 receives all data packets arriving from the NICs 1910 and NDIS driver 1915, and routes each data packet to the NAT engine 1945. The NAT engine 1945 uses Dynamic Host Configuration Protocol (DHCP) to dynamically isolate the IP addresses of the applications 1935 from the external network 1905. As shown in Figure 19, the dynamic NAT engine 1945 translates the IP address of the application 1935 (IP address x) to a different IP address (IP address z) while interfacing with the NIC, and translates the IP address z back to the IP address x when sending data to the operating system 1930. Thus, the intermediate driver 1920 provides IP address z to the external network 1905, while isolating IP address x from the external network. The NAT engine 1945 performs a similar translation on MAC addresses, if necessary. As shown, the NAT engine 1945 is part of the intermediate driver 1920. However, one skilled in the art will recognize that the NAT engine 1945 may be located elsewhere, e.g., on the mobile security system 345, part of the firewall 1925, etc.

After the NAT engine 1945 translates the IP address, the intermediate driver 1920 directs each data packet to the firewall 1925. The firewall 1925 decides what to do with each data

packet (allow, deny, or reject) and permits only the allowed data packets to proceed to the operating system 1930. The intermediate driver 1920 receives each allowed data packet back from the firewall 1925 and routes each allowed data packet to an application 1935.

For outgoing data packets, the intermediate driver 1920 receives each data packet from the application 1935 and routes each data packet to the NAT engine 1945. The NAT engine 1945 translates the IP and/or MAC address associated with the data packet as described above. The intermediate driver 1920 then receives each data packet (containing the translated IP and/or MAC address) back from the NAT engine 1945 and routes each data packet to the external network 1905.

In this way, the network system 1900 is able to isolate the IP and MAC addresses of internal computers/applications from the external network 1905, while not requiring the use of a hardware-based firewall or more than one NIC. Network isolation and separation is achieved even if the firewall lacks more than one NIC.

Thus, a connection between a mobile security system 345 and a mobile device 310 may be implemented while using the principles of NAT and DHCP, so that end-user applications running on the mobile device 310 will "see" protected virtual IP and MAC addresses, while devices connected to the external network see different physical IP and MAC addresses. The present invention provides similar protection and IP hiding that a hardware-based firewall having two network ports (internal and external) provides to a mobile device, but without the need to use a hardware-based firewall and two or more network ports.

Figure 23 is a flowchart of a method 2300 of routing a data communication from an external network (such as the external network 1905) to an application (such as application 1935), in accordance with an embodiment of the present invention. In step 2305, a NIC (such as NIC 1910) receives a data communication from the external network. Data specifying an external IP address and an external MAC address are embedded in the data communication. In step 2310, the data communication is routed to an intermediate driver (such as the intermediate driver 1920),

which in turn routes the data communication to a NAT engine (such as the NAT engine 1945). The NAT engine contains a translations table for IP and MAC addresses.

In step 2315, the NAT engine uses DHCP to translate the external IP and MAC addresses embedded in the data communication into internal IP and MAC addresses. The NAT engine then substitutes the internal IP and MAC addresses for the external IP and MAC addresses in the data communication. In this way, the IP and MAC addresses of internal computers/applications are isolated from the external network.

In step 2320, the intermediate driver routes the data communication to a firewall (such as the firewall 1925). In step 2325, the firewall analyzes the data communication for malicious code. In step 2330, the firewall decides what to do with the data communication. If the data communication was found to contain malicious code, then the method 2300 proceeds to step 2335. In step 2335, the firewall rejects the data communication and prevents it from proceeding to the application. The method 2300 then ends.

If the data communication was not found to contain malicious code, then the method 2300 proceeds to step 2340. In step 2340, the firewall allows the data communication. The intermediate driver receives the data communication back from the firewall and routes the data communication to the application. The method 2300 then ends.

Figure 24 is a flowchart of a method 2400 of routing a data communication from an application (such as application 1935) to an external network (such as the external network 1905), in accordance with an embodiment of the present invention. In step 2405, the application initiates a data communication. The application may embed data specifying an internal IP address and an internal MAC address in the data communication. In other embodiments, the internal IP address and the internal MAC address may be embedded by an operating system (such as the operating system 1930).

In step 2410, the data communication is routed to an intermediate driver (such as the intermediate driver 1920), which in turn routes the data communication to a NAT engine (such

as the NAT engine 1945). The NAT engine contains a translations table for IP and MAC addresses. In step 2415, the NAT engine uses DHCP to translate the internal IP and MAC addresses embedded in the data communication into external IP and MAC addresses. The NAT engine then substitutes the external IP and MAC addresses for the internal IP and MAC addresses in the data communication. In this way, the IP and MAC addresses of internal computers/applications are isolated from the external network.

In step 2420, the internal driver routes the data communication to the external network via a NIC (such as NIC 1910). The method 2400 then ends.

Hybrid Firewall

Figure 20 shows a prior art network system 2000 having separate network and personal firewalls. The network system 2000 includes an external network 2005 (such as the Internet), a network firewall 2010, and personal computers 2015 (denoted as 2015a, 2015b, etc.). The network firewall 2010 may reside on an external device or computer. The network firewall 2010 comprises a first NIC 2020, a NAT gateway 2025 and a second NIC 2030. Each personal computer 2015 comprises a personal firewall 2035 (denoted as 2035a, 2035b, etc.) and an application 2040 (denoted as 2040a, 2040b, etc.).

In operation, the network firewall 2010 uses the NAT gateway 2025 to translate the IP address of the personal computer 2015a (denoted as IP address x) and the IP address of the personal computer 2015b (denoted as IP address y) into a public IP address z, and thus hide the IP addresses of the personal computers 2105. The network firewall 2010 performs a similar translation on the MAC addresses of the personal computers 2015. The network firewall 2010 also performs security measures such as antivirus, anti-spyware, anti-adware, etc. Because the network firewall 2010 is earlier in the network than the personal firewall 2035, it can stop malicious code before it enters the system 2000. However, because the network firewall 2010 is application insensitive and at a lower layer of the information stack, its processes for malicious code detection are limited.

The personal firewall 2035 also performs security measures such as antivirus, anti-spyware, anti-adware, etc. Because the personal firewall 2035 is application sensitive and at a higher layer of the information stack, its processes for malicious code detection can be more thorough and focused.

Figure 21 shows a network system 2100 comprising a hybrid firewall 2110 in accordance with an embodiment of the present invention. The network system 2100 includes an external network 2105 (such as the Internet), a hybrid network/personal firewall 2110, and personal computers 2115 (denoted as 2115a, 2115b, etc.).

The hybrid firewall 2110 may reside on an external device or computer. In other embodiments, the hybrid firewall 2110 may reside on the mobile security system 345, shown in Figures 10A-10C. The hybrid firewall 2110 comprises a first NIC 2120, a NAT engine 2125 and a second NIC 2130.

Each personal computer 2115 comprises an agent 2135 (denoted as 2135a, 2135b, etc.) and one or more applications 2140 (denoted as 2140a, 2140b, etc.). As shown in Figure 21, the network system 2100 comprises only two personal computers 2115, but in other embodiments the network system 2100 may comprise more than two personal computers.

In operation, the hybrid firewall 2110 uses the NAT engine 2125, which contains a translations table for IP and MAC addresses, to translate the IP address of the personal computer 2115a (denoted as IP address x) and the IP address of the personal computer 2115b (denoted as IP address y) into a public IP address z, and thus hide the IP addresses of the personal computers. The network firewall 2110 performs a similar translation on the MAC addresses of the personal computers 2115.

The hybrid firewall 210 is capable of performing both the network firewall and personal firewall security measures. Because the hybrid firewall 2010 is at the same level as the traditional network firewall 2035, it can stop malicious code before it enters the system 2100.

Further, because the hybrid firewall 2110 is application sensitive, the hybrid firewall 2110 can perform the processes of the traditional personal firewall 2035.

To enable the hybrid firewall 2110 to be application sensitive, the agents 2135 send packets of data to the hybrid firewall 2110, each packet comprising data identifying the application 2140 associated with the packet. Because each packet comprises data identifying the application 2140 that is associated with the packet, the hybrid firewall 2110 can act as a personal firewall 2035 to handle application-level security. Then, the hybrid firewall 2110 can transmit a subset of the data packets, by extracting at least the application-identifying data, to the external network 2105.

Figure 22 shows a network system 2200 comprising a hybrid firewall 2210 and configured according to the embodiment of the present invention shown in Figure 10A. The network system 2200 includes an external network 2205 (such as the Internet), a hybrid network/personal firewall 2210, and a mobile device 2215.

The hybrid firewall 2210 may reside on an external device in a pocket-size, handheld-size, keychain-size, or possibly smaller housing. The hybrid firewall 2210 comprises an ED plug 2245 (such as a USB plug) for communicating with an ED port 2230 (such as a USB port) contained within the mobile device 2215. The hybrid firewall 2210 also comprises a NAT engine 2225. In other embodiments, the hybrid firewall 2210 may be installed in the mobile device 2215, or connected to the mobile device 2215 by a wireless or another network wire connection.

The mobile device 2215 comprises a NIC 220, the ED port 2230, an agent 2235, one or more applications 2240, and an intermediate driver 2250 (such as MINIPort in the Microsoft Windows operating system). As shown in Figure 22, the network system 2200 comprises only one mobile device 2215 and hybrid firewall 2210, but in other embodiments the network system 2200 may comprise more than one mobile device and hybrid firewall.

In operation, the intermediate driver 2250 directs traffic arriving from the NIC 2220 to the hybrid firewall 2210 via the ED port 2230 and ED plug 2245. The hybrid firewall 2210 decides what to do with the traffic (allow, deny, or reject) and permits only the allowed traffic to proceed to an application 2240.

The hybrid firewall 2210 uses the NAT engine 2225, which contains a translations table for IP and MAC addresses, to translate the IP address of the mobile device 2215 into a public IP address, and thus hide the IP address of the mobile device 2215. The hybrid firewall 2210 performs a similar translation on the MAC address of the mobile device 2215.

The application 2240 can send packets of data via the ED port 2230 and ED plug 2235 to the hybrid firewall 2210 for transmission to the external network 2205. The agent 2235 associates data identifying the application 2240 with the packets of data that are sent to the hybrid firewall 2210. Each packet thus comprises data identifying the application 2240 associated with the packet. Because each packet comprises data identifying the application 2240 associated with the packet, the hybrid firewall 2210 can act as a personal firewall to handle application security.

Figure 25 is a flowchart of a method 2500 of routing a data communication from an external network (such as the external network 2105 or 2205) to an application (such as application 2140 or 2240), in accordance with an embodiment of the present invention. In step 2505, a NIC (such as NIC 2120 or 2220) receives a data communication from the external network. Data specifying an external IP address and an external MAC address are embedded in the data communication. In step 2510, the data communication is routed to a hybrid network/personal firewall (such as the firewall 2110 or 2210) that comprises a NAT engine (such as the NAT engine 2125 or 2225) containing a translations table for IP and MAC addresses. The hybrid firewall is at the same level as a traditional network firewall and is application sensitive.

In step 2515, the NAT engine uses DHCP to translate the external IP and MAC addresses embedded in the data communication into internal IP and MAC addresses. The NAT engine then substitutes the internal IP and MAC addresses for the external IP and MAC addresses in the

data communication. In this way, the IP and MAC addresses of internal computers/applications are isolated from the external network.

In step 2520, the hybrid firewall associates the data communication with an application. The hybrid firewall makes this association based upon data packets previously received by the firewall that comprised application-identifying information.

In step 2525, the hybrid firewall analyzes the data communication for malicious code. Because the hybrid firewall is at the same level as a traditional network firewall, it can stop malicious code before it reaches a computer (such as computer 2115 or 2215). Further, because the hybrid firewall is application sensitive, the hybrid firewall can perform the function of a traditional personal firewall to handle application-level security.

In step 2530, the firewall decides what to do with the data communication. If the data communication was found to contain malicious code, then the method 2500 proceeds to step 2535. In step 2535, the firewall rejects the data communication and prevents it from proceeding to the application. The method 2500 then ends.

If the data communication was not found to contain malicious code, then the method 2500 proceeds to step 2540. In step 2540, the firewall allows the data communication, and the data communication is routed to the application. The method 2500 then ends.

Figure 26 is a flowchart of a method 2600 of routing a data communication from an application (such as application 2140 or 2240) to an external network (such as the external network 2105 or 2205), in accordance with an embodiment of the present invention. In step 2605, the application initiates a data communication. The application may embed data specifying an internal IP address and an internal MAC address in the data communication. In other embodiments, the internal IP address and the internal MAC address may be embedded by an operating system or by an agent (such as the agent 2135 or 2235) running on a computer.

In step 2610, data identifying the application is embedded in the data communication. This step may be performed by the application, by an operating system, or by an agent (such as the agent 2135 or 2235) running on a computer. In one embodiment, an agent running on the same computer as the application creates packets of data, each packet comprising data identifying the application associated with the packet. Because each packet comprises data identifying the application that is associated with the packet, a downstream hybrid firewall (such as the firewall 2110 or 2210) can act as a personal firewall to handle application-level security.

In step 2615, the data communication is routed to a hybrid network/personal firewall (such as the firewall 2110 or 2210) that comprises a NAT engine (such as the NAT engine 2125 or 2225) containing a translations table for IP and MAC addresses. The hybrid firewall is at the same level as a traditional network firewall and is application sensitive.

In step 2620, the hybrid firewall extracts and removes the application-identifying information from the data communication. In step 2625, the NAT engine uses DHCP to translate the internal IP and MAC addresses embedded in the data communication into external IP and MAC addresses. The NAT engine then substitutes the external IP and MAC addresses for the internal IP and MAC addresses in the data communication. In this way, the IP and MAC addresses of internal computers/applications are isolated from the external network.

In step 2630, the data communication (minus data identifying the application, internal IP address, and internal MAC address) is routed to the external network via a NIC (such as NIC 2120 or 2220). The method 2600 then ends.

The foregoing description of the preferred embodiments of the present invention is by way of example only, and other variations and modifications of the above-described embodiments and methods are possible in light of the foregoing teaching. Although the network sites are being described as separate and distinct sites, one skilled in the art will recognize that these sites may be a part of an integral site, may each include portions of multiple sites, or may include combinations of single and multiple sites. The various embodiments set forth herein may be implemented utilizing hardware, software, or any desired combination thereof. For that

matter, any type of logic may be utilized which is capable of implementing the various functionality set forth herein. Components may be implemented using a programmed general purpose digital computer, using application specific integrated circuits, or using a network of interconnected conventional components and circuits. Connections may be wired, wireless, modem, etc. The embodiments described herein are not intended to be exhaustive or limiting. The present invention is limited only by the following claims.

CLAIMS

1. A computer comprising:

an application associated with an application address;

a network interface coupled to receive incoming data packets from and transmit outgoing data packets to an external network;

a network address translation engine configured to translate between the application address and a public address; and

a driver for automatically forwarding the outgoing data packets to the network address translation engine to translate the application address to the public address, and for automatically forwarding the incoming data packets to the network address translation engine to translate the public address to the application address.

2. The computer of claim 1, wherein the network address translation engine is part of the driver.

3. The computer of claim 1, wherein the network address translation engine is part of a firewall.

4. The computer of claim 3, wherein the firewall is located on a mobile security system.

5. The computer of claim 1, wherein the network address translation engine is configured to use Dynamic Host Configuration Protocol.

6. The computer of claim 1, wherein the computer is configured to send data packets identifying the application to a firewall, and the firewall is configured to handle both network-level security and application-level security.

7. A system comprising:

a network interface;

a firewall in communication with the network interface configured to handle both network-level security and application-level security; and

a computer in communication with the firewall, having one or more applications, and being configured to send data packets identifying the one or more applications to the firewall.

8. The system of claim 7, wherein:

each data packet is associated with one of the one or more applications; and

each data packet comprises data identifying the application associated with the data packet.

9. The system of claim 8, wherein the firewall is configured to use the data identifying the application associated with the data packet to handle application-level security, to create a data packet subset by removing the data identifying the application from the data packet, and to send the data packet subset to an external network.

10. The system of claim 7, wherein the network interface is configured to receive incoming data from an external network, and to route the incoming data to the firewall.

11. The system of claim 7, wherein:

each application is associated with at least one address; and

the firewall is configured to dynamically isolate the address from an external network.

12. The system of claim 11, wherein the firewall is configured to dynamically isolate the address from the external network through the use of Dynamic Host Configuration Protocol.

13. A method within a personal computer of processing incoming data associated with a public address, the method comprising:

receiving the data from an external network;

translating the public address into an internal address associated with an application;

analyzing the data for malicious code; and

routing the data to the application if the data does not comprise malicious code.

14. The method of claim 13, wherein the analyzing step comprises analyzing the data for malicious code at both the network level and the application level.

15. The method of claim 13, wherein the translating step uses Dynamic Host Configuration Protocol.

16. A method within a computer of processing outgoing data, the method comprising:

receiving outgoing data from an application, the application being associated with an internal address;

translating the internal address into a public address; and

routing at least a subset of the outgoing data to an external network using the public address, thereby dynamically isolating the internal address from the external network.

17. The method of claim 16, wherein the translating step uses Dynamic Host Configuration Protocol.

18. The method of claim 16, further comprising:

configuring the outgoing data into one or more data packets;

associating each of the one or more data packets with the application; and

embedding application-identifying data in each of the one or more data packets.

19. The method of claim 18,

further comprising creating one or more data packet subsets by removing the application-identifying data from each of the one or more data packets,

wherein the routing step comprises routing the one or more data packet subsets to the external network.

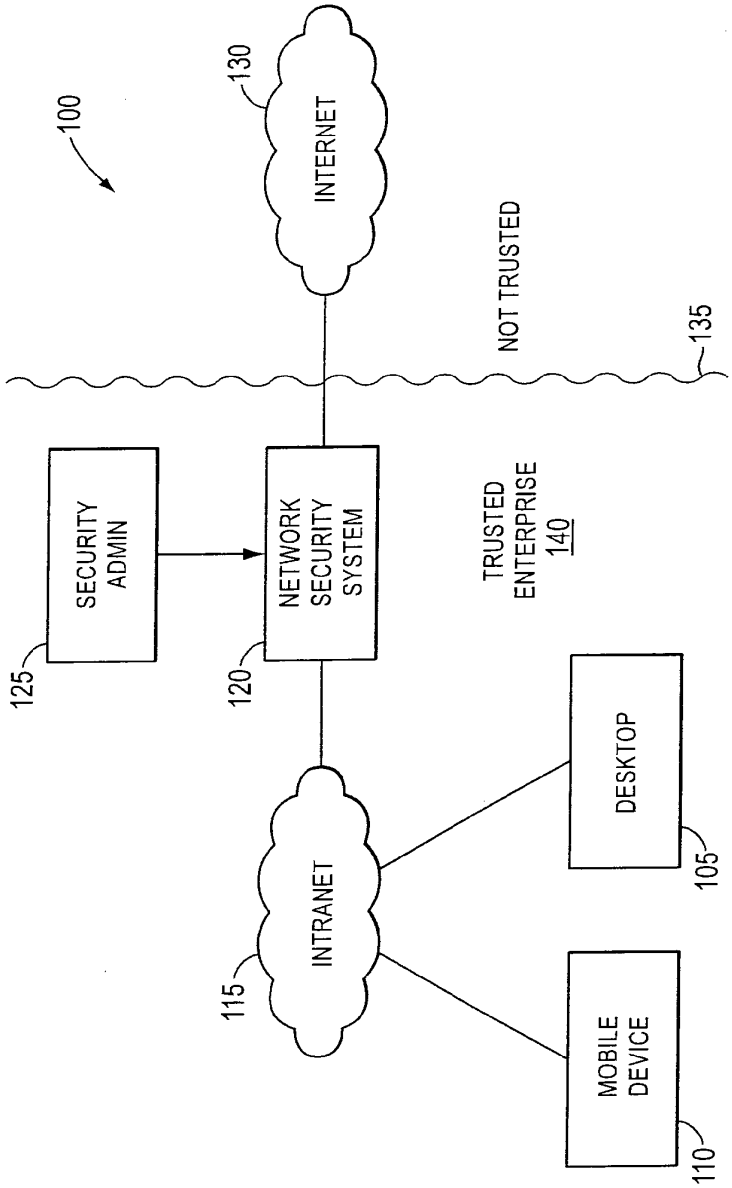


FIG. 1
(PRIOR ART)

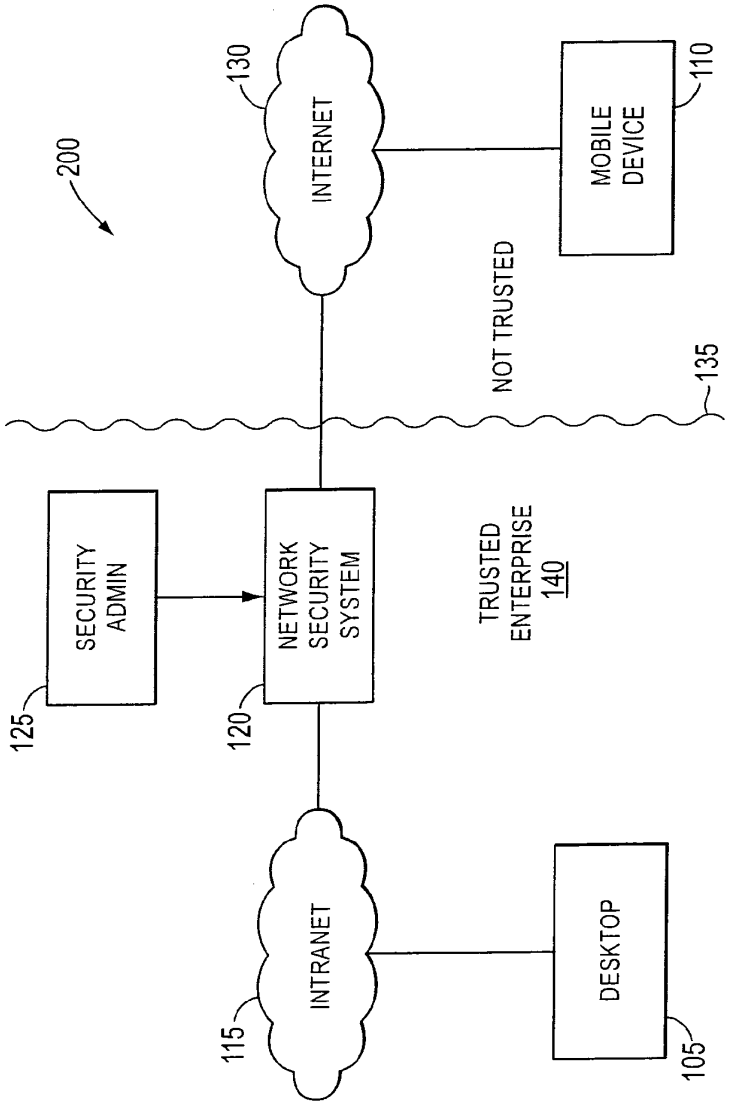


FIG. 2
(PRIOR ART)

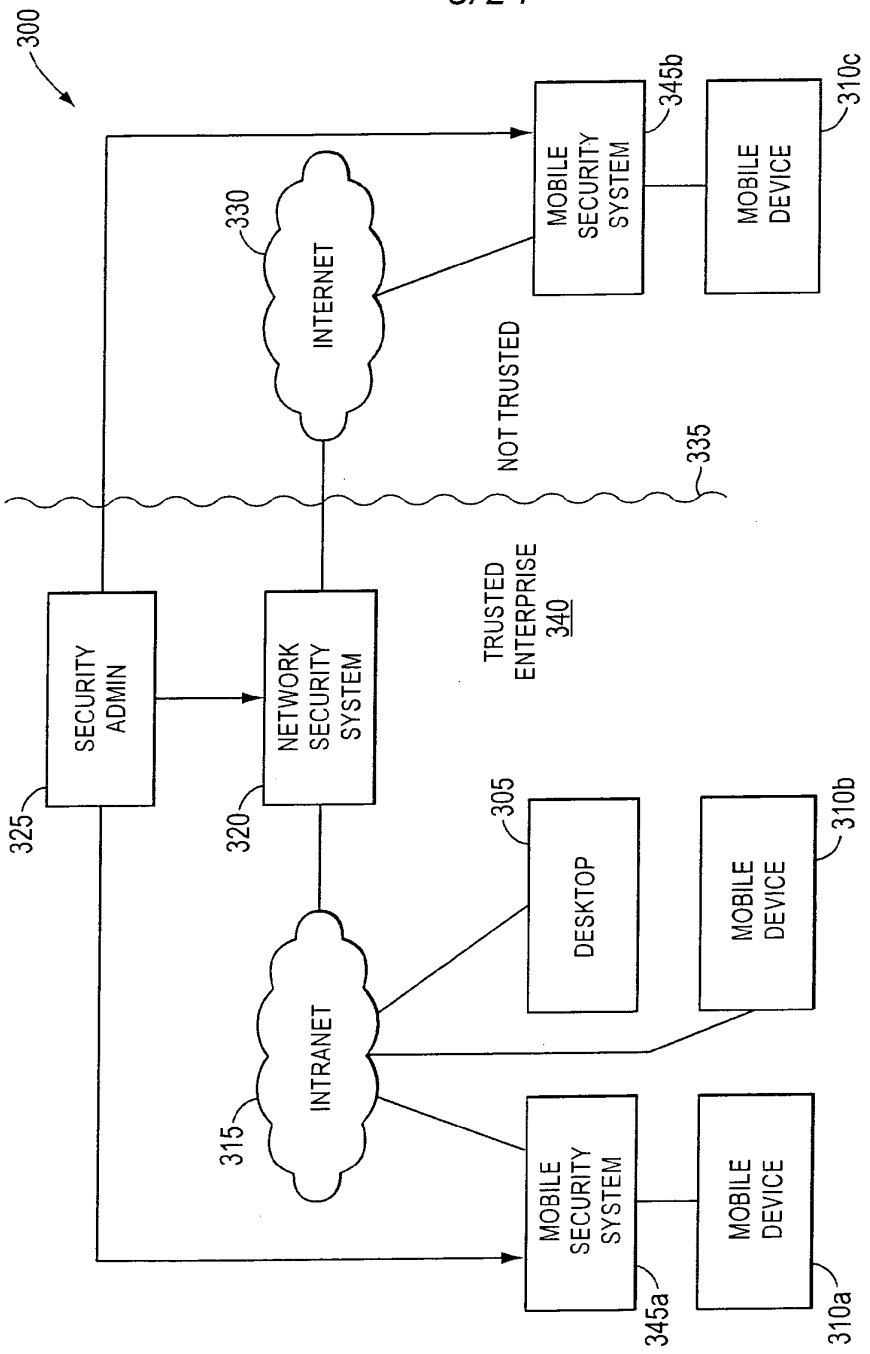

300
MOBILE SECURITY SYSTEM
345b
MOBILE DEVICE
310c
330
INTERNET
NOT TRUSTED
335
TRUSTED ENTERPRISE 340
SECURITY ADMIN
325
NETWORK SECURITY SYSTEM
320
305
DESKTOP
MOBILE DEVICE
310b
INTRANET
315
MOBILE SECURITY SYSTEM
345a
MOBILE DEVICE
310a

FIG. 3

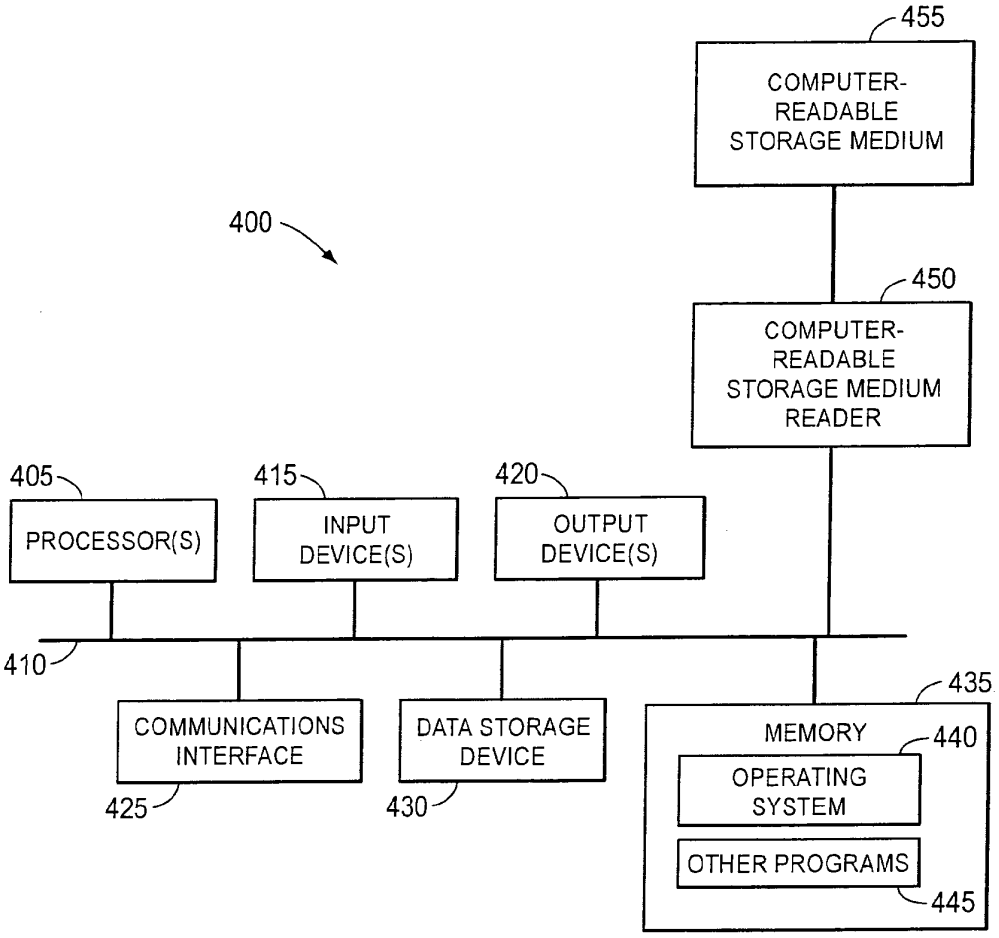

455
COMPUTER-READABLE STORAGE MEDIUM
400
450
COMPUTER-READABLE STORAGE MEDIUM READER
405
PROCESSOR(S)
415
INPUT DEVICE(S)
420
OUTPUT DEVICE(S)
410
435
COMMUNICATIONS INTERFACE
425
DATA STORAGE DEVICE
430
MEMORY
440
OPERATING SYSTEM
OTHER PROGRAMS
445

FIG. 4

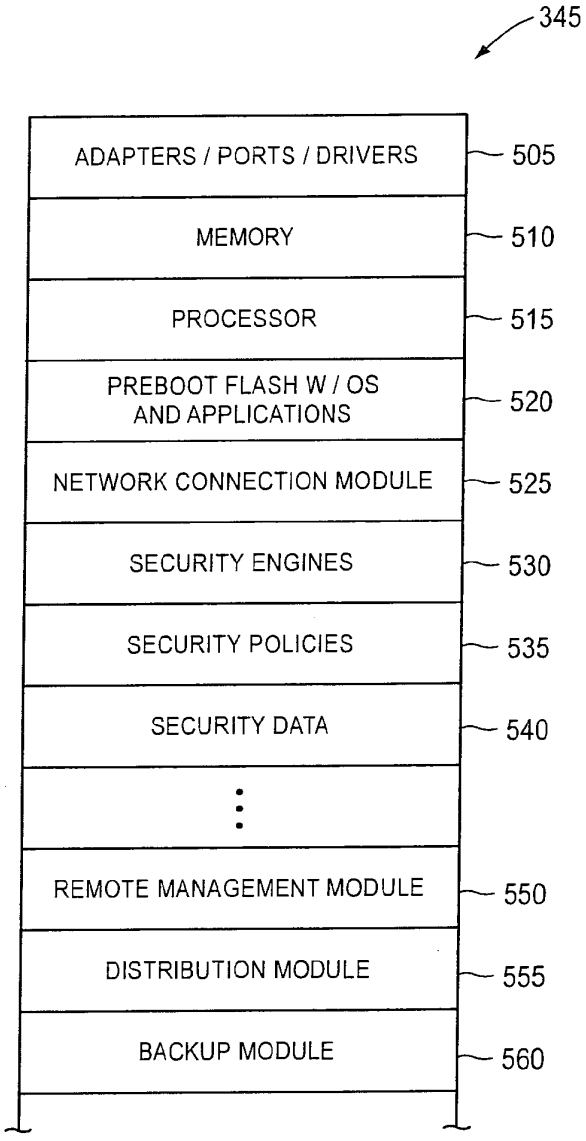

345
ADAPTERS / PORTS / DRIVERS
505
MEMORY
510
PROCESSOR
515
PREBOOT FLASH W / OS AND APPLICATIONS
520
NETWORK CONNECTION MODULE
525
SECURITY ENGINES
530
SECURITY POLICIES
535
SECURITY DATA
540
REMOTE MANAGEMENT MODULE
550
DISTRIBUTION MODULE
555
BACKUP MODULE
560

FIG. 5

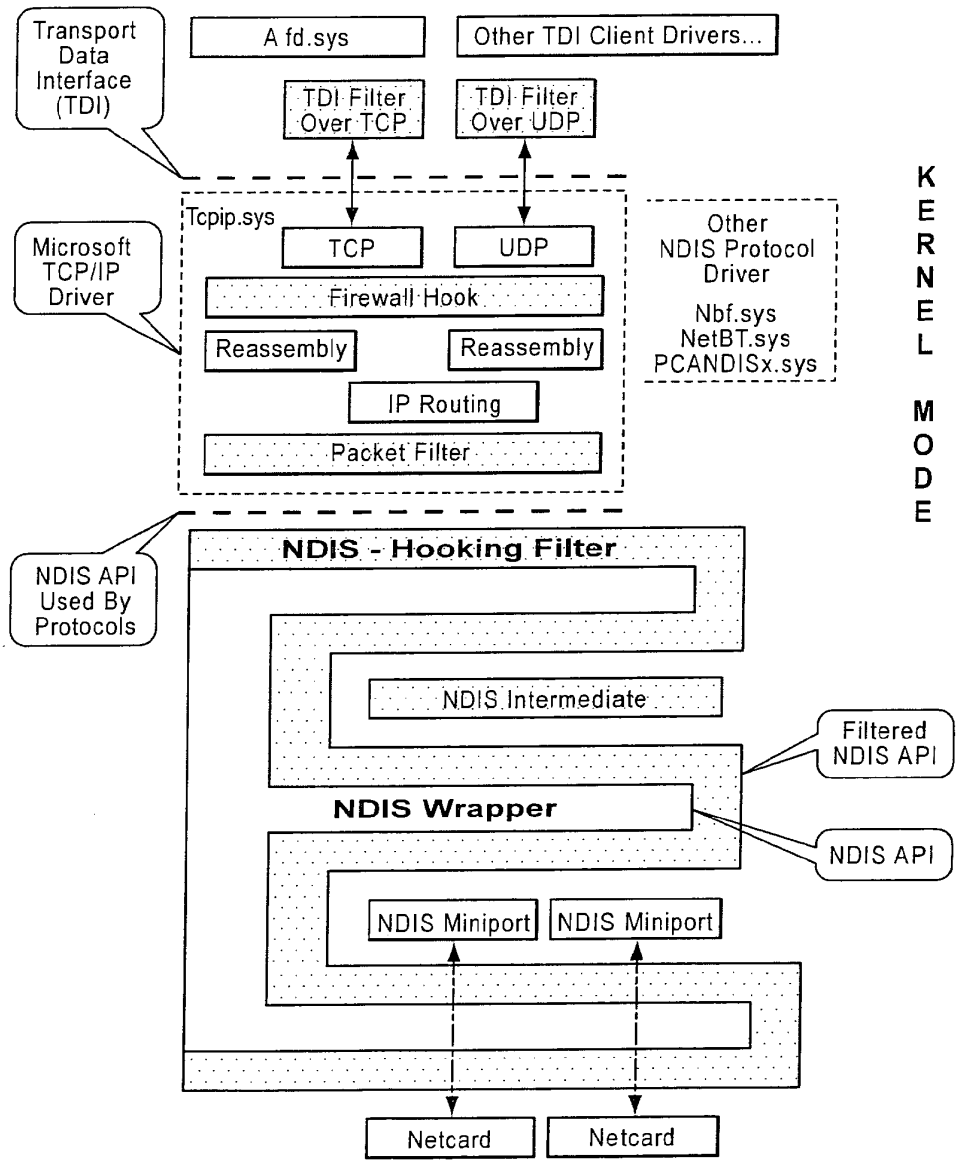

Transport Data Interface (TDI)
A fd.sys
Other TDI Client Drivers...
TDI Filter Over TCP
TDI Filter Over UDP
Tcpip.sys
TCP
UDP
Firewall Hook
Reassembly
Reassembly
IP Routing
Packet Filter
Microsoft TCP/IP Driver
Other NDIS Protocol Driver
Nbf.sys
NetBT.sys
PCANDISx.sys
KERNEL MODE
NDIS API Used By Protocols
NDIS - Hooking Filter
NDIS Intermediate
Filtered NDIS API
NDIS Wrapper
NDIS API
NDIS Miniport
NDIS Miniport
Netcard
Netcard

FIG. 6

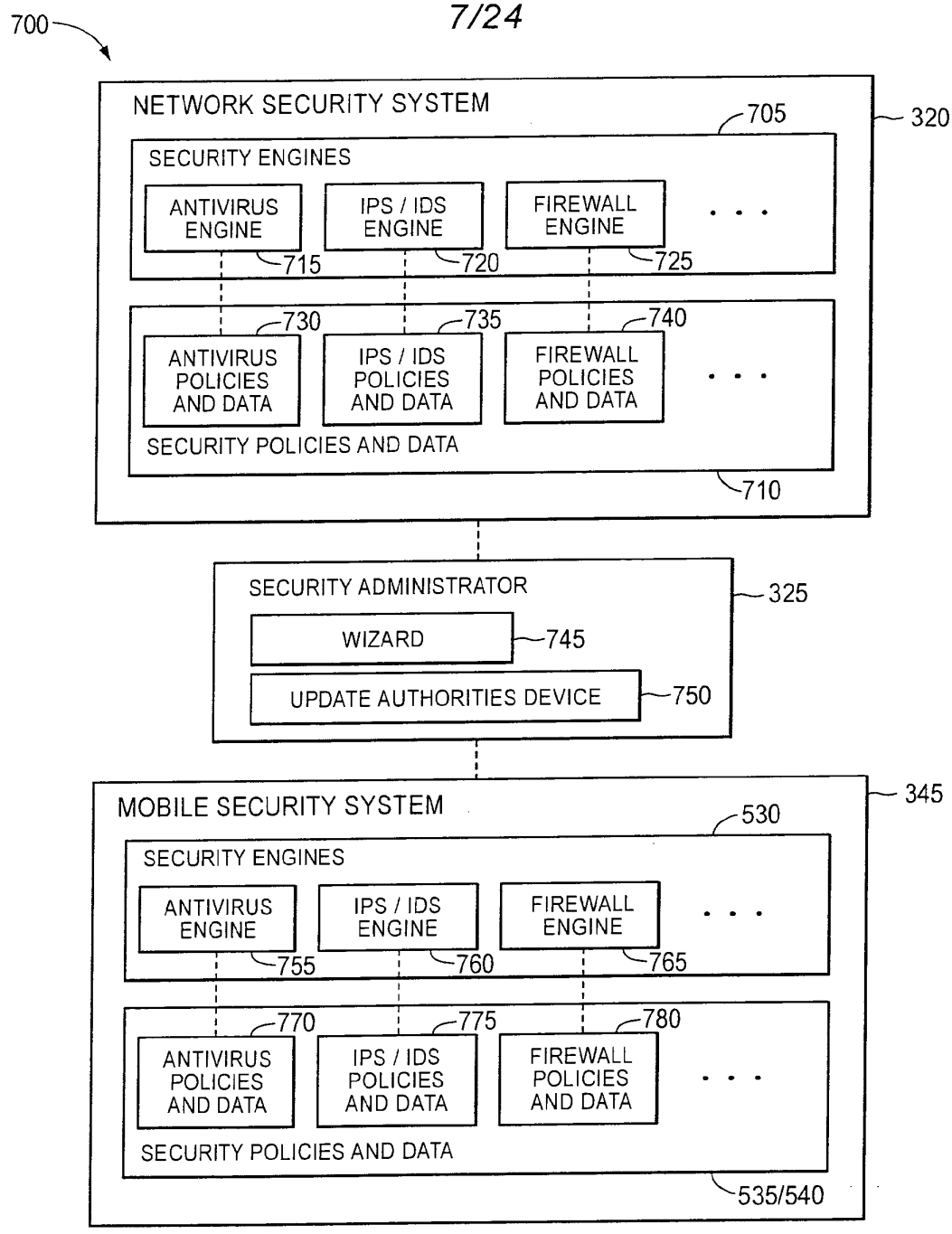

700
NETWORK SECURITY SYSTEM
705
320
SECURITY ENGINES
ANTIVIRUS ENGINE
IPS / IDS ENGINE
FIREWALL ENGINE
715
720
725
730
735
740
ANTIVIRUS POLICIES AND DATA
IPS / IDS POLICIES AND DATA
FIREWALL POLICIES AND DATA
SECURITY POLICIES AND DATA
710
SECURITY ADMINISTRATOR
325
WIZARD
745
UPDATE AUTHORITIES DEVICE
750
MOBILE SECURITY SYSTEM
345
530
SECURITY ENGINES
ANTIVIRUS ENGINE
IPS / IDS ENGINE
FIREWALL ENGINE
755
760
765
770
775
780
ANTIVIRUS POLICIES AND DATA
IPS / IDS POLICIES AND DATA
FIREWALL POLICIES AND DATA
SECURITY POLICIES AND DATA
535/540

FIG. 7

8/24

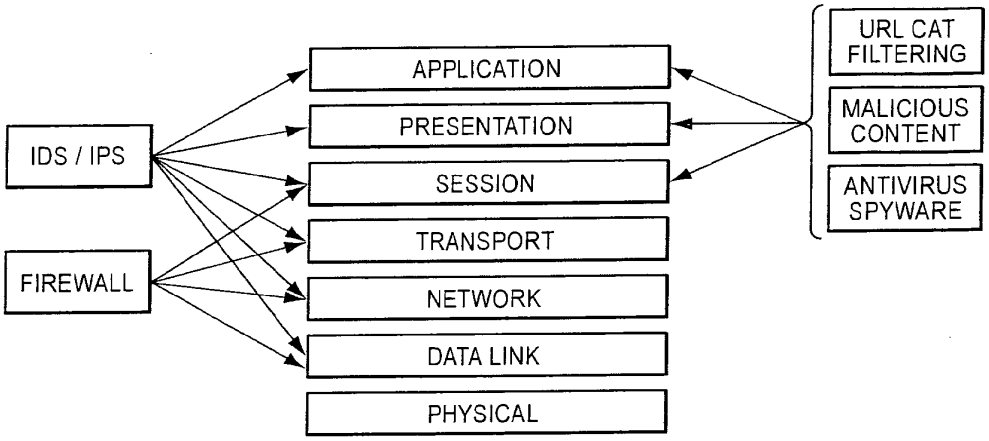


FIG. 8

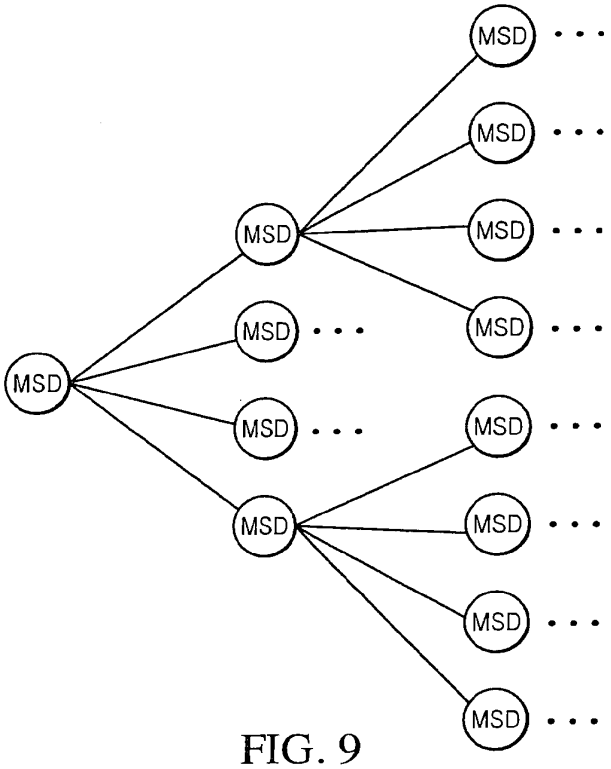


FIG. 9

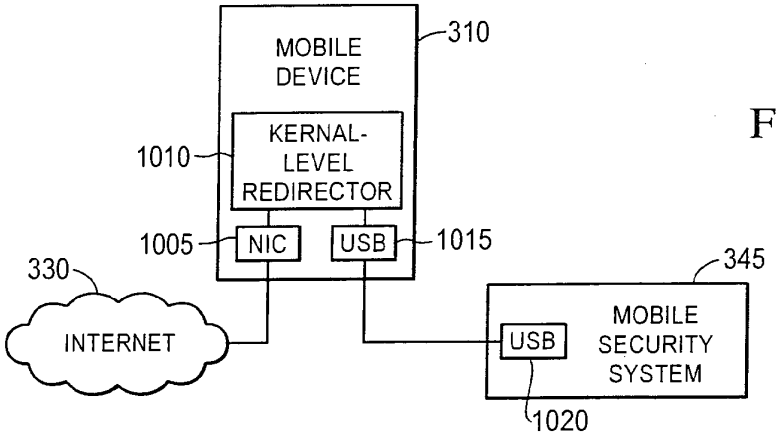


FIG. 10A

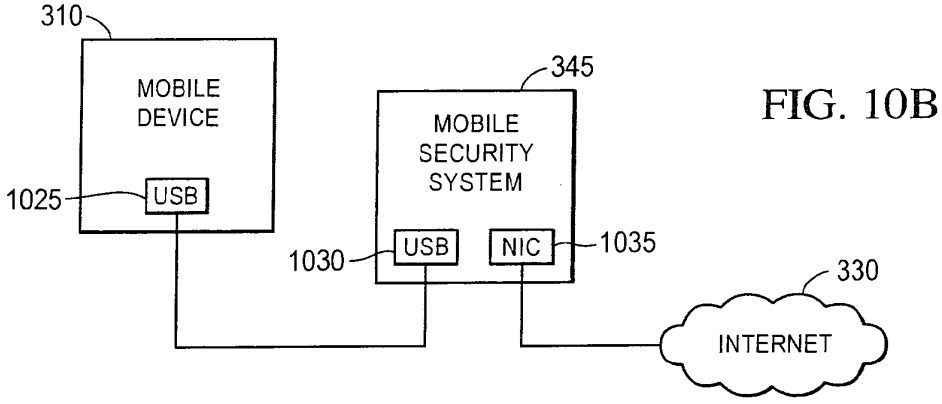


FIG. 10B

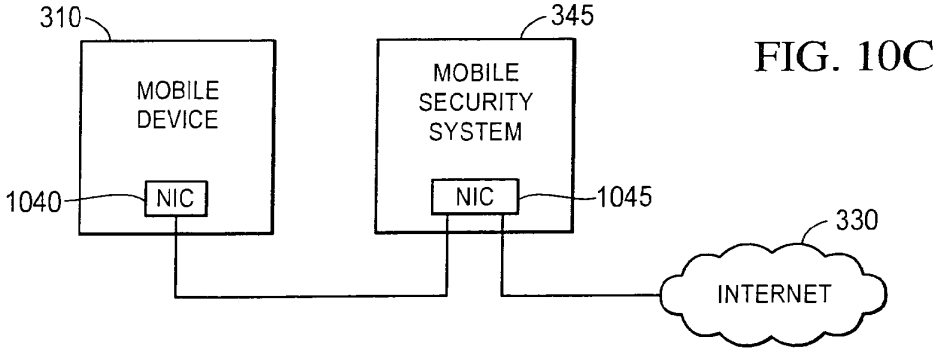


FIG. 10C

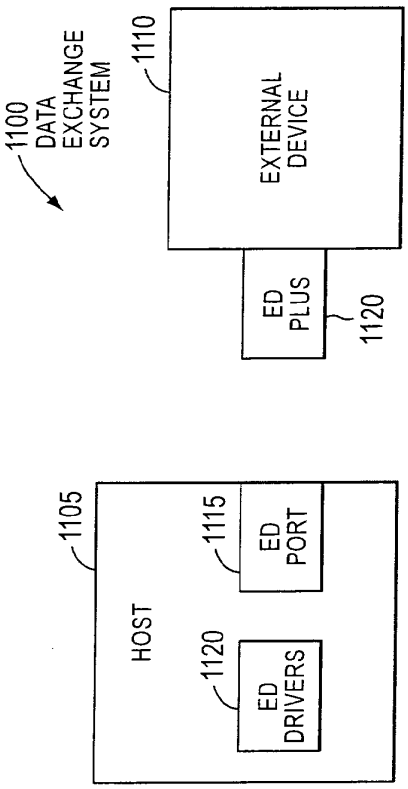


FIG. 11
(PRIOR ART)

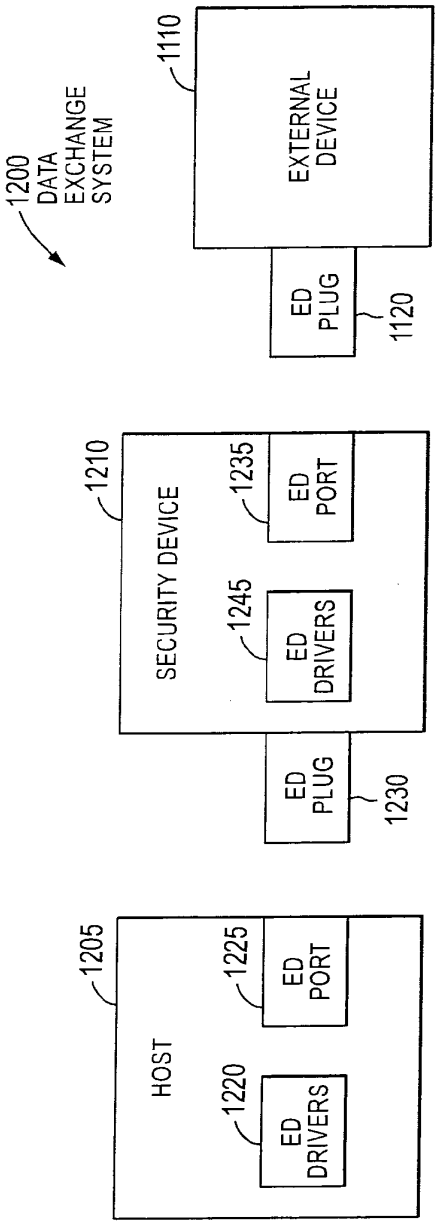


FIG. 12

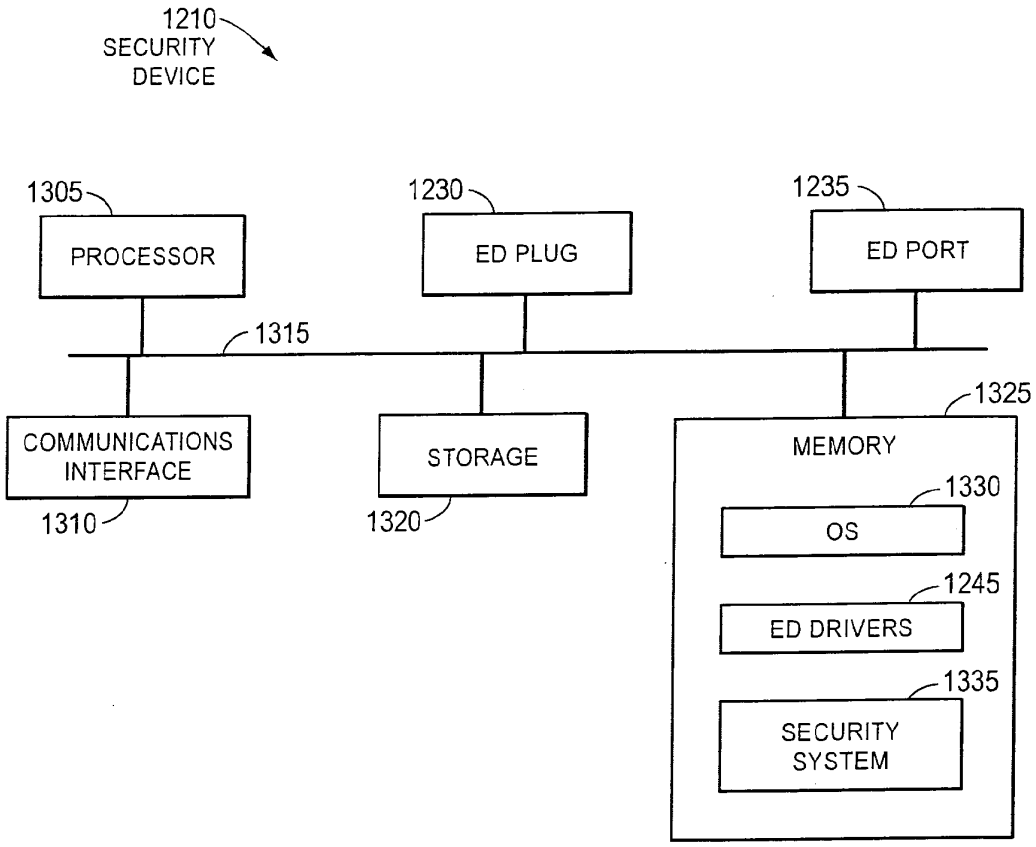

1210
SECURITY DEVICE
1305
PROCESSOR
1230
ED PLUG
1235
ED PORT
1315
COMMUNICATIONS INTERFACE
1310
STORAGE
1320
1325
MEMORY
1330
OS
1245
ED DRIVERS
1335
SECURITY SYSTEM

FIG. 13

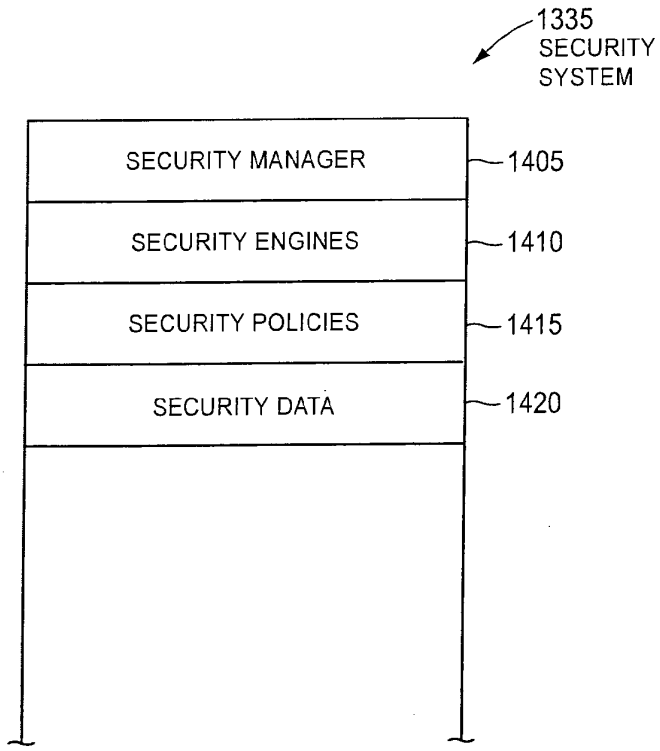

1335
SECURITY
SYSTEM
SECURITY MANAGER
1405
SECURITY ENGINES
1410
SECURITY POLICIES
1415
SECURITY DATA
1420

FIG. 14

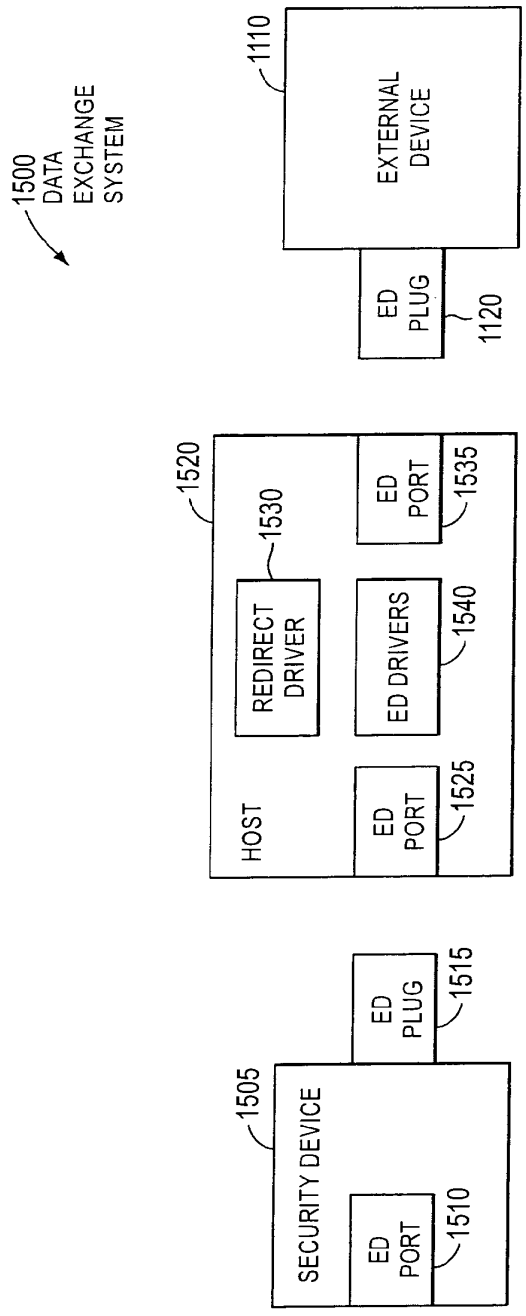

1500
DATA
EXCHANGE
SYSTEM
1110
EXTERNAL
DEVICE
ED
PLUG
1120
1520
HOST
REDIRECT
DRIVER
1530
ED DRIVERS
1540
ED
PORT
1535
ED
PORT
1525
1505
SECURITY DEVICE
ED
PLUG
1515
ED
PORT
1510

FIG. 15

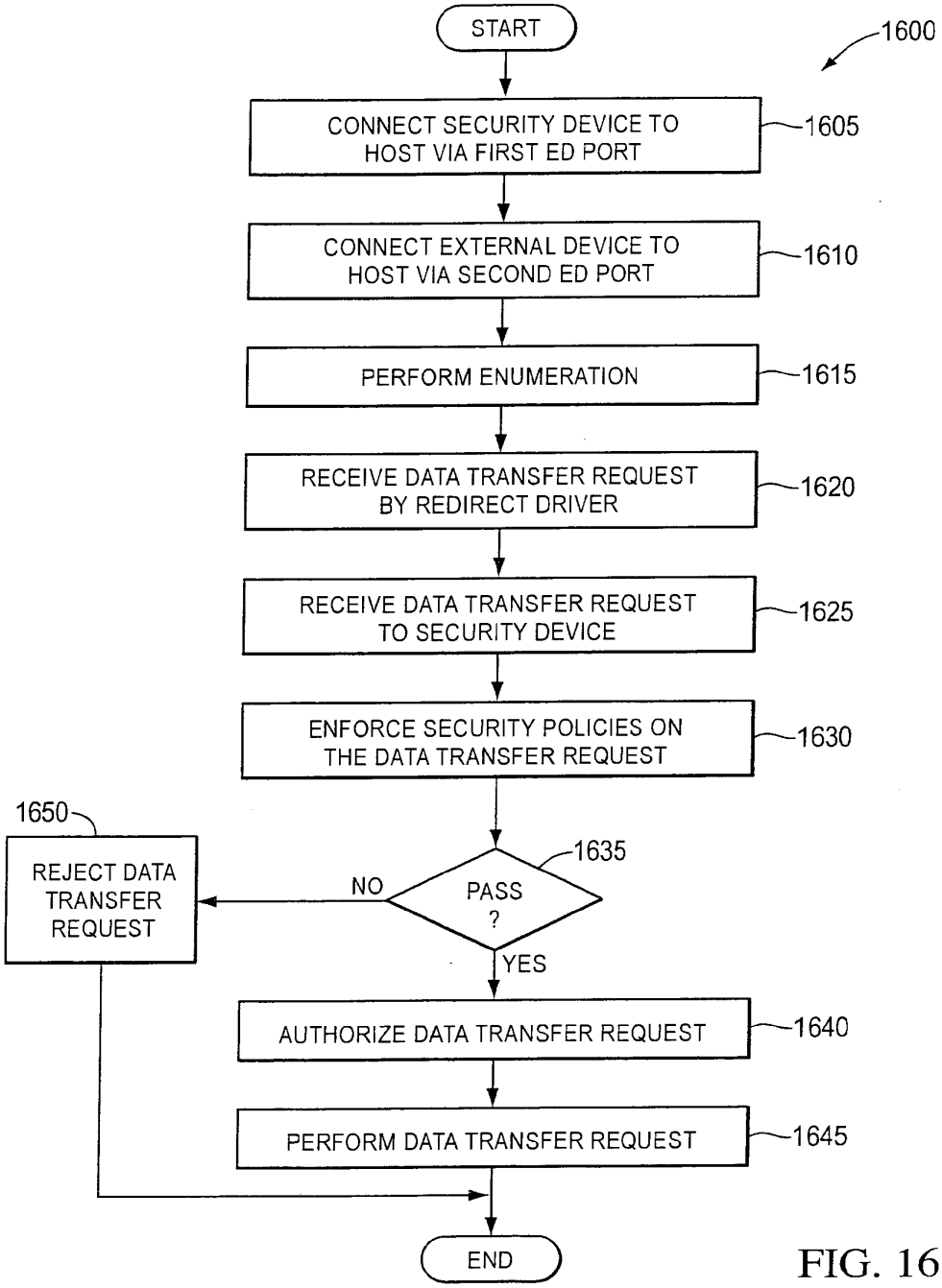

START
1600
CONNECT SECURITY DEVICE TO HOST VIA FIRST ED PORT
1605
CONNECT EXTERNAL DEVICE TO HOST VIA SECOND ED PORT
1610
PERFORM ENUMERATION
1615
RECEIVE DATA TRANSFER REQUEST BY REDIRECT DRIVER
1620
RECEIVE DATA TRANSFER REQUEST TO SECURITY DEVICE
1625
ENFORCE SECURITY POLICIES ON THE DATA TRANSFER REQUEST
1630
1650
REJECT DATA TRANSFER REQUEST
NO
1635
PASS ?
YES
AUTHORIZE DATA TRANSFER REQUEST
1640
PERFORM DATA TRANSFER REQUEST
1645
END

FIG. 16

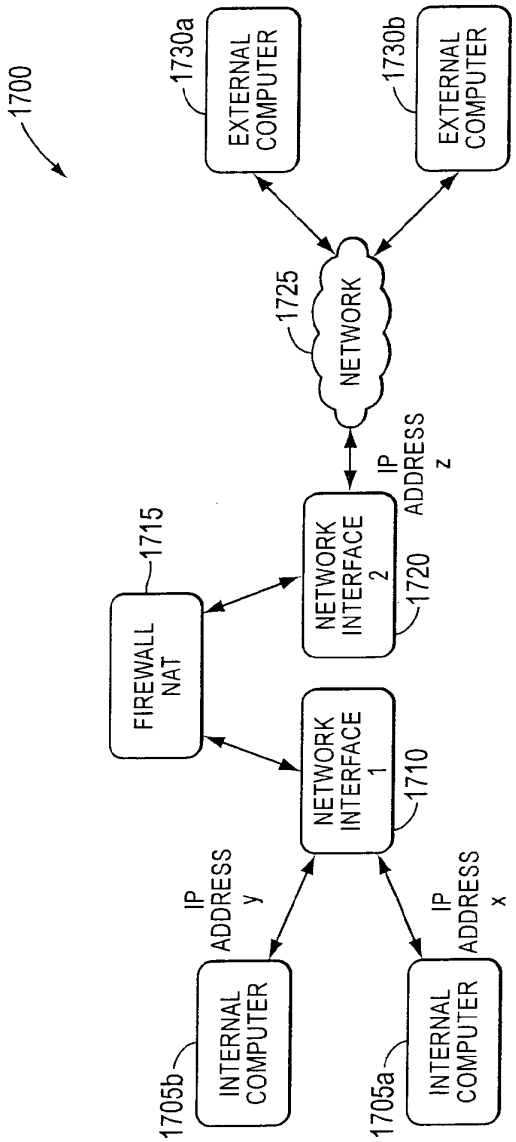


FIG. 17
(PRIOR ART)

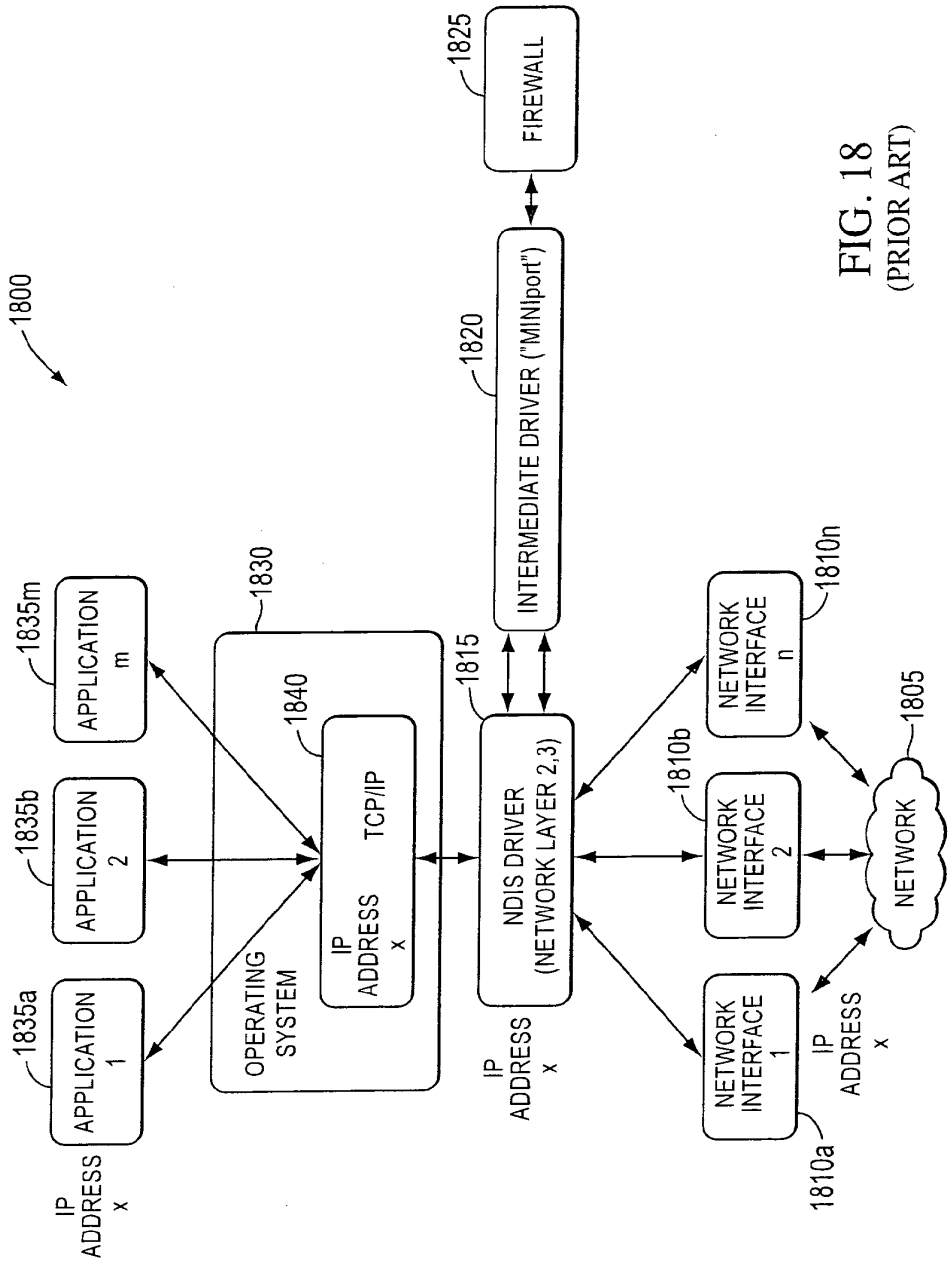


FIG. 18
(PRIOR ART)

17/24

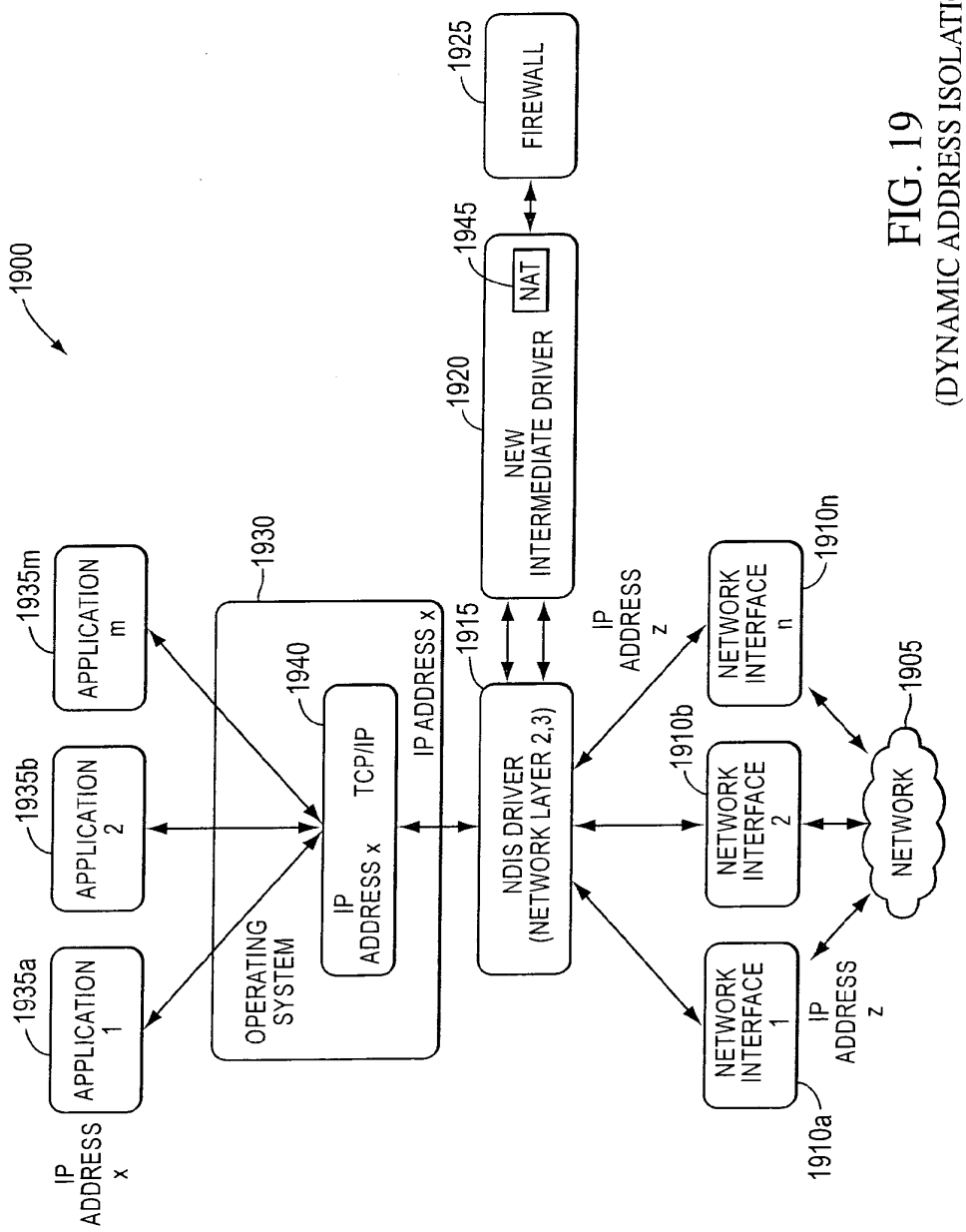


FIG. 19
(DYNAMIC ADDRESS ISOLATION)

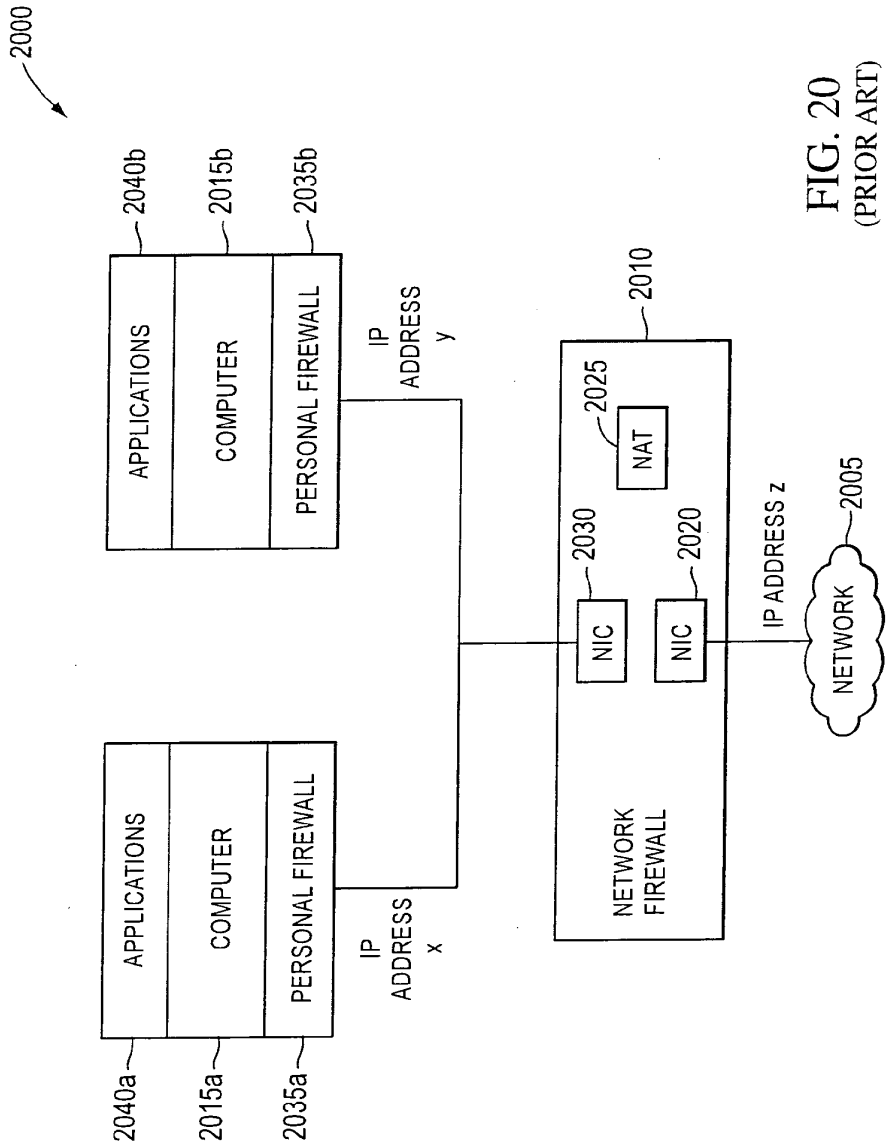


FIG. 20
(PRIOR ART)

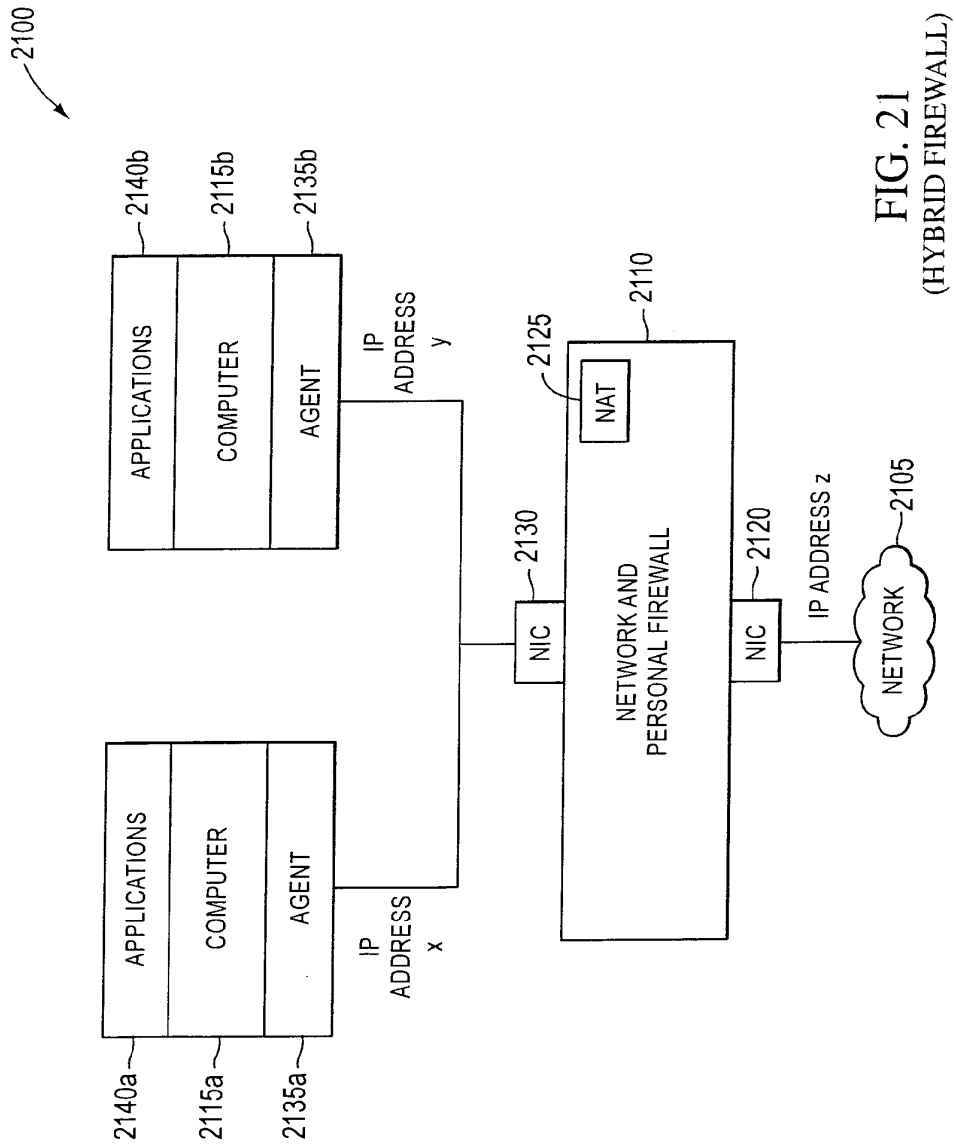


FIG. 21
(HYBRID FIREWALL)

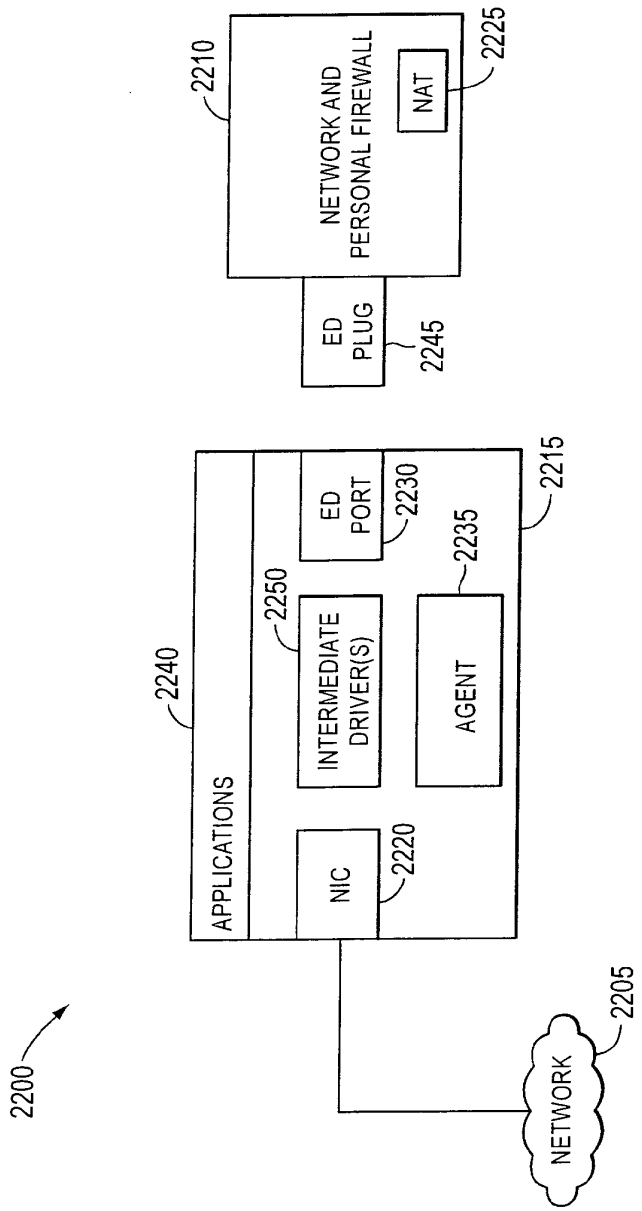


FIG. 22
(HYBRID FIREWALL EXAMPLE)

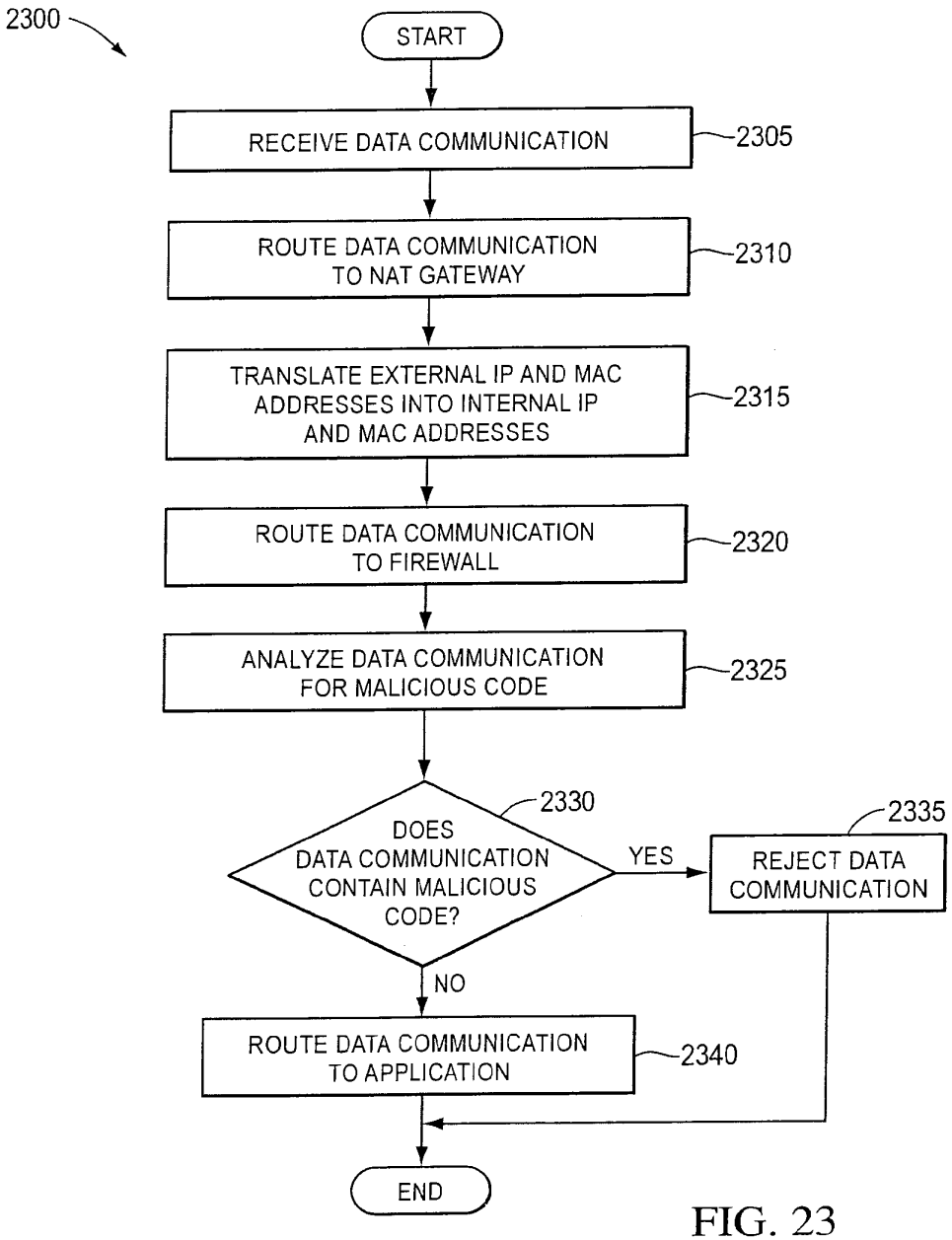

2300
START
RECEIVE DATA COMMUNICATION
2305
ROUTE DATA COMMUNICATION TO NAT GATEWAY
2310
TRANSLATE EXTERNAL IP AND MAC ADDRESSES INTO INTERNAL IP AND MAC ADDRESSES
2315
ROUTE DATA COMMUNICATION TO FIREWALL
2320
ANALYZE DATA COMMUNICATION FOR MALICIOUS CODE
2325
DOES DATA COMMUNICATION CONTAIN MALICIOUS CODE?
2330
YES
REJECT DATA COMMUNICATION
2335
NO
ROUTE DATA COMMUNICATION TO APPLICATION
2340
END

FIG. 23

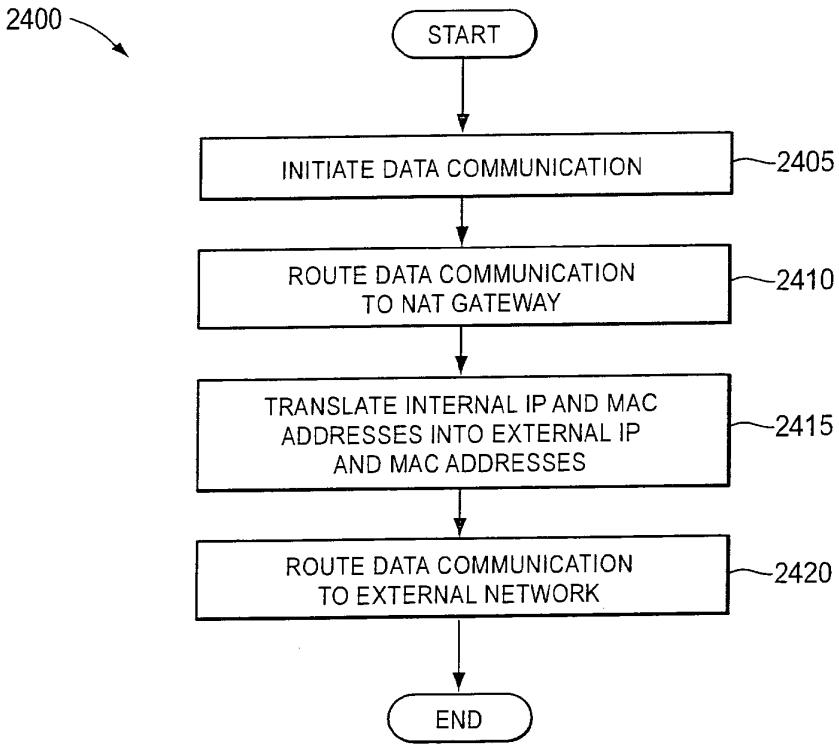

2400
START
INITIATE DATA COMMUNICATION
2405
ROUTE DATA COMMUNICATION TO NAT GATEWAY
2410
TRANSLATE INTERNAL IP AND MAC ADDRESSES INTO EXTERNAL IP AND MAC ADDRESSES
2415
ROUTE DATA COMMUNICATION TO EXTERNAL NETWORK
2420
END

FIG. 24

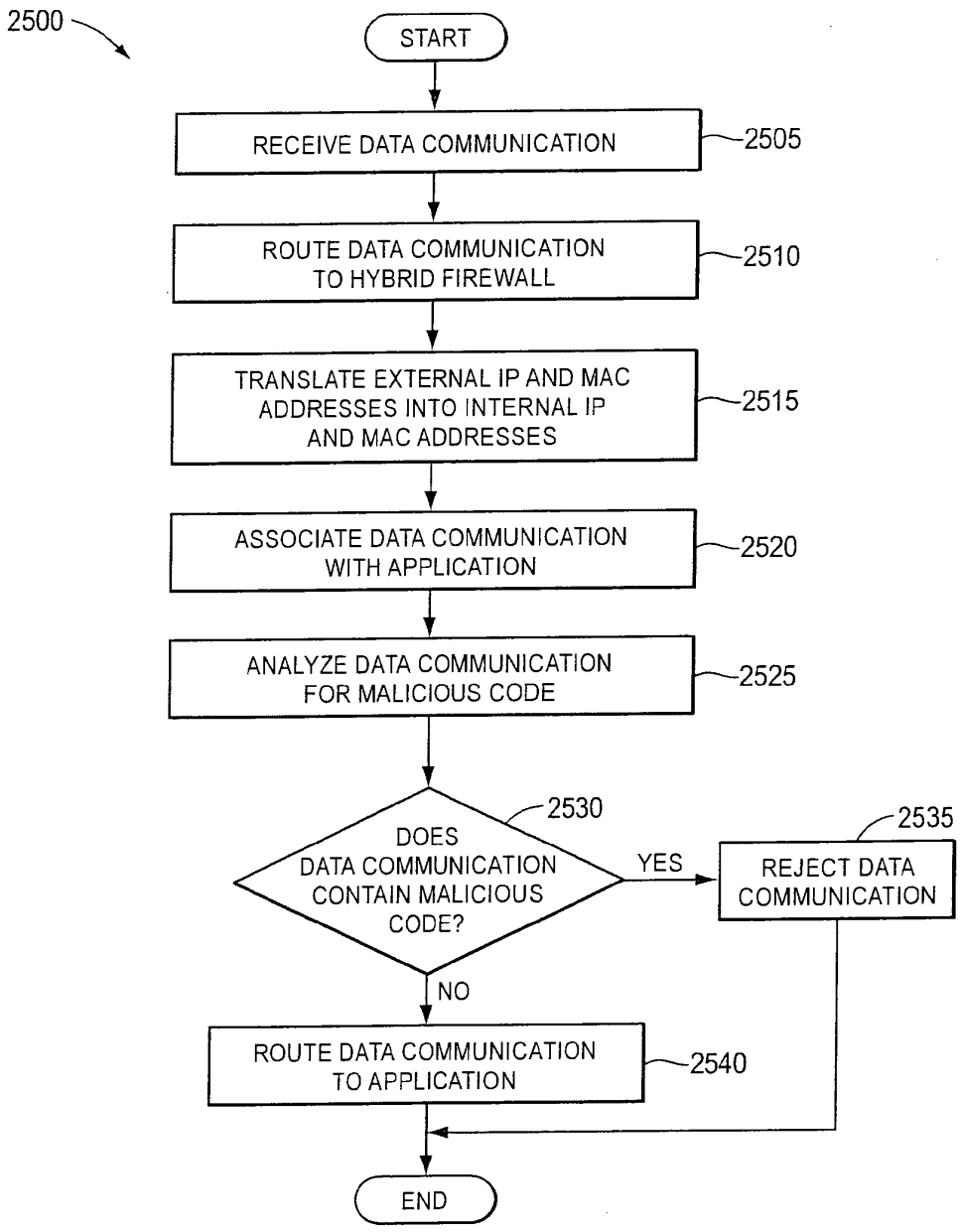

2500
START
RECEIVE DATA COMMUNICATION
2505
ROUTE DATA COMMUNICATION TO HYBRID FIREWALL
2510
TRANSLATE EXTERNAL IP AND MAC ADDRESSES INTO INTERNAL IP AND MAC ADDRESSES
2515
ASSOCIATE DATA COMMUNICATION WITH APPLICATION
2520
ANALYZE DATA COMMUNICATION FOR MALICIOUS CODE
2525
DOES DATA COMMUNICATION CONTAIN MALICIOUS CODE?
2530
YES
REJECT DATA COMMUNICATION
2535
NO
ROUTE DATA COMMUNICATION TO APPLICATION
2540
END

FIG. 25

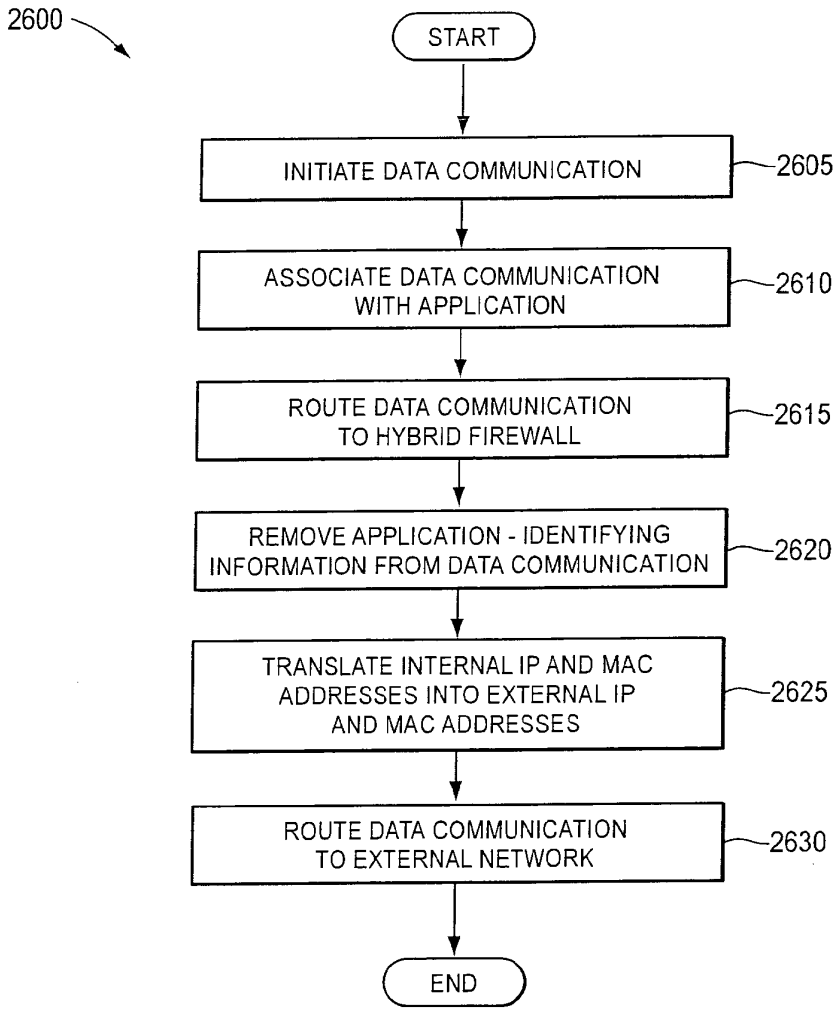

2600
START
INITIATE DATA COMMUNICATION
2605
ASSOCIATE DATA COMMUNICATION WITH APPLICATION
2610
ROUTE DATA COMMUNICATION TO HYBRID FIREWALL
2615
REMOVE APPLICATION - IDENTIFYING INFORMATION FROM DATA COMMUNICATION
2620
TRANSLATE INTERNAL IP AND MAC ADDRESSES INTO EXTERNAL IP AND MAC ADDRESSES
2625
ROUTE DATA COMMUNICATION TO EXTERNAL NETWORK
2630
END

FIG. 26

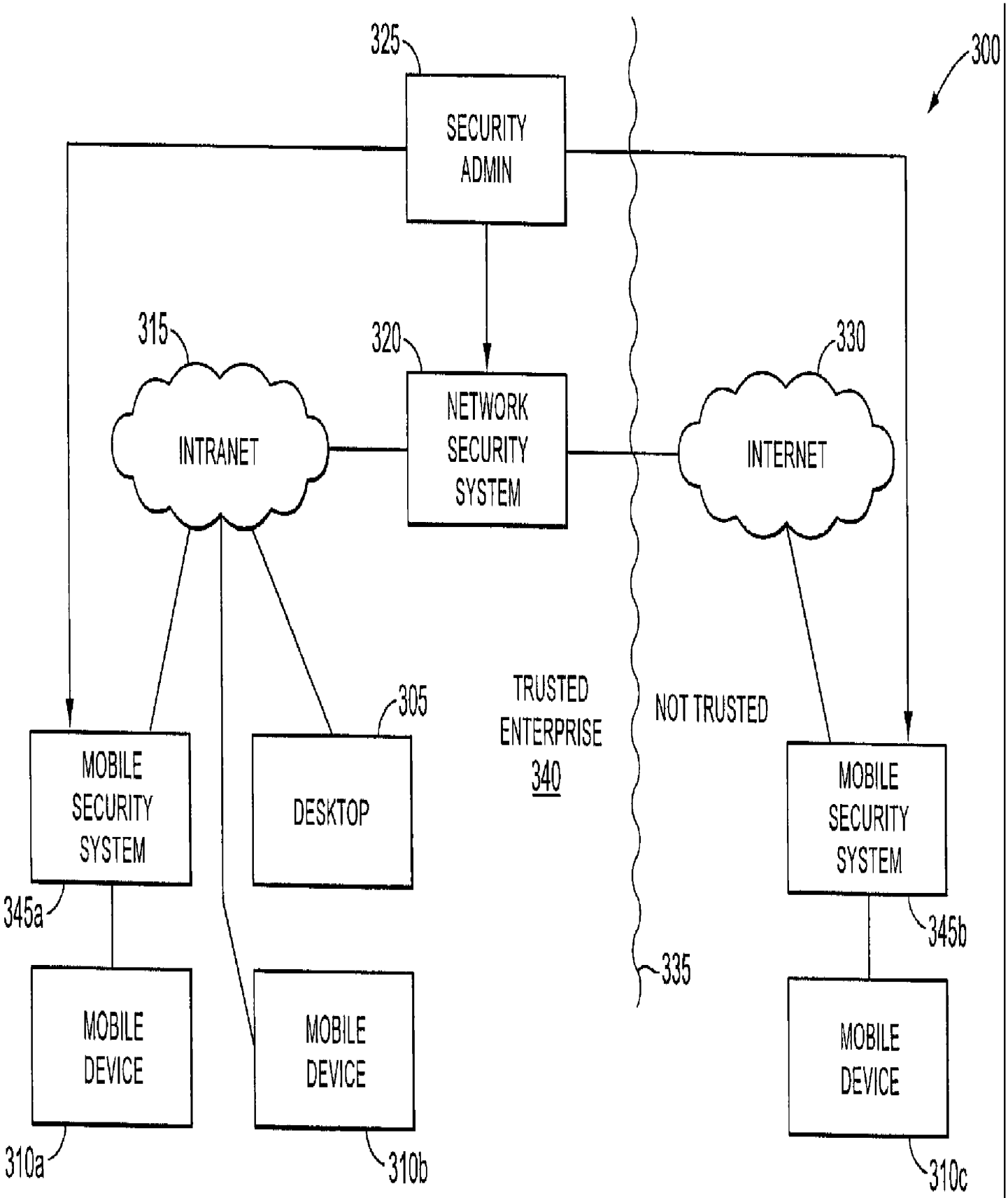

325
300
SECURITY ADMIN
315
320
330
INTRANET
NETWORK SECURITY SYSTEM
INTERNET
TRUSTED ENTERPRISE 340
NOT TRUSTED
305
MOBILE SECURITY SYSTEM
DESKTOP
MOBILE SECURITY SYSTEM
345a
345b
335
MOBILE DEVICE
MOBILE DEVICE
MOBILE DEVICE
310a
310b
310c

FIG. 3

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

(11) EP 1 850 575 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
31.10.2007 Bulletin 2007/44

(51) Int Cl.:
H04M 15/28 *(2006.01)* ***H04M 17/00*** *(2006.01)*
H04Q 7/32 *(2006.01)* *H04Q 7/38* *(2006.01)*

(21) Application number: **06252276.8**

(22) Date of filing: **27.04.2006**

(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

(71) Applicant: **Research In Motion Limited**
Waterloo, Ontario N2L 3W8 (CA)

(72) Inventor: **Rybak, Michal A.**
Kitchener, Ontario, N2R 1B1 (CA)

(74) Representative: **Fennell, Gareth Charles et al**
Kilburn & Strode
20 Red Lion Street
London WC1R 4PJ (GB)

(54) Method and apparatus for monitoring and controlling wireless resource usage

(57) A mobile communications device (116) comprises a wireless resource usage module (216) operable to assist the user of the mobile communications device (116) and/or his or her employer in monitoring and/or controlling the level of resources consumed by the user in a billing period.

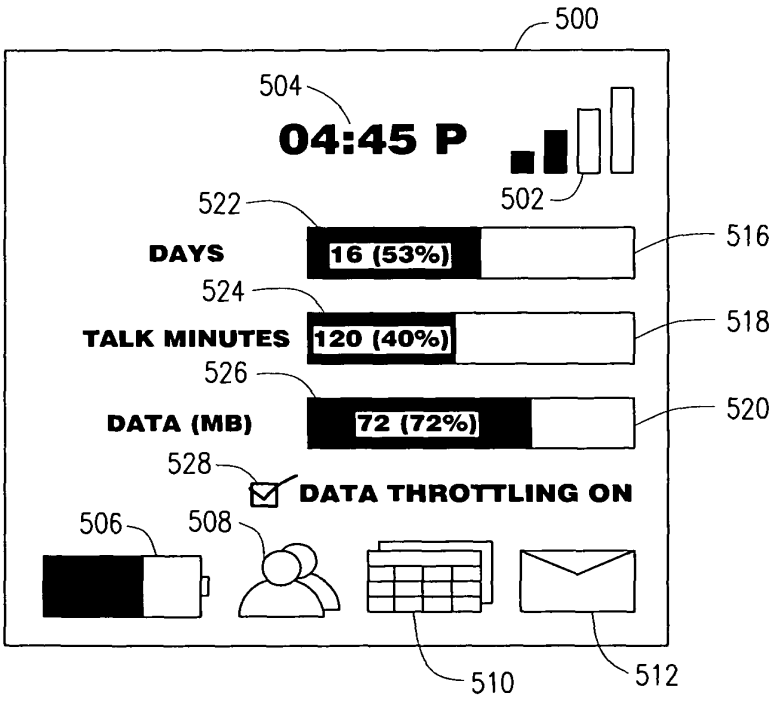


FIG. 7

EP 1 850 575 A1

Printed by Jouve, 75001 PARIS (FR)

Description

TECHNICAL FIELD OF THE APPLICATION

[0001] The present disclosure generally relates to wireless packet data service networks. More particularly, and not by way of any limitation, the present disclosure is directed to a mobile communications device and related data service network employing features suitable for monitoring and controlling wireless service usage.

BACKGROUND

[0002] Wireless service is generally offered by wireless service providers according to certain wireless service access plans. Most wireless service access plans include limitations as to the quantity of wireless access available in a given time. For example, a first wireless service access plan may provide for a certain number of cellular telephone voice minutes per month. Certain plans provide for unlimited cellular voice minutes during off-peak periods along with a limited number of minutes available during peak periods. Wireless service access plans may also provide for specified levels of wireless data access per month. While cellular telephone minutes are generally quantified in minutes per month, wireless data access is generally quantified in some units of bandwidth per month (e.g., megabytes per month). In either event, a wireless service provider will generally continue to provide service above the specified level, but will charge an additional premium for the usage above the level specified in the wireless service access plan.

SUMMARY OF THE DISCLOSURE

[0003] In one embodiment, the present disclosure is directed to a method for monitoring resource usage of a mobile communications device comprising the steps of acquiring a mobile communication plan profile associated with a subscriber, the plan profile including at least a value representing a limit of mobile communication resource usage within a specified calendar period; acquiring resource consumption data relative to the specified calendar period; calculating usage statistics based on the resource consumption data and the plan profile; and presenting the usage statistics to an entity.

[0004] In another embodiment, the present disclosure is directed to a mobile communications device comprising at least one storage area for containing a mobile communication service plan profile associated with a subscriber, the mobile communication service plan profile including at least a value representing a limit of mobile communication resource usage within a specified period; at least one storage area for containing resource consumption data relative to the specified period; and a wireless resource usage control module for calculating usage statistics based on the resource consumption data and the service plan profile.

BRIEF DESCRIPTION OF THE DRAWINGS

[0005] A more complete understanding of the embodiments of the present disclosure may be had by reference to the following Detailed Description when taken in conjunction with the accompanying drawings wherein:

[0006] Figure 1 depicts an exemplary network environment including a wireless packet data service network wherein an embodiment of the present disclosure may be practiced;

[0007] Figure 2 depicts a software architectural view of a mobile communications device operable to route incoming messages according to one embodiment;

[0008] Figure 3 depicts a block diagram of a mobile communications device operable to route incoming messages according to one embodiment;

[0009] Figure 4 depicts a flow chart for a method of monitoring and controlling wireless service access according to one embodiment; and

[0010] Figure 5 depicts a screen shot of a mobile communications device according to one embodiment;

[0011] Figure 6 depicts a screen shot of a mobile communications device according to a second embodiment;

[0012] Figure 7 depicts a screen shot of a mobile communications device having an embodiment of the usage monitoring application open;

[0013] Figure 8 depicts a screen shot of a usage monitoring application embodiment suitable for monitoring the wireless usage of a group of users; and

[0014] Figure 9 depicts a flow chart of a usage throttling method according to one embodiment.

DETAILED DESCRIPTION OF THE DRAWINGS

[0015] A system and method of the present 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.

[0016] Referring now to the drawings, and more particularly to Figure 1, depicted therein is an exemplary network environment 100 including a wireless packet data service network 112 wherein an embodiment of the present system may be practiced. An enterprise network 102, which may be a packet-switched network, can include one or more geographic sites and be organized as a local area network (LAN), wide area network (WAN) or metropolitan area network (MAN), et cetera, for serving a plurality of corporate users.

[0017] A number of application servers 104-1 through 104-N disposed as part of the enterprise network 102 are operable to provide or effectuate a host of internal and external services such as email, video mail, Internet access, corporate data access, messaging, calendaring and scheduling, information management, and the like. Accordingly, a diverse array of personal information ap-

pliances such as desktop computers, laptop computers, palmtop computers, et cetera, although not specifically shown in Figure 1, may be operably networked to one or more of the application servers 104-i, i = 1, 2,...,N, with respect to the services supported in the enterprise network 102.

[0018] Additionally, a remote services server 106 may be interfaced with the enterprise network 102 for enabling a corporate user to access or effectuate any of the services from a remote location using a suitable mobile communications device 116. A secure communication link with end-to-end encryption may be established that is mediated through an external IP network, i.e., a public packet-switched network such as the Internet 108, as well as the wireless packet data service network 112 operable with mobile communications device 116 via suitable wireless network infrastructure that includes a base station (BS) 114 .

[0019] In one embodiment, a trusted relay network 110 may be disposed between the Internet 108 and the infrastructure of wireless packet data service network 112. By way of example, mobile communications device 116 may be a data-enabled handheld device capable of receiving and sending messages, web browsing, interfacing with corporate application servers, et cetera.

[0020] For purposes of the present disclosure, the wireless packet data service network 112 may be implemented in any known or heretofore unknown mobile communications technologies and network protocols. For instance, the wireless packet data service network 112 may be comprised of a General Packet Radio Service (GPRS) network that provides a packet radio access for mobile devices using the cellular infrastructure of a Global System for Mobile Communications (GSM)-based carrier network. In other implementations, the wireless packet data service network 112 may comprise an Enhanced Data Rates for GSM Evolution (EDGE) network, an Integrated Digital Enhanced Network (IDEN), a Code Division Multiple Access (CDMA) network, or any 3rd Generation (3G) network.

[0021] By way of providing an exemplary embodiment, the teachings of the present disclosure will be illustrated within the network environment 100, although those skilled in the art should readily recognize that the scope of the present disclosure is not limited thereby. Furthermore, a plan information server 109 may be coupled to any of the networks 102, 108, 110, 112 described above for purposes of the present disclosure as will be set forth below in greater detail.

[0022] Figure 2 depicts a software architectural view of a mobile communications device according to one embodiment. A multi-layer transport stack (TS) 206 is operable to provide a generic data transport protocol for any type of corporate data, including email, via a reliable, secure and seamless continuous connection to a wireless packet data service network.

[0023] As illustrated in the embodiment of Figure 2, an integration layer 204A is operable as an interface between a radio layer 202 and the transport stack 206 of mobile communications device 116. Likewise, another integration layer 204B is provided for interfacing between the transport stack 206 and a user applications layer 207 supported on the mobile communications device 116, e.g., email 208, calendar/scheduler 210, contact management 212 and browser 214. Although not specifically shown, the transport stack 206 may also be interfaced with the operating system of mobile communications device 116. In another implementation, the transport stack 206 may be provided as part of a data communications client module operable as a host-independent virtual machine on a mobile device. As seen in Figure 2, a usage control module 216 is coupled to radio layer 202 and transport stack 206. Usage control module 216 is operable to assist the user of mobile communications device 116 in controlling his or her usage of wireless services in a manner described more fully below.

[0024] The bottom layer (Layer 1) of the transport stack 206 is operable as an interface to the wireless network's packet layer. Layer 1 handles basic service coordination within the exemplary network environment 100 shown in Figure 1. For example, when a mobile communications device roams from one carrier network to another, Layer 1 verifies that the packets are relayed to the appropriate wireless network and that any packets that are pending from the previous network are rerouted to the current network. The top layer (Layer 4) exposes various application interfaces to the services supported on the mobile communications device. The remaining two layers of the transport stack 206, Layer 2 and Layer 3, are responsible for datagram segmentation/reassembly and security, compression and routing, respectively.

[0025] Figure 3 depicts a block diagram of a mobile communications device according to one embodiment. It will be recognized by those skilled in the art upon reference hereto that although an embodiment of mobile communications device 116 may comprise an arrangement similar to one shown in Figure 3, there can be a number of variations and modifications, in hardware, software or firmware, with respect to the various modules depicted. Accordingly, the arrangement of Figure 3 should be taken as illustrative rather than limiting with respect to the embodiments of the present disclosure.

[0026] A microprocessor 302 providing for the overall control of an embodiment of mobile communications device 116 is operably coupled to a communication subsystem 304 which includes a receiver 308 and transmitter 314 as well as associated components such as one or more local oscillator (LO) modules 310 and a processing module such as a digital signal processor 312. As will be apparent to those skilled in the field of communications, the particular design of the communication module 304 may be dependent upon the communications network with which the mobile communications device 116 is intended to operate.

[0027] In one embodiment, the communication module 304 is operable with both voice and data communica-

tions. Regardless of the particular design, however, signals received by antenna 306 through base station 114 are provided to receiver 308, 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 digital signal processor 312, and provided to transmitter 314 for digital-to-analog (D/A) conversion, frequency up conversion, filtering, amplification and transmission over the air-radio interface via antenna 316.

[0028] Microprocessor 302 also interfaces with further device subsystems such as auxiliary input/output (I/O) 318, serial port 320, display 322, keyboard 324, speaker 326, microphone 328, random access memory (RAM) 330, a short-range communications subsystem 332, and any other device subsystems generally labeled as reference numeral 333. To control access, a Subscriber Identity Module (SIM) or Removable User Identity Module (RUIM) interface 334 is also provided in communication with the microprocessor 302.

[0029] In one implementation, SIM/RUIM interface 334 is operable with a SIM/RUIM card having a number of key configurations 344 and other information 346 such as identification and subscriber-related data. Operating system software and transport stack software may be embodied in a persistent storage module (i.e., non-volatile storage) such as Flash memory 335. In one implementation, Flash memory 335 may be segregated into different areas, e.g., storage area for computer programs 336 as well as data storage regions such as device state 337, address book 339, other personal information manager (PIM) data 341, and other data storage areas generally labeled as reference numeral 343. Usage control module 216 is operably connected to flash memory 335, including transport stack 206, as shown. In one exemplary implementation, the logic associated with the usage control module 216 is operable to access one or more storage areas, e.g., non-volatile storage areas 335, that contain various values relative to monitoring resource usage (i.e., resource consumption data) as will be set forth below. Additionally, the logic associated with the usage control module 216 is operable to access the subscriber's usage plan profile (e.g., a cellular telephone voice communication service plan profile, a wireless data transmission service plan profile, etc., which may be locally stored (e.g., in non-volatile areas), or downloaded, or otherwise available to the mobile communications device) for purposes of effectuating resource usage monitoring and/or throttling.

[0030] Figure 4 depicts a flow chart detailing the operation of usage control module 216 according to one embodiment. The process begins in block 400 with acquisition of the subscriber's usage plan profile, which includes at least one resource usage limit. Such limits may include, for example, limits as to the total number of on-peak cellular voice minutes per month, limits as to the total number of megabytes of data per month and/or limits as to the number of short messaging service (SMS) messages sent per month, as examples.

[0031] After the usage plan profile is acquired in block 400, the present date and time is acquired in block 402, along with the date and time of the beginning of the current billing period in block 404. Generally, the billing period will be one month and will begin at 12:00 am on a particular day of each month, but there is nothing within the spirit and scope of the present disclosure limiting the methods herein to such an arrangement. Given the date and time for the beginning of the current period and the current date and time, the usage control module 216 can determine the elapsed time since the beginning of the current billing period, as elaborated in block 406.

[0032] The date and time for the end of the current billing period is acquired in block 408. Given the date and time of the beginning of the current billing period and the date and time of the end of the current billing period, the usage control module 216 can calculate the total time of the current billing period, as elaborated in block 410.

[0033] The usage control module 216 acquires the quantity of current period usage of at least one limited wireless resource in block 412. This resource may be on-peak cellular voice minutes, megabytes of data or quantity of SMS messages, as examples. Given the total amount of the wireless resource available in the current billing period and the total amount of usage of that wireless resource so far in the current billing period, the usage control module 216 calculates, in block 414, a usage quotient representing the proportion of the resource which has already been consumed in the current billing period. For example, if the subscriber's service plan provides for 200 on peak minutes per month and the subscriber has used 100 minutes, the usage quotient would equal 100/200, or 50%.

[0034] In a similar manner, the usage control module 216 calculates, using the quantity of time elapsed in the current billing period and the total length of the current billing period, an elapsed days quotient representing the proportion of time in the current billing period which has already elapsed. For example, if the current month has 30 days, and 9 days have elapsed, the elapsed days quotient would equal 9/30, or 30%. This step is elaborated in block 416. The usage quotient and elapsed days quotient may be displayed to the user or provided to a management entity (block 418).

[0035] Process flow subsequent to block 418 is dependent on the relative values of the calculated statistics such as the usage quotient and the elapsed days quotient. If the proportion of the resource consumed in the current billing period is at or below the proportion of time elapsed in the current billing period, then the subscriber is unlikely to exceed the limit specified in the service plan and no corrective action is necessary. If, however, the proportion of the resource consumed in the current billing period exceeds the proportion of time elapsed so far in the current billing period, then the subscriber is consum-

ing the limited resource at a rate making it likely that he or she will exceed the limit specified in the service plan, and corrective action may be necessary, as elaborated in detail below.

[0036] In decision block 420, usage control module 216 inquires as to whether the usage quotient (designated E) is greater than the elapsed days quotient (designated F). If the usage quotient is not greater than the elapsed days quotient, then there is not significant cause for alarm and process flow proceeds to decision block 422. If the usage quotient is greater than the elapsed days quotient, then there is cause for alarm and process flow proceeds to block 424.

[0037] In the event that the subscriber is on track to meet or undershoot his or her usage limit for the current billing period, and process flow has proceeded to decision block 422, the usage control module 216 determines whether the subscriber's wireless access is currently being "throttled" by the usage control module 216. In other words, usage control module 216 determines whether prior usage conditions have placed usage control module 216 in a mode in which it is restricting the subscriber's access to wireless services. Such a restriction may include, for example, a reduced data transfer rate, or some limit as to the number of cellular voice minutes or SMS messages available per day or per hour.

[0038] If the subscriber's wireless access is not being throttled by usage control module 216, then process flow proceeds to block 428, wherein the current cycle of the wireless access control process comes to an end. If the subscriber's wireless access is, however, being throttled by usage control module 216 due to a previous overrun, then process flow proceeds to block 426, wherein usage control module 216 adjusts the wireless access parameters for mobile communications device 116.

[0039] In certain embodiments, adjustment of the throttled wireless access parameters may entail removal of all throttling of wireless access once the usage quotient equals or is less than the elapsed days quotient. In other embodiments, adjustment of the wireless access parameters may entail a reduction in the degree of throttling proportional to the difference between the usage quotient and the elapsed days quotient. In such an embodiment, so long as the usage quotient is only slightly lower than the elapsed days quotient, a certain level of throttling may continue to be imposed, with the goal of generating a "buffer" of wireless resources. In any event, after adjustment of the wireless access parameters, process flow proceeds to block 428, where the current cycle of the wireless access control process ends.

[0040] Returning to block 420, when the usage quotient exceeds the elapsed days quotient, reflecting the fact that the subscriber is consuming wireless resources at a rate expected to result in a budget overrun, process flow will proceed from block 420 to block 424. In block 424, usage control module 216 will determine whether the subscriber or some other party has activated an alarm function. The usage control module may have the capability to provide wireless usage overrun alarms to the subscriber and/or to other individuals or components in a network. If the alarm function is activated, process flow proceeds to block 430, wherein at least one alarm is generated to at least one individual or network component, and then to block 432. This alarm may be of any a number of types, including audio, video and tactile alarms. If the alarm function is deactivated, process flow proceeds directly to block 432.

[0041] In block 432, usage control module 216 determines whether the wireless resource throttling function has been activated, either by the subscriber or by some other individual or component. If the wireless resource throttling function has not been activated, process flow proceeds directly to block 428, where the current cycle of the wireless access control process ends. If the wireless resource throttling function has been activated, process flow proceeds to block 434.

[0042] In block 434, usage control module 216 adjusts wireless access parameters in order to control consumption of one or more wireless resources by the subscriber. As described above, in certain embodiments, the throttling may take the form of a pre-set usage limit imposed whenever throttling is deemed necessary. In other embodiments, the usage limit may vary within a range. The usage limit may vary, for example, according to the difference between the usage quotient and the elapsed days quotient. In such an arrangement, where the usage quotient of a wireless resource exceeds the elapsed days by 10%, the usage control module may reduce the maximum rate of consumption of the wireless resource by a proportional percentage, which could be 10%, 20% or 5%, as examples. In certain embodiments, the degree of throttling may be linearly proportional to the degree of projected overrun, while in others the degree of throttling may be geometrically proportional, so that minor overruns would have negligible effects on bandwidth, which would become increasingly dramatic as usage overruns increased. Any and all of the above are within the spirit and scope of the present disclosure. After the parameters are adjusted by the specific algorithm employed, process flow then proceeds from block 434 to block 428, where the current cycle ends.

[0043] Figure 5 depicts one embodiment of a user interface screen 500 for a mobile communications device. For example, screen 500 displays information to the user of mobile communications device 116. Certain information, such as time readout 504, will generally be presented on screen 500 in textual format. In order to maximize special efficiency, however, other information is presented on screen 500 in a graphical format including a set of descriptive icons. Representative icons shown on screen 500 include a wireless signal strength icon 502, a battery strength icon 506, contacts icon 508, calendar icon 510, message icon 512 and wireless resource usage icon 514.

[0044] Each of icons 502, 506, 508, 510, 512, 514 has a specific function within mobile communications device 116, and each may generally be associated with a spe-

cific software application. Contacts icon 508, for example, may generally be associated with a software application such as contact management application 212 (shown in Figure 2), while calendar icon 510 and message icon 512 may be associated with calendar/scheduler application 210 and email application 208, respectively.

[0045] Wireless resource usage icon 514 is exemplified with three separate horizontal bars that may represent different parameters depending on the application. In one embodiment, one bar may represent the passage of time over the billing period, a second bar may represent peak cellular voice minutes used in the current billing period and a third bar may represent data bandwidth used in the current billing period. By comparing the size of bars representing wireless resource usage to the size of bars representing the passage of time, a subscriber can monitor his or her rate of usage. In alternate embodiments, the bars may represent other parameters, which may include the number of off-peak cellular telephone voice minutes used and/or the number of SMS messages sent/received in the current billing period, as examples.

[0046] An alternative embodiment of a display screen is shown in Figure 6 and designated 600. Display screen 600 is similar to screen 500, having a signal strength meter icon 602, a current time display 604, a battery strength meter icon 606, a contacts icon 608, a calendar icon 610 and a message icon 612, each of which corresponds to a similar icon depicted in Figure 5. In contrast to display screen 500, display screen 600 has a rotary wireless resource usage icon 614 in place of the horizontal bar wireless resource usage icon 514 shown in Figure 5. In place of linear bars, wireless resource usage icon 614 employs rotary elements, including a needle pivoting about the center of the icon and a sector and marker disposed at the circumference thereof. Any of the elements may represent any of the parameters heretofore described.

[0047] Figure 7 depicts display screen 500 at a separate point in time at which an embodiment of the user interface application for usage control module 216 is open. An elapsed days graphical indicator 516 reflects the proportion of the current billing period elapsed as compared to the total span of the current billing period. Similarly, voice minutes graphical indicator 518 and data resources graphical indicator 520 reflect the proportion of each resource consumed as compared to the total amount of each resource available in the current billing period. Textual indicators 522, 524, 526 provide the same information as graphical resource indicators 516, 518, 520, but in alphanumeric rather than graphical format.

[0048] By comparing the state of resource indicators 518, 520, 524, 526 to elapsed days indicators 516, 522, a subscriber can quickly determine whether his or her rate of usage is likely to exceed the allotted resources for the current billing period. In order to assist the subscriber in controlling resource usage, a throttling indicator 528 reflects whether or not wireless bandwidth throttling is currently activated. In certain embodiments, throttling may be controlled by the subscriber, while in other embodiments throttling may be controlled partly or completely by a process external to mobile communications device 116 or by another individual.

[0049] Display screen 500 as shown in Figure 7 is only representative of one embodiment of the present disclosure. Alternative embodiments may incorporate additional information or less information. In certain embodiments, for example, the throttling indicator 528 may reflect a variable quantity representing the degree of throttling being imposed on wireless communications rather than functioning as a simple on/off indicator as shown in Figure 7. In certain other embodiments, an alarm control indicator may be included as part of the display. These and other variations are within the spirit and scope of the present disclosure.

[0050] Figure 8 depicts a display screen 850 designed to assist enterprise managers in controlling wireless resource usage at the department level. A set of employees having mobile communications devices are displayed in tabular format. For a first employee, Alex Jones, a set of resource bars 852, 854, 856 are shown reflecting the level of Alex Jones' usage of certain wireless resources in the current billing period. The information for an employee also includes his or her name 858, employee number 860 and telephone number 862. The information also includes a throttling control indicator 864. In certain embodiments, throttling control indicator 864 may only reflect whether throttling is activated on the employee's mobile communications device, while in other embodiments it may control whether throttling is activated. While not specifically described for each person shown, the same information is presented for each of the seven individuals, as seen in Figure 8.

[0051] A department summary is included in the lower-right corner of Figure 8, which reflects the total resource usage for the department. This information is provided via graphical resource usage indicators 880, 882, 884 along with textual resource usage indicators 886, 888 and an estimated budget overrun amount 890. Given this information, a manager can budget, and in certain cases control, wireless resource usage within his or her department.

[0052] Corporate control of resource usage can be employed in a number of ways. In certain embodiments, a manager may be given the power to disallow resource usage above a certain limit, which may be expressed in minutes, megabytes or dollars, as examples. A manager may also be tasked with the option to allow unlimited usage through the admin tool. In certain embodiments, the management console may show data for one or more users spanning multiple billing periods. Assuming a user is consistently over or under one or more of his or her allocated resource limits, the management console may highlight the user to the manager for possible plan alteration.

[0053] In embodiments employing some form of usage

throttling mechanism, the manner of usage throttling can vary depending on the application. One method of throttling is depicted in Figure 9. According to the embodiment of Figure 9, throttling is imposed when data usage is higher than expected, while a data boost may be provided when data usage is lower than expected.

[0054] Process flow begins in block 902 and proceeds from there to decision block 904. In decision block 904, a data usage control module, which may include logic or software instructions, determines whether data usage has been greater than expected. If usage is greater than expected, process flow is directed to block 906, where the data usage control module slows down the data transfer rate. If usage is not greater than expected, process flow is directed to decision block 908.

[0055] In decision block 908, data usage control module determines whether usage is less than expected. If data usage is less than expected, process flow is directed to block 910, where the data usage control module speeds up the data transfer rate. If data usage is not less than expected, no throttling mechanism is imposed process flow is directed to block 912, where the process ends.

[0056] As those of skill in the art will appreciate, the present disclosure encompasses a wide variety of individual embodiments and applications within its broader teachings. For example, in certain embodiments, a mobile communications device may be operable to query for a period beginning and period end (or beginning and duration) and from this information measure the elapsed time by comparing the difference from the beginning to the current time on the device against the duration. Also, the device may be operable to measure consumption since the beginning of the billing period.

[0057] In an alternate embodiment, a server may supply the proportion between the resources used and resources available as well as between the time elapsed and time available directly to the device, such that little or no computation is required on the device itself. In certain embodiments, a system may be operable to work with non-periodic "pay as you go" plans. Such a system may, for example, display a portion of used vs. total available resources since the last resource purchase, where the used indicator resets to 0 at the time of purchase. Alternatively, the system may display the remaining resources as a bulk quantity. The current available resources may be acquired from a server, or the system can maintain its own running total by adding up all the purchases and subtracting out the measured usage. In addition, such a "pay as you go" system may display the remaining number of days, projected based on the current consumption rate.

[0058] In certain applications, a combination of the above may be employed. Where, for example, a customer has purchased a monthly plan which provides for a certain level of resources while allowing for the pre-purchase of additional resources during the billing period, the elapsed time vs. time period display would remain, though the resource usage bars could actually go "backward" to reflect the additional resource capacity available after additional resources are purchased.

[0059] In certain embodiments, the resource usage bars may change in appearance if maximum resource usage is exceeded. According to one embodiment, the bar length is proportional to the usage percentage up until 100% of resource usage is reached. After 100% of available resource usage is exceeded, the bar length may then be proportional to the fraction of the planned 100% vs. the running total usage. In certain embodiments, the color or other appearance characteristic of the bars may change at this transition. Further, the device may be operable to display the current price or expense per unit time being incurred by usage of the resource.

[0060] The device may be operable to take into account any periods during which additional resource usage does not incur additional cost under the current billing plan. These may include, for example, nights and weekends. When the device is operating within an unlimited usage period, the usage indicator may be hidden or grayed out.

[0061] Billing plan details stored within the device or elsewhere may contain information about any number of overlapping conditional periods. The server may simply provide the current utilization ratios directly. Alternately, the server may provide static information about the plan, such as the starting and ending conditions for a given period, which may include the time of day or day of the week. From this information, the device could then determine the period within which it is operating and the quantity of resources consumed. Alternately, the device may calculate the ratios from durations and current consumption and elapsed time values provided by the server.

[0062] In certain embodiments, the device may be operable to display the level of resource utilization incurred within a number of different periods without respect to the period within which the device is currently operating.

[0063] In certain embodiments, the device may roam to a network on which it does not have pre-allocated resources. In this situation, the device is in a similar situation to that in which all pre-paid resources have been consumed. In this situation, the device may be operable to begin displaying the immediate rate of resource usage in either resource terms or monetary terms.

[0064] It is believed that the operation and construction of the embodiments of the present disclosure 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 monitoring resource usage of a mobile communications device (116) comprising the steps of:

   acquiring (400) a mobile communication plan profile associated with a subscriber, the plan profile including at least a value representing a limit of mobile communication resource usage within a specified calendar period;
   acquiring (402, 404, 408, 412) resource consumption data relative to the specified calendar period;
   calculating (414, 416) usage statistics based on the resource consumption data and the plan profile; and
   presenting (418) the usage statistics to an entity.

2. The method of claim 1 wherein the specified calendar period is a month.

3. The method of claim 1 wherein at least a portion of the resource consumption data represents cellular telephone usage in minutes.

4. The method of claim 1 wherein at least a portion of the resource consumption data represents wireless data usage in megabytes.

5. The method of claim 1 wherein the usage statistics are displayed to a user of the mobile communications device.

6. The method of claim 1 wherein an alert is generated depending on the usage statistics.

7. A mobile communications device (116) comprising:

   at least one storage area (335) for containing a mobile communication service plan profile associated with a subscriber, the mobile communication service plan profile including at least a value representing a limit of mobile communication resource usage within a specified period;
   at least one storage area (335) for containing resource consumption data relative to the specified period; and
   a wireless resource usage control module (216) for calculating usage statistics based on the resource consumption data and the service plan profile.

8. The mobile communications device (116) of claim 7 wherein at least a portion of the resource consumption data represents cellular telephone usage in minutes.

9. The mobile communications device (116) of claim 7 wherein at least a portion of the resource consumption data represents wireless data usage in megabytes.

10. The mobile communications device (116) of claim 7 wherein the wireless resource usage control module (216) is operable to throttle the amount of bandwidth provided depending on the usage statistics.

11. The mobile communications device (116) of claim 7 wherein the wireless resource usage control module (216) is operable to generate an alert depending on the usage statistics.

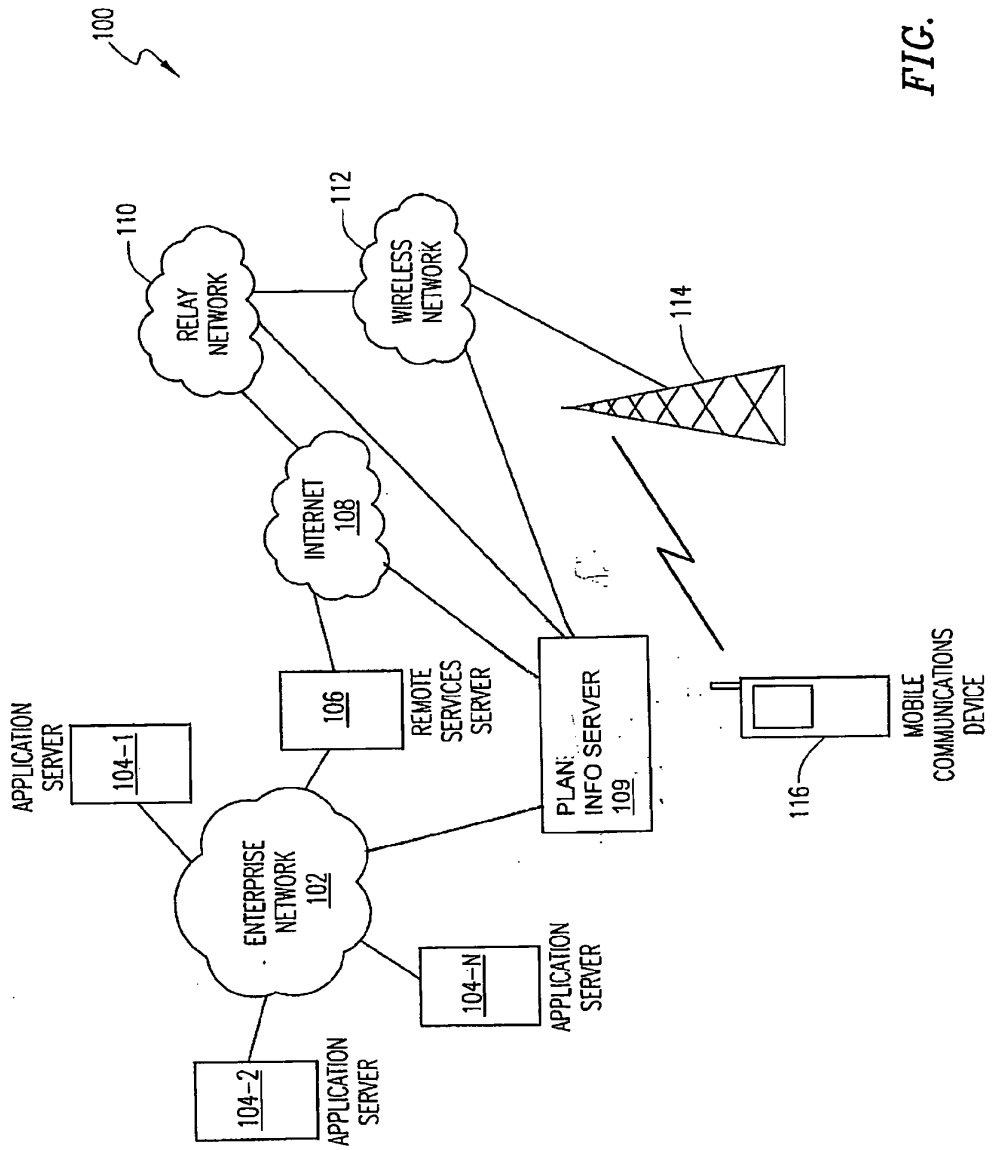

100
110
RELAY NETWORK
112
WIRELESS NETWORK
114
INTERNET 108
106
REMOTE SERVICES SERVER
PLAN INFO SERVER 109
APPLICATION SERVER
104-1
ENTERPRISE NETWORK 102
104-N
APPLICATION SERVER
104-2
APPLICATION SERVER
116
MOBILE COMMUNICATIONS DEVICE

FIG. 1

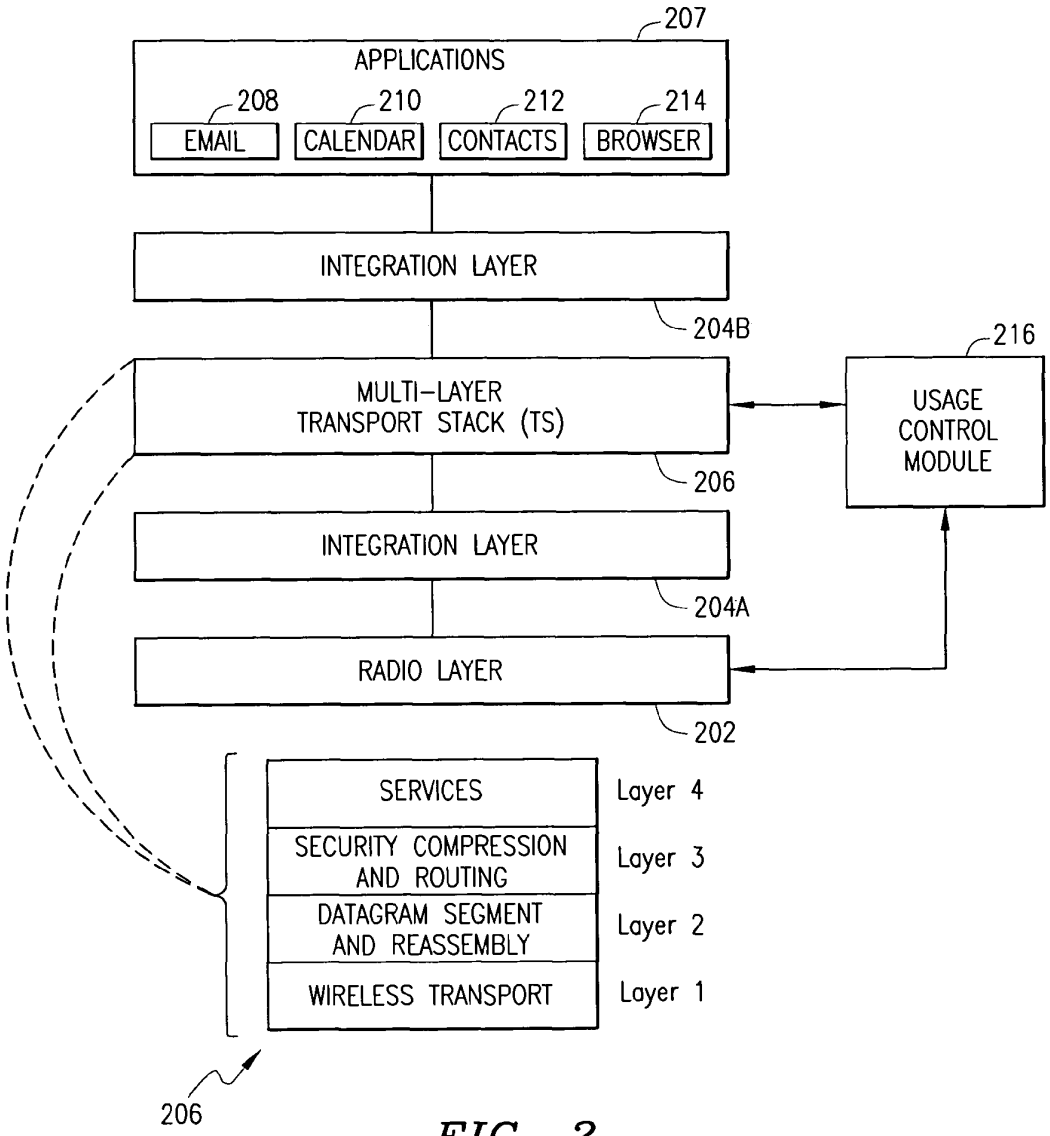

207
APPLICATIONS
208
EMAIL
210
CALENDAR
212
CONTACTS
214
BROWSER
INTEGRATION LAYER
204B
216
MULTI-LAYER
TRANSPORT STACK (TS)
USAGE
CONTROL
MODULE
206
INTEGRATION LAYER
204A
RADIO LAYER
202
SERVICES
Layer 4
SECURITY COMPRESSION
AND ROUTING
Layer 3
DATAGRAM SEGMENT
AND REASSEMBLY
Layer 2
WIRELESS TRANSPORT
Layer 1
206

FIG. 2

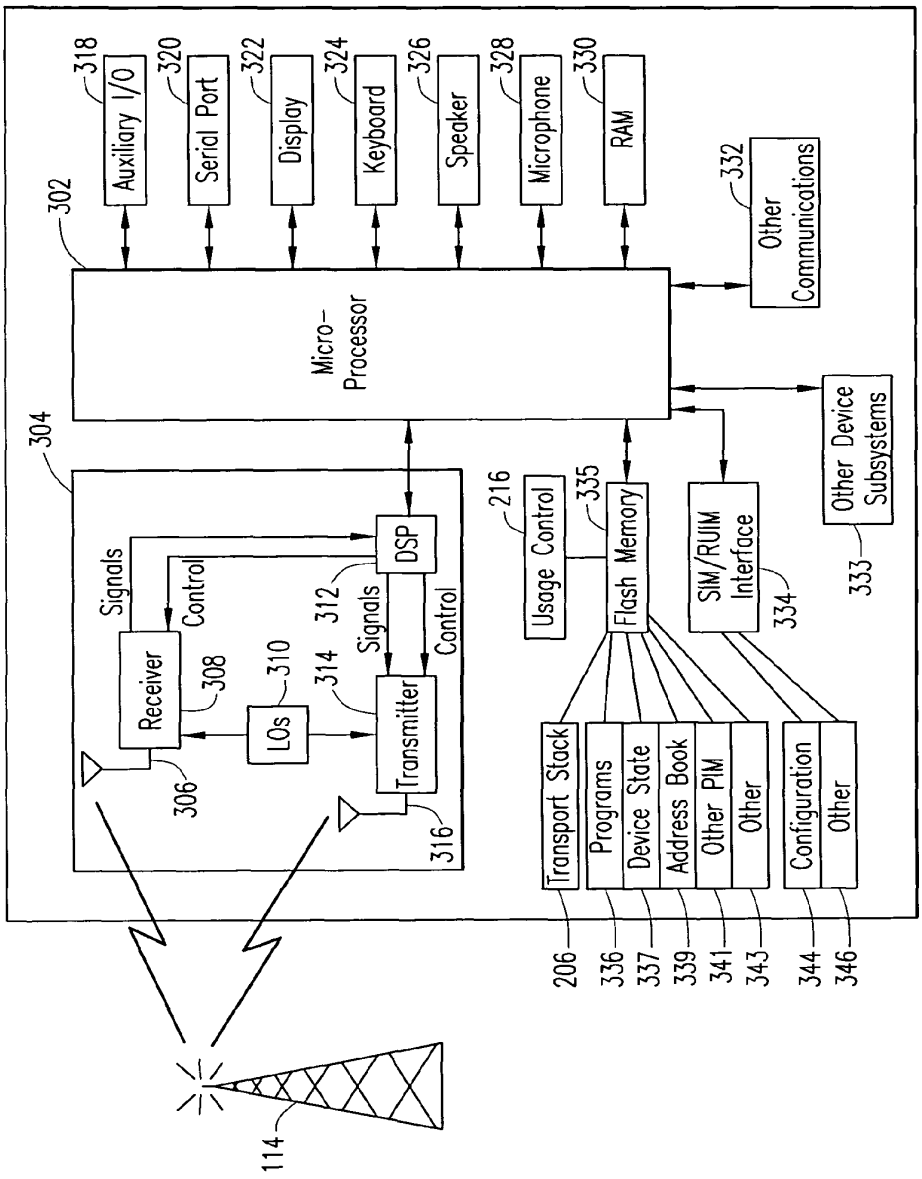

318
Auxiliary I/O
320
Serial Port
322
Display
324
Keyboard
326
Speaker
328
Microphone
330
RAM
332
Other Communications
302
Micro-Processor
304
Signals
Control
Receiver
308
306
LOs
310
314
312
Signals
DSP
Control
Transmitter
316
216
Usage Control
335
Flash Memory
SIM/RUIM Interface
334
333
Other Device Subsystems
Transport Stack
Programs
Device State
Address Book
Other PIM
Other
Configuration
Other
206
336
337
339
341
343
344
346
114

FIG. 3

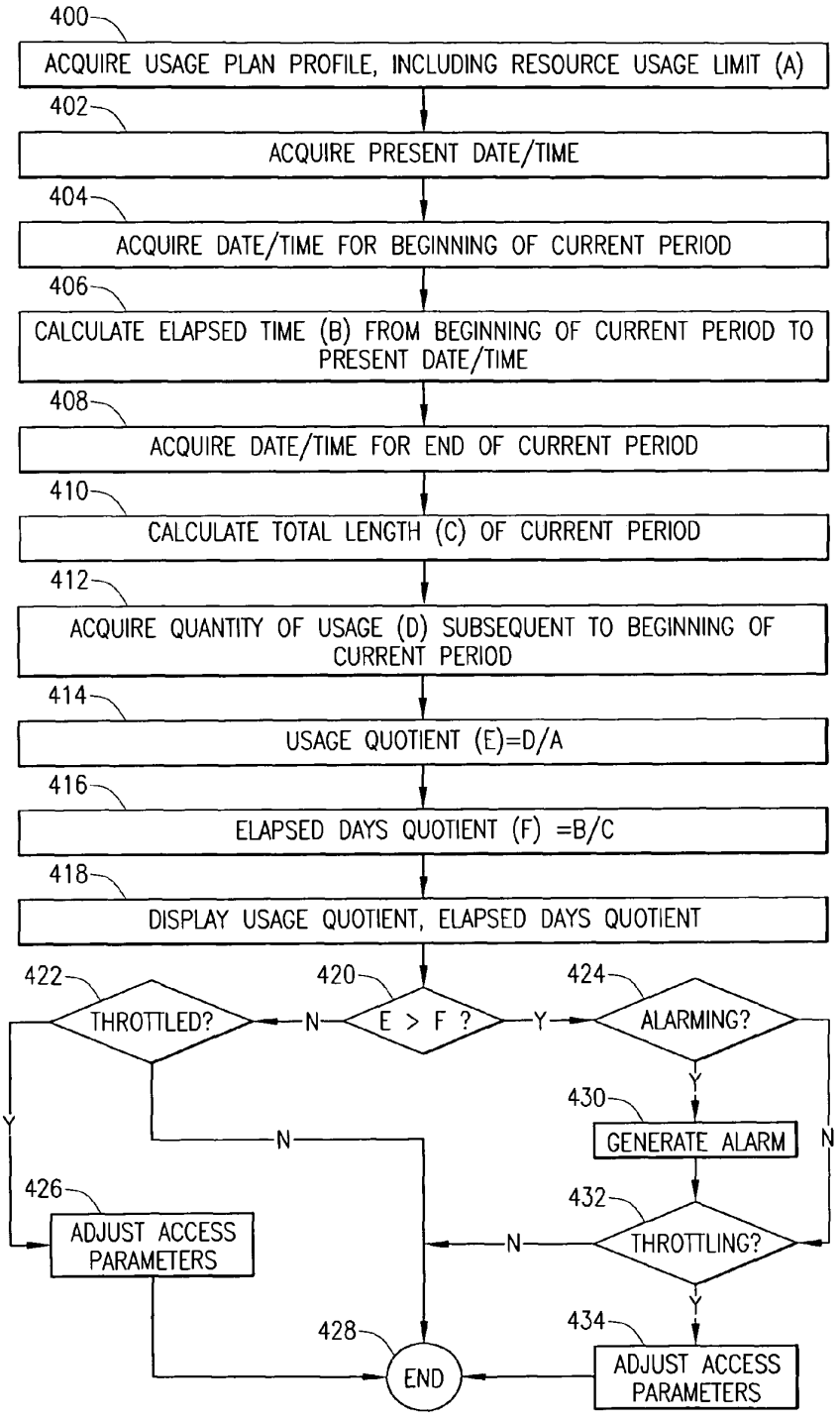

400
ACQUIRE USAGE PLAN PROFILE, INCLUDING RESOURCE USAGE LIMIT (A)
402
ACQUIRE PRESENT DATE/TIME
404
ACQUIRE DATE/TIME FOR BEGINNING OF CURRENT PERIOD
406
CALCULATE ELAPSED TIME (B) FROM BEGINNING OF CURRENT PERIOD TO PRESENT DATE/TIME
408
ACQUIRE DATE/TIME FOR END OF CURRENT PERIOD
410
CALCULATE TOTAL LENGTH (C) OF CURRENT PERIOD
412
ACQUIRE QUANTITY OF USAGE (D) SUBSEQUENT TO BEGINNING OF CURRENT PERIOD
414
USAGE QUOTIENT (E)=D/A
416
ELAPSED DAYS QUOTIENT (F) =B/C
418
DISPLAY USAGE QUOTIENT, ELAPSED DAYS QUOTIENT
420
E > F ?
N
Y
422
THROTTLED?
Y
N
426
ADJUST ACCESS PARAMETERS
424
ALARMING?
Y
N
430
GENERATE ALARM
432
THROTTLING?
N
Y
434
ADJUST ACCESS PARAMETERS
428
END

FIG. 4

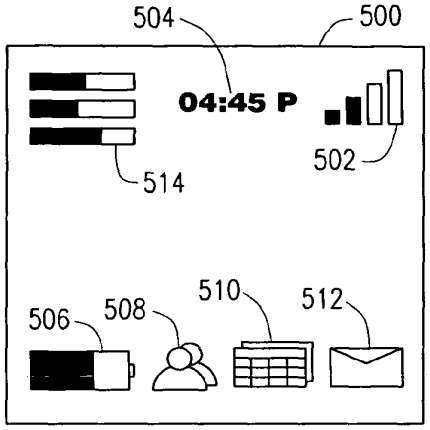


FIG. 5

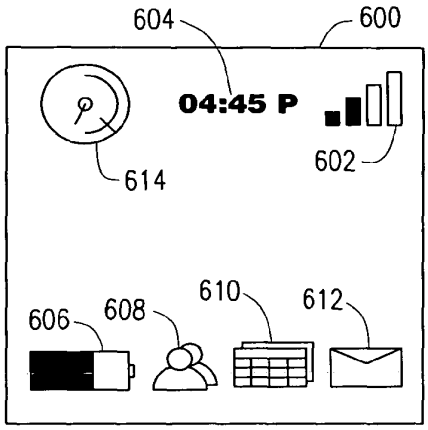


FIG. 6

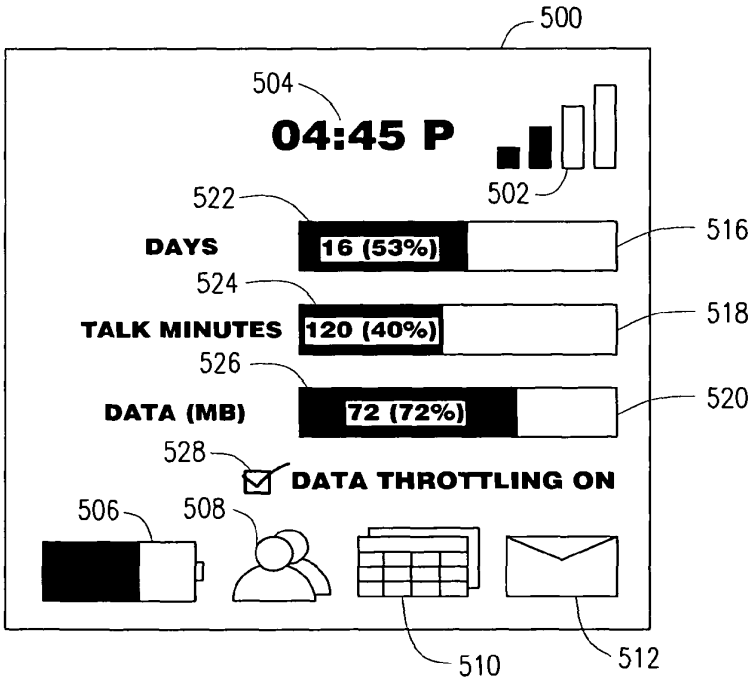


FIG. 7

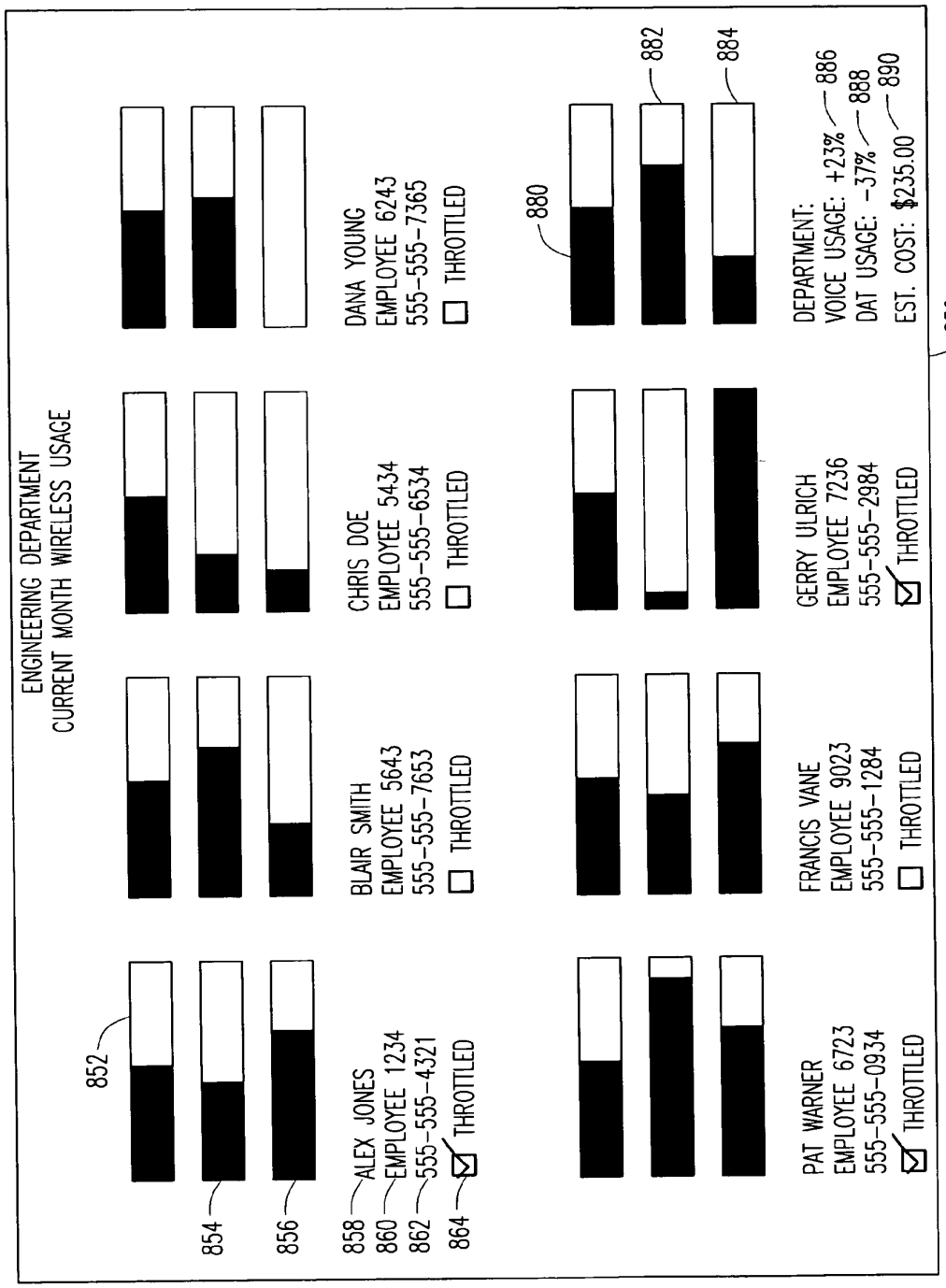

ENGINEERING DEPARTMENT
CURRENT MONTH WIRELESS USAGE
852
854
856
858 ALEX JONES
860 EMPLOYEE 1234
862 555-555-4321
864 THROTTLED
BLAIR SMITH
EMPLOYEE 5643
555-555-7653
THROTTLED
CHRIS DOE
EMPLOYEE 5434
555-555-6534
THROTTLED
DANA YOUNG
EMPLOYEE 6243
555-555-7365
THROTTLED
880
882
884
PAT WARNER
EMPLOYEE 6723
555-555-0934
THROTTLED
FRANCIS VANE
EMPLOYEE 9023
555-555-1284
THROTTLED
GERRY ULRICH
EMPLOYEE 7236
555-555-2984
THROTTLED
DEPARTMENT:
VOICE USAGE: +23%
DAT USAGE: -37%
EST. COST: $235.00
886
888
890
850

FIG. 8

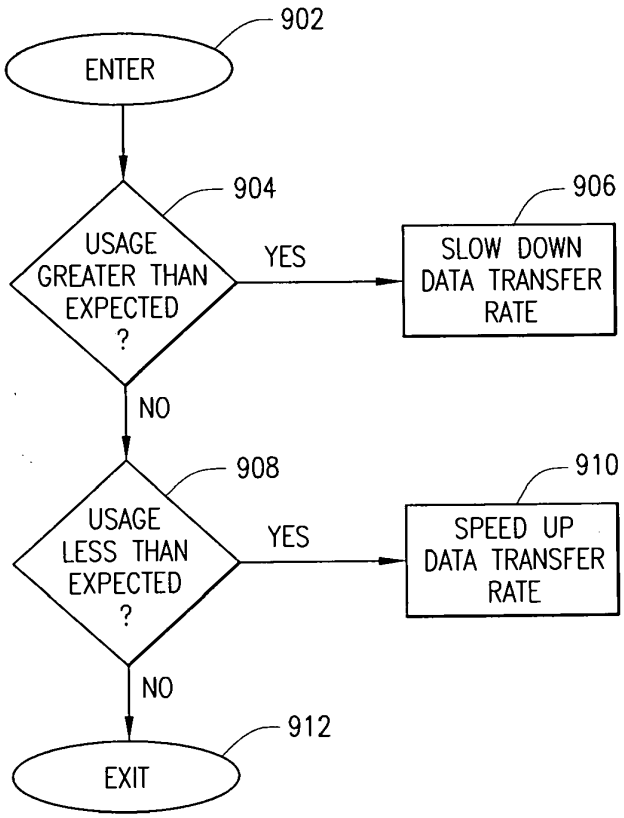

902
ENTER
904
USAGE GREATER THAN EXPECTED ?
YES
906
SLOW DOWN DATA TRANSFER RATE
NO
908
USAGE LESS THAN EXPECTED ?
YES
910
SPEED UP DATA TRANSFER RATE
NO
912
EXIT

FIG. 9

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 06 25 2276

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	US 2001/055961 A1 (NAKAJIMA TAKETOSI) 27 December 2001 (2001-12-27) * paragraphs [0023] - [0046] * * figures 1,2 *	1,2,4-7, 9-11	INV. H04M15/28 H04M17/00 ADD. H04Q7/32 H04Q7/38
X	WO 00/70860 A (ERICSSON, INC) 23 November 2000 (2000-11-23) * page 8, line 6 - page 9, line 16 * * page 12, line 13 - page 17, line 17 * * figures 3,4,9,10,11A,11B *	1-9,11	
X	EP 1 528 781 A (BOUYGUES TELECOM) 4 May 2005 (2005-05-04) * paragraphs [0002], [0003], [0019] - [0032], [0034], [0040], [0045] * * figures 1-6 *	1-5,7-9	
X	WO 02/058326 A (TELEFONAKTIEBOLAGET L M ERICSSON ; ERICSSON, ANDREAS) 25 July 2002 (2002-07-25) * page 3, line 13 - page 6, line 15 * * page 8, lines 9-25 * * figures 1-3 *	1,2,4-7, 9,11	TECHNICAL FIELDS SEARCHED (IPC) H04M H04Q
X	WO 2004/030390 A (BRIGHT STAR TECHNOLOGIES, INC; BEKANICH, JOSEPH) 8 April 2004 (2004-04-08) * page 15, line 22 - page 21, line 21 * * page 26, line 14 - page 27, line 20 * * figures 8-13 *	1-9,11	
X	US 2002/151293 A1 (TYSOR ARTHUR JAMES) 17 October 2002 (2002-10-17) * paragraphs [0022] - [0048] * * figures 3,5A,5B,6 *	1-3,5-8, 11	

-/--

1 The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	28 June 2006	Kanlis, A

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)

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 06 25 2276

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	WO 2006/000994 A (KONINKLIJKE PHILIPS ELECTRONICS N.V; MOTTE, STEFAAN; MASSCHELEIN, MARC) 5 January 2006 (2006-01-05) * page 3, line 31 - page 6, line 18 * -----	7,9,10	

TECHNICAL FIELDS SEARCHED (IPC)

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	28 June 2006	Kanlis, A

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

1

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 06 25 2276

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.

28-06-2006

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2001055961 A1	27-12-2001	CN 1305268 A	25-07-2001
		GB 2364213 A	16-01-2002
		HK 1036703 A1	30-06-2005
		JP 3509670 B2	22-03-2004
		JP 2001168916 A	22-06-2001
WO 0070860 A	23-11-2000	AT 303038 T	15-09-2005
		AU 4465100 A	05-12-2000
		CN 1361974 A	31-07-2002
		DE 60022181 D1	29-09-2005
		DE 60022181 T2	01-06-2006
		EP 1179262 A1	13-02-2002
		JP 2003500904 T	07-01-2003
		US 6493547 B1	10-12-2002
EP 1528781 A	04-05-2005	FR 2861942 A1	06-05-2005
WO 02058326 A	25-07-2002	JP 2004517586 T	10-06-2004
WO 2004030390 A	08-04-2004	NONE	
US 2002151293 A1	17-10-2002	NONE	
WO 2006000994 A	05-01-2006	NONE	

EPO FORM P0459

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

Electronic Acknowledgement Receipt	
EFS ID:	23538644
Application Number:	14667516
International Application Number:	
Confirmation Number:	5348
Title of Invention:	Network System With Common Secure Wireless Message Service Serving Multiple Applications on Multiple Wireless Devices
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	James E. Harris/Ann Taylor
Filer Authorized By:	James E. Harris
Attorney Docket Number:	RALEP007C11C4
Receipt Date:	18-SEP-2015
Filing Date:	24-MAR-2015
Time Stamp:	15:29:12
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	P007C11C4.pdf	614937 be1589fd87b69f15b0f7c041e0d30d268f2b6f1f	no	11
Warnings:					
Information:					

2	Foreign Reference	2066_Fujitsu.pdf	856885 72e75495c5d83e30e4fbefee0e38a1bb25a5405f	no	22
Warnings:					
Information:					
3	Foreign Reference	2067_Kyocera.pdf	641903 024bbc366c4ffca0d6206fd9400790e51cab71c3	no	27
Warnings:					
Information:					
4	Foreign Reference	2068_Citrix.pdf	14110049 6b5308424d6052f222f99c6297e0f2cd005b02d2	no	118
Warnings:					
Information:					
5	Foreign Reference	2069_CN1508734A.pdf	3021193 c8818fe2ac00cd927bb1eb76517cffb16566e7c4	no	24
Warnings:					
Information:					
6	Foreign Reference	2070_CA2688553.pdf	2542550 eaac858569669488781074475 9dc83d1126bb215	no	72
Warnings:					
Information:					
7	Foreign Reference	2071_EP1850575A1.pdf	306349 f0b875706a2088fd443e7a61ffec5c6632823551	no	18
Warnings:					
Information:					
8	Non Patent Literature	3044_Jing.pdf	233308 23bf275a591ba14bba9ea0e8edf96ff232de6df3	no	41
Warnings:					
Information:					
9	Non Patent Literature	3045_Rivadeneyra.pdf	140975 e344ac7c8eee7e286c50068b497b45c8a4dbefbe	no	11
Warnings:					
Information:					
10	Non Patent Literature	3046_loopt.pdf	380265 711a9ba25d7f71b9274655d90ad2022e3b79c85c	no	17
Warnings:					
Information:					

11	Non Patent Literature	3047_MobilInternet.pdf	168840 0ed6b3905753995265d6ebaf790a5696b8b5efb3	no	3
Warnings:					
Information:					
12	Non Patent Literature	3048_GoldCoast.pdf	164580 e7407b7a4570d9ebfc790e44249d0cdb07f36182	no	2
Warnings:					
Information:					
13	Non Patent Literature	3049_Richtel.pdf	92162 6eecd8013a6328084fb9f16f25afc3b9619c9dee	no	3
Warnings:					
Information:					
14	Non Patent Literature	3050_Kim.pdf	94063 d57c26581b209a675dcd915b2be9c9e56a005a1f	no	4
Warnings:					
Information:					
15	Non Patent Literature	3051_Koutsopoulou.pdf	113527 7992fa4c1d1306edb1de247f743fd1ce8b1f3e7d	no	9
Warnings:					
Information:					
16	Non Patent Literature	3052_Sun.pdf	102743 66e9aab3798130ba2a58b46d24cec206617531de	no	8
Warnings:					
Information:					
17	Non Patent Literature	3053_Sabat.pdf	389581 c6862777fa3e8b3a13a7509f02610e154cf4299d	no	31
Warnings:					
Information:					
18	Non Patent Literature	3054_Nuzman.pdf	580822 f0c09248f7c9794a5ea827b4d574c49719823113	no	19
Warnings:					
Information:					
		Total Files Size (in bytes):	24554732		

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/667,516	03/24/2015	Gregory G. Raleigh	RALEP007C11C4

CONFIRMATION NO. 5348

106963
Headwater Partners I LLC
555 Twin Dolphin Drive, Suite 310
Redwood Shores, CA 94065

PUBLICATION NOTICE

OC000000076323483

Title: Network System With Common Secure Wireless Message Service Serving Multiple Applications on Multiple Wireless Devices

Publication No.US-2015-0200882-A1
Publication Date:07/16/2015

NOTICE OF PUBLICATION OF APPLICATION

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

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

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

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

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

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

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	14667516
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C4

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	6578076	B1	2003-06-10	Putzolu, David Matthew	
	2	7084775	B1	2006-08-01	Smith, Michael R.	
	3	7133695	B2	2006-11-07	Beyda, William J.	
	4	7260382	B1	2007-08-21	Lamb et al.	
	5	7271765	B2	2007-09-18	Stilp et al.	
	6	7627872	B2	2009-12-01	Hebeler et al.	
	7	7684370	B2	2010-03-23	Kezys, Vytautas Robertas	
	8	7685530	B2	2010-03-23	Sherrard et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C4

	9	7760137	B2	2010-07-20	Martucci et al.	
	10	7843843	B1	2010-11-30	Albert L. Papp et al.	
	11	7925778	B1	2011-04-12	Wijnands et al.	
	12	7936736	B2	2011-05-03	Proctor, Jr. et al.	
	13	7937450	B2	2011-05-03	Janik, Craig M.	
	14	8010082	B2	2011-08-30	Sutaria et al.	
	15	8019846	B2	2011-09-13	ROELENS et al.	
	16	8050705	B2	2011-11-01	Sicher et al.	
	17	8086791	B2	2011-12-27	Caulkins, Jason	
	18	8103285	B2	2012-01-24	Kalhan, Amit	
	19	8155666	B2	2012-04-10	Alizadeh-Shabdiz, Farshid	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C4

	20	8233433	B2	2012-07-31	Kalhan, Amit	
	21	8259692	B2	2012-09-04	Bajko, Gabor	
	22	8406736	B2	2013-03-26	Das et al.	
	23	8489110	B2	2013-07-16	Frank et al.	
	24	8495181	B2	2013-07-23	Venkatraman et al.	
	25	8532610	B2	2013-09-10	Manning Cassett et al.	
	26	8571598	B2	2013-10-29	Valavi, John J.	
	27	8634425	B2	2014-01-21	Gorti et al.	
	28	8739035	B2	2014-05-27	Trethewey, Jim	
	29	8825109	B2	2014-09-02	Montemurro et al.	
	30	8831561	B2	2014-09-09	Sutaria et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C4

	31	8880047	B2	2014-11-04	Konicek et al.	
	32	8930238	B2	2015-01-06	Coffman et al.	
	33	8977284	B2	2015-03-10	Reed, Mark J.	
	34	9014973	B2	2015-04-21	Ruckart, John	

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	20040259534	A1	2004-12-23	Chaudhari et al.	
	2	20060072451	A1	2006-04-06	Ross, Alan D.	
	3	20070005795	A1	2007-01-04	Gonzalez, Ruben	
	4	20070293191	A1	2007-12-20	Mir et al.	
	5	20070294410	A1	2007-12-20	Pandya et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C4

	6	20080050715	A1	2008-02-28	Golczewski et al.	
	7	20080282319	A1	2008-11-13	Fontijn et al.	
	8	20090197612	A1	2009-08-06	Kiiskinen, Arto	
	9	20100151866	A1	2010-06-17	Karpov et al.	
	10	20110145920	A1	2011-06-16	Mahaffey et al.	
	11	20130326356	A9	2013-12-05	Zheng 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	101080055	CN	A	2007-11-28	Tencent Technology (Shenzhen) Co., Ltd.		☐
	2	101335666	CN	A	2008-12-31	Hangzhou H3C Technologies Co., Ltd.		☐
	3	1567818	CN	A	2005-01-19	Huawei Tech. Co. Ltd.		☐

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C4

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]
	1	Ahmed et al., "A Context-Aware Vertical Handover Decision Algorithm for Multimode Mobile Terminals and Its Performance," BenQ Mobile, Munich Germany; University of Klagenfurt, Klagenfurt, Austria; 2006	☐
	2	Kassar et al., "An overview of vertical handover decision strategies in heterogeneous wireless networks," ScienceDirect, University Pierre & Marie Curie, Paris, France, 6/5/2007	☐
	3	Sadeh et al., "Understanding and Capturing People's Privacy Policies in a Mobile Social Networking Application," ISR School of Computer Science, Carnegie Mellon University, 2007	☐
	4	Schiller et al., "Location-Based Services," The Morgan Kaufmann Series in Data Management Systems, 2004	☐

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	14667516
	Filing Date	2015-03-24
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C4

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.

☐ Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ None

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	/James E. Harris/	Date (YYYY-MM-DD)	2015-06-26
Name/Print	James E. Harris	Registration Number	40013

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] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 12/28 (2006.01)
H04L 29/06 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200710123501.9

[43] 公开日 2008 年 12 月 31 日

[11] 公开号 CN 101335666A

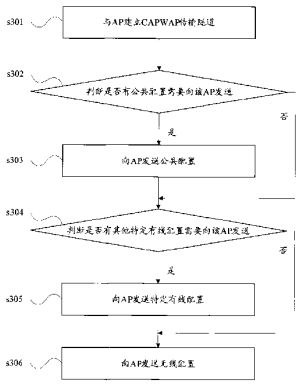
[22] 申请日 2007.6.29
[21] 申请号 200710123501.9
[71] 申请人 杭州华三通信技术有限公司
地址 310053 浙江省杭州市高新技术产业开发区之江科技工业园六和路 310 号华为杭州生产基地
[72] 发明人 史 扬 张志飞
[74] 专利代理机构 北京挺立专利事务所
代理人 龚家骅
权利要求书 3 页 说明书 13 页 附图 4 页

[54] 发明名称

一种配置发送的方法、接入控制设备和接入点

[57] 摘要

本发明公开了一种配置发送方法，包括如下步骤：接入点接入时，获取需要向所述接入点发送的至少一个配置文件，该配置文件中包括供接入点进行接入的配置信息；向接入点发送该配置文件。 本发明还提供了一种接入控制设备和接入点。 通过使用本发明，实现了 CAPWAP 能够灵活支持新的配置下发需求，特别是 ACL，Qos 等有线相关的配置需求，保证 CAPWAP 协议的扩展性，实现有线和无线网络的统一管理，同时避免因为扩展 TLV 带来的繁琐的工作。



1、一种配置发送方法，其特征在于，包括如下步骤：

接入点接入时，获取需要向所述接入点发送的至少一个配置文件，所述配置文件中包括供所述接入点进行接入的配置信息；

向所述接入点发送所述配置文件。

2、如权利要求 1 所述配置发送方法，其特征在于，所述配置文件为：

包括公共配置信息的公共配置文件、包括特定有线配置信息的有线配置文件中的至少一种。

3、如权利要求 1 所述配置发送方法，其特征在于，所述向接入点发送配置文件的步骤具体为：

将所述配置文件通过至少一个配置数据请求 CFG Data Request 消息向接入点发送；

接收到所述接入点响应的配置数据响应 CFG Data Response 消息时，若所述配置文件的发送未完成，继续发送下一 CFG Data Request 消息直至所述发送完成。

4、如权利要求 1 所述配置发送方法，其特征在于，所述向接入点发送配置文件的步骤具体为：

将所述配置文件预先存储在接入点能够连接的网络设备上；

通知所述接入点所述网络设备的地址，以供所述接入点获取所述配置文件。

5、如权利要求 1 所述配置发送方法，其特征在于，所述向接入点发送配置文件后还包括：

根据无线接入点控制与配置协议，在向所述接入点发送的协议消息中填加无线配置信息；

向所述接入点发送所述包括无线配置信息的协议消息。

6、一种配置发送方法，其特征在于，包括如下步骤：

获取接入控制设备发送的至少一个配置文件，所述配置文件中包括接入所述接入控制设备所需的配置信息；

根据所述配置文件中的配置信息，更新本地的配置。

7、如权利要求 6 所述配置发送方法，其特征在于，所述获取接入控制设备发送的配置文件的步骤具体为：

接收所述接入控制设备通过至少一个 CFG Data Request 消息发送的所述配置文件；

接收所述 CFG Data Request 消息完毕时，向所述接入控制设备响应 CFG Data Response 消息；

所述配置文件的发送未完成时，继续接收下一 CFG Data Request 消息并响应 CFG Data Response 消息直至所述发送完成。

8、如权利要求 6 所述配置发送方法，其特征在于，所述获取接收接入控制设备发送的配置文件的步骤具体为：

接收所述接入控制设备通知的存储有配置文件的网络设备的地址；

根据所述网络设备的地址，获取所述配置文件。

9、如权利要求 6 所述配置发送方法，其特征在于，在所述根据配置文件中的配置信息，更新本地的配置的步骤后，还包括步骤：

接收所述接入控制设备发送的包括无线配置信息的协议消息；

根据无线接入点控制与配置协议以及所述无线配置信息更新本地的无线配置。

10、一种配置发送方法，其特征在于，包括如下步骤：

接入点接入时，获取需要向所述接入点发送的至少一个配置文件，所述配置文件中包括供所述接入点进行接入的配置信息；

向所述接入点发送所述配置文件。

11、如权利要求 10 所述配置发送方法，其特征在于，所述配置文件中包括公共配置信息、有线配置信息、无线配置信息中的一种或多种。

12、一种接入控制设备，其特征在于，包括：

配置获取模块，用于接入点接入时，获取需要向所述接入点发送的至少一个配置文件；

配置发送模块，用于将所述配置获取模块获取的配置文件，向所述接入点发送。

13、如权利要求 12 所述接入控制设备，其特征在于，还包括:

配置存储模块，用于存储向接入点发送的配置文件，并在需要时向所述配置发送模块发送，所述配置文件中包括公共配置信息、有线配置信息、无线配置信息中的一种或多种。

14、如权利要求 12 所述接入控制设备，其特征在于，还包括:

接收模块，用于当所述配置发送模块通过CFG Data Request消息发送配置文件时，接收接入点响应的CFG Data Response消息并通知所述配置存储模块，以继续所述配置文件的发送直至完成。

15、一种接入点，其特征在于，包括:

终端获取模块，用于获取接入控制设备发送的至少一个配置文件;

终端配置模块，用于根据所述终端获取模块接收到的配置文件，更新本地的配置。

16、如权利要求 15 所述接入点，其特征在于，所述终端配置模块进一步包括:

解析子模块，用于解析所述配置文件并获得可执行的配置命令;

处理子模块，用于根据所述解析子模块获得的配置命令更新本地的配置。

17、如权利要求 15 所述接入点，其特征在于，还包括:

终端发送模块，用于接收来自接入控制设备的用来发送配置文件的 CFG Data Request 消息，并用于当所述终端获取模块完成对于接收接入控制设备发送的 CFG Data Request 消息的接收时，向所述接收接入控制设备响应 CFG Data Response 消息。

一种配置发送的方法、接入控制设备和接入点

技术领域

本发明涉及通信技术领域，尤其涉及一种配置发送的方法、接入控制设备和接入点。

背景技术

802.11 WLAN（Wireless Local Area Network，无线局域网）网络提供了一种局域网的无线连接服务。AP（Access Point，接入点）是无线局域网的一个重要组成设备，是一个无线收发设备，用于将从有线网络（例如 Internet）接收到的数据转换成无线信号发送，将接收到的无线信号转换成数据并转发到有线网络。

802.11 WLAN 网络目前已经广泛地应用于企业等用户。这些用户的 AP 设备数量多、安全敏感、对 Qos（Quality of Service，服务质量）有严格要求，需要有效地管理手段来保证网络可管理性，降低用户的操作管理成本。

针对企业用户的需求，IETF 组织成立了专门的 WG（Work Group，工作组）制定 CAPWAP（Configuration and Provisioning for Wireless Access Points，无效接入点控制与配置）协议草案，预计在很快将成为正式的标准。传统意义的 AP 如目前家庭普遍使用的 AP 设备，用于完成 802.11 协议定义的完整功能。CAPWAP WG 提出了 Fit AP 的概念，Fit AP 主要完成实时性功能如消息确认、发送 Beacon 帧等，而对 AP 的管理、用户认证等功能需要通过 AC（Access Controller，接入控制设备）协同完成。

CAPWAP 协议定义了 AP 和 AC 之间将建立控制和数据隧道来完成网络的控制和转发。在向无线用户提供接入之前，AC 必须完成对 AP 的参数配置以完成控制平面的建立。现有技术中 AC 向 AP 发送配置的流程如图 1 所示，包括:

步骤 s101、AP 向网络中广播 Discover Request（发现请求）消息，寻找

网络中存在的 AC。

此步骤为 AP 寻找 AC 的阶段。AP 以广播方式发送 Discover Request 消息，寻找网络中可以使用的 AC。

步骤 s102、接收到该 Discover Request 消息的 AC 向该 AP 返回 Discover Response（发现响应）消息。

AC 接收到 AP 的 Discover Request 消息后，向该 AP 发送 Discover Response 消息作为响应。

步骤 s103、AP 向 AC 发送 Join Request（加入请求）消息。

AP 接收到 AC 发送的 Discover Response 消息后，与该 AC 建立 DLTS（Datagram Transport Layer Security，数据报传输层安全性）连接，并向 AC 发送向 AC 发送 Join Request 消息。

步骤 s104、AC 向 AP 发送 Join Response（加入响应）消息。

AC 接收到 AP 的 Join Request 消息后，向该 AP 发送 Join Response 消息作为响应，通知 AP 可以开始对其提供服务。

步骤 s105、AC 与 AP 之间建立 CAPWAP 隧道。

步骤 s106～s107、AP 与 AC 之间通过 Configuration status request（配置状态请求）和 Configuration status Response（配置状态响应）消息进行交互，实现 AC 对 AP 的配置下发。

步骤 s108～s109、AP 与 AC 之间通过 Configuration Update Request（配置更新请求）和 Configuration Update Response（配置更新响应）消息进行交互，实现 AC 对 AP 的配置更新。

上述步骤 s106～s109 中，Configuration status request、Configuration status Response、Configuration Update Request 和 Configuration Update Response 消息中通过携带 TLV（Type Length Value，类项长度值）来实现对 Radio，WLAN service，Qos 等配置。CAPWAP 协议中定义的 TLV 格式如图 2 所示，其中 Type 项（16bit）和 Length 项（16bit）分别标识了 Value 一项中携带的内容和长度。

现有技术中这个配置方法主要是面向无线属性的配置，没有对有线相关属性的配置。而 WLAN 网络并不是一个独立于有线网络的另一个网络，特别

是当 AP 也进行本地数据转发，如即 CAWPAP 定义的 Local Bridge（本地桥接）模式），AP 需要知道整个网络中的 ACL（Access Control List，访问控制列表）、Qos 等策略。

如果对于有线相关的配置下发仍然通过扩展新的 TLV 方式来实现，必然增加很大工作量，而且 CAPWAP 要进行大量的 TLV 扩展。有线和无线配置紧密耦合的方式必然影响 CAPWAP 协议的扩展性。另外，在 TLV 的扩展上，特定的 TLV 扩展对应了特定的软件版本。而在配置时要求 AC 和 AP 同时支持相同版本的 TLV，如果 AC 和 AP 版本不配套将影响 TLV 配置的下发。因此在对 TLV 的扩展不是进行有线配置下发的有效方法。

发明内容

本发明要解决的问题是提供一种配置发送方法、接入控制设备和接入点，以实现 CAPWAP 协议下 AC 根据不同 AP 的需求向 AP 发送不同的有线和无线配置。

为达到上述目的，本发明实施例的技术方案提供一种配置发送方法，包括如下步骤：

接入点接入时，获取需要向所述接入点发送的至少一个配置文件，所述配置文件中包括供所述接入点进行接入的配置信息；

向所述接入点发送所述配置文件。

其中，所述配置文件为：

包括公共配置信息的公共配置文件、包括特定有线配置信息的有线配置文件中的至少一种。

其中，所述向接入点发送配置文件的步骤具体为：

将所述配置文件通过至少一个配置数据请求 CFG Data Request 消息向接入点发送；

接收到所述接入点响应的配置数据响应 CFG Data Response 消息时，若所述配置文件的发送未完成，继续发送下一 CFG Data Request 消息直至所述发送完成。

其中，所述向接入点发送配置文件的步骤具体为：

将所述配置文件预先存储在接入点能够连接的网络设备上；

通知所述接入点所述网络设备的地址，以供所述接入点获取所述配置文件。

其中，所述向接入点发送配置文件后还包括：

根据无线接入点控制与配置协议，在向所述接入点发送的协议消息中填加无线配置信息；

向所述接入点发送所述包括无线配置信息的协议消息。

本发明实施例的技术方案还提供一种在接入控制设备上执行的计算机程序，包括若干指令用以执行上述配置发送方法。

本发明实施例的技术方案还提供一种存储介质，存储上述在接入控制设备上执行的计算机程序。

本发明实施例的技术方案还提供一种计算机设备，包括用以执行上述配置发送方法的软件及与软件配合的硬件。

本发明实施例的技术方案还提供一种配置发送方法，包括如下步骤：

获取接入控制设备发送的至少一个配置文件，所述配置文件中包括接入所述接入控制设备所需的配置信息；

根据所述配置文件中的配置信息，更新本地的配置。

其中，所述获取接入控制设备发送的配置文件的步骤具体为：

接收所述接入控制设备通过至少一个 CFG Data Request 消息发送的所述配置文件；

接收所述 CFG Data Request 消息完毕时，向所述接入控制设备响应 CFG Data Response 消息；

所述配置文件的发送未完成时，继续接收下一 CFG Data Request 消息并响应 CFG Data Response 消息直至所述发送完成。

其中，所述获取接收接入控制设备发送的配置文件的步骤具体为：

接收所述接入控制设备通知的存储有配置文件的网络设备的地址；

根据所述网络设备的地址，获取所述配置文件。

其中，在所述根据配置文件中的配置信息，更新本地的配置的步骤后，还包括步骤:

接收所述接入控制设备发送的包括无线配置信息的协议消息;

根据无线接入点控制与配置协议以及所述无线配置信息更新本地的无线配置。

本发明实施例的技术方案还提供一种在接入点上执行的计算机程序，包括若干指令用以执行上述配置发送方法。

本发明实施例的技术方案还提供一种存储介质，存储上述在接入点上执行的计算机程序。

本发明实施例的技术方案还提供一种计算机设备，包括用以执行上述配置发送方法的软件及与软件配合的硬件。

本发明实施例的技术方案还提供一种配置发送方法，包括如下步骤:

接入点接入时，获取需要向所述接入点发送的至少一个配置文件，所述配置文件中包括供所述接入点进行接入的配置信息;

向所述接入点发送所述配置文件。

其中，所述配置文件中包括公共配置信息、有线配置信息、无线配置信息中的一种或多种。

本发明实施例的技术方案还提供一种接入控制设备，包括:

配置获取模块，用于接入点接入时，获取需要向所述接入点发送的至少一个配置文件;

配置发送模块，用于将所述配置获取模块获取的配置文件，向所述接入点发送。

其中，还包括:

配置存储模块，用于存储向接入点发送的配置文件，并在需要时向所述配置发送模块发送，所述配置文件中包括公共配置信息、有线配置信息、无线配置信息中的一种或多种。

其中，还包括:

接收模块，用于当所述配置发送模块通过CFG Data Request消息发送配置

文件时，接收接入点响应的CFG Data Response消息并通知所述配置存储模块，以继续所述配置文件的发送直至完成。

本发明实施例的技术方案还提供一种接入点，包括：

终端获取模块，用于获取接入控制设备发送的至少一个配置文件；

终端配置模块，用于根据所述终端获取模块接收到的配置文件，更新本地的配置。

其中，所述终端配置模块进一步包括：

解析子模块，用于解析所述配置文件并获得可执行的配置命令；

处理子模块，用于根据所述解析子模块获得的配置命令更新本地的配置。

其中，还包括：

终端发送模块，用于接收来自接入控制设备的用来发送配置文件的 CFG Data Request 消息，并用于当所述终端获取模块完成对于接收接入控制设备发送的 CFG Data Request 消息的接收时，向所述接收接入控制设备响应 CFG Data Response 消息。

本发明实施例的技术方案还提供一种网络，包括前述的接入控制设备以及前述的接入点。

与现有技术相比，本发明具有以下优点：

实现了 CAWPAP 能够灵活支持新的配置下发需求，特别是 ACL，Qos 等有线相关的配置需求，保证 CAPWAP 协议的扩展性，实现有线和无线网络的统一管理，同时避免因为扩展 TLV 带来的繁琐的工作。

附图说明

图 1 是现有技术中 AC 向 AP 发送配置的流程图；

图 2 是现有技术中 CAPWAP 协议中定义的 TLV 格式示意图；

图 3 是本发明的实施例中配置发送方法的流程图；

图 4 是本发明的实施例中 CAPWAP 协议控制消息的格式示意图；

图 5 是本发明的实施例中 AC 与 AP 间配置发送的信令流程图；

图 6 是本发明的实施例中接入控制设备的结构示意图；

图 7 是本发明的实施例中接入点的结构示意图。

具体实施方式

以下结合附图和实施例，对本发明的实施方式做进一步说明。

本发明中的实施例中，将AC向AP发送配置的过程分为了三个部分:

第一部分为向AP发送公共配置。该公共配置为所有的AP在配置时都会使用的相同配置，主要包括有线配置，也可能包括部分无线配置。对于这部分配置可以存储在一个公共配置文件中。

第二部分为向AP发送有线配置。

对于特定的AP，除了公共配置外，可能还存在其他特别的有线配置。该有线配置可以根据AC对不同AP的控制策略在配置内容上有所不同，因此需要保存为不同的配置文件。或因不同厂商的AP支持的配置命令格式不同，而需要保存为不同的配置文件。AC可以将使用同一配置格式及配置策略的配置保存在独立的配置文件中，并在需要时独立下发，从而管理支持不同配置方式的AP。

第三部分为向AP发送无线配置。

该部分即当前的CAPWAP协议过程，具体的，AC可以通过与AP的消息交互，如通过在Configuration Status Request/Configuration Status Response，Configuration Update Request/Configuration Update Response中携带相关的无线配置的TLV，实现无线配置的发送。

以上三个配置发送过程对于特定的AP不一定全部存在，如对于某些AP可能不需要进行公共配置的发送，对于另外的某些AP可能不需要进行特定有线配置的发送。

本发明的实施例中一种配置发送的方法以AC对AP依次进行公共配置、有线配置、无线配置的发送为例，其中公共配置和有线配置的发送位于AC与AP的Join过程后、通过Configuration Status Request/Configuration Status Response消息交互进行无线配置下发前。如图3所示，该配置发送包括以下步骤:

步骤s301、AC与AP建立CAPWAP隧道。

步骤s302、AC判断是否有公共配置需要向AP发送，需要发送时进行步骤s303，否则进行步骤s304。

对于被管理的AP，像ACL，Qos等策略配置（一般称为全局配置），与该AC相连接的所有AP一般会共用相同的配置。这些配置，可以保存在一个公共配置文件中，如appublic.cfg，并在AP与AC建立CAPWAP隧道后，作为第一个配置下发给AP。

在该公共配置文件的格式上，可以采用文本文件txt的格式。在该文件中包括对不同的项的具体设置。例如在文件中，对于每一需要进行配置的公共配置中的内容，通过Type和Value项进行表示。其中Type项表示Value一项中所携带的内容的标识，Value项表示具体的配置内容。例如，假设在预先设置的公共配置编制规则中ACL的标识为4096，则需要在公共配置中进行ACL的设置时，将Type项设置为4096，并在Value项中携带需要向AP发送的ACL内容。AP在接收到该公共配置文件后，可以根据Type项的值得知该配置是对ACL的配置，并根据Value项的值对ACL进行配置。当然也可直接通过字符串对不同的配置内容进行标识，并通过Value项的值携带具体的配置。

步骤s303、AC向AP发送该公共配置。

在该公共配置的发送方式上，可以采取以下方式:

方式一: AC可以将appublic.cfg通过多个CFG Data request（配置数据请求）消息发送给AP。

每次AP收到消息后，向AC发送CFG Data response（配置数据响应）消息确认收到了配置。完成配置文件传输后，AP执行配置文件更新本地配置。

该CFG Data request消息和CFG Data response消息的格式可以参考现有CAPWAP协议中的控制消息的格式。现有CAPWAP协议中的控制消息的格式如图4所示，包括Message Type（消息类型）项、Sequence Number（顺序号）项、Message Element Length（消息信元长度）项、Flags（标识）项以及Message Element（消息信元）项。其中，通过Message Type项标识了控制消息的类型与功能，Sequence Number项用于对接收到的Request消息和返回的Response消息进行对应，Message Element Length项为Message Element项的长度，Flags项

为0，Message Element项为控制消息的相关具体内容。对于Message Type项，现有的CAPWAP协议中已经对一些控制消息进行了定义，如1代表Discovery Request消息，2代表Discovery Response消息等，因此通过扩展该Message Type项并使用新的标识，可以对CFG Data Request和CFG Data Response消息进行定义。

进行消息类型的定义后，AC可以根据和AP预先约定的发送方式，将公共配置向AP发送，例如AC约定每次向AP发送1000bit的内容，则AC将公共配置文件中前1000bit的内容添加在CFG Data Request消息中向AP发送，并在消息的末尾设置标识位。AP接收该CFG Data Request消息完毕后，向AC发送CFG Data Response消息作为响应。接收到该消息后，AC继续向通过CFG Data Request消息向AP发送公共配置，直至所有的公共配置发送完成。

方式二：AC可以通知AP通过其他协议，如tftp（Trivial File Transfer Protocol，普通文件传输协议）协议或ftp（File Transfer Protocol，文件传输协议）协议来获得公共配置。具体的，AC可以通知AP存储有该公共配置文件的tftp或ftp服务器的地址，以及可能需要的登录密码，由AP登录该tftp或ftp服务器，下载配置文件后，执行该配置文件更新本地配置。

步骤s304、AC判断是否有其他特定有线配置需要向该AP发送，需要发送时进行步骤s305，否则进行步骤s306。

除了公共配置外，对于特定的AP还可能还有其他特定有线配置。这些配置并不属于公共配置，可以保存在一个独立的配置文件，该配置文件名称可以对应AP的标示，如AP + AP序列号.cfg。

这些独立的配置文件可以保证系统的兼容性，例如当网络中出现不同厂商的AP，而这些AP支持不同的配置方式（配置文件格式）。系统可以把这些AP的配置保存在各自独立的配置文件中。通过这些不同AP配置的独立下发，可以实现AC同时管理来不同厂商的AP。

步骤s305、AC向AP发送该有线配置。

在该有线配置的发送方式上，可以参考步骤s303中AC在发送公共配置时所采取的不同发送方式。AP在接收到该有线配置文件后，执行该配置文件更

新本地配置。至此，AP完成了公共配置和有线配置的流程。

步骤s306、AC向AP发送无线配置。

该步骤中，通过当前CAPWAP协议中已经定义的与无线相关配置对应的TLV，AC与AP交互Configuration status request、Configuration status Response、Configuration Update Request或Configuration Update Response等消息实现对Radio、WLAN service、Qos等与无线相关的配置。AP收到配置后，更新本地无线配置。至此，AC向AP发送配置的流程结束。

上述实施例中AC对AP依次进行公共配置、有线配置、无线配置的信令流程图如图5所示，

步骤 s501、AP 向网络中广播 Discover Request 消息，寻找网络中存在的 AC。

步骤 s502、接收到该 Discover Request 消息的 AC 向该 AP 返回 Discover Response 消息。

步骤 s503、AP 向 AC 发送 Join Request 消息。

步骤 s504、AC 向 AP 发送 Join Response 消息。

步骤 s505、AC 与 AP 之间建立 CAPWAP 隧道。

步骤 s506～s507、AC 与 AP 之间通过 CFG Data Request 和 CFG Data Response 消息进行交互，实现公共配置和特定有线配置的下发。

步骤 s508～s509、AP 与 AC 之间通过 Configuration status request 和 Configuration status Response 消息进行交互，实现 AC 对 AP 的无线配置下发。

步骤 s510～s511、AP 与 AC 之间通过 Configuration Update Request 和 Configuration Update Response 消息进行交互，实现 AC 对 AP 的无线配置更新。

在上述实施例中，以AC对AP依次进行公共配置、有线配置、无线配置的下发为例，描述了本发明中一种发送配置的方法。该配置发送的顺序主要是基于一般情况下发送配置的顺序，即先公共配置后特定配置、先有线配置后无线配置。但是，在发送配置时所采用的顺序不限于以上顺序。另外，在不同的配置发送步骤，还需要考虑不同配置间的关系。以上述实施例为例，AC需要考虑对于某些AP只发送其特定的有线配置即可，而不需要下公共配置。

另外，在公共配置与特定的有线配置存在冲突时，应该通过设定优先级关系或修改配置文件以达到避免配置冲突的问题。

通过使用上述实施例中提供的配置发送方法，实现了CAWPAP能够灵活支持新的配置下发需求，特别是ACL，Qos等有线相关的配置需求，保证CAPWAP协议的扩展性，实现有线和无线网络的统一管理，同时避免因为扩展TLV带来的繁琐的工作。

本发明的另一实施例中，提供了一种接入控制设备，如图6所示，包括:

配置存储模块10，用于存储需要向AP发送的配置文件。该配置文件具体为：包括公共配置信息的公共配置文件，以及包括特定有线配置的有线配置文件。其中，公共配置文件一般只有一个，其中主要包括有线配置，也可能同时包括无线设置。而有线配置文件可能很多，其文件个数由所需要的不特定有线配置的数量而定，不同的特定有线配置存储在不同的有线配置文件中。在具体的实现中，该存储模块10可能为AC上的存储实体，也可能为AC之外的tftp或ftp服务器等存储实体。

配置获取模块20，用于对不同的AP的状态，获取需要向该AP发送的公共配置和/或有线配置。并将需要向该AP发送的公共配置和/或特定有线配置通知配置发送模块30。

配置发送模块30，用于在接收到配置获取模块20发送的需要向AP发送的公共配置或特定的有线配置时，向AP发送该公共配置或特定的有线配置。发送方式从配置存储模块10中获取需要发送的内容并通过CFG Data Request消息发送；或在配置存储模块10为外部tftp或ftp服务器等存储实体时，通知AP该存储该公共配置或特定有线配置的服务器的地址。

接收模块 40，用于当配置发送模块 30 通过 CFG Data Request 消息发送有线配置时，接收接入点响应的 CFG Data Response 消息。并通知配置发送模块30，以继续公共配置或特定有线配置的发送直至完成。

本发明的另一实施例中，还提供了一种接入点，如图7所示，包括:

终端获取模块 50，用于接收接入控制设备发送的配置文件。获取方法可以为接收接入控制设备发送的 CFG Data Request 消息，或从接收接入控制设

备通知的网络设备通过 tftp 或 ftp 协议获取。

终端配置模块 60，用于根据终端获取模块 50 接收到的配置文件，更新本地的配置。该模块进一步包括解析子模块 61，用于解析配置文件并获得可执行的配置命令；以及处理子模块 62，用于根据解析子模块 61 获得的配置命令更新本地的配置。

终端发送模块 70，用于终端获取模块 50 完成对于接收接入控制设备发送的 CFG Data Request 消息的接收时，向接收接入控制设备响应 CFG Data Response 消息。

通过使用以上实施例所提供的接入控制设备和接入点，实现了 CAWPAP 能够灵活支持新的配置下发需求，特别是 ACL，Qos 等有线相关的配置需求，保证 CAPWAP 协议的扩展性，实现有线和无线网络的统一管理，同时避免因为扩展 TLV 带来的繁琐的工作。

以上方式中，仍然是通过在 Configuration Status Request/Configuration Status Response，Configuration Update Request/Configuration Update Response 中携带相关的无线配置的 TLV，实现无线配置的发送。这样做可以和现有的 CAPWAP 协议相兼容，然而，无线配置部分同样可以纳入到公共配置和特定配置中来，无线配置不再特殊化处理，可以统一到一个公共配置及各个特有配置中，而各个特有配置也不在局限为特定有线配置。本发明通过将各种配置纳入到一个或者多个配置文件中然后下发给 AP，AP 接收以后解析这些文件获取其中的配置命令完成配置工作。其通过一次开发就可以解决以后所有新增配置的问题，因为无论新增什么配置，只需要把它纳入到配置文件中即可，AP 就可以通过解析文件获得配置。

通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到本发明可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本发明各个实

施例所述的方法。

以上公开的仅为本发明的几个具体实施例，但是，本发明并非局限于此，任何本领域的技术人员能思之的变化都应落入本发明的保护范围。

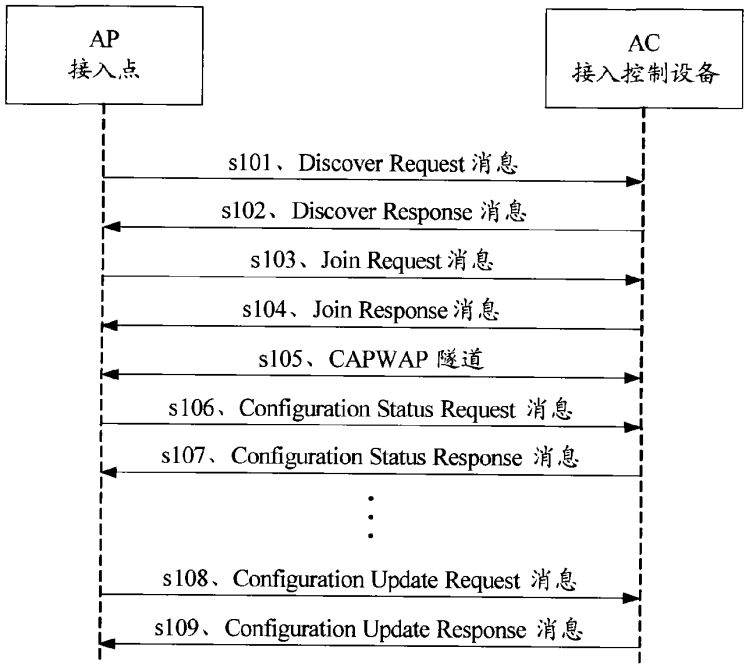

AP
接入点
AC
接入控制设备
s101、Discover Request 消息
s102、Discover Response 消息
s103、Join Request 消息
s104、Join Response 消息
s105、CAPWAP 隧道
s106、Configuration Status Request 消息
s107、Configuration Status Response 消息
s108、Configuration Update Request 消息
s109、Configuration Update Response 消息

图 1

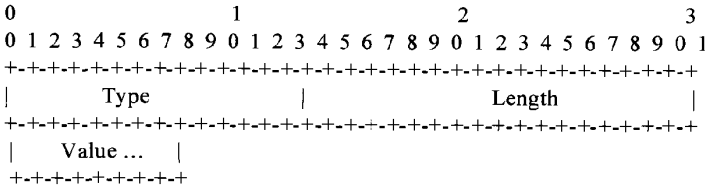

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Type
Length
Value ...

图 2

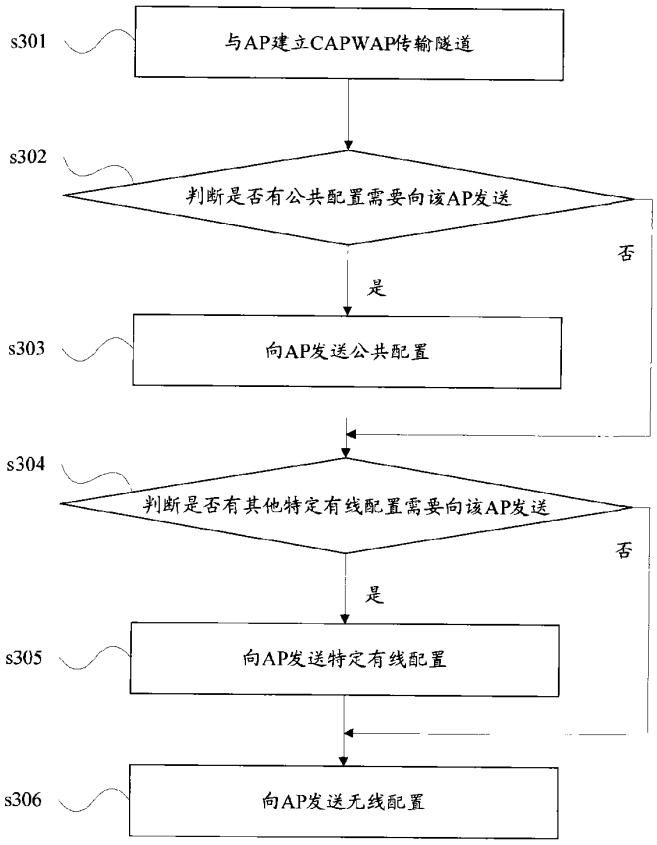

s301
与AP建立CAPWAP传输隧道
s302
判断是否有公共配置需要向该AP发送
否
是
s303
向AP发送公共配置
s304
判断是否有其他特定有线配置需要向该AP发送
否
是
s305
向AP发送特定有线配置
s306
向AP发送无线配置

图 3

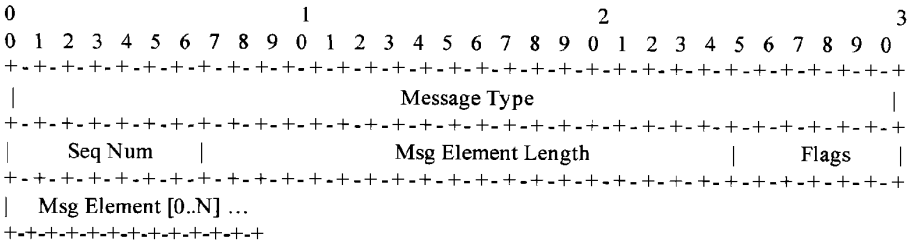

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Message Type
Seq Num
Msg Element Length
Flags
Msg Element [0..N] ...

图 4

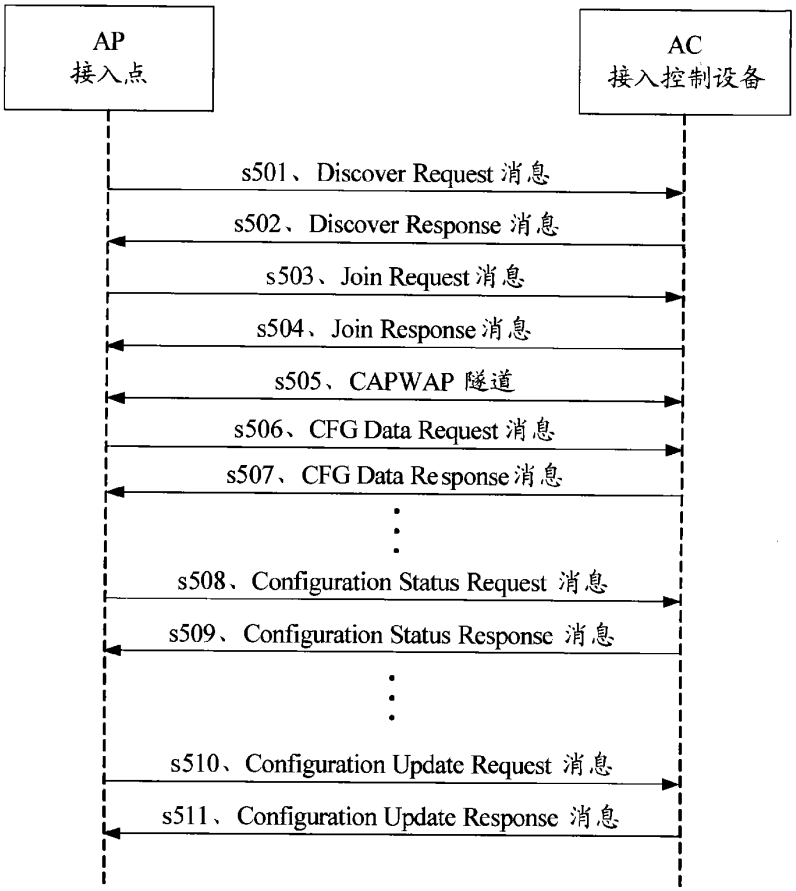

AP
接入点
AC
接入控制设备
s501、Discover Request 消息
s502、Discover Response 消息
s503、Join Request 消息
s504、Join Response 消息
s505、CAPWAP 隧道
s506、CFG Data Request 消息
s507、CFG Data Response 消息
s508、Configuration Status Request 消息
s509、Configuration Status Response 消息
s510、Configuration Update Request 消息
s511、Configuration Update Response 消息

图 5

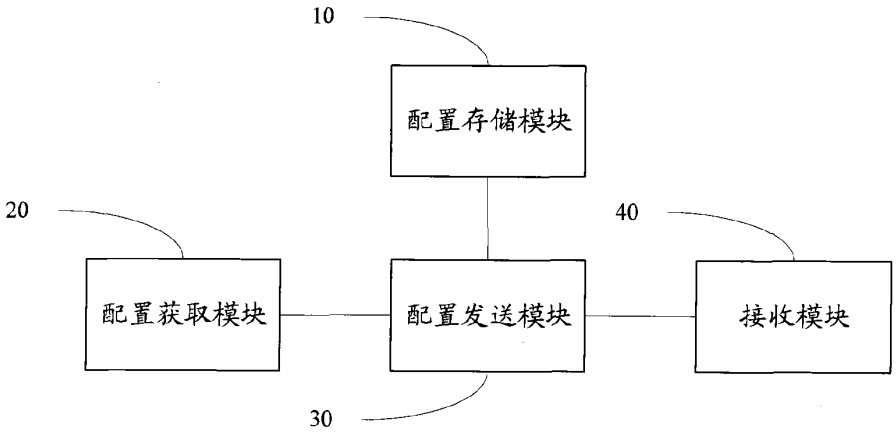

10
配置存储模块
20
40
配置获取模块
配置发送模块
接收模块
30

图 6

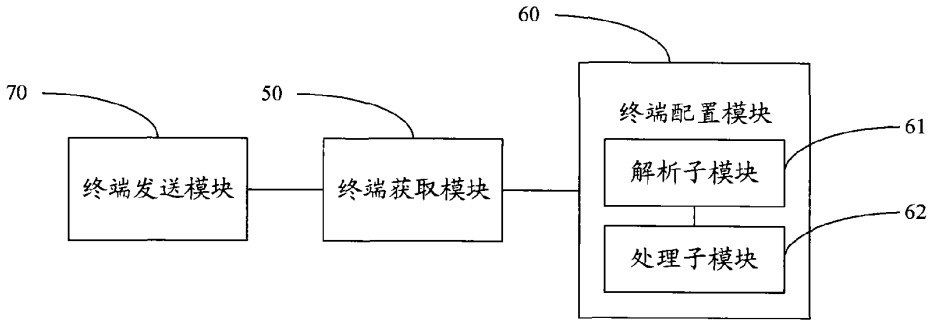

60
70
50
终端配置模块
61
终端发送模块
终端获取模块
解析子模块
62
处理子模块

图 7

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04Q 7/32 (2006.01)
H04M 1/247 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200610157819.4

[43] 公开日 2007 年 11 月 28 日

[11] 公开号 CN 101080055A

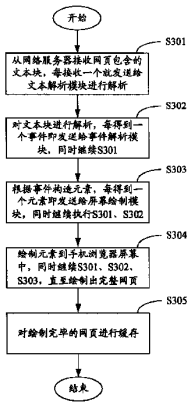
[22] 申请日 2006.12.21
[21] 申请号 200610157819.4
[71] 申请人 腾讯科技（深圳）有限公司
地址 518057 广东省深圳市高新科技园南区高新南一道飞亚达高科技大厦 5－10 层
[72] 发明人 纪 宇
[74] 专利代理机构 深圳市顺天达专利商标代理有限公司
代理人 郭伟刚 蔡晓红
权利要求书 4 页 说明书 12 页 附图 3 页

[54] 发明名称

一种基于手机浏览器快速浏览网页的方法、系统及设备

[57] 摘要

本发明涉及移动通信领域，提供了一种基于手机浏览器快速浏览网页的方法、系统及设备。 所述方法包括以下步骤：A. 所述手机浏览器利用其网络收发模块从网络服务器接收所述网页包含的文本块，且每接收到一个文本块就将其发送给文本解析模块；B. 对所接收到的文本块进行解析，得到与所述文本块对应的事件，且每解析得到一个事件即发送至事件处理模块，同时继续执行步骤 A；C. 根据所述文本块对应的事件构造元素，且每构造出一个元素即发送至屏幕绘制模块，同时继续执行步骤 A 和 B；D. 每接收到一个元素，就将其绘制到手机浏览器的屏幕中，同时继续执行步骤 A、B、C，直至绘制出完整网页。 本发明提高了手机浏览器浏览网页时的显示效率。



1、一种基于手机浏览器快速浏览网页的系统，包括手机浏览器和网络服务器，所述手机浏览器包括网络收发模块、文本解析模块、事件处理模块和屏幕绘制模块，其特征在于，所述网络收发模块、文本解析模块、事件处理模块和屏幕绘制模块以并行的方式运行，包括:

所述手机浏览器利用其网络收发模块从所述网络服务器接收所述网页包含的文本块，且每接收到一个文本块就将其发送给所述手机浏览器中的文本解析模块;

所述文本解析模块与所述网络收发模块相连，对所接收到的文本块进行解析并得到与所述文本块对应的事件，且每解析得到一个事件即发送至事件处理模块中，同时网络收发模块继续接收文本块;

所述事件处理模块与所述文本解析模块相连，根据所述文本块对应的事件构造元素，且每构造出一个元素即发送至屏幕绘制模块，同时网络收发模块继续接收文本块，且文本解析模块继续对所接收到的文本块进行解析;

所述屏幕绘制模块每接收到一个元素，就将其绘制到手机浏览器的屏幕中，同时网络收发模块继续接收文本块，且文本解析模块继续对所接收到的文本块进行解析，以及事件处理模块根据继续根据所接收到的文本块对应的事件构造新的元素。

2、根据权利要求1所述的基于手机浏览器快速浏览网页的系统，其特征在于，所述手机浏览器进一步包括缓存模块，所述缓存模块与所述屏幕绘制模块相连，用于缓存所述屏幕绘制模块绘制的网页。

3、一种手机浏览器，包括网络收发模块、文本解析模块、事件处理模块

和屏幕绘制模块，其特征在于，所述网络收发模块、文本解析模块、事件处理模块和屏幕绘制模块以并行的方式运行，包括:

所述手机浏览器利用其网络收发模块从网络服务器接收所述网页包含的文本块，且每接收到一个文本块就将其发送给所述手机浏览器中的文本解析模块;

所述文本解析模块与所述网络收发模块相连，对所接收到的文本块进行解析并得到与所述文本块对应的事件，且每解析得到一个事件即发送至事件处理模块中，同时网络收发模块继续接收文本块;

所述事件处理模块与所述文本解析模块相连，根据所述文本块对应的事件构造元素，且每构造出一个元素即发送至屏幕绘制模块，同时网络收发模块继续接收文本块，且文本解析模块继续对所接收到的文本块进行解析;

所述屏幕绘制模块每接收到一个元素，就将其绘制到手机浏览器的屏幕中，同时网络收发模块继续接收文本块，且文本解析模块继续对所接收到的文本块进行解析，以及事件处理模块根据继续根据所接收到的文本块对应的事件构造新的元素。

4、根据权利要求3所述的手机浏览器，其特征在于，所述手机浏览器进一步包括缓存模块，所述缓存模块与所述屏幕绘制模块相连，用于缓存所述屏幕绘制模块绘制出的网页。

5、根据权利要求3或4所述的手机浏览器，其特征在于，所述手机浏览器设置有至少一个流量控制模式，用于限制所述手机浏览器在访问网页时所要下载文件的大小。

6、一种基于手机浏览器快速浏览网页的方法，其特征在于，所述方法包括以下步骤:

A.所述手机浏览器利用其网络收发模块从网络服务器接收所述网页包含的文本块，且每接收到一个文本块就将其发送给所述手机浏览器中的文本解析模块；

B.所述文本解析模块对所接收到的文本块进行解析，得到与所述文本块对应的事件，且每解析得到一个事件即发送至事件处理模块中，同时继续执行步骤A；

C.所述事件处理模块根据所述文本块对应的事件构造元素，且每构造出一个元素即发送至屏幕绘制模块，同时继续执行步骤A和B；

D.所述屏幕绘制模块每接收到一个元素，就将其绘制到手机浏览器的屏幕中，同时继续执行步骤A、B、C，直至绘制出完整网页。

7、根据权利要求6所述的基于手机浏览器快速浏览网页的方法，其特征在于，所述步骤B中对文本块进行解析并得到对应事件的过程包括：

B1.从所述文本块中检测到一个文档开始标记，则产生一个开始文档树事件；

B2.继续检测到一个Tag开始标记，则产生一个开始元素事件；

B3.继续检测到一个Tag结束标记，则产生一个结束元素事件；

B4.当检测到一个文档结束标记，则产生一个结束文档树事件，并将所生成的事件发送给所述手机浏览器的事件处理模块进行处理。

8、根据权利要求7所述的基于手机浏览器快速浏览网页的方法，其特征在于，所述步骤C中根据事件构造元素的过程包括：

C1.当收到所述开始文档树事件，则新建一个文档树，并设置当前游标为所述文档树的根节点；

C2.当收到所述开始元素事件，则生成一个新的元素，并将其设置为当前

游标节点的子节点;

C3.当收到所述结束元素事件，则计算当前游标元素的Rect，若所述游标元素的Rect与屏幕Rect存在交集，则产生绘制元素事件;

C4.当收到所述结束文档树事件，则结束当前线程，并将所生成的元素发送到所述手机浏览器的屏幕绘制模块进行绘制。

9、根据权利要求6所述的基于手机浏览器快速浏览网页的方法，其特征在于，所述方法在步骤D之后进一步包括:

E.将所绘制出的网页的对象树存储到所述手机浏览器中，用于用户再次访问时的提取显示。

10、根据权利要求6所述的基于手机浏览器快速浏览网页的方法，其特征在于，所述方法在步骤A之前进一步包括：对所述手机进行内存检测，若内存不足则释放缓存。

一种基于手机浏览器快速浏览网页的方法、系统及设备

技术领域

本发明涉及移动通信领域，更具体地说，涉及一种基于手机浏览器快速浏览网页的方法、系统及设备。

背景技术

随着因特网和移动通信技术的发展和融合，利用手机浏览器浏览网页已日益普及。

现有技术实现手机浏览器浏览网页所采取的方式是，首先下载完显示网页所需的全部文本及图片信息，然后在浏览器中统一显示。由于该现有技术的下载方式受限于网络速度，往往会导致网页显示得非常慢。

另一现有技术则采取将文本图片分步下载并显示的方式，也即：首先下载完文本文件，显示文本文件，然后下载图片，最后再显示完整的网页。该现有技术相对于前一技术，在网页显示效率方面有所提高，但仍不乐观。

因此需要一种新的方法，能够通过手机浏览器快速浏览网页。

发明内容

本发明的目的在于提供一种基于手机浏览器快速浏览网页的系统，旨在解决现有技术在利用手机浏览器浏览网页时显示效率低下的问题。

本发明的目的还在于提供一种基于手机浏览器快速浏览网页的设备，以更好地解决现有技术中存在的上述问题。

本发明的目的还在于提供一种基于手机浏览器快速浏览网页的方法，以更好地解决现有技术中存在的上述问题。

为了实现发明目的，所述基于手机浏览器快速浏览网页的系统包括手机浏览器和网络服务器，所述手机浏览器包括网络收发模块、文本解析模块、事件处理模块和屏幕绘制模块，所述网络收发模块、文本解析模块、事件处理模块和屏幕绘制模块以并行的方式运行，包括：

所述手机浏览器利用其网络收发模块从所述网络服务器接收所述网页包含的文本块，且每接收到一个文本块就将其发送给所述手机浏览器中的文本解析模块；

所述文本解析模块对所接收到的文本块进行解析，得到与所述文本块对应的事件，且每解析得到一个事件即发送至事件处理模块中，同时网络收发模块继续接收文本块；

所述事件处理模块根据所述文本块对应的事件构造元素，且每构造出一个元素即发送至屏幕绘制模块，同时网络收发模块继续接收文本块，且文本解析模块继续对所接收到的文本块进行解析；

所述屏幕绘制模块每接收到一个元素，就将其绘制到手机浏览器的屏幕中，同时网络收发模块继续接收文本块，且文本解析模块继续对所接收到的文本块进行解析，以及事件处理模块根据继续根据所接收到的文本块对应的事件构造新的元素。

所述手机浏览器进一步包括缓存模块，所述缓存模块与所述屏幕绘制模块相连，用于缓存所述屏幕绘制模块绘制的网页。

为了更好地实现发明目的，所述手机浏览器包括网络收发模块、文本解析模块、事件处理模块和屏幕绘制模块，所述网络收发模块、文本解析模块、事

件处理模块和屏幕绘制模块以并行的方式运行，包括:

所述手机浏览器利用其网络收发模块从网络服务器接收所述网页包含的文本块，且每接收到一个文本块就将其发送给所述手机浏览器中的文本解析模块;

所述文本解析模块对所接收到的文本块进行解析，得到与所述文本块对应的事件，且每解析得到一个事件即发送至事件处理模块中，同时网络收发模块继续接收文本块;

所述事件处理模块根据所述文本块对应的事件构造元素，且每构造出一个元素即发送至屏幕绘制模块，同时网络收发模块继续接收文本块，且文本解析模块继续对所接收到的文本块进行解析;

所述屏幕绘制模块每接收到一个元素，就将其绘制到手机浏览器的屏幕中，同时网络收发模块继续接收文本块，且文本解析模块继续对所接收到的文本块进行解析，以及事件处理模块根据继续根据所接收到的文本块对应的事件构造新的元素。

所述手机浏览器进一步包括缓存模块，所述缓存模块与所述屏幕绘制模块相连，用于缓存所述屏幕绘制模块绘制出的网页。

所述手机浏览器设置有至少一个流量控制模式，用于限制所述手机浏览器在访问网页时所要下载文件的大小。

为了更好地实现发明目的，所述基于手机浏览器快速浏览网页的方法包括以下步骤:

A.所述手机浏览器利用其网络收发模块从网络服务器接收所述网页包含的文本块，且每接收到一个文本块就将其发送给所述手机浏览器中的文本解析模块;

B.所述文本解析模块对所接收到的文本块进行解析，得到与所述文本块对应的事件，且每解析得到一个事件即发送至事件处理模块中，同时继续执行步骤A;

C.所述事件处理模块根据所述文本块对应的事件构造元素，且每构造出一个元素即发送至屏幕绘制模块，同时继续执行步骤A和B;

D.所述屏幕绘制模块每接收到一个元素，就将其绘制到手机浏览器的屏幕中，同时继续执行步骤A、B、C，直至绘制出完整网页。

所述步骤B中对文本块进行解析并得到对应事件的过程包括:

B1.从所述文本块中检测到一个文档开始标记，则产生一个开始文档树事件;

B2.继续检测到一个Tag开始标记，则产生一个开始元素事件;

B3.继续检测到一个Tag结束标记，则产生一个结束元素事件;

B4.当检测到一个文档结束标记，则产生一个结束文档树事件，并将所生成的事件发送给所述手机浏览器的事件处理模块进行处理。

所述步骤C中根据事件构造元素的过程包括:

C1.当收到所述开始文档树事件，则新建一个文档树，并设置当前游标为所述文档树的根节点;

C2.当收到所述开始元素事件，则生成一个新的元素，并将其设置为当前游标节点的子节点;

C3.当收到所述结束元素事件，则计算当前游标元素的Rect，若所述游标元素的Rect与屏幕Rect存在交集，则产生绘制元素事件;

C4.当收到所述结束文档树事件，则结束当前线程，并将所生成的元素发送到所述手机浏览器的屏幕绘制模块进行绘制。

所述方法在步骤D之后进一步包括:

E.将所绘制出的网页的对象树存储到所述手机浏览器中，用于用户再次访问时的提取显示。

所述方法在步骤A之前进一步包括：对所述手机进行内存检测，若内存不足则释放缓存。

本发明通过将文本流转换成事件流，并利用手机浏览器中的各个模块以并行的方式对各事件进行解析、处理和绘制，从而提高了手机浏览器浏览网页时的显示效率；另外将所绘制的网页以对象树的形式进行缓存，进一步提高了网页的显示效率；此外还通过检查内存和进行流量控制，保证了浏览的安全性。

附图说明

图1是本发明中基于手机浏览器快速浏览网页的系统结构图;

图2是本发明中基于手机浏览器快速浏览网页的实现示意图;

图3是本发明中基于手机浏览器快速浏览网页的方法流程图。

具体实施方式

为了使本发明的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

在本发明中，手机浏览器利用其网络收发模块从网络服务器接收网页包含的文本块，且每接收到一个文本块就将其发送给手机浏览器中的文本解析模块；文本解析模块对所接收到的文本块进行解析，得到与文本块对应的事件，且每解析得到一个事件即发送至事件处理模块中，同时网络收发模块继续接收

文本块；事件处理模块根据文本块对应的事件构造元素，且每构造出一个元素即发送至屏幕绘制模块，同时网络收发模块继续接收文本块，且文本解析模块继续对所接收到的文本块进行解析；屏幕绘制模块每接收到一个元素，就将其绘制到手机浏览器的屏幕中，同时网络收发模块继续接收文本块，且文本解析模块继续对所接收到的文本块进行解析，以及事件处理模块根据继续根据所接收到的文本块对应的事件构造新的元素，直至绘制出完整网页。这种并行处理的方式极大地提高了手机浏览器浏览网页时的显示效率。

图1示出了本发明中基于手机浏览器快速浏览网页的系统结构，包括手机浏览器100和网络服务器200。

其中网络服务器200用于存储网络数据，并当用户通过手机浏览器100发送网页访问请求时，将该网页所包含的网络数据以文本块的形式返回给手机浏览器100。

手机浏览器100包括网络收发模块101、文本解析模块102、事件处理模块103、屏幕绘制模块104和缓存管理模块105，其中：

（1）网络收发模块101与网络服务器200之间进行通信，当用户期望浏览一个网页时，其根据用户的操作发送网页访问请求给网络服务器200，并接收返回的文本块形式的网页数据，然后将网页数据的这些文本块转发至文本解析模块102中进行处理。

（2）文本解析模块102与网络收发模块101和事件处理模块103相连，用于对网络收发模块101转发的文本块进行解析，得到相应的事件。本发明中并不是在网络收发模块101接收完网页的所有数据之后才将其发送到文本解析模块102中进行解析，而是在网络收发模块101接受完第一文本块之后就将其发送给

文本解析模块102，文本解析模块102立刻解析该第一文本块，得到与其对应的第一事件。在文本解析模块102对第一文本块进行解析的同时，网络收发模块101继续接收其他文本块。

（3）事件处理模块103与文本解析模块102、屏幕绘制模块104相连，用于对文本解析模块102解析得到的事件进行进一步处理，构造出与事件对应的元素。本发明中也并不是在文本解析模块102解析完所有的文本块之后才开始进行事件处理，而是在文本解析模块102解析得到第一事件之后就将该第一事件发送给事件处理模块103，事件处理模块103立刻处理该第一事件，构造其对应的第一元素。在事件处理模块103构造第一元素的同时，网络收发模块101继续接收其他文本块，且文本解析模块102继续对接收到的其他文本块进行解析。

（4）屏幕绘制模块104与事件处理模块103和缓存管理模块105相连，用于将事件处理模块103构造得到的元素绘制到手机浏览器100的屏幕上，直至最终绘制出完整的网页。本发明中也并不是在事件处理模块103构造出所有元素之后才开始进行绘制，而是在事件处理模块103构造出第一元素之后就将该第一元素发送给屏幕绘制模块104，屏幕绘制模块104立刻对该第一元素进行判断，若该第一元素的Rect值与屏幕Rect存在交集，则将该第一元素绘制到手机浏览器100的屏幕上。在屏幕绘制模块104绘制第一元素的同时，网络收发模块101继续接收其他文本块，且文本解析模块102继续对接收到的其他文本块进行解析，以及事件处理模块103继续构造其他元素。按照以上的并行处理方式，最终可快速地绘制出完整网页。

关于网络收发模块101、文本解析模块102、事件处理模块103、屏幕绘制模块104相互协作并行处理的具体过程，可参考附图2。

（5）缓存管理模块105与屏幕绘制模块104相连，用于缓存屏幕绘制模块

104所绘制出的网页的对象树，当用户再次访问该网页时则可根据该缓存管理模块105中的网页的对象树进行显示，进一步加快了网页显示的效率。

图2是本发明中基于手机浏览器100快速浏览网页的实现示意图。由该图可知，本发明中接收、解析、构造元素、绘制这四个步骤并不是单纯的串行处理：

各个模块内部所执行的操作是串行的，例如，网络收发模块101按时间顺序以串行方式接收各个文本块，文本解析模块102按时间顺序以串行方式对各个文本块进行解析并得到相应的事件，事件处理模块103按时间顺序以串行方式根据各个事件构造对应的元素，屏幕绘制模块104按时间顺序以串行方式将各元素绘制到手机浏览器100屏幕中的相应位置。

但是在整体上，各个模块对不同文本块的处理过程却是并行的，在本发明的其中一个实施例中，以图2进行说明如下：网络收发模块101接收到第一文本块并发送给文本解析模块102；当文本解析模块102对该第一文本块进行解析以得到第一事件的同时，网络收发模块101在接收第二文本块；当事件处理模块103根据第一事件构造第一元素的同时，网络收发模块101有可能正在接收第三文本块，且文本解析模块102则在对第二文本块进行解析；当屏幕绘制模块104将第一元素绘制到屏幕上的同时，网络收发模块101有可能正在接收第四文本块，且文本解析模块102则在对第三文本块进行解析，以及事件处理模块103正在根据第二事件构造第二元素。

利用以上的并行处理方式，可极大地提高网页显示的速度。例如，现有技术中显示一张网页时，需10秒钟读取完该网页包含的全部网络数据，3秒钟进行解析，3秒钟根据解析得到的事件构造出所有元素，5秒钟完成显示，则显示出来需要21秒。而在本发明中，若手机屏幕是128*128像素，用户访问的网页

经过排版后128像素宽、1024像素高，网络收发模块101只需要2秒钟左右可以读取128像素宽、128像素高的内容，其将此内容传递给文本解析模块102，文本解析模块102利用1秒钟完成解析，事件处理模块103用1秒钟构造元素，屏幕绘制模块104只需2秒钟完成绘制并显示，这样便只需要6秒钟就可以显示完占满用户手机屏幕的内容，在用户阅读内容的同时，继续作后续内容的收取、解析、构造和绘制显示。

图3示出了本发明中基于手机浏览器100快速浏览网页的方法流程。

在执行所有步骤之前，当用户期望浏览一个网页时，则通过手机浏览器100发送网页访问请求，该网页访问请求通过手机浏览器100中的网络收发模块101发送至网络服务器200。

在步骤S301中，网络收发模块101接收网络服务器200返回的上述网页包含的HTTP数据，这些数据以文本块的形式传送给网络收发模块101，网络收发模块101再将所接收到的文本块转发至文本解析模块102中。本发明中网络收发模块101并不是接收完网页的全部数据之后才将其发送，而是每接收到一个文本块则将其发送给文本解析模块102进行处理，同时网络收发模块101继续接收该网页的其他文本块。步骤S301的具体过程包括：若网络收发模块101收取到一个新的网页文档，则产生一个新文档（new Document）事件，自身继续收取文档。本发明中，网络收发模块101收取到一个文本块，则产生一个新文本块（new Document Block）事件，并将其立即发送给文本解析模块102进行解析。收取完所有文本块，则产生一个结束文档（end Document）事件，结束自己的线程。

在步骤S302中，文本解析模块102每次接收到网络收发模块101发送过来的文本块之后，则立刻对其进行解析，得到与该文本块对应的事件，且每解析得

到一个事件即发送至事件处理模块103中，同时继续执行步骤S301接收其他文本块。步骤S302中解析的具体过程包括：（1）对所接收到的文本块进行检测，当检测到一个文档开始标记（如<html>）时，则产生一个开始文档树事件；（2）继续检测到一个Tag开始标记（如<body>）时，则产生一个开始元素事件；（3）继续检测到一个Tag结束标记（如</body>）时，则产生一个结束元素事件；（4）当检测到一个文档结束标记（如</html>）时，则产生一个结束文档树事件。完成上述解析，则得到文本块对应的事件，并将该事件发送给手机浏览器100的事件处理模块103进行处理。在本发明的一个实施例中，若由于网络传输等因素造成网络收发模块101所接到到的是非完整性文档，如一个文档有5K字节，网络中断导致网络收发模块101仅收取了3K，则当文本解析模块102在对其进行解析时也将产生结束文档树事件，并通知事件处理模块103解析结束。

在步骤S303中，事件处理模块103根据文本块对应的事件构造元素，且每构造出一个元素即发送至屏幕绘制模块104中，同时继续执行步骤S301接收其他文本块，以及继续执行步骤S302对所接收到的文本块进行解析。步骤S303中根据事件构造元素的具体过程包括：（1）当事件处理模块103收到文本解析模块102发送的开始文档树事件，则新建一个文档树，并设置当前游标为该文档树的根节点；（2）当事件处理模块103继续接收到文本解析模块102发送的开始元素事件，则生成一个新的元素，并将其设置为当前游标节点的子节点；（3）当事件处理模块103继续接收到文本解析模块102发送的结束元素事件，则对游标元素进行排版，计算出游标元素的Rect，并同时更新此结点的父结点、爷爷结点直至根节点的Rect，如该游标元素的Rect与屏幕Rect（SR）存在交集，则产生一个绘制元素事件，同时调整游标，将游标节点的父结点设置为当前游标节点；（4）当事件处理模块103继续接收到文本解析模块102发送的结束文

档树事件，则结束当前线程，并将所生成的元素发送到手机浏览器100的屏幕绘制模块104中进行绘制。

在步骤S304中，屏幕绘制模块104每接收到事件处理模块103发送的一个绘制元素事件及相应的元素，就将该元素绘制到手机浏览器100屏幕上的对应位置，同时继续执行步骤S301、S302、S303，直至绘制出完整网页。关于对每一个元素进行绘制的具体过程，可参考现有技术。

如上所述，以上步骤S301、S302、S303、S304的执行过程，并不是一个简单的串行过程，在整体上是一个并行处理的过程，在一个步骤执行的同时其他步骤对应的线程也在运行，这样可在最短的时间内绘制出网页并显示给用户。

此外，在步骤S305中，当屏幕绘制模块104绘制出完整网页后，则将该网页的对象树存入缓存管理模块105中，这样当用户再次访问该网页时，则可直接提取该对象树显示出网页，进一步提高了效率。

本发明在实现快速浏览网页的同时，还考虑到安全浏览问题。由于手机在访问内容较多的互联网网页时，很可能会因为网页太大或者手机内存资源受限而造成手机浏览器100程序死机。为了解决这个问题，本发明提供了两种方法：

（1）引入内存检测（Check Memory）机制：在每个需要花费大量内存空间的函数入口都执行该内存检测机制，且在每一次申请内存时，都检查是否申请成功。如果内存检测的返回结果是“出错”（false），说明手机空余内存不足，或者申请内存失败，此种情况下应首先释放缓存，设置已经释放的标志，再回调到失败的函数本身。如果已经释放缓存仍然在内存检测时返回false，则产生内存不足错误，并且提示用户。

（2）在手机浏览器100中引入流量控制，典型的例如，可允许用户在手机浏览器100中设置三种流量控制模式：系统控制，限定单张网页最大流量，以及不下载图片。当用户选择“系统控制”时，每次下载网页或图片前，比较已下载文件和即将下载文件的大小总和与系统预设的允许大小值，如果大于系统预设的允许大小值，则不下载；当用户选择“限制单张网页最大流量”时，每次下载网页或图片前，比较已下载文件和即将下载文件的大小总和与用户设定的单张网页最大流量，大于用户设定值，则不下载；当用户选择“不下载图片”时，则不下载所有图片。

应当作出说明的是，本发明典型的应用但是并不限于在手机浏览器中浏览网页的情形，基于其他相关或类似的电子设备浏览网页时，也可以采用本发明的上述方法。

以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等，均应包含在本发明的保护范围之内。

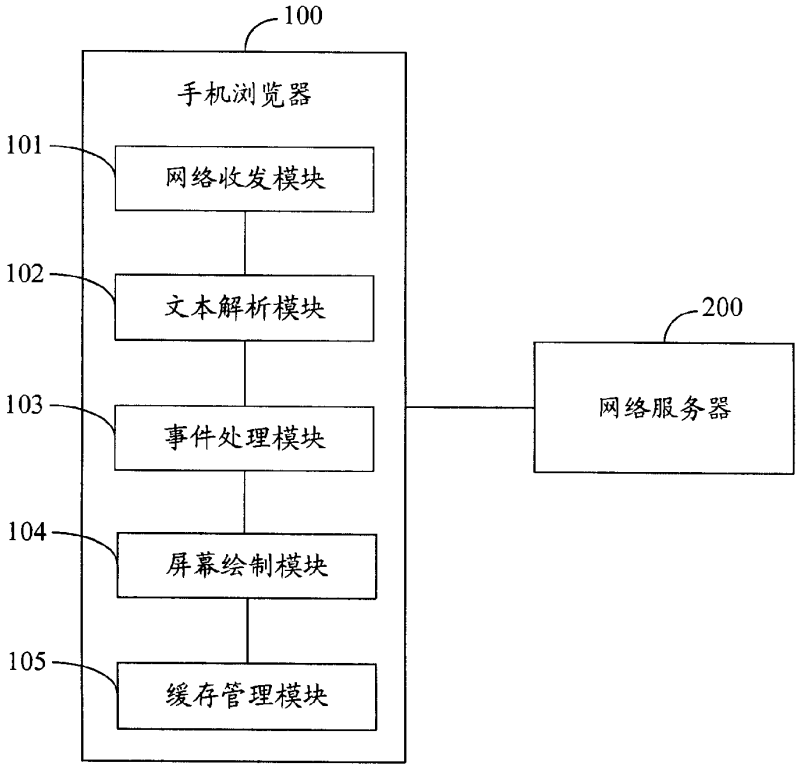

100
手机浏览器
101
网络收发模块
102
文本解析模块
103
事件处理模块
104
屏幕绘制模块
105
缓存管理模块
200
网络服务器

图 1

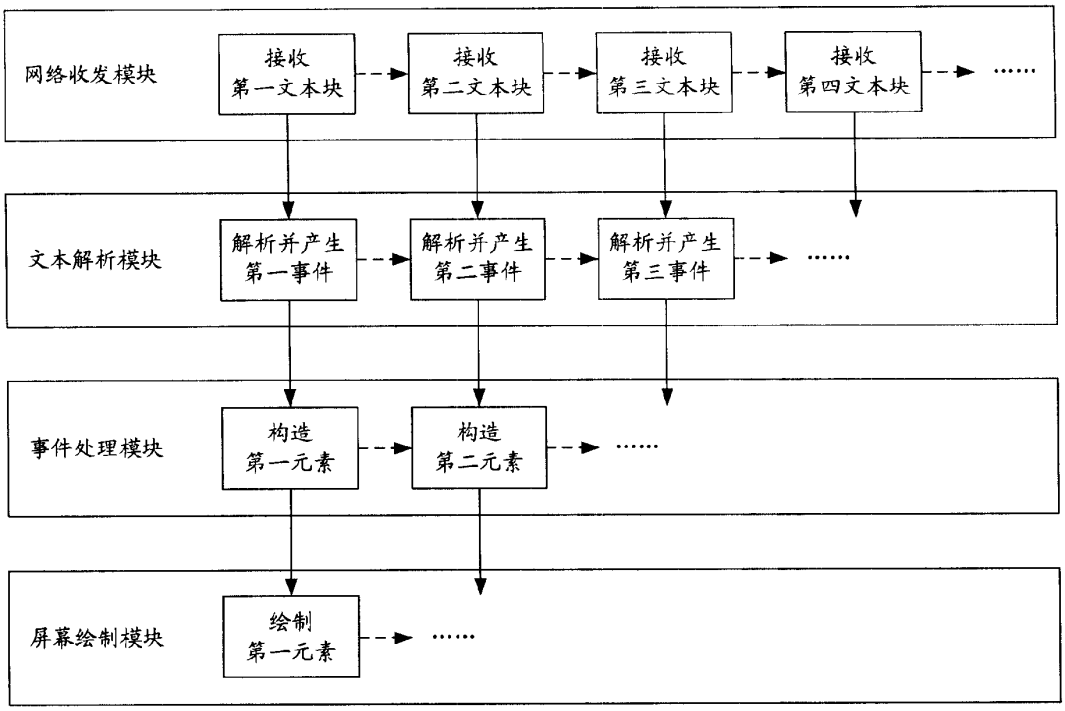

网络收发模块
接收
第一文本块
接收
第二文本块
接收
第三文本块
接收
第四文本块
……
文本解析模块
解析并产生
第一事件
解析并产生
第二事件
解析并产生
第三事件
……
事件处理模块
构造
第一元素
构造
第二元素
……
屏幕绘制模块
绘制
第一元素
……

图 2

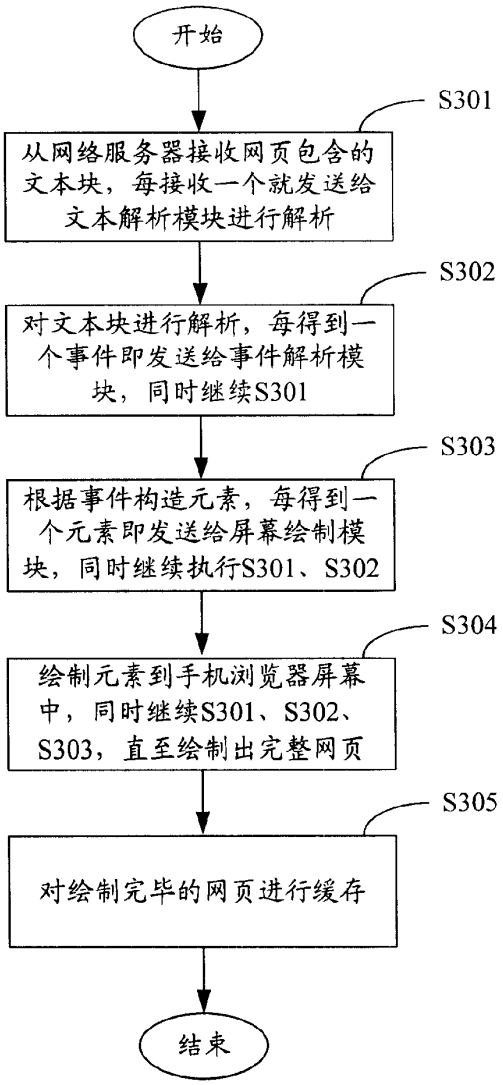

开始
S301
从网络服务器接收网页包含的文本块，每接收一个就发送给文本解析模块进行解析
S302
对文本块进行解析，每得到一个事件即发送给事件解析模块，同时继续S301
S303
根据事件构造元素，每得到一个元素即发送给屏幕绘制模块，同时继续执行S301、S302
S304
绘制元素到手机浏览器屏幕中，同时继续S301、S302、S303，直至绘制出完整网页
S305
对绘制完毕的网页进行缓存
结束

图 3

[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04L 12/14
H04M 17/00

[12] 发明专利申请公开说明书

[21] 申请号 03137490.5

[43] 公开日 2005 年 1 月 19 日

[11] 公开号 CN 1567818A

[22] 申请日 2003.6.25 [21] 申请号 03137490.5

[71] 申请人 华为技术有限公司
地址 518057 广东省深圳市科技园科发路华为用服大厦
[72] 发明人 张 庆 于 泽 严雪松

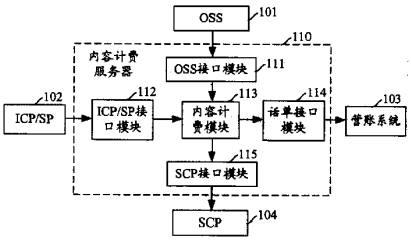
[74] 专利代理机构 北京德琦知识产权代理有限公司
代理人 宋志强 王 琦

权利要求书 3 页 说明书 13 页 附图 1 页

[54] 发明名称 一种数据业务的内容计费方法及其计费系统

[57] 摘要

本发明公开了一种数据业务的内容计费方法，该方法将计费规则定制为计费规则部件，当用户执行数据业务时，根据数据业务、用户信息和互联网内容提供商/业务提供商(ICP/SP)获得的内容计费记录信息，使用相应的计费规则部件，进行内容计费。本发明同时公开了一种业务的内容计费系统，该系统由专用的内容计费服务器来实现，其包含运营支撑系统(OSS)接口模块、ICP/SP 接口模块、内容计费模块、付费接口模块。本发明的这种内容计费方法及其计费系统，具有独立性、灵活性、可扩展性、开放性和分布性的特点，实现了根据数据业务内容进行计费，满足了数据业务中灵活多样的计费要求。



ISSN1008-4274

1、一种数据业务的内容计费方法，其特征在于，该方法包括以下步骤：

1）按照不同数据业务类型的不同计费规则，定制一个或一个以上计费规则部件；

2）预先保存签约数据业务用户的用户信息；

3）当用户执行数据业务时，根据该数据业务、步骤2）所述的用户信息和互联网内容提供商/业务提供商（ICP/SP）获得的内容计费记录信息，使用相应的计费规则部件，进行内容计费。

2、如权利要求1所述的内容计费方法，其特征在于，所述的步骤1）进一步包括：为每个计费规则部件设置一个计费因子，通过对计费因子的组合实现多种计费规则的组合计费。

3、如权利要求1所述的内容计费方法，其特征在于，所述的用户信息至少包括：用户开户信息、付费类型、用户属性、欠费记录；所述的内容计费记录信息至少包括：数据业务类型、该数据业务执行的时间、执行该数据业务的数据流量、该数据业务执行的次数。

4、如权利要求3所述的内容计费方法，其特征在于，所述的步骤3）包括以下步骤：

31）根据数据业务类型，在相应的计费规则部件中取出相应的计费规则，再根据该数据业务执行的时间、执行该数据业务的数据流量、该数据业务执行的次数，使用该计费规则进行计费；

32）判断该用户付费类型是否为预付费，如果是预付费则将计费结果发送给预付费处理设备，预付费处理设备按计费结果从该用户的帐户中扣除费用；否则为后付费用户，将计费结果发送给营帐系统。

5、如权利要求4所述的内容计费方法，其特征在于：当对移动数据业务进行计费时，所述的预付费处理设备为业务控制节点（SCP）。

6、如权利要求4所述的内容计费方法，其特征在于：该方法进一步包括，

步骤3）获得的计费结果由营帐系统根据用户需要生成用户帐单。

7、一种数据业务的内容计费系统，其特征在于，该系统包含内容计费服务器，该内容计费服务器至少包含：

运营支撑系统（OSS）接口模块，将OSS与内容计费模块相连，从OSS中获取签约数据业务用户的用户信息，发送给内容计费模块；

互联网内容提供商/业务提供商（ICP/SP）接口模块，将ICP/SP与内容计费模块相连， ICP/SP将内容计费记录信息发送给内容计费模块；

内容计费模块，根据数据业务类型、数据业务用户的用户信息、内容计费记录对数据业务进行计费，并根据付费类型生成计费结果；

付费接口模块，与内容计费模块相连，根据付费类型将计费结果发送给相应的付费处理设备。

8、如权利要求7所述的内容计费系统，其特征在于，所述的付费接口模块包含：

预付费接口模块，将预付费处理设备与内容计费模块相连，将内容计费模块产生的预付费用户的计费结果发送给预付费处理设备。

话单接口模块，将内容计费模块与营帐系统相连；将内容计费模块产生的后付费用户的计费结果发送给营帐系统。

9、如权利要求8所述的内容计费系统，其特征在于，所述的预付费接口模块为：业务控制节点（SCP）接口模块，将SCP与内容计费模块相连，将内容计费模块产生的预付费用户的计费结果发送给SCP。

10、如权利要求7所述的内容计费系统，其特征在于，所述的内容计费模块至少包含：

计费引擎，与OSS和ICP/SP分别相连，从OSS中获取签约数据业务用户的用户信息，接收ICP/SP发送的内容计费记录信息，并将用户信息和内容计费记录信息发送给批价部件；

批价部件，保存不同数据业务类型的基本费率，根据数据业务类型、数据

业务用户的用户信息、内容计费记录从计费规则部件中取出相应的计费规则，对数据业务进行计费，并根据付费类型生成计费结果；

计费规则部件，根据不同数据业务类型存储不同的计费规则。

11、如权利要求 7 所述的内容计费系统，其特征在于，所述的用户信息至少包括：用户开户信息、付费类型、用户属性、欠费记录；所述的内容计费记录信息至少包括：数据业务类型、该数据业务执行的时间、执行该数据业务的数据流量、该数据业务执行的次数。

12、如权利要求 8 所述的内容计费系统，其特征在于，所述的话单接口模块为话单接口机，其与内容计费模块通过以文件格式传输信息。

13、如权利要求 9 所述的内容计费系统，其特征在于：所述的内容计费服务器与 OSS 为实时的同步消息接口，或以文件形式进行数据传输；内容计费服务器与 ICP/SP、内容计费服务器与 SCP 之间均按照运营商接口规范进行连接。

14、如权利要求 13 所述的内容计费系统，其特征在于，所述内容计费服务器与 ICP/SP 采用消息或文件方式进行交互；内容计费服务器与 SCP 之间采用扩展移动点到点协议（EMPP）协议消息进行交互。

15、如权利要求 8 所述的内容计费系统，其特征在于：话单接口模块与营帐系统以文件传输协议（FTP）或文件传输访问和管理（FTAM）传输信息，在用户需要时营帐系统通过话单接口模块到内容计费服务器取计费结果。

16、如权利要求 7 所述的内容计费系统，其特征在于，所述的内容计费服务器包含一个以上服务器；计费引擎与计费规则部件分布在不同的服务器主机上。

一种数据业务的内容计费方法及其计费系统

技术领域

本发明涉及数据业务的计费技术，特别涉及一种数据业务的内容计费方法及其计费系统。

背景技术

目前，根据通用移动通信系统（UMTS）论坛报告9的分析，3G数据业务分成内容连接类和移动性类两大类，内容连接类可以划分成：移动Internet接入和企业Intranet/Extranet接入；移动性类可以划分成：客户化信息、娱乐；多媒体消息业务；基于位置的业务；另外还有增强话音共6类业务。

这6类业务代表了3G业务的主要需求。今天以话音为主宰的移动通信领域，将来一定会是一个以数据业务为中心的环境。在任何时间任何地点能够接入Internet的内容将明确成为3G的重要任务。

3G计费是3G解决方案的一个重要组成部分。虽然3G业务是多种多样的，前景是诱人的，但如果没有相应的计费解决方案，不建立相应的价值链体系，即运行商无法运营，那么一切都是空谈。

目前传统的计费系统都是针对语音业务来设计的，一般根据呼叫持续的时间、主被叫的距离等因素进行计费。即传统计费与呼叫时长及主被叫位置相关，而与消费的业务内容无关。

目前的3G计费系统，仍然以语音业务的计费为主，其计费策略普遍采用硬编码的方式，即计费公式在代码中写死，一旦计费费率表确定，其计费算法也就相应固定。

硬编码方式的主要缺点在于代码重用性、灵活性差，如果增加新的需求则需要更改大量代码，代码间耦合性大，修改涉及面广，不易维护，也不利于计

费系统的稳定性。针对3G业务对计费灵活性的要求，此种实现方式显然不能满足。

另外一种方法是使用脚本的方式固化计费策略，使用脚本语言实现计费公式。使用脚本语言虽然可以非常灵活的增加新的计费策略，修改计费公式时也不必修改代码，但由于计费公式一般比较复杂，使用脚本实现有很大的困难、可读性很差。除此之外，对脚本语言的解释对系统性能也会产生一定的影响。

现有 3G 计费系统是由移动通信系统原有的设备整合来实现的，即计费功能融合在 SSP 或 SCP 中，由 SSP/SCP 完成对用户的计费功能。

传统的话音业务计费是和用户消费的内容无关的，只与时长（用户的通话时间）、距离（本地通话或长途）有关，因此不必上报业务信息或内容属性等，同时不关心用户消费业务的流量、次数，只需要在 SSP/SCP 侧统计用户的通话时间，由 SSP/SCP 完成对用户的计费功能后，由营帐系统根据计费结果，生成用户帐单，在用户需要时提交给用户。

3G 最吸引人的地方在于“永远在线”的服务，即只要打开手机就可以享受到丰富多采的业务内容，因此仅限于语音业务的传统计费系统明显不能满足多样化业务所带来的多样化内容计费的需求。因此传统的话音计费不能满足内容计费的需要。

且由于现有技术的计费系统通过移动通信系统原有的设备整合来实现，占用了移动通信系统的资源，计费过程繁琐，灵活性差，不能适应日益发展的丰富多采的数据业务的计费需要。

发明内容

有鉴于此，本发明的目的在于提供一种数据业务的内容计费方法，实现根据业务内容进行计费，满足数据业务中灵活多样的计费要求。

本发明的另一个目的在于提供一种数据业务的内容计费系统，节省移动通信系统资源，实现根据业务内容进行计费，满足数据业务中灵活多样的计

费要求。

根据上述目的的一个方面，本发明提供了一种数据业务的内容计费方法，该方法包括以下步骤：

1）按照不同数据业务类型的不同计费规则，定制一个或一个以上计费规则部件；

2）预先保存签约数据业务用户的用户信息；

3）当用户执行数据业务时，根据该数据业务、步骤2）所述的用户信息和互联网内容提供商/业务提供商（ICP/SP）获得的内容计费记录信息，使用相应的计费规则部件，进行内容计费。

其中，所述的步骤1）可以进一步包括：为每个计费规则部件设置一个计费因子，通过对计费因子的组合实现多种计费规则的组合计费。

所述的用户信息至少可以包括：用户开户信息、付费类型、用户属性、欠费记录；所述的内容计费记录信息至少可以包括：数据业务类型、该数据业务执行的时间、执行该数据业务的数据流量、该数据业务执行的次数。

所述的步骤3）可以包括以下步骤：

31）根据数据业务类型，在相应的计费规则部件中取出相应的计费规则，再根据该数据业务执行的时间、执行该数据业务的数据流量、该数据业务执行的次数，使用该计费规则进行计费；

32）判断该用户付费类型是否为预付费，如果是预付费则将计费结果发送给预付费处理设备，预付费处理设备按计费结果从该用户的帐户中扣除费用；否则为后付费用户，将计费结果发送给营帐系统。

当对移动数据业务进行计费时，所述的预付费处理设备可以为业务控制节点（SCP）。

根据上述目的的另一个方面，本发明提供了一种内容计费系统，该系统包含专用的内容计费服务器，该内容计费服务器至少包含：

运营支撑系统（OSS）接口模块，将OSS与内容计费模块相连，从OSS中

获取签约数据业务用户的用户信息，发送给内容计费模块；

互联网内容提供商/业务提供商（ICP/SP）接口模块，将 ICP/SP 与内容计费模块相连， ICP/SP 将内容计费记录信息发送给内容计费模块；

内容计费模块，根据数据业务类型、数据业务用户的用户信息、内容计费记录对数据业务进行计费，并根据付费类型生成计费结果；

付费接口模块，与内容计费模块相连，根据付费类型将计费结果发送给相应的付费处理设备。该付费接口模块可以包含：

预付费接口模块，将预付费处理设备与内容计费模块相连，将内容计费模块产生的预付费用户的计费结果发送给预付费处理设备。

话单接口模块，将内容计费模块与营帐系统相连；将内容计费模块产生的后付费用户的计费结果发送给营帐系统。

其中，所述的预付费接口模块可以为：业务控制节点（SCP）接口模块，将 SCP 与内容计费模块相连，将内容计费模块产生的预付费用户的计费结果发送给 SCP。

所述的内容计费模块至少可以包含：

计费引擎，与 OSS 和 ICP/SP 分别相连，从 OSS 中获取签约数据业务用户的用户信息，接收 ICP/SP 发送的内容计费记录信息，并将用户信息和内容计费记录信息发送给批价部件；

批价部件，保存不同数据业务类型的基本费率，根据数据业务类型、数据业务用户的用户信息、内容计费记录从计费规则部件中取出相应的计费规则，对数据业务进行计费，并根据付费类型生成计费结果；

计费规则部件，根据不同数据业务类型存储不同的计费规则。

所述的用户信息至少可以包括：用户开户信息、付费类型、用户属性、欠费记录；所述的内容计费记录信息至少可以包括：数据业务类型、该数据业务执行的时间、执行该数据业务的数据流量、该数据业务执行的次数。

所述的话单接口模块可以为话单接口机，其与内容计费模块通过以文件格

式传输信息。

所述的内容计费服务器与 OSS 可以为实时的同步消息接口，或以文件形式进行数据传输；内容计费服务器与 ICP/SP、内容计费服务器与 SCP 之间均可以按照运营商接口规范进行连接。

所述内容计费服务器与 ICP/SP 可以采用消息或文件方式进行交互；内容计费服务器与 SCP 之间可以采用扩展移动点到点协议（EMPP）协议消息进行交互。

话单接口模块与营帐系统可以以文件传输协议（FTP）或文件传输访问和管理（FTAM）传输信息，在用户需要时营帐系统通过话单接口模块到内容计费服务器取计费结果。

所述的内容计费服务器可以包含一个以上服务器；计费引擎与计费规则部件分布在不同的服务器主机上。

由本发明的技术方案可见，本发明的这种内容计费系统及其计费方法，将计费规则定制为计费规则部件，当用户执行数据业务时，根据数据业务、用户信息和互联网内容提供商/ 业务提供商（ICP/SP）获得的内容计费记录信息，使用相应的计费规则部件，进行内容计费，实现了根据数据业务内容进行计费，满足了数据业务中灵活多样的计费要求。

附图说明

图 1 为本发明一个较佳实施例的内容计费实现框图；

图 2 为图 1 所示实施例中内容计费模块的实现框图。

具体实施方式

为使本发明的目的、技术方案和优点更加清楚明白，下面结合实施例和附图，对本发明进一步详细说明。

本发明的这种数据业务的内容计费方法，是为了满足 3G 业务的特点，采用根据业务内容进行计费的方式。并根据计费需求的灵活多变，定制不同

的计费规则。也就是说，本发明能够根据计费规则定制不同的计费公式，对计费策略、折扣策略等实现灵活组合、易于扩充。

本发明的这种数据业务的内容计费方法，首先按照不同数据业务类型的不同计费规则，定制一个或一个以上计费规则部件；同时预先保存签约数据业务用户的用户信息，该用户信息可以包括：用户开户信息、付费类型、用户属性、欠费记录等。

其中，在定制计费规则部件时，参考了下列因素：

A、不同 ICP/SP 可能有不同的计费策略；

B、不同业务可能有不同的资费策略，如游戏，不同游戏可能的收费不同；

C、支持按时长计费，如游戏，时间长短收费不同；

D、支持基于内容的流量计费，如下载图片，按照流量计费，但是费率根据不同的图片有所区别；

E、支持按使用次数计费（包括按条、按页面、按次计费），如下载图片、MP3、铃声等；

F、支持按时间段或日期采用不同的计费策略；如某些日期免费促销、每天的某些时间段访问给予一定折扣等；

G、支持平价计费、支持签约费（月租）+按使用次数或时长或流量等计费策略；

H、支持用户个性化的计费，不同用户可以根据自身情况选择不同的资费或计费策略；

I、支持随使用量不同（时长、流量、次数）采用不同的计费策略，其类似于跳档；

J、广告业务，支持用户访问ICP的广告送费服务，又可以分为赠送使用费和赠送使用量两种；

K、支持接入不同的数据网络采用不同的计费策略，考虑QoS等因素；

L、支持在不同区域或地区运用不同的计费策略，有可能在各“热点地区”

向用户收费不同。比如，可以相对于“办公区”的概念，对“生活区”收取更低的费用；

M、支持封顶费用。

除此之外，折扣是SP和网络运营商吸引用户的非常重要的手段，无论是传统的语音业务，还是面向3G的移动数据业务，折扣的地位都是举足轻重的。折扣方式多种多样，目前普遍使用的折扣方式主要有以下几种：

a、时间段折扣——保留现有的日常、星期、节假日折扣方式。这种方式也可以扩展到按流量计费的计费模式中。

b、累计折扣——包括时长累计折扣、流量累计折扣、条目累计折扣、金额累计折扣等4种折扣方式。

c、一次累计折扣——按照一次使用总量、一次使用总金额折扣

d、用户折扣——对某种集团用户进行统一的折扣。可在所有折扣基础上累乘。

e、业务折扣——对某种业务进行统一折扣。

本发明在具体实施中根据上述因素，定制了多个计费规则部件。一种业务的计费可以通过批价部件和一个或多个计费规则部件来实现。计费规则部件可以进行组合计费，同时为一种组合设置一个计费因子，在实际计费过程中用批价部件中的基本费率和计费因子实现多种附加计费规则的组合计费。

在实际应用中，数据业务的计费策略可以用批价部件中保存的基本费率信息+附加计费规则部件的计费因子信息”来描述。

例如：对应于互联网内容提供商的短信业务，那么其基本费率信息可以如表一所示，表一为一种短信业务简单的费率表。

费率 ID	计费模式	计费单位	费率值
1	1（按次计费）	1（次）	10（分）

表一

表一的含义就是对按次计费的业务，每次收 10 分钱。

不同的用户附加的计费因子可能不同，如果要求用户同时享受累积折扣、时间折扣，计费因子信息可以如表二所示，表二为一种短信业务计费因子表。

计费因子 ID	折扣标识	折扣索引	折扣部件
0	3（代表累积折扣）	0	累积折扣
0	5（代表时间折扣）	1	时间折扣

表二

表二对应了两种折扣，相当于将两种折扣组合成了一个计费因子。

上述两个表都是基本信息，实际应用中的表结构不仅限于此。

对应于累积折扣，如表三所示，表三为累积折扣表。

折扣 ID	折扣下限	折扣类型	折扣值
0（对应于计费因子表中的“折扣索引”字段）	30	0（表示百分比折扣）	80

表三

表三的含义就是当用户累积使用业务达到 30 次后，可以享受 8 折优惠

同样的，如表四所示，表四为时间折扣表。

折扣索引	起始时间	结束时间	折扣类型	折扣值
1	22:00:00	23:59:59	0(表示百分比折扣)	50

表四

表四的含义就是在 22：00~23：59 分使用业务的用户，都可以享受 5 折优

惠。

将基本费率信息与计费因子信息相结合，就得到了一种计费策略，这样的一个计费策略就可以和一个业务相绑定。参见表五，表五为短信业务的一种计费策略。

业务 ID	费率索引	计费因子索引
8888	1	0

表五

其中 ID 为 8888 的业务代表短信业务，其计费策略就是：按次计费业务，每次收费 10 分，同时如果用户累积使用 30 次以上，可以享受 8 折优惠，如果在 22：00~23：59 之间享受业务，又可以享受 5 折优惠。

如果一个用户已经使用该业务 30 次，又在 22：30 使用该业务，那么该用户的实际收取金额=1（次）*10（分）*0.8*0.5=4（分）

如果需求产生变动，要求除支持以上两种折扣之外，再增加一种用户折扣，那么计费因子描述表只需进行修改，修改后的计费因子描述表参见表六。

计费因子 ID	折扣标识	折扣索引	折扣部件
0	3	0	累积折扣
0	5	1	时间折扣
0	6	2	用户折扣

表六

这样，启动用户折扣部件，就可以轻而易举的实现动态增加一种折扣类型了，完全不需要做代码的修改，真正达到了动态灵活配置计费规则的目的。其中 6 代表用户折扣。

例如：一个个人移动用户签约了互联网内容提供商的短信业务，当该用户接收短信时，互联网内容提供商向内容计费服务器发送内容计费记录，其中包含了该用户执行的是短信业务、发送短信的条数、发送的时间等信息。内容计费服务器收到该内容计费记录后，取出 OSS 预先存储在内容计费服务器中的该

用户的个人信息，包括该用户的开户信息、付费类型（例如本用户为预付费用户）、该用户属性为个人用户、该用户没有欠费记录、用户已付费情况等信息。内容计费服务器根据该用户执行的是短信业务、发送短信的时间、发送短信的数目已超出预定额度，以及该用户为个人用户、且没有欠费记录，判断该用户应该享有表六所述的三种折扣，因此使用表六中ID号为0的计费因子进行计费，然后内容计费服务器将该计费结果发送给SCP，SCP在该用户的帐户上扣除相应的费用。

当用户执行数据业务时，根据数据业务、用户信息和互联网内容提供商/ 业务提供商（ICP/SP）获得的内容计费记录信息，使用相应的计费规则部件，进行内容计费。其中内容计费记录信息可以包括：数据业务类型、该数据业务执行的时间、执行该数据业务的数据流量、该数据业务执行的次数。

其中内容计费可以由以下步骤来实现：

步骤 A、根据数据业务类型，在相应的计费规则部件中取出相应的计费规则，再根据该数据业务执行的时间、执行该数据业务的数据流量、该数据业务执行的次数，使用该计费规则进行计费；

步骤 B、判断该用户付费类型是否为预付费，如果是预付费则将计费结果发送给预付费处理设备，对于移动数据业务是业务控制节点（SCP），预付费处理设备按计费结果从该用户的帐户中扣除费用；否则为后付费用户，将计费结果发送给营帐系统。

步骤C、营帐系统根据用户需要取出计费结果，生成用户帐单。

参见图1，图1为本发明一个较佳实施例的内容计费实现框图。本实施例是对移动数据业务进行计费。其中内容计费系统由专用的内容计费服务器110来实现，该内容计费服务器110与OSS 101、ICP/SP 102、SCP 104和营帐系统分别相连。内容计费服务器110与OSS 101为实时的同步消息接口，或以文件形式进行数据传输 ，ICP/SP 102、SCP 104之间均按照运营商接口规范进行连接。其中，内容计费服务器110与ICP/SP102采用消息或文件方式进行交互；内容计费服务

器110与SCP 104之间采用EMPP协议消息进行交互。本实施例的接口均按照运营商接口规范设计，有利于与外部其他设备的对接。

本实施例中的内容计费服务器 110 包含了：

运营支撑系统（OSS）接口模块 111，将 OSS 101 与内容计费模块 113 相连，从 OSS 101 中获取签约移动数据业务用户的用户信息，发送给内容计费模块 113；

互联网内容提供商/ 业务提供商（ICP/SP）接口模块 112，将 ICP/SP102 与内容计费模块相连 113，ICP/SP 102 将内容计费记录信息发送给内容计费模块 110。

内容计费模块 113 是内容计费的主要功能模块，参见图 2，图 2 为图 1 所示实施例中内容计费模块的实现框图。内容计费模块 113 包含：计费引擎 201，其通过 OSS 接口模块 111、ICP/SP 接口模块与 OSS101 及 ICP/SP102 分别相连）从 OSS 101 中获取签约移动数据业务用户的用户信息，接收 ICP/SP 102 发送的内容计费记录信息，并将用户信息和内容计费记录信息发送给批价部件 202。

批价部件 202，存储了不同移动数据业务类型的基本费率，根据移动数据业务类型、移动数据业务用户的用户信息、内容计费记录从相应的一个或多个计费规则部件 203 中取出相应的计费规则，对移动数据业务进行计费，并根据付费类型生成计费结果。

本实施例的内容计费服务器110预先定制了多个计费规则部件203，其根据不同移动数据业务类型分别存储不同的计费规则。计费规则部件203可以根据移动数据业务的变化，随时进行增加、删除和修改。可见，本实施例的内容计费系统以组件的方式实现，增加新需求即相当于增加新组件，对原有代码没有影响。同时各组件可以对外提供开放性接口，易于扩展。

总之，内容计费模块 113，根据移动数据业务类型、移动数据业务用户的用户信息、内容计费记录对移动数据业务进行计费，并根据付费类型生成计费结果。

业务控制节点（SCP）接口模块 115，将 SCP 104 与内容计费模块 113 相连，将内容计费模块 113 产生的预付费用户的计费结果发送给业务控制节点 104；

话单接口模块 114，将内容计费模块 113 与营帐系统 103 相连；将内容计费模块 113 产生的后付费用户的计费结果发送给营帐系统 103。

本实施例中的业务控制节点（SCP）接口模块 115 和话单接口模块 114 构成了付费接口模块，根据数据业务的付费类型将计费结果发送给相应的计费处理设备——业务控制节点 104 或营帐系统 103。

话单接口模块 114 与营帐系统以 FTP 或 FTAM 传输信息，在用户需要时营帐系统通过话单接口模块 114 到内容计费服务器 110 取计费结果。话单接口模块 114 可以由一个独立的话单接口机来实现，其与内容计费模块 113 通过以文件格式传输信息。

在本实施例的内容计费服务器 110 计费过程中，用户信息和内容计费记录信息是计费中的重要信息，该用户信息具体可以包括：用户开户信息、付费类型、用户属性、欠费记录；内容计费记录信息具体可以包括：移动数据业务类型、该移动数据业务执行的时间、执行该移动数据业务的数据流量、该移动数据业务执行的次数。

另外，本实施例的内容计费服务器110可以由多个服务器来实现；其中，计费引擎201可以由专用的服务器来实现，批价部件202和计费规则部件203分布在其他的专用的服务器主机上。这样计费引擎201与计费规则部件203分布在不同主机上，能够确保内容计费系统的性能。

本实施例的内容计费系统，使用专用的服务器来实现，不依赖于其他设备，与其他设备的交互采用消息机制或 API 函数调用机制，使内容计费模块具有较高的独立性，可以进行独立的测试，减少了开发与测试的工作量，易于维护。

同时，本实施例可以动态增加或修改计费规则部件的组合，无需修改代码或重启计费系统，具有很大的灵活性，最大限度的满足了计费需求的灵活

多变的特性。

由上述的实施例可见，本发明的这种数据业务的内容计费方法及其计费系统，具有独立性、灵活性、可扩展性、开放性和分布性的特点，实现了根据数据业务内容进行计费，满足了数据业务中灵活多样的计费要求。

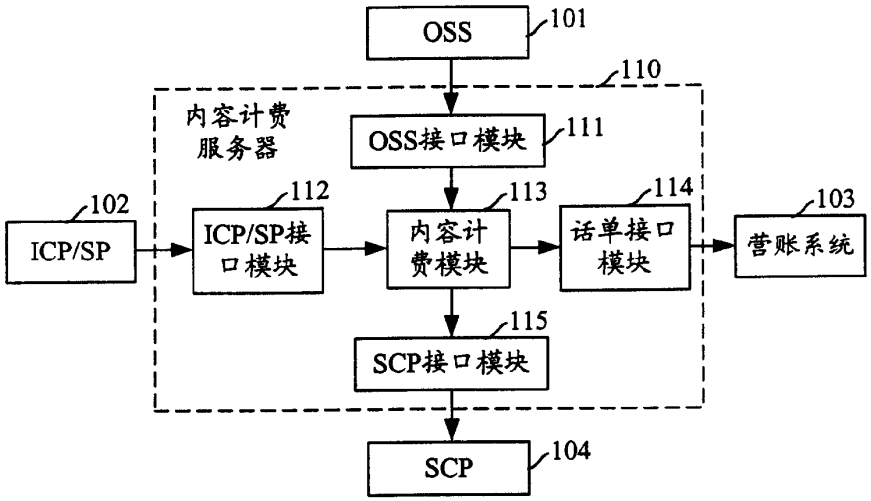

OSS
101
110
内容计费
服务器
OSS接口模块
111
102
ICP/SP
112
ICP/SP接
口模块
113
内容计
费模块
114
话单接口
模块
103
营账系统
115
SCP接口模块
SCP
104

图 1

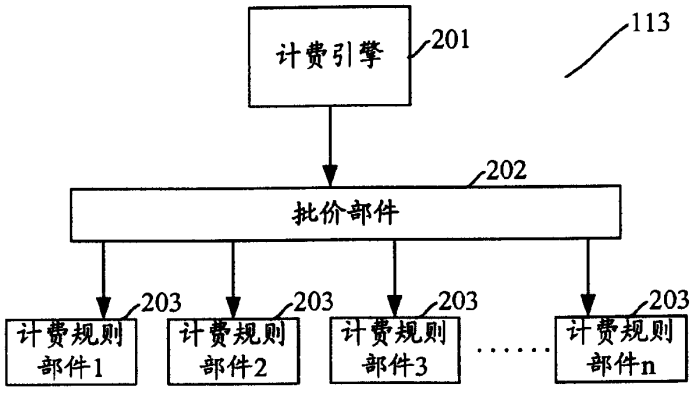

计费引擎
201
113
202
批价部件
203
计费规则
部件1
203
计费规则
部件2
203
计费规则
部件3
203
计费规则
部件n

图 2

Search Images Maps Gmail Drive Calendar Translate Docs More »

Google Patents Application Grant English Chinese Advanced Patent Search

Find prior art Discuss this application View PDF Download PDF

A content charging method of data service and charging system thereof

CN 1567818 A

Publication number	CN1567818 A
Publication type	Application
Application number	CN 03137490
Publication date	19 Jan 2005
Filing date	25 Jun 2003
Priority date	25 Jun 2003
Also published as	CN100550747C, CN101159566A, CN101159566B
Inventors	张庆, 于泽, 严雪松
Applicant	华为技术有限公司
Export Citation	BiBTeX, EndNote, RefMan

Referenced by (9), Classifications (3), Legal Events (3)

External Links: SIPO, Espacenet

ABSTRACT

The invention discloses a data service content charging method, customizing the charging rules as charging rule parts, as user executes data service, according to data service, user information and the content charging record obtained by Internet content provider/service provider (ICP/SP), using the corresponding charging rule part to making content charging. At the same time, it discloses a service content charging system, implemented by special content charging server and containing operation supporting system (OSS), ICP/SP interface module, content charging module, and payment interface module. It has the characters of independency, flexibility, extendability, openness and distributivity, realizes the charge according to data service content and meets the flexible and various charging requirements in data service.

DESCRIPTION translated from Chinese

A data service content charging method and charging system

Technical Field

The present invention relates to a data service charging technology, and more particularly to a data content service charging method and charging system.

Background

Currently, according to Universal Mobile Telecommunications System (UMTS) Forum Report 9 analysis, 3G data connection business into content categories and mobility class two categories, content connection type can be divided into: mobile Internet access and corporate Intranet / Extranet access; Mobility category can be divided into: customer information, entertainment; multimedia message service; location-based services; in addition to a total of six class enhanced voice services.

This 6 class of business represents a major demand for 3G services. Today, voice-dominated field of mobile communications, the future will be a data-centric business environment. Content at any time and any place to access the Internet will clearly be an important task of 3G.

3G billing is an important part of the 3G solutions. While 3G services are varied, prospects are tempting, but if there is no corresponding accounting solutions that do not establish the corresponding value chain system, which operators can not operate, then all talk.

Current traditional billing systems are designed for voice traffic, generally based on call duration, distance and other factors calling and called for billing. Namely the traditional billing and call duration and the Lord called location-related, regardless of the business content consumption.

The current 3G billing system, still based billing of voice services, its accounting policy commonly used hard-coded way, that the accounting formula in the code writing dead, once the billing rate tables to determine which accounting method correspondingly fixed.

CLAIMS (16) translated from Chinese

A method of data service billing content, characterized in that the method comprises the following steps: 1) according to the different types of data traffic of different charging rules, the one or more custom charging rules member; 2) pre-stored signed data service user's user information; 3) When the user performs data services, according to the data service, step 2) content of the user information and Internet content providers / service provider (ICP / SP) billing record information obtained using the corresponding charging rule components, content billing.

2. The content charging method according to claim 1, wherein said step a) further comprises: providing a charging member charging rules for each factor, by a combination of factors to achieve a variety of billing combination accounting rules for accounting.

3. The content billing method according to claim 1, wherein the user information includes at least: user account information, payment types, user attributes, arrears records; and the content billing record information including at least : data service type, time the data service for execution of data flow of the data service, the number of times the data service execution.

The content charging method according to claim 3, wherein said step 3) comprises the steps of: 31) in accordance with the type of data service, remove the corresponding charging rule corresponding charging rule member, then the data service based on the time for execution of data flow of the data service, the number of times the data service execution, an accounting rule for accounting; 32) to determine whether the type of user fees prepaid, if the prepaid The results will be sent to the prepaid billing processing equipment, processing equipment by prepaid billing deductions result from the user's account; otherwise, post-paid subscribers will be sent the results to the tent billing system.

5. The content billing method according to claim 4, wherein: when

The main disadvantage is that the hard-coded code reuse, flexibility is poor, if the increase in new demand you need to change a lot of code, the code coupling between large, modification covers a wide, easy to maintain, is not conducive to the stability of the charging system. Billing flexibility for 3G services requirements, such implementations obviously can not meet.

Another way is to use a script curing accounting policy, using a scripting language for accounting formula. While using a scripting language can be very flexible to add new accounting policy, modify the accounting formula also having to modify the code, but is generally more complex due to the accounting formula, using scripts have great difficulty, poor readability. In addition, the interpretation of the scripting language for system performance will have some impact.

Billing systems existing 3G mobile communication system is composed of original equipment integration to achieve, namely accounting functions integrated in the SSP or SCP, the SSP / SCP complete user billing capabilities.

Traditional voice services and content user consumption billing is irrelevant, only the long (user talk time), distance (local or long-distance calls), and therefore do not have to report business information or content attributes, but users do not care about the consumer business traffic times, just in SSP / SCP side statistics users talk time, after the SSP / SCP complete user accounting function, the tent system based on accounting results generated user bill, presented to the user needs users.

3G the most attractive place is "always on" service, as long as open the phone you can enjoy the rich and varied business content, therefore limited to traditional voice services billing system obviously can not meet the diverse business brings diverse content billing requirements. Thus traditional voice billing does not meet the needs of content billing.

And because the prior art billing system via a mobile communication system to achieve the integration of existing equipment, takes up the resources of mobile communication systems, billing process cumbersome, inflexible, unable to meet the growing data business colorful count Fee required.

DISCLOSURE

In view of this, the present invention is to provide a data service content charging methods to achieve billing based on business content, data services to meet flexible billing requirements.

Another object of the present invention is to provide a data service content billing systems, saving mobile communication system resources, billing based on business content, data services to meet flexible billing requirements.

In accordance with one aspect of the above object, the present invention provides a data service billing content, the method comprising the steps of: 1) according to the different types of data traffic of different charging rules, one or more custom charging rules member; 2) the business user subscription data previously stored user information; 3) When the user performs data services, according to the data service, user information and Internet content provider in step 2) above / service provider (ICP / SP) obtained content billing record information, use the appropriate charging rule means content billing.

Wherein said step 1) may further comprise: providing a charging member charging rules for each factor, billing factor by charging a variety of combinations to achieve a combination of charging rules.

The user information may include at least: user account information, payment types, user attributes, arrears records; billing record information of the content may be at least include: the type of data service, the data service time for execution of the data service data traffic, the data service execution times.

Said step 3) may comprise the steps of: 31) in accordance with the type of data billing for mobile data services, prepaid processing equipment for the service control point (SCP).

Content billing method according to claim 6, wherein: the method further comprises, billing the result of step 3) obtained by the tent system according to the user needs to generate user billing.

A data service content billing system, wherein the system comprises content billing server, the content accounting server includes at least: Operations Support System (OSS) interface module, connect OSS and content billing module, Get the OSS in business user subscription data user information to the content billing module; Internet content provider / service provider (ICP / SP) interface module, connect ICP / SP and content billing module, ICP / SP will content billing record information to the billing module content; content billing module, based on the type of data services, data services, user's user information, content billing records billing data services, and generates accounting results based on the type of pay; Pay Interface module is connected to the content billing module, according to the type of charge will send the results to the appropriate billing payment processing equipment.

8. The content metering system according to claim 7, characterized in that said interface module comprises charge: prepaid interface module, the processing of prepaid billing module connected to the device with the content, the content of the billing module generates prepaid user accounting result to a prepaid processing equipment. If a single interface module, connect content billing module and tent systems; the content billing module generates after paying user accounting results to the camp system.

9. The content metering system according to claim 8, characterized in that the said prepaid module interfaces: service control point (SCP) interface module, the contents of the billing module connected to the SCP, the contents of the billing module generating prepaid subscribers accounting result to the SCP.

10. The content billing system according to claim 7, wherein the content of the billing module comprising at least: billing engine, connected respectively OSS and ICP / SP, get a business user subscription data from the OSS user information, content billing record information received ICP / SP transmitted, and user information and content billing record information to grant price components; grant price component, save the basic rate of different types of data traffic, according to the data type of business, data service user's user information, content billing record is removed from the charging rule corresponding charging rule parts, billing for data services, and generates accounting results based on the type of charge, charging rules parts, depending on the type of data service store different charging rules.

11. The content billing system according to claim 7, wherein the user information includes at least: user account information, payment types, user attributes, arrears records; content billing record information includes at least : data service type, time the data service for execution of data flow of the data service, the number of times the data service execution.

12. The content billing system according to claim 8, wherein said interface module for the bill if a single interface machine, its content billing module to transmit information by file format.

13. The content billing system according to claim 9, wherein: the content accounting server and OSS real-time synchronous message interface, or as files for data transmission; the content accounting server and ICP / SP , content billing server between SCP and are in

service, remove the corresponding charging rule corresponding charging rule component, then the data service based on the time for execution of the data flow of the data service, the number of times the data service execution, an accounting rule for accounting; 32) to determine whether the type of user fees prepaid, if prepaid will send the results to the prepaid billing processing equipment, processing equipment by prepaid plan fee deductions result from the user's account; otherwise, post-paid subscribers will be sent the results to the tent billing system.

When billing for mobile data services, prepaid processing device may be the service control point (SCP).

According to another aspect of the above object, the present invention provides a content billing system, which includes a dedicated server content billing, content billing server that includes at least: Operations Support System (OSS) interface module, the OSS and content Billing module is connected, access the user's subscription data service user information from OSS, and sent to the billing module content; Internet content provider / service provider (ICP / SP) interface module, connect ICP / SP and content billing module , ICP / SP will send the contents of the billing record information to the billing module content; content billing module, based on the type of data services, data services, user's user information, content billing records data services billing, and paying according to the type of generation accounting result; pay interface module is connected to the content billing module, according to the type of charge will send the results to the appropriate billing payment processing equipment. The pay-interface module comprising: a prepaid interface module, a prepaid processing billing module connected devices and content, the content billing module generates prepaid subscribers accounting result to a prepaid processing equipment.

If a single interface module, connect content billing module and tent systems; the content billing module generates after paying user accounting results to the camp system.

Wherein the prepaid interface module can be: service control point (SCP) interface module, connect the SCP and content billing module, content billing module generates prepaid subscribers accounting result to the SCP.

The contents of the billing module can at least contain: billing engine, connected respectively OSS and ICP / SP, business users get subscription data user information from OSS, the content billing record information received ICP / SP to send, and user information and content billing record information to grant price components; grant price component, save the basic rate of different types of data traffic, according to the data service type, data service user's user information, content billing records from the accounting rule member Remove the appropriate accounting rules, data service billing, and generates accounting results based on the type of charge; charging rules parts, depending on the data stored in different types of business accounting rules.

The user information may include at least: user account information, payment types, user attributes, arrears records; billing record information of the content may be at least include: the type of data service, the data service time for execution of the data service data traffic, the data service execution times.

The CDRs CDR interface module can interface machine, with content billing module to transmit information to a file format.

The content of the accounting servers and OSS for real-time synchronous message interface, or as files for data transmission; can be carried out according to the operator interface specification between the content accounting server and ICP / SP, content billing server and SCP connection.

The content accounting server and ICP / SP can be used to interact with the message or file mode; the content may be used between the accounting server and SCP (EMPP) mobile PPP protocol message extension to interact.

If a single interface module and tent system can File Transfer Protocol (FTP) or File Transfer Access and Management (FTAM) transmit information when the user needs tent system via CDR interface module to fetch the content accounting server accounting results.

The content of the accounting server may contain one or more servers; billing and charging rules engine components distributed across different server host.

Seen from the aspect of the present invention, the content of the billing system and accounting methods of the present invention, the accounting rules for the charging rules customized parts, when the user performs data services, according to data services, user information and internet content provider content billing record information / service provider (ICP / SP) obtained using the corresponding charging rule parts, content billing, billing realized according to the data service content to meet the data services in flexible terms fee requirements.

accordance with the operator interface specification for the connection.

14. The content billing system as claimed in claim 13, characterized in that the content accounting server and ICP / SP messages or files using interactive manner; moving from point to point by the extended content billing server and SCP Protocol (EMPP) protocol message interaction.

15. The content billing system according to claim 8, wherein: if a single tent system interface module File Transfer Protocol (FTP) or File Transfer Access and Management (FTAM) transmit information when the user needs tent system By bill to content billing server interface modules take accounting results.

16. The content billing system according to claim 7, wherein the content of the accounting server contains more than one server; billing and charging rules engine components distributed across different server host.

Brief Description

Figure 1 is an example of content billing invention a preferred embodiment of realization diagram; Figure 2 is a block diagram of realization content billing module shown in FIG. 1 embodiment.

DETAILED DESCRIPTION

For the purposes of this invention, technical solutions and advantages more apparent, the following Examples and accompanying drawings, the present invention is described in further detail.

This data service content billing method of the present invention is to meet the characteristics of 3G services, the use of billing approach based on business content. And flexible billing based on the ever-changing needs, customize different charging rules. That is, the present invention can be customized according to different accounting rules billing formula, accounting policy, discount strategy flexible combination, easy expansion.

This data service content billing method of the present invention, the first data according to different accounting rules for different types of services, customized billing rule one or more parts; at the same time the business user subscription data previously stored user information, the user information including: user account information, payment types, user attributes, arrears records.

Among them, the custom component charging rules, the reference to the following factors: A, different ICP / SP may have different charging policies; B, different services may have different pricing strategies, such as different games, different games may charge; C, support long time and billing, such as casino games, duration and costs; D, support content-based traffic accounting, such as downloading pictures, according to traffic accounting, but the rates differ depending on the image; E, supported by using the number of billing (including Article, by page, pay-per), such as downloading pictures, MP3, ring tones; F, supported by time period or date using different accounting policies; as certain date free promotion, every day Some time access to give some discounts; G, support parity billing, support contract fee (monthly) + per use or duration or flow and other accounting policies; H, supports billing of individual users, different user You can choose according to their different tariff or billing strategy; I, the amount of support with the use of different (length, flow, frequency) using different accounting policies, which are similar to hop gear; J, advertising, allowing users to access the ICP advertising delivery fee service, and it can be divided Get royalty and Get amounts of the two to use; K, support access to different data networks using different accounting policies, and other factors to consider QoS; different L, support the use in different regions or areas billing policy, it is possible in the "hot spots" in different charge to the user. For example, with respect to the concept of "work area" on the "living area" to charge lower fees; M, support capping costs.

In addition, the discount is a very important means of SP and network operators to attract users, whether traditional voice services, or 3G for mobile data services, and discounts are pivotal position. Discount variety of ways, the current widespread use of rebates are the following: a, period discount - retaining the existing daily, week, holidays rebates. This approach can be extended to a metered charging mode.

b, the cumulative discount - including long cumulative discount, discount the cumulative flow, cumulative entry discount, the cumulative amount of discounts and other four kinds of rebates.

c, a cumulative discount - in accordance with the first use of the total, the total amount of time you use the discount d, user discounts - for certain user groups unified discount. All discounts can be tiring ride basis.

e, business discounts - for certain business unified discount.

In a specific embodiment of the present invention according to the above factors, a number of accounting rules customized components. Charging a business can be achieved by the grant price component and one or more charging rules components. Charging Rules components can be combined billing, and set a billing factor is a combination of the actual billing process using the grant price component of the base rate and billing factor to achieve a combination of a variety of additional charging rules count fee.

Basic Rate Information + billing factor information in practical applications, data services charging policies can be stored in approved price component parts of additional charging rules "to describe.

For example: corresponds to the short message service Internet content providers, its basic rate information as shown in Table I, Table I as a simple SMS tariff.

Image not available. View PDF

Table I Table it is the meaning of the pay-per-service, per charge 10 cents.

Different users additional accounting factor may be different, if the requirements of users while enjoying BONUS time discount factor accounting information as shown in Table II, Table II as a short message service charging factor table.

Image not available. View PDF

Table II Table II correspond to two discount, equivalent to two kinds of discount combined into a billing factor.

Both tables are basic information, practical application of the table structure is not limited to this.

Corresponding to the cumulative discount, as shown in Table III, Table 3 gives the BONUS table.

Image not available. View PDF

Table III Table III cumulative meaning that when users use the business 30 times, you can enjoy 20% discount Similarly, as shown in Table IV. Table IV is the time discount table.

Image not available. View PDF

Table 4 and Table IV meaning that at 22:00 ~ 23:59 minutes using business users, you can enjoy 50% discount.

The basic rate information and billing information combined factors, we get an accounting policy, such a billing policy can and bound to a business. Table V. Table V as an accounting policy SMS service.

Image not available. View PDF

Table V wherein the agent ID to SMS 8888, the accounting policy is: pay-per-service, a charge of 10 points, but if you use more than 30 times the cumulative, you can enjoy a 20% discount, if at 22:00 ~ 23: 59 between enjoying the business, you can enjoy a 50% discount.

If a user has used the service 30 times, and use the service at 22:30, then the user's actual charge amount = 1 (time) * 10 (points) * 0.8 * 0.5 = 4 (points) if demand fluctuates, Requirements In addition to supporting these two discount outside, and then add a user discount factor accounting description then just make changes, the revised accounting factor description in Table VI.

Image not available. View PDF

Table VI Thus, the launch customer discount member, you can easily add a dynamic type of discount, you do not need to modify the code completely, thereby achieving a dynamic and flexible accounting rules configuration purposes. Including six representatives user discounts.

For example: an individual mobile users subscribing to Internet content providers short message service, when the user receives messages, Internet content providers to send content billing records to the content accounting server, which contains the short message service is performed by the user, sending the number of text messages, send the time and other information. After the content accounting server receives the content billing records, remove OSS previously stored in the content accounting server in the user's personal information, including the user's account information, payment types (such as this user prepaid users), the user attributes for individual users, the user has no arrears records, and other information the user has paid. SMS content accounting server is performed based on the user, time to send text messages, send text messages number has exceeded a predetermined amount, and the user for individual users, and no arrears records to determine if the user should have the table of the six Three discount, so use Table 6 ID number is 0 billing factors accounting, billing and content billing server sends the results to the SCP, SCP deduct the cost on the user's account.

When the user performs data services, according to data services, content billing record information of the user information and Internet content providers / service provider (ICP / SP) obtained using the corresponding charging rule parts, content billing. Wherein the content billing record information may include: data service type, time the data service for execution of data flow of the data service, the number of times the data service execution.

Wherein the content billing can be achieved by the following steps: Step A, according to the data type of business, remove the corresponding charging rules in the corresponding parts in the accounting rules, according to the time the data service for execution of data flow of the data service the number of times the data service execution, an accounting rule for accounting; procedure B, determine whether the user charges prepaid type, if it is pre-paid billing results will be sent to the prepaid-processing equipment, for mobile data services is a service control point (SCP), prepaid billing processing apparatus according to the results of deductions from the user's account; otherwise, post-paid subscribers will be sent the results to the tent billing system.

Procedure C, tent system takes the accounting results based on user needs, to generate user billing.

Referring to Figure 1, Figure 1 is a block diagram of an invention implement content billing preferred embodiment. In this embodiment, the mobile data service billing. Wherein the content billing system consists of a dedicated server 110 to implement content billing, content billing server 110 and OSS 101, ICP / SP 102, SCP 104 and tents are connected to the system. Content billing server 110 and OSS 101 is a real-time synchronous message interface, or as files for data

transmission, ICP / SP 102, between SCP 104 in accordance with the operator interface specification for the connection. Wherein the content accounting server 110 and ICP / SP102 messages or files using interactive mode; the content accounting server used between 110 and SCP 104 EMPP protocol messages to interact. Interface to the present embodiment in accordance with the operator interface specification design is conducive to docking and other external devices.

In this embodiment of the content billing server 110 includes: operations support systems (OSS) interface module 111, the OSS 101 is connected with the contents of the billing module 113 to obtain the user's mobile data service contract user information from OSS 101 and send it to content billing module 113; Internet content provider / service provider (ICP / SP) interface module 112, the ICP / SP102 and content billing module connected to 113, ICP / SP 102 content billing record information to the content billing module 110.

Content billing module 113 is the main function module content billing, see Figure 2, Figure 2 is a block diagram shown in Figure 1 to achieve the implementation of the contents of the accounting module. Content billing module 113 comprises: billing engine 201, which, ICP / SP interface module OSS101 and ICP / SP102 respectively connected via OSS interface module 111) to obtain the user's mobile data service contract user information from OSS 101, a receiving ICP / SP 102 content billing record information sent and the user information and content billing record information to grant price component 202.

Grant price component 202 stores a basic rate of different types of mobile data services, mobile data services based on the type of mobile data service user's user information, content billing records removed from the corresponding one or more of the appropriate accounting rules section 203 accounting rules, mobile data services billing, and generate results based on accounting charge type.

Content billing server 110 of the present embodiment a plurality of pre-charging rules customized member 203, which depending on the type of mobile data services are stored in different charging rules. Charging Rules section 203 may vary as mobile data services, at any time to add, delete and modify. Visible, content billing system of the present embodiment by way of implementation of the components, add the new requirement is equivalent to adding new components, there is no effect on the original code. At the same time the components can provide external open interfaces, easy to expand.

In short, content billing module 113, based on the type of mobile data services, mobile data service user's user information, content billing record for mobile data services billing, and generate results based on accounting charge type.

Service control point (SCP) interface module 115, the SCP 104 billing module 113 is connected with the content, content billing module 113 generates prepaid subscribers accounting result to the service control node 104; if a single interface module 114, the content billing module 113 is connected with the camp system 103; the contents of the billing module 113 generates after paying user accounting system 103 sends the results to the tent.

In this embodiment of the service control point (SCP) interface module 115, and then a single interface module 114 constitutes a charge interface module, based on the type of data services paid billing results will be sent to the appropriate accounting treatment equipment - service control node 104 or tent system 103.

If a single interface module 114 and tent systems to FTP or FTAM transfer information when the user needs tent system interface module 114 through the bill to take the accounting content billing server 110 results. If a single interface module 114 may be composed of a separate bill to implement the interface machine, with content billing module 113 to transmit information by file format.

In this embodiment, the content accounting server 110 billing process, user information and content billing record information is important billing information, the user information may include: user account information, payment types, user attributes, arrears record; content billing record information may include: a mobile data service type, time of the mobile data services for execution of the data flow of mobile data services, the number of times the mobile data service execution.

Further, the content accounting server 110 of the present embodiment may be implemented by a plurality of servers; wherein the billing engine 201 may be implemented by a dedicated server, rating and charging rules 202 parts 203 parts distributed in other dedicated server host. Such billing and charging rules engine 201 203 members distributed on different hosts, to ensure the performance of the contents of the billing system.

Examples of content billing system of this embodiment, the use of a dedicated server to achieve, is not dependent on other devices, messaging mechanism or API function calls to interact with other equipment used to make the contents of the billing module with high independence can be independent testing, reducing the effort required to develop and test, easy to maintain.

Also, the present embodiment can dynamically add or modify parts of combination accounting rules, without modifying the code or restart the billing system with great flexibility, and satisfy the changing needs Flexible billing features.

Seen from the above-described embodiment, the data traffic of the invention content billing method and billing system, independence, flexibility, scalability, openness and distribution characteristics, to achieve a data service based on content billing, data services to meet the flexible billing requirements.

REFERENCED BY

Citing Patent	Filing date	Publication date	Applicant	Title
CN100394737C	11 Jul 2005	11 Jun 2008	西安大唐电信有限公司	Method for accessing network server and supporting system
CN100596074C	9 Feb 2007	24 Mar 2010	华为技术有限公司	Charge mode providing method and charge control system
CN101582776B	15 May 2008	21 Nov 2012	浙江大学	Service charging method and service charging system
CN101800824A *	4 Mar 2010	11 Aug 2010	中兴通讯股份有限公司	Method and device for charging
CN102098650A *	21 Jan 2011	15 Jun 2011	中国联合网络通信集团有限公司	Content charging-based flow adaptive method and system
CN102098650B	21 Jan 2011	3 Jul 2013	中国联合网络通信集团有限公司	Content charging-based flow adaptation method and system
CN102255734A *	19 May 2010	23 Nov 2011	华为技术有限公司	Charging method of content business, apparatus and system thereof
WO2006116894A1 *	29 Apr 2005	9 Nov 2006	Utstarcom Telecom Co Ltd	A method of flexible setting the charging mode in ims system
WO2007051416A1 *	2 Nov 2006	10 May 2007	Huawei Tech Co Ltd	A charging method and system

* Cited by examiner

CLASSIFICATIONS

International Classification	H04W4/24, H04M17/00, H04L12/14

LEGAL EVENTS

Date	Code	Event	Description
14 Oct 2009	C14	Granted	
7 Dec 2005	C10	Request of examination as to substance	
19 Jan 2005	C06	Publication	

Google Home - Sitemap - USPTO Bulk Downloads - Privacy Policy - Terms of Service - About Google Patents - Send Feedback

Electronic Acknowledgement Receipt

EFS ID:	22761797
Application Number:	14667516
International Application Number:	
Confirmation Number:	5348
Title of Invention:	Network System With Common Secure Wireless Message Service Serving Multiple Applications on Multiple Wireless Devices
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	James E. Harris/Ann Taylor
Filer Authorized By:	James E. Harris
Attorney Docket Number:	RALEP007C11C4
Receipt Date:	26-JUN-2015
Filing Date:	24-MAR-2015
Time Stamp:	19:06:26
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	P007C11C4.pdf	613655 777ad701240342b19b5547dacd118273d0239792	no	8
Warnings:					
Information:					

2	Foreign Reference	2063.pdf	2400276 5c7addfc40b293a3442a4c140083d3fc5d876114	no	21
Warnings:					
Information:					
3	Foreign Reference	2064.pdf	2345898 db3b0051c6d9ab3dfa64f05d6324394e5fc54486	no	20
Warnings:					
Information:					
4	Foreign Reference	2065.pdf	2381976 7796f26254f7db3b899626b2e7332663eaff0633	no	25
Warnings:					
Information:					
5	Non Patent Literature	3040_Ahmed.pdf	698684 312cdbfa74f55adbbd7f0eee7032be26a77e3ad5	no	10
Warnings:					
Information:					
6	Non Patent Literature	3041_Kassar.pdf	840076 1b87a4e38876abbcb73a0c7a689d940a997ba013	no	14
Warnings:					
Information:					
7	Non Patent Literature	3042_Kaufmann.pdf	3412131 987a5e9e6c5cadcf6cd5982f4c181ac27b6dafe7	no	283
Warnings:					
Information:					
8	Non Patent Literature	3043_Sadeh.pdf	1095284 adc744cb7b194a97b6f3ac3e1b28a65e042a8d9f	no	16
Warnings:					
Information:					
			Total Files Size (in bytes):	13787980	

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

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

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

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

PTO/SB/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	14667516
Filing Date	2015-03-24
First Named Inventor	Raleigh
Art Unit	2431
Examiner Name	not yet assigned
Attorney Docket Number	RALEP007C11C4

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	5577100		1996-11-19	McGREGOR et al.	
	2	5794142		1998-08-11	VANTTILA et al.	
	3	5892900		1999-04-06	GINTER et al.	
	4	5903845		1999-05-11	BUHRMANN et al.	
	5	5933778		1999-08-03	BUHRMANN et al.	
	6	5940472		1999-08-17	NEWMAN et al.	
	7	6047268		2000-04-04	BARTOLI et al.	
	8	6078953		2000-06-20	VAID et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	9	6098878		2000-08-08	DENT et al.	
	10	6141686		2000-10-31	JACKOWSKI et al.	
	11	6148336		2000-11-14	THOMAS et al.	
	12	6198915		2001-03-06	McGREGOR et al.	
	13	6263055		2001-07-17	GARLAND et al.	
	14	6317584		2001-11-13	ABU-AMARA et al.	
	15	6418147		2002-07-09	WIEDEMAN, Robert A.	
	16	6449479		2002-09-10	SANCHEZ, Eduardo	
	17	6532235		2003-03-11	BENSON et al.	
	18	6532579		2003-03-11	SATO et al.	
	19	6539082		2003-03-25	LOWE et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	20	6563806		2003-05-13	YANO et al.	
	21	6574321		2003-06-03	COX et al.	
	22	6574465		2003-06-03	MARSH et al.	
	23	6603969		2003-08-05	VUORISTO et al.	
	24	6639975		2003-10-28	O'NEAL et al.	
	25	6650887		2003-11-18	McGREGOR et al.	
	26	6651101		2003-11-18	GAI et al.	
	27	6658254		2003-12-02	PURDY et al.	
	28	6684244		2004-01-27	GOLDMAN et al.	
	29	6725031		2004-04-20	WATLER et al.	
	30	6765864		2004-07-20	NATARAJAN et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	31	6785889		2004-08-31	WILLIAMS, Peter	
	32	6829596		2004-12-07	FRAZEE, Steve	
	33	6829696		2004-12-07	BALMER et al.	
	34	6920455		2005-07-19	WESCHLER, Paul	
	35	6952428		2005-10-04	NECKA et al.	
	36	6965667		2005-11-15	TRABANDT et al.	
	37	6996076		2006-02-07	FORBES et al.	
	38	6998985		2006-02-14	REISMAN et al.	
	39	7024200		2006-04-04	McKENNA et al.	
	40	7027408		2006-04-11	NABKEL et al.	
	41	7042988		2006-05-09	JUITT et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	42	7058968		2006-06-06	ROWLAND et al.	
	43	7069248		2006-06-27	HUBER, Adriano	
	44	7092696		2006-08-15	HOSAIN et al.	
	45	7142876		2006-11-28	TROSSEN et al.	
	46	7158792		2007-01-02	COOK et al.	
	47	7174174		2007-02-06	BORIS et al.	
	48	7180855		2007-02-20	LIN , Wei	
	49	7197321		2007-03-27	ERSKINE et al.	
	50	7242920		2007-07-10	MORRIS, Robert P.	
	51	7245901		2007-07-17	McGREGOR et al.	
	52	7280816		2007-10-09	FRATTI et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	53	7280818		2007-10-09	CLAYTON, Steve	
	54	7289489		2007-10-30	KUNG et al.	
	55	7290283		2007-10-30	COPELAND III, John A.	
	56	7317699		2008-01-08	GODFREY et al.	
	57	7322044		2008-01-22	HRASTAR, Scott E.	
	58	7324447		2008-01-29	MORFORD, Michael Robert	
	59	7325037		2008-01-29	LAWSON, Karen L.	
	60	7349695		2008-03-25	OOMMEN et al.	
	61	7353533		2008-04-01	WRIGHT et al.	
	62	7356337		2008-04-08	FLORENCE, Shahar	
	63	7366497		2008-04-29	NAGATA, Hideaki	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	64	7373136		2008-05-13	WATLER et al.	
	65	7388950		2008-06-17	ELSEY et al.	
	66	7401338		2008-07-15	BOWEN et al.	
	67	7403763		2008-07-22	MAES, Stephane H.	
	68	7418253		2008-08-26	KAVANAH, Alan	
	69	7421004		2008-09-02	FEHER, Kamilo	
	70	7450591		2008-11-11	KORLING et al.	
	71	7450927		2008-11-11	CRESWELL et al.	
	72	7486185		2009-02-03	CULPEPPER et al.	
	73	7499537		2009-03-03	ELSEY et al.	
	74	7516219		2009-04-07	MOGHADDAM et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	75	7574731		2009-08-11	FASCENDA, Anthony C.	
	76	7580857		2009-08-25	VanFLEET et al.	
	77	7610328		2009-10-27	HAASE et al.	
	78	7617516		2009-11-10	HUSLAK et al.	
	79	7620065		2009-11-17	FALARDEAU, Eric	
	80	7620162		2009-11-17	AARON et al.	
	81	7647047		2010-01-12	MOGHADDAM et al.	
	82	7650137		2010-01-19	JOBS et al.	
	83	7668903		2010-02-23	EDWARDS et al.	
	84	7693720		2010-04-06	KENNEWICK et al.	
	85	7720505		2010-05-18	GOPI et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	86	7734784		2010-06-08	ARAUJO et al.	
	87	7747240		2010-06-29	BRISCOE et al.	
	88	7747699		2010-06-29	PRUEITT et al.	
	89	7792708		2010-09-07	ALVA, Jessi	
	90	7797204		2010-09-14	BALENT, Bruce F.	
	91	7797401		2010-09-14	STEWART et al.	
	92	7822837		2010-10-26	URBAN et al.	
	93	7848768		2010-12-07	OMORI et al.	
	94	7868778		2011-01-11	KENWRIGHT, David Norris	
	95	7873705		2011-01-18	KALISH, Dan	
	96	7882029		2011-02-01	WHITE, Craig R.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	97	7929960		2011-04-19	MARTIN et al.	
	98	7937069		2011-05-03	RASSAM, Frederic	
	99	7941184		2011-05-10	PRENDERGAST et al.	
	100	7949529		2011-05-24	WEIDER et al.	
	101	7957511		2011-06-07	DRUDIS et al.	
	102	7975184		2011-07-05	GOFF et al.	
	103	7984130		2011-07-19	BOGINENI et al.	
	104	7986935		2011-07-26	D'SOUZA et al.	
	105	8005459		2011-08-23	BALSILLIE, Jim	
	106	8010080		2011-08-30	THENTHIRUPERAI et al.	
	107	8010081		2011-08-30	ROSKOWSKI, Steve	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	108	8015133		2011-09-06	WU et al.	
	109	8015234		2011-09-06	LUM et al.	
	110	8019687		2011-09-13	WANG et al.	
	111	8023425		2011-09-20	RALEIGH, Gregory G.	
	112	8095666		2012-01-10	SCHMIDT et al.	
	113	8099077		2012-01-17	CHOWDHURY et al.	
	114	8099517		2012-01-17	JIA et al.	
	115	8144591		2012-03-27	GHAI et al.	
	116	8170553		2012-05-01	BENNETT, James D.	
	117	6606744		2003-08-12	MIKURAK, Michael G.	
	118	7336960		2008-02-26	ZAVALKOVSKY et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	119	8190675		2012-05-29	TRIBBETT, David	
	120	8194549		2012-06-05	HUBER et al.	
	121	8200775		2012-06-12	MOORE, James F.	
	122	8135392		2012-03-13	MARCELLINO et al.	
	123	7953808		2011-05-31	SHARP et al.	
	124	6502131		2002-12-31	VAID, Aseem et al.	
	125	6505114		2003-01-07	LUCIANI, Sergio	
	126	6763000		2004-07-13	WALSH, Peter J.	
	127	6967958		2005-11-22	ONO, Yoshiyuki et al.	
	128	7644267		2010-01-05	YLIKOSKI, Martti et al.	
	129	7710932		2010-05-04	MUTHUSWAMY, Sivakumar et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	130	7881199		2011-02-01	KRSTULICH, Zlatko	
	131	7886047		2011-02-08	POTLURI, Dora	
	132	7911975		2011-03-22	DROZ, Patrick et al.	
	133	8050275		2011-11-01	IYER, Jayaraman R.	
	134	8194553		2012-06-05	LIANG, Zhi Yong et al.	
	135	8239520		2012-08-07	GRAH, Adrian	
	136	7890084		2011-02-15	Dudziak, Thaddeus Jude et al.	
	137	7890111		2011-02-15	Bugenhagen, Michael K.	
	138	6226277		2001-05-01	Chuah, Mooi Choo	
	139	6839340		2005-01-04	Voit, Eric A. et al.	
	140	6922562		2005-07-26	Ward, Stephen L. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	141	7620041		2009-11-17	Dunn, Jeffrey H. et al.	
	142	7627314		2009-12-01	Carlson, Steven I. et al.	
	143	7792538		2010-09-07	Kozisek, Steven E.	
	144	7801523		2010-09-21	Kenderov, Stoyan	
	145	7877090		2011-01-25	Maes, Stephane H.	
	146	7912025		2011-03-22	Pattenden, Christopher E. S. et al.	
	147	7948968		2011-05-24	Voit, Eric A. et al.	
	148	7970426		2011-06-28	Poe, Brian R. et al.	
	149	8185158		2012-05-22	Tamura, Motoshi et al.	
	150	8254915		2012-08-28	Kozisek, Steven E.	
	151	7418257		2008-08-26	Kim, Myong-Ju	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	152	8126123		2012-02-28	Cai, Yigang et al.	
	153	7903553		2011-03-08	Liu, Enhui	
	154	8155620		2012-04-10	Wang, Jun et al.	
	155	8238287		2012-08-07	Gopi, Paramesh et al.	
	156	7113997		2006-09-26	Jayapalan, Jay et al.	
	157	5594777		1997-01-14	Makkonen, Matti et al.	
	158	8244241		2012-08-14	Montemurro, Michael	
	159	7756534		2010-07-13	Anupam, Vinod et al.	
	160	7636574		2009-12-22	Poosala, Viswanath	
	161	6678516		2004-01-13	Nordman, Ian et al.	
	162	6477670		2002-11-05	Ahmadvand, Nima	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	163	6038452		2000-03-14	Strawczynski, Leo et al.	
	164	8108520		2012-01-31	Ruutu, Jussi et al.	
	165	7778643		2010-08-17	Laroia, Rajiv et al.	
	166	7668176		2010-02-23	Chuah, Mooi Choo	
	167	7515608		2009-04-07	Yuan, Yuan et al.	
	168	7251218		2007-07-31	Jorgensen, Jacob W.	
	169	7002920		2006-02-21	Ayyagari, Deepak et al.	
	170	7685131		2010-03-23	Batra, Vishal Singh et al.	
	171	7283561		2007-10-16	Picher-Dempsey, Heidi	
	172	7212491		2007-05-01	Koga, Takahiro	
	173	6683853		2004-01-27	Kannas, Chris et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	174	7609700		2009-10-27	Ying, Wen-Ping et al.	
	175	8255515		2012-08-28	MELMAN, David et al.	
	176	7945240		2011-05-17	KLOCK, Jacqueline et al.	
	177	7912056		2011-03-22	BRASSEM, Wayne	
	178	7920529		2011-04-05	MAHLER, Roger et al.	
	179	8184530		2012-05-22	SWAN, Tim L. et al.	
	180	8214536		2012-07-03	ZHAO, Wen	
	181	8213363		2012-07-03	YING, Wen-Ping et al.	
	182	8255689		2012-08-28	KIM, Eun Ah et al.	
	183	7746854		2010-06-29	AMBE, Shekhar et al.	
	184	7068600		2006-06-27	CAIN, Joseph Bibb	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	185	6876653		2005-04-05	AMBE, Shekhar et al.	
	186	6631122		2003-10-07	ARUNACHALAM, Vaidhyanathan et al.	
	187	7599288		2009-10-06	COLE, Raymond E. et al.	
	188	7546629		2009-06-09	ALBERT, Anthony et al.	
	189	7747730		2010-06-29	HARLOW, James D.	
	190	7609650		2009-10-27	ROSKOWSKI, Steve et al.	
	191	6581092		2003-06-17	MOTOYAMA, Tetsuro	
	192	7283963		2007-10-16	FITZPATRICK, John E. et al.	
	193	8271049		2012-09-18	SILVER, Andrew et al.	
	194	7644151		2010-01-05	JERRIM, John et al.	
	195	8291238		2012-10-16	GINTER, Karl L. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	196	8068824		2011-11-29	SHAN, Xueshan et al.	
	197	7228354		2007-06-05	CHAMBLISS, David Darden et al.	
	198	5283904		1994-02-01	CARSON, David G. et al.	
	199	8208919		2012-06-26	KOTECHA, Lalit Ratilal	
	200	8185152		2012-05-22	GOLDNER, Alla	
	201	7844728		2010-11-30	ANDERSON, Thomas W. et al.	
	202	7873344		2011-01-18	BOWSER, Robert et al.	
	203	7856226		2010-12-21	WONG, Ellis L. et al.	
	204	7948952		2011-05-24	HURTTA, Tuija et al.	
	205	7957020		2011-06-07	MINE, Ryuta et al.	
	206	7346410		2008-03-18	UCHIYAMA, Kenji	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	207	7167078		2007-01-23	POURCHOT, Shawn C.	
	208	8102814		2012-01-24	RAHMAN, Shahriar I. et al.	
	209	7970350		2011-06-28	SHEYNMAN, Arnold	
	210	8094551		2012-01-10	HUBER, Kurt Donald et al.	
	211	8135388		2012-03-13	Gailloux, Michael A. et al.	
	212	6947723		2005-09-20	Gurnani, Roger et al.	
	213	8350700		2013-01-08	Fast, Raymond D. et al.	
	214	8204190		2012-06-19	Bang, Jung-Hee et al.	
	215	7865182		2011-01-04	Macaluso, Anthony G.	
	216	7962622		2011-06-14	Friend, John et al.	
	217	7583964		2009-09-01	Wong, Gregory A.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	218	7565141		2009-07-21	Macaluso, Anthony G.	
	219	7373179		2008-05-13	Stine, Ted et al.	
	220	7236780		2007-06-26	Benco, David S.	
	221	7039403		2006-05-02	Wong, Gregory A.	
	222	8370477		2013-02-05	Short, Joel E. et al.	
	223	8364806		2013-01-29	Short, Joel E. et al.	
	224	8279067		2012-10-02	BERGER, Thomas R. et al.	
	225	8213296		2012-07-03	SHANNON, Frank M. et al.	
	226	8019868		2011-09-13	RAO, Goutham et al.	
	227	8005988		2011-08-23	MAES, Stephane H.	
	228	7978627		2011-07-12	TAYLOR, William Scott et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	229	7711848		2010-05-04	MAES, Stephane H.	
	230	6782412		2004-08-24	BROPHY, Kevin et al.	
	231	6081591		2000-06-27	SKOOG, Frederick H.	
	232	6064878		2000-05-16	DENKER, John Stewart et al.	
	233	7730123		2010-06-01	ERICKSON, Richard R. et al.	
	234	8024397		2011-09-20	ERICKSON, Richard R. et al.	
	235	8156206		2012-04-10	KILEY, Kevin J. et al.	
	236	8126722		2012-02-28	ROBB, Terence Alan et al.	
	237	6754470		2004-06-22	Hendrickson, Keith et al.	
	238	8122128		2012-02-21	Burke, II, Robert M. et al.	
	239	8149823		2012-04-03	Turcan, Diane Brown et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	240	8131256		2012-03-06	MARTTI, Jyrki et al.	
	241	6381316		2002-04-30	JOYCE, Simon James et al.	
	242	7965983		2011-06-21	SWAN, Tim et al.	
	243	8284740		2012-10-09	O'CONNOR, Dennis M.	
	244	8116223		2012-02-14	TIAN, Dan et al.	
	245	6154738		2000-11-28	CALL, Charles Gainor	
	246	8423016		2013-04-16	BUCKLEY, Adrian et al.	
	247	6035281		2000-03-07	Crosskey, James P. et al.	
	248	6996393		2006-02-07	Pyhalammi, Seppo et al.	
	249	7760711		2010-07-20	Kung, Fen-Chung et al.	
	250	8000318		2011-08-16	Wiley, William L. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	251	8098579		2012-01-17	Ray, Amar N. et al.	
	252	8155670		2012-04-10	Fullam, Scott et al.	
	253	8374090		2013-02-12	Morrill, Robert J. et al.	
	254	7457265		2008-11-25	Julka, Vibhor et al.	
	255	7729326		2010-06-01	Sekhar, Ramesh	
	256	7929973		2011-04-19	Zavalkovsky, Arthur et al.	
	257	7945945		2011-05-17	Graham, Richard et al.	
	258	8059530		2011-11-15	Cole, Terry L.	
	259	8280354		2012-10-02	Smith, Christopher et al.	
	260	8266681		2012-09-11	Deshpande, Sumit B. et al.	
	261	8331293		2012-12-11	Sood, Kapil	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	262	8019820		2011-09-13	Son, Giyeong et al.	
	263	8155155		2012-04-10	Chow, Albert T. et al.	
	264	8191116		2012-05-29	Gazzard, Daryl	
	265	6292828		2001-09-18	Williams, David L.	
	266	7043226		2006-05-09	Yamauchi, Toshiaki	
	267	7472189		2008-12-30	Mallya, Arvind R. et al.	
	268	7944948		2011-05-17	Chow, Albert T. et al.	
	269	7802724		2010-09-28	Nohr, Steven Paul	
	270	8005009		2011-08-23	McKee, Neil et al.	
	271	7760861		2010-07-20	Croak, Marian et al.	
	272	8060463		2011-11-15	Spiegel, Joel R.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	273	8224773		2012-07-17	Spiegel, Joel R.	
	274	8352980		2013-01-08	Howcroft, Jerald Robert	
	275	8386386		2013-02-26	Zhu, Kevin	
	276	8340718		2012-12-25	Colonna, Massimo et al.	
	277	8385896		2013-02-26	Proctor Jr., James A. et al.	
	278	8320949		2012-11-27	Matta, Sudheer Poorna Chandra	
	279	8279864		2012-10-02	Wood, Daniel M.	
	280	8271045		2012-09-18	Parolkar, Satish et al.	
	281	8233883		2012-07-31	De Froment, Eric	
	282	8224382		2012-07-17	Bultman, Michael J.	
	283	8184590		2012-05-22	Rosenblatt, Ariel	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	284	8174970		2012-05-08	Adamczyk, Maria et al.	
	285	8165576		2012-04-24	Raju, Vishwanath et al.	
	286	8073721		2011-12-06	Lewis, Lundy	
	287	8032899		2011-10-04	Archer, Charles J. et al.	
	288	7974624		2011-07-05	Gallagher, Michael D. et al.	
	289	7907970		2011-03-15	Park, Vincent D. et al.	
	290	7778176		2010-08-17	Morford, Michael Robert	
	291	7725570		2010-05-25	Lewis, Lundy	
	292	7634388		2009-12-15	Archer, Charles J. et al.	
	293	7633438		2009-12-15	Tysowski, Piotr Konrad	
	294	7593417		2009-09-22	Wang, James et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	295	7551922		2009-06-23	Roskowski, Steve et al.	
	296	7545782		2009-06-09	Rayment, Stephen G. et al.	
	297	7039037		2006-05-02	Wang, Jiwei R. et al.	
	298	6928280		2005-08-09	Xanthos, James et al.	
	299	6765925		2004-07-20	Sawyer, Wilson et al.	
	300	5889477		1999-03-30	Fastenrath, Ulrich	

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] ¡	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]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	1	1463238	EP		2004-09-29	Alcatel		☐
	2	1739518	EP		2007-01-03	Research In Motion Limited		☐
	3	1772988	EP		2007-04-11	Huawei Technologies Co., Ltd.		☐
	4	1978772	EP		2008-10-08	British Telecommunications Public Limited Company		☐
	5	1999065185	WO		1999-12-16	British Telecommunications Public Limited Company		☐
	6	2003014891	WO		2003-02-20	The Boeing Company		☐
	7	2003058880	WO		2003-07-17	Telia AB		☐
	8	2004028070	WO		2004-04-01	Credant Technologies, Inc.		☐
	9	2004077797	WO		2004-09-10	Boston Communications Group, Inc. (Erskine)		☐
	10	2004095753	WO		2004-11-04	Motorola Inc.		☐
	11	2006004467	WO		2006-01-12	Telefonaktiebolaget LM Ericsson		☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	12	2006050758	WO		2006-05-18	Telefonaktiebolaget LM Ericsson		☐
	13	2006073837	WO		2006-07-13	Symbol Technologies, Inc.		☐
	14	2006077481	WO		2006-07-27	TrueContext Corporation		☐
	15	2006130960	WO		2006-12-14	Mobidia, Inc.		☐
	16	2007001833	WO		2007-01-04	Symbol Technologies, Inc.		☐
	17	2007014630	WO		2007-02-08	Telefonaktiebolaget LM Ericsson		☐
	18	2007018363	WO		2007-02-15	Upresto, Inc.		☐
	19	2007053848	WO		2007-05-10	Mobile Armor, LLC		☐
	20	2007069245	WO		2007-06-21	Yoggie Security Systems, Inc.		☐
	21	2007107701	WO		2007-09-27	British Telecommunications Public Limited Company		☐
	22	2008017837	WO		2008-02-14	Symbian Software Limited		☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	23	2008051379	WO		2008-05-02	Verizon Services Corp.		☐
	24	2008066419	WO		2008-06-05	Telefonaktiebolaget LM Ericsson		☐
	25	2008080139	WO		2008-07-03	Integrated Mobile, Inc.		☐
	26	2008080430	WO		2008-07-10	Telecom Italia S.P.A.		☐
	27	2008099802	WO		2008-08-21	NEC Corporation		☐
	28	2010088413	WO		2010-08-05	Headwater Partners I LLC		☐
	29	2006120558	WO		2006-11-16	Nokia Corp.		☐
	30	1889777A	CN		2006-07-19	Huawei Tech. Co. Ltd.		☐
	31	101155343A	CN		2006-09-29	Huawei Tech. Co. Ltd.		☐
	32	101035308A	CN		2006-03-09	Huawei Tech. Co. Ltd.		☐
	33	2007124279	WO		2007-11-01	Cisco Technology, Inc., et al.		☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	34	2005008995	WO		2005-01-27	Starhub Ltd.		☐
	35	1998058505	WO		1998-12-23	Sonera Oy		☐
	36	2007097786	WO		2007-08-30	Sony Ericsson Mobile Communications AB		☐

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	3rd Generation Partnership Project, "Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) Enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) Access," Release 8, Document No. 3GPP TS 23.401, V8.4.0, December 2008	☐
	2	3rd Generation Partnership Project, "Technical Specification Group Services and System Aspects; Policy and Charging Control Architecture," Release 8, Document No. 3GPP TS 23.203, V8.4.0, December 2008	☐
	3	ALONISTIOTI et al., "Intelligent Architectures Enabling Flexible Service Provision and Adaptability," 2002	☐
	4	Amazon Technologies, Inc., "Kindle™ User's Guide," 3rd Edition, Copyright 2004-2009	☐
	5	CHANDRASEKHAR et al., "Femtocell Networks: A Survey," June 28, 2008	☐
	6	CHAOUCHI et al., "Policy Based Networking in the Integration Effort of 4G Networks and Services," 2004 IEEE	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	7	Cisco Systems, Inc., "Cisco Mobile Exchange (CMX) Solution Guide: Chapter 2 - Overview of GSM, GPRS, and UMTS," November 4, 2008	☐
	8	DIKAIAKOS et al., "A Distributed Middleware Infrastructure for Personalized Services," November 24, 2003	☐
	9	European Commission, "Data Roaming Tariffs - Transparency Measures," [online] retrieved from http://web.archive.org/web/20081220232754/http://ec.europa.eu/information_society/activities/roaming/data/measures/index_en.htm, December 20, 2008 [retrieved May 16, 2012]	☐
	10	FAROOQ et al., "An IEEE 802.16 WiMax Module for the NS-3 Simulator," March 2-6, 2009	☐
	11	HAN et al., "Information Collection Services for Qos-Aware Mobile Applications," 2005	☐
	12	HARTMANN et al., "Agent-Based Banking Transactions & Information Retrieval - What About Performance Issues?" 1999	☐
	13	Hewlett-Packard Development Company, LP, "IP Multimedia Services Charging," white paper, January 2006	☐
	14	HOSSAIN et al., "Gain-Based Selection of Ambient Media Services in Pervasive Environments," Mobile Networks and Applications. 03 October 2008	☐
	15	KNIGHT et al., "Layer 2 and 3 Virtual Private Networks: Taxonomy, Technology, and Standarization Efforts," IEEE Communications Magazine, June 2004	☐
	16	KOUTSOPOULOU et al., "Middleware Platform for the Support of Charging Reconfiguration Actions," 2005	☐
	17	KYRIAKAKOS et al., "Ubiquitous Service Provision in Next Generation Mobile Networks," Proceedings of the 13th IST Mobile and Wireless Communications Summit, Lyon, France, June 2004	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	18	LI, Yu, "Dedicated E-Reading Device: The State of the Art and The Challenges," Scroll, Vol. 1, No. 1, 2008	☐
	19	NILSSON et al., "A Novel MAC Scheme for Solving the QoS Parameter Adjustment Problem in IEEE802.11e EDCA," February 2006	☐
	20	OPPLIGER, Rolf, "Internet Security: Firewalls and Bey," Communications of the ACM, May 1997, Vol. 40. No. 5	☐
	21	RAO et al., "Evolution of Mobile Location-Based Services," Communication of the ACM, December 2003	☐
	22	STEGLICH, Stephan, "I-Centric User Interaction," November 21, 2003	☐
	23	VAN EIJK, et al., "GigaMobile, Agent Technology for Designing Personalized Mobile Service Brokerage," July 1, 2002	☐
	24	ZHU et al., "A Survey of Quality of Service in IEEE 802.11 Networks," IEEE Wireless Communications, August 2004	☐
	25	ANTON, B. et al., "Best Current Practices for Wireless Internet Service Provider (WISP) Roaming"; Release Date February 2003, Version 1.0; Wi-Fi Alliance – Wireless ISP Roaming (WISPr)	☐

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	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

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.

☐ Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ None

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	/James E. Harris/	Date (YYYY-MM-DD)	2015-04-29
Name/Print	James E. Harris	Registration Number	40013

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.

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	14667516
Filing Date	2015-03-24
First Named Inventor	Raleigh
Art Unit	2431
Examiner Name	not yet assigned
Attorney Docket Number	RALEP007C11C4

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	20020022472		2002-02-21	WATLER et al.	
	2	20020120540		2002-08-29	KENDE et al.	
	3	20020131404		2002-09-19	MEHTA et al.	
	4	20020138601		2002-09-26	PIPONIUS et al.	
	5	20020176377		2002-11-28	HAMILTON, Thomas E.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	6	20020199001		2002-12-26	WENOCUR et al.	
	7	20030004937		2003-01-02	SALMENKAITA et al.	
	8	20030005112		2003-01-02	KRAUTKREMER, Todd Joseph	
	9	20030013434		2003-01-16	ROSENBERG et al.	
	10	20030018524		2003-01-23	FISHMAN et al.	
	11	20030046396		2003-03-06	RICHTER et al.	
	12	20030050070		2003-03-13	MASHINSKY et al.	
	13	20030050837		2003-03-13	KIM, Do Sik	
	14	20030088671		2003-05-08	KLINKER et al.	
	15	20030133408		2003-07-17	CHENG et al.	
	16	20030161265		2003-08-28	CAO et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	17	20030182420		2003-09-25	JONES et al.	
	18	20030182435		2003-09-25	REDLICH et al.	
	19	20030220984		2003-11-27	JONES et al.	
	20	20030224781		2003-12-04	MILFORD et al.	
	21	20030229900		2003-12-11	REISMAN, Richard	
	22	20030236745		2003-12-25	HARTSELL et al.	
	23	20040019539		2004-01-29	RAMAN et al.	
	24	20040021697		2004-02-05	BEATON et al.	
	25	20040030705		2004-02-12	BOWMAN-AMUAH, Michel K.	
	26	20040044623		2004-03-04	WAKE et al.	
	27	20040047358		2004-03-11	CHEN et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	28	20040073672		2004-04-15	FASCENDA, Anthony C.	
	29	20040082346		2004-04-29	SKYTT et al.	
	30	20040098715		2004-05-20	AGHERA et al.	
	31	20040103193		2004-05-27	PANDYA et al.	
	32	20040107360		2004-06-03	HERRMANN et al.	
	33	20040127200		2004-07-01	SHAW et al.	
	34	20040132427		2004-07-08	LEE et al.	
	35	20040168052		2004-08-26	CLISHAM et al.	
	36	20040198331		2004-10-07	COWARD et al.	
	37	20040236547		2004-11-25	RAPPAPORT et al.	
	38	20040249918		2004-12-09	SUNSHINE, Roger N.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	39	20050021995		2005-01-27	LAL et al.	
	40	20050048950		2005-03-03	MORPER, Hans-Jochen	
	41	20050055291		2005-03-10	BEVENTE et al.	
	42	20050055309		2005-03-10	WILLIAMS et al.	
	43	20050060266		2005-03-17	DEMELLO et al.	
	44	20050097516		2005-05-05	DONNELLY et al.	
	45	20050107091		2005-05-19	VANNITHAMBY et al.	
	46	20050128967		2005-06-16	SCOBBIE, Donald MacGregor	
	47	20050166043		2005-07-28	ZHANG et al.	
	48	20050183143		2005-08-18	ANDERHOLM et al.	
	49	20050198377		2005-09-08	FERGUSON et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	50	20050216421		2005-09-29	BARRY et al.	
	51	20050228985		2005-10-13	YLIKOSKI et al.	
	52	20050238046		2005-10-27	HASSAN et al.	
	53	20050246282		2005-11-03	NASLUND et al.	
	54	20050250508		2005-11-10	GUO et al.	
	55	20050254435		2005-11-17	MOAKLEY et al.	
	56	20050266825		2005-12-01	CLAYTON, Steve	
	57	20050266880		2005-12-01	GUPTA, Vivek G.	
	58	20060014519		2006-01-19	MARSH et al.	
	59	20060019632		2006-01-26	CUNNINGHAM et al.	
	60	20060026679		2006-02-02	ZAKAS, Philip H.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	61	20060034256		2006-02-16	ADDAGATLA et al.	
	62	20060040642		2006-02-23	BORIS et al.	
	63	20060045245		2006-03-02	AARON et al.	
	64	20060048223		2006-03-02	LEE et al.	
	65	20060072646		2006-04-06	FEHER, Kamilo	
	66	20060085543		2006-04-20	HRASTAR et al.	
	67	20060112016		2006-05-25	ISHIBASHI, Yoshihito	
	68	20060143098		2006-06-29	LAZARIDIS, Mihal	
	69	20060165060		2006-07-27	DUA, Robin	
	70	20060178917		2006-08-10	MERRIAM et al.	
	71	20060178918		2006-08-10	MIKURAK, Michael G.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	72	20060183462		2006-08-17	KOLEHMAINEN, Mikko	
	73	20060190314		2006-08-24	HERNANDEZ, Rick	
	74	20060199608		2006-09-07	DUNN et al.	
	75	20060206904		2006-09-14	WATKINS et al.	
	76	20060218395		2006-09-28	MAES, Stephane H.	
	77	20060233108		2006-10-19	KRISHNAN, Murali R.	
	78	20060233166		2006-10-19	BOU-DIAB et al.	
	79	20060236095		2006-10-19	SMITH et al.	
	80	20060242685		2006-10-26	HEARD et al.	
	81	20060258341		2006-11-16	MILLER et al.	
	82	20060291477		2006-12-28	CROAK et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	83	20070019670		2007-01-25	FALARDEAU, Eric	
	84	20070022289		2007-01-25	ALT et al.	
	85	20070036312		2007-02-15	CAI et al.	
	86	20070055694		2007-03-08	RUGE et al.	
	87	20070061243		2007-03-15	RAMER et al.	
	88	20070076616		2007-04-05	NGO et al.	
	89	20070093243		2007-04-26	KAPADEKAR et al.	
	90	20070100981		2007-05-03	ADAMCZYK et al.	
	91	20070101426		2007-05-03	LEE et al.	
	92	20070104126		2007-05-10	CALHOUN et al.	
	93	20070130315		2007-06-07	FRIEND et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	94	20070140113		2007-06-21	GEMELOS, Steven	
	95	20070140275		2007-06-21	BOWMAN et al.	
	96	20070198656		2007-08-23	MAZZAFERRI et al.	
	97	20070220251		2007-09-20	ROSENBERG et al.	
	98	20070226225		2007-09-27	YIU et al.	
	99	20070243862		2007-10-18	COSKUN et al.	
	100	20070248100		2007-10-25	ZUBERI et al.	
	101	20070254675		2007-11-01	ZORLU OZER et al.	
	102	20070255848		2007-11-01	SEWALL et al.	
	103	20070259673		2007-11-08	WILLARS et al.	
	104	20070263558		2007-11-15	SALOMONE, Leonardo	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	105	20070274327		2007-11-29	KAARELA et al.	
	106	20070282896		2007-12-06	WYDROUG et al.	
	107	20070294395		2007-12-20	STRUB et al.	
	108	20070298764		2007-12-27	CLAYTON, Steve	
	109	20080005285		2008-01-03	ROBINSON et al.	
	110	20080005561		2008-01-03	BROWN et al.	
	111	20080010452		2008-01-10	HOLTZMAN et al.	
	112	20080039102		2008-02-14	SEWALL et al.	
	113	20080049630		2008-02-28	KOZISEK et al.	
	114	20080052387		2008-02-28	HEINZ et al.	
	115	20080059474		2008-03-06	LIM, Keng	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	116	20080059743		2008-03-06	BYCHKOV et al.	
	117	20080060066		2008-03-06	WYNN et al.	
	118	20080062900		2008-03-13	RAO, Bindu Rama	
	119	20080064367		2008-03-13	NATH et al.	
	120	20080066149		2008-03-13	LIM, Keng	
	121	20080066150		2008-03-13	LIM, Keng	
	122	20080082643		2008-04-03	STORRIE et al.	
	123	20080083013		2008-04-03	SOLIMAN et al.	
	124	20080095339		2008-04-24	ELLIOTT et al.	
	125	20080098062		2008-04-24	BALIA, Hinal K.	
	126	20080109679		2008-05-08	WRIGHT et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	127	20080120688		2008-05-22	QIU et al.	
	128	20080127304		2008-05-29	GINTER et al.	
	129	20080130534		2008-06-05	TOMIOKA, Tazuko	
	130	20080130656		2008-06-05	KIM et al.	
	131	20080132268		2008-06-05	CHOI-GROGAN et al.	
	132	20080134330		2008-06-05	KAPOOR et al.	
	133	20080147454		2008-06-19	WALKER et al.	
	134	20080160958		2008-07-03	ABICHANDANI et al.	
	135	20080162637		2008-07-03	ADAMCZYK et al.	
	136	20080162704		2008-07-03	POPLETT et al.	
	137	20080164304		2008-07-10	NARASIMHAN et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	138	20080167027		2008-07-10	GAUTIER et al.	
	139	20080167033		2008-07-10	BECKERS, Michel	
	140	20080168523		2008-07-10	ANSARI et al.	
	141	20080177998		2008-07-24	APSANGI et al.	
	142	20080183812		2008-07-31	PAUL et al.	
	143	20080184127		2008-07-31	RAFEY et al.	
	144	20080189760		2008-08-07	ROSENBERG et al.	
	145	20080207167		2008-08-28	BUGENHAGEN, Michael K.	
	146	20080212470		2008-09-04	CASTANEDA et al.	
	147	20080221951		2008-09-11	STANFORTH et al.	
	148	20080222692		2008-09-11	ANDERSSON et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	149	20080225748		2008-09-18	KHEMANI et al.	
	150	20080229385		2008-09-18	FEDER et al.	
	151	20080229388		2008-09-18	MAES, Stephane H.	
	152	20080256593		2008-10-16	VINBERG et al.	
	153	20080268813		2008-10-30	MAES, Stephane H.	
	154	20080298230		2008-12-04	LUFT et al.	
	155	20080305793		2008-12-11	GALLAGHER et al.	
	156	20080311885		2008-12-18	DAWSON et al.	
	157	20080316923		2008-12-25	FEDDERS et al.	
	158	20080318547		2008-12-25	BALLOU et al.	
	159	20080318550		2008-12-25	DeATLEY, Dallas	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	160	20080319879		2008-12-25	CARROLL et al.	
	161	20090005005		2009-01-01	FORSTALL et al.	
	162	20090013157		2009-01-08	BEAULE, Stephane	
	163	20090054030		2009-02-26	GOLDS, David	
	164	20090068984		2009-03-12	BURNETT, R. Alan	
	165	20090077622		2009-03-19	BAUM et al.	
	166	20090079699		2009-03-26	SUN, Jian	
	167	20090113514		2009-04-30	HU, Q. James	
	168	20090125619		2009-05-14	ANTANI, Snehal S.	
	169	20090180391		2009-07-16	PETERSEN et al.	
	170	20090197585		2009-08-06	AARON, Jeffrey A.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	171	20090257379		2009-10-15	ROBINSON et al.	
	172	20090271514		2009-10-29	THOMAS et al.	
	173	20090286507		2009-11-19	O'NEIL et al.	
	174	20090287921		2009-11-19	ZHU et al.	
	175	20090288140		2009-11-19	HUBER et al.	
	176	20100017506		2010-01-21	FADELL, Anthony	
	177	20100042675		2010-02-18	FUJII, Hiroshi	
	178	20100043068		2010-02-18	VARADHAN et al.	
	179	20100071053		2010-03-18	ANSARI et al.	
	180	20100082431		2010-04-01	RAMER et al.	
	181	20100103820		2010-04-29	FULLER et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	182	20100188975		2010-07-29	RALEIGH, Gregory G.	
	183	20100188990		2010-07-29	RALEIGH, Gregory G.	
	184	20100188992		2010-07-29	RALEIGH, Gregory G.	
	185	20100188994		2010-07-29	RALEIGH, Gregory G.	
	186	20100191576		2010-07-29	RALEIGH, Gregory G.	
	187	20100191612		2010-07-29	RALEIGH, Gregory G.	
	188	20100191846		2010-07-29	RALEIGH, Gregory G.	
	189	20100192170		2010-07-29	RALEIGH, Gregory G.	
	190	20100192212		2010-07-29	RALEIGH, Gregory G.	
	191	20100195503		2010-08-05	RALEIGH, Gregory G.	
	192	20100197268		2010-08-05	RALEIGH, Gregory G.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	193	20100198698		2010-08-05	RALEIGH et al.	
	194	20100198939		2010-08-05	RALEIGH, Gregory G.	
	195	20100325420		2010-12-23	KANEKAR, Tushar	
	196	20110126141		2011-05-26	KING et al.	
	197	20080132201		2008-06-05	KARLBERG, Johan	
	198	20080081606		2008-04-03	COLE, Terry L.	
	199	20090248883		2009-10-01	SURYANARAYANA et al.	
	200	20100144310		2010-06-10	BEDINGFIELD, James Carlton	
	201	20080085707		2008-04-10	FADELL, Tony	
	202	20090046723		2009-02-19	RAHMAN, Reshad A. et al.	
	203	20080219268		2008-09-11	DENNISON, Larry R.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	204	20080005285		2008-01-03	ROBINSON, James David et al.	
	205	20090315735		2009-12-24	BHAVANI, Neeraj S. et al.	
	206	20090219170		2009-09-03	CLARK, Ryan C. et al.	
	207	20090067372		2009-03-12	SHAH, Keyur C. et al.	
	208	20080262798		2008-10-23	KIM, Eun Ah et al.	
	209	20100103820		2010-04-29	FULLER, Randy et al.	
	210	20100153781		2010-06-17	HANNA, Stephen R.	
	211	20090307746		2009-12-10	DI, Jinwen et al.	
	212	20050009499		2005-01-13	KOSTER, Karl	
	213	20010053694		2001-12-20	IGARASHI, Yoichiro et al.	
	214	20100041364		2010-02-18	LOTT, Robert Wayne et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	215	20100027469		2010-02-04	GURAJALA, Ravindra Babu et al.	
	216	20090299857		2009-12-03	BRUBAKER, Curtis M.	
	217	20080051076		2008-02-28	O'Shaughnessy, John et al.	
	218	20080313730		2008-12-18	Iftimie, Sorin et al.	
	219	20110173678		2011-07-14	KAIPPALLIMALIL, John et al.	
	220	20080235511		2008-09-25	O'BRIEN, William G. et al.	
	221	20080240373		2008-10-02	WILHELM, Robert D.	
	222	20100027559		2010-02-04	LIN, Hung-Ming et al.	
	223	20020116338		2002-08-22	GONTHIER, Jean-Charles et al.	
	224	20070061878		2007-03-15	HAGIU, Costin et al. et al.	
	225	20100020822		2010-01-28	ZERILLO, Anthony J. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	226	20040203755		2004-10-14	BRUNET, Jeffrey et al.	
	227	20090172077		2009-07-02	ROXBURGH, David et al.	
	228	20080120668		2008-05-22	Yau, Frank Chuen-Foo	
	229	20030171112		2003-09-11	Lupper, Alfred et al.	
	230	20070300252		2007-12-27	Acharya, Swarup et al.	
	231	20050007993		2005-01-13	Chambers, Mahdi et al.	
	232	20020164983		2002-11-07	Raviv, Li-On et al.	
	233	20070280453		2007-12-06	Kelley, Sean S.	
	234	20100241544		2010-09-23	Benson, Dan et al.	
	235	20090157792		2009-06-18	Fiatal, Trevor	
	236	20070109983		2007-05-17	Shankar, Rohit et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	237	20020049074		2002-04-25	Eisinger, Bernd et al.	
	238	20020161601		2002-10-31	Nauer, Bernhard et al.	
	239	20040132427		2004-07-08	Lee, Wan-Yeon et al.	
	240	20060068796		2006-03-30	Millen, Stephanie L. et al.	
	241	20010048738		2001-12-06	Baniak, Paul G. et al.	
	242	20070033197		2007-02-08	Scherzer, Shimon et al.	
	243	20110013569		2011-01-20	Scherzer, Shimon et al.	
	244	20110159818		2011-06-30	Scherzer, Shimon et al.	
	245	20120020296		2012-01-26	Scherzer, Shimon et al.	
	246	20120196644		2012-08-02	Scherzer, Shimon et al.	
	247	20120238287		2012-09-20	Scherzer, Shimon	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	248	20130058274		2013-03-07	Scherzer, Shimon et al.	
	249	20130084835		2013-04-04	Scherzer, Shimon et al.	
	250	20090005000		2009-01-01	Baker, Matthew et al.	
	251	20090006116		2009-01-01	Baker, Matthew et al.	
	252	20090006200		2009-01-01	Baker, Matthew et al.	
	253	20110081881		2011-04-07	Baker, Matthew Donald et al.	
	254	20110082790		2011-04-07	Baker, Matthew Donald et al.	
	255	20130029653		2013-01-31	Baker, Matthew Donald et al.	
	256	20130065555		2013-03-14	Baker, Matthew Donald et al.	
	257	20060135144		2006-06-22	Jothipragasam, Premkumar	
	258	20080089295		2008-04-17	Keeler, James D. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	259	20080022354		2008-01-24	Grewal, Karanvir et al.	
	260	20040102182		2004-05-27	Reith, Lothar et al.	
	261	20030233332		2003-12-18	Keeler, James D. et al.	
	262	20080250053		2008-10-09	Aaltonen, Janne et al.	
	263	20070155365		2007-07-05	Kim, Sung-Jun et al.	
	264	20130144789		2013-06-06	Aaltonen, Janne et al.	
	265	20100131584		2010-05-27	Johnson, William J.	
	266	20100080202		2010-04-01	Hanson, Mark	
	267	20070147324		2007-06-28	McGary, Faith	
	268	20070168499		2007-07-19	Chu, Jing-Long	
	269	20070025301		2007-02-01	Petersson, Justus et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	270	20070140145		2007-06-21	Kumar, Surender et al.	
	271	20080120129		2008-05-22	Seubert, Michael et al.	
	272	20060174035		2006-08-03	Tufail, Mudassir	
	273	20110264923		2011-10-27	Kocher, Paul C. et al.	
	274	20080201266		2008-08-21	Chua, Huina et al.	
	275	20060156398		2006-07-13	Ross, Alan D. et al.	
	276	20060173959		2006-08-03	McKelvie, Samuel J. et al.	
	277	20100284327		2010-11-11	Miklos, Gyorgy	
	278	20070033194		2007-02-08	Srinivas, Davanum M. et al.	
	279	20050079863		2005-04-14	Macaluso, Anthony G.	
	280	20060114832		2006-06-01	Hamilton, Thomas E. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	281	20040225898		2004-11-11	Frost, D. Gabriel et al.	
	282	20080070550		2008-03-20	Hose, David Alan	
	283	20110019574		2011-01-27	Malomsoky, Szaboles et al.	
	284	20030188117		2003-10-02	Yoshino, Kenji et al.	
	285	20040255145		2004-12-16	Chow, Jerry	
	286	20050055595		2005-03-10	Frazer, Mark et la.	
	287	20070259656		2007-11-08	Jeong, Jong Woo	
	288	20080263348		2008-10-23	Zaltsman, Etai et al.	
	289	20080313315		2008-12-18	Karaoguz, Jeyhan et al.	
	290	20090282127		2009-11-12	LeBlanc, Michael et al.	
	291	20100167696		2010-07-01	Smith, Christopher David et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	292	20030188006		2003-10-02	Bard, Steven R.	
	293	20060160536		2006-07-20	Chou, Joey	
	294	20060168128		2006-07-27	Sistla, Amber et al.	
	295	20040203833		2004-10-14	Rathunde, Dale F. et al.	
	296	20050186948		2005-08-25	Gallagher, Michael D. et al.	
	297	20070147317		2007-06-28	Smith, Brian K. et al.	
	298	20080270212		2008-10-30	Blight, Jeffrey et al.	
	299	20080056273		2008-03-06	Pelletier, Ghyslain et al.	
	300	20110110309		2011-05-12	Bennett, James D.	

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]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	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]
	1		☐

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	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

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.

☐ Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ None

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	/James E. Harris/	Date (YYYY-MM-DD)	2015-04-29
Name/Print	James E. Harris	Registration Number	40013

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.

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	14667516
Filing Date	2015-03-24
First Named Inventor	Raleigh
Art Unit	2431
Examiner Name	not yet assigned
Attorney Docket Number	RALEP007C11C4

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	8447980		2013-05-21	Godfrey, James A. et al.	
	2	8429403		2013-04-23	Moret, Eric et al.	
	3	8411587		2013-04-02	Curtis, William et al.	
	4	8396929		2013-03-12	Helfman, Nadav et al.	
	5	8363658		2013-01-29	Delker, Jason R. et al.	
	6	8265004		2012-09-11	Toutonghi, Michael J.	
	7	8233895		2012-07-31	Tysowski, Piotr Konrad	
	8	7685254		2010-03-23	Pandya, Ashish A.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	9	7181017		2007-02-20	Nagel, Robert H. et al.	
	10	6965872		2005-11-15	Grdina, Jerome M.	
	11	8402540		2013-03-19	Kapoor, Harsh et al.	
	12	8135657		2012-03-13	Kapoor, Harsh et al.	
	13	8271992		2012-09-18	Chatley, Scott P. et al.	
	14	8315999		2012-11-20	Chatley, Scott P. et al.	
	15	8332375		2012-12-11	Chatley, Scott P. et al.	
	16	8468337		2013-06-18	Gaur, Santosh P. et al.	
	17	8477778		2013-07-02	Lehmann Jr., L. Curtis et al.	
	18	6640097		2003-10-28	Corrigan, Louis et al.	
	19	7039713		2006-05-02	Van Gunter, David et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	20	5915008		1999-06-22	Dulman, Scott	
	21	8126476		2012-02-28	Vardi, Yosef et al.	
	22	8000276		2011-08-16	Scherzer, Shimon et al.	
	23	8358638		2013-01-22	Scherzer, Tamir et al.	
	24	8356336		2013-01-15	Johnston, Keith et al.	
	25	8307067		2012-11-06	Ryan, Nicholas M.	
	26	7286848		2007-10-23	Vireday, Richard P. et al.	
	27	7313237		2007-12-25	Bahl, Paramvir et al.	
	28	7444669		2008-10-28	Bahl, Paramvir et al.	
	29	7548976		2009-06-16	Bahl, Paramvir et al.	
	30	8027339		2011-09-27	Short, Joel E. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	31	8095112		2012-01-10	Chow, Richard et al.	
	32	7881697		2011-02-01	Baker, Matthew Donald et al.	
	33	7899438		2011-03-01	Baker, Matthew Donald et al.	
	34	7945238		2011-05-17	Baker, Matthew Donald et al.	
	35	8078140		2011-12-13	Baker, Matthew Donald et al.	
	36	8285249		2012-10-09	Baker, Matthew Donald et al.	
	37	7493659		2009-02-17	Wu, Handong et al.	
	38	7801985		2010-09-21	Pitkow, Jim et al.	
	39	8242959		2012-08-14	Mia, Rashidus S. et al.	
	40	8326319		2012-12-04	Davis, Richard W.	
	41	7102620		2006-09-05	Harries, Andrew Stanely Guy et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	42	7139569		2006-11-21	Kato, Akira	
	43	7529204		2009-05-05	Bourlas, Yair et al.	
	44	7720960		2010-05-18	Pruss, Richard Manfred et al.	
	45	7969950		2011-06-28	Iyer, Pradeep J. et al.	
	46	8032409		2011-10-04	Mikurak, Michael G.	
	47	8045973		2011-10-25	Chambers, Michael D.	
	48	8116781		2012-02-14	Chen, Xixian et al.	
	49	8126396		2012-02-28	Bennett, James D.	
	50	8351898		2013-01-08	Raleigh, Gregory G.	
	51	5630159		1997-05-13	Zancho, William F.	
	52	5633484		1997-05-27	Zancho, William F. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	53	5814798		1998-09-29	Zancho, William F.	
	54	7039403		2006-05-02	Wong, Gregory A.	
	55	7583964		2009-09-01	Wong, Gregory A.	
	56	7593730		2009-09-22	Khandelwal, Deepak et al.	
	57	7948953		2011-05-24	Melkote, Keerti G. et al.	
	58	8200509		2012-06-12	Kenedy, Andrew Alexander et al.	
	59	8270972		2012-09-18	Otting, Marcia J. et al.	
	60	7929959		2011-04-19	DeAtley, Dallas et al.	
	61	7478420		2009-01-13	Wright, Michael et al.	
	62	7502672		2009-03-10	Kolls, H. Brock	
	63	7756757		2010-07-13	Oakes III, Charles Lee	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	64	7930446		2011-04-19	Kesselman, Alex et al.	
	65	8078163		2011-12-13	Lemond, Eric et al.	
	66	8068829		2011-11-29	Lemond, Eric et al.	
	67	8086497		2011-12-27	Oakes III, Charles Lee	
	68	8166040		2012-04-24	Brindisi, Richard G. et al.	
	69	6934249		2005-08-23	Bertin, Olivier et al.	
	70	7774456		2010-08-10	Lownsbrough, Derek Leigh et al.	
	71	8447607		2013-05-21	Weider, Chris et al.	
	72	8504729		2013-08-06	Pezzutti, David A.	
	73	8495227		2013-07-23	Kaminsky, David L. et al.	
	74	8472371		2013-06-25	Bari, Farooq et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	75	8134954		2012-03-13	Godfrey, James A. et al.	
	76	7535880		2009-05-19	Hinman, Brian L. et al.	
	77	7499438		2009-03-03	Hinman, Brian L. et al.	
	78	7496652		2009-02-24	Pezzutti, David	
	79	6957067		2005-10-18	Iyer, Pradeep J. et al.	
	80	6654814		2003-11-25	Britton, Kathryn H. et al.	
	81	8374592		2013-02-12	Proctor, Jr. James A. et al.	
	82	8325638		2012-12-04	Jin, Haipeng et al.	
	83	8116749		2012-02-14	Proctor Jr., James Arthur et al.	
	84	8090616		2012-01-03	Proctor Jr., James Arthur et al.	
	85	8090359		2012-01-03	Proctor Jr., James Arthur et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	86	8150431		2012-04-03	Wolovitz, Lionel et al.	
	87	8483135		2013-07-09	Cai, Yigang et al.	
	88	6104700		2000-08-15	Haddock, Stephen R. et al.	
	89	8185127		2012-05-22	Cai, Zheng et al.	
	90	8521110		2013-08-27	Rofougaran, Ahmadreza	
	91	7310424		2007-12-18	Gehring, Stephan Walter et al.	
	92	7356011		2008-04-08	Waters, Christopher J.F. et al.	
	93	7546460		2009-06-09	Maes, Stephane H.	
	94	7921463		2011-04-05	Sood, Kapil et al.	
	95	7940751		2011-05-10	Hansen, Christopher J.	
	96	8122249		2012-02-21	Falk, Rainer et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	97	8495360		2013-07-23	Falk, Rainer et al.	
	98	8520589		2013-08-27	Bhatt, Yogesh et al.	
	99	6542992		2003-04-01	Peirce, Kenneth L. et al.	
	100	8185093		2012-05-22	Jheng, Yu-Syuan et al.	
	101	8296404		2012-10-23	McDysan, Dave et al.	
	102	8195163		2012-06-05	Gisby, Doug et al.	
	103	8437734		2013-05-07	Ray, Amar N. et al.	
	104	7460837		2008-12-02	Diener, Neil R.	
	105	7653394		2010-01-26	McMillin, Brian K.	
	106	8130793		2012-03-06	Edwards, Stephen K. et al.	
	107	8509082		2013-08-13	Heinz, John M. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	108	8526329		2013-09-03	Mahany, Ronald L. et al.	
	109	5983270		1999-11-09	Abraham, Dalen M. et al.	
	110	6598034		2003-07-22	Kloth, Axel K.	
	111	7032072		2006-04-18	Quinn, Michael J. et al.	
	112	7580356		2009-08-25	Mishra, Sanjeev K. et al.	
	113	7742406		2010-06-22	Muppala, Suresh	
	114	7953877		2011-05-31	Vemula, Narendra et al.	
	115	7957381		2011-06-07	Clermidy, Fabien et al.	
	116	8031601		2011-10-04	Feroz, Azeem et al.	
	117	8255534		2012-08-28	Assadzadeh, Alireza	
	118	8489720		2013-07-16	Morford, Michael Robert et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	119	7774323		2010-08-10	Helfman, Nadav	
	120	7043268		2006-05-09	Yukie, Satoru et al.	
	121	7113780		2006-09-26	McKenna, Daniel Bernard et al.	
	122	8166554		2012-04-24	John, Pramod	
	123	7697540		2010-04-13	Haddad, Reda et al.	
	124	6748195		2004-06-08	Phillips, W. Garland	
	125	8583499		2013-11-12	De Judicibus, Dario et al.	
	126	8352360		2013-01-08	De Judicibus, Dario et al.	
	127	8463232		2013-06-11	Tuli, Amol et al.	
	128	7958029		2011-06-07	Bobich, Thomas et al.	
	129	7540408		2009-06-02	Levine, Judah Joseph et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	130	7826427		2010-11-02	Sood, Kapil et al.	
	131	8483694		2013-07-09	Lewis, Allan D. et al.	
	132	8351592		2013-01-08	Freeny, Jr., Charles C. et al.	
	133	7610396		2009-10-27	Taglienti, Claudio et al.	
	134	7984511		2011-07-19	Kocher, Paul Carl et al.	
	135	7987510		2011-07-26	Kocher, Paul C. et al.	
	136	8571993		2013-10-29	Kocher, Paul C. et al.	
	137	8543265		2013-09-24	Ekhaguere, David E. et al.	
	138	6873988		2005-03-29	Hermann, Conrad K. et al.	
	139	7013469		2006-03-14	Smith, Adam W. et al.	
	140	7203169		2007-04-10	Okholm, Jon Eric et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	141	7286834		2007-10-23	Walter, Edward	
	142	7555757		2009-06-30	Smith, Adam W. et al.	
	143	7574509		2009-08-11	Nixon, Mark J. et al.	
	144	7826607		2010-11-02	de Carvalho Resende, Mauricio Guilherme et al.	
	145	7940685		2011-05-10	Breslau, Lee Michel et al.	
	146	8196199		2012-06-05	Hrastar, Scott E. et al.	
	147	8204505		2012-06-19	Jin, Haipeng et al.	
	148	8228818		2012-07-24	Chase, Christopher J. et al.	
	149	8320244		2012-11-27	Muqattash, Alaa et al.	
	150	8411691		2013-04-02	Aggarwal, Rahul	
	151	8461958		2013-06-11	Saenz, Jorge E. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	152	8484327		2013-07-09	Werner, Eran et al.	
	153	8522039		2013-08-27	Hyndman, Arn et al.	
	154	8544105		2013-09-24	Mclean, Ivan H. et al.	
	155	8571474		2013-10-29	Chavez, Timothy R. et al.	
	156	5774532		1998-06-30	Gottlieb, Louis G. et al.	
	157	8095124		2012-01-10	Balia, Hinal K.	
	158	7797060		2010-09-14	Grgic, Richard J. et al.	
	159	7930327		2011-04-19	Craft, David Jones et al.	
	160	8264965		2012-09-11	Dolganow, Andrew et a.	
	161	6885997		2005-04-26	Roberts, David T.	
	162	8229394		2012-07-24	Karlberg, Johan	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	163	8495700		2013-07-23	Shahbazi, Majid	
	164	8548427		2013-10-01	Chow, Paulo S.T. et al.	
	165	8572117		2013-10-29	Rappaport, Theodore S.	
	166	8589955		2013-11-19	Roundtree, Brian et al.	
	167	8660853		2014-02-25	Robb, Terence A. et al.	
	168	8601125		2013-12-03	Huang, Shibi et al	
	169	8046449		2011-10-25	Yoshiuchi, Hideya	
	170	8635164		2014-01-21	Rosenhaft, Matthew et al.	
	171	8566236		2013-10-22	Busch, James David	
	172	8528068		2013-09-03	Weglein, Joseph et al.	
	173	8442015		2013-05-14	Behzad, Arya et al	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	174	7853255		2010-12-14	Karaoguz, Jeyhan et al	
	175	7720464		2010-05-18	Batta, Puneet	
	176	8300575		2012-10-30	Willars, Per	
	177	8666395		2014-03-04	Silver, Andrew	
	178	8315593		2012-11-20	Gallant, John K. et al.	
	179	8180881		2012-05-15	Seo, Kyoung-Il et al.	
	180	7539132		2009-05-26	Werner, Carl E. et al.	
	181	7805606		2010-09-28	Birger, Chet et al.	
	182	8347378		2013-01-01	Merkin, Aaron E. et al.	
	183	6185576		2001-02-06	McIntosh, Lowrie	
	184	8175574		2012-05-08	Panda, Biswaranjan et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	185	8375128		2013-02-12	Tofighbakhsh, Mostafa et al.	
	186	8527410		2013-09-03	Markki, Outi et al.	
	187	7320029		2008-01-15	Rinne, Janne Petri et al.	
	188	8275415		2012-09-25	Huslak, Nicholas S.	
	189	8554876		2013-10-08	Winsor, Gerald W.	
	190	8191124		2012-05-29	Wynn, Simon et al.	
	191	7805140		2010-09-28	Friday, Robert J. et al.	
	192	8605691		2013-12-10	Soomro, Amjad et al.	
	193	8655357		2014-02-18	Gazzard, Daryl Robert et al.	
	194	8706863		2014-04-22	Fadell, Anthony	
	195	6640334		2003-10-28	Rasmussen, John H.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	196	7668612		2010-02-23	Okkonen, Harri	
	197	5325532		1994-06-28	Crosswy, Wm. Caldwell et al.	
	198	7614051		2009-11-03	Glaum, Jeffrey D. et al.	
	199	5131020		1992-07-14	Liebesny, John P. et al.	
	200	8370483		2013-02-05	Choong et al.	
	201	8670334		2014-03-11	Keohane et al.	
	202	8693323		2014-04-08	McDysan, David E.	
	203	7409447		2008-08-05	Assadzadeh, Alireza	
	204	8725899		2014-05-13	Short, Joel et al.	
	205	8676925		2014-03-18	Liu, Jiawei et al.	
	206	8645518		2014-02-04	David, Scott L.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	207	7756056		2010-07-13	Kim et al	
	208	8131281		2012-03-06	Hildner et al.	
	209	8160598		2012-04-17	Savoor, Raghvendra	
	210	8375136		2013-02-12	Roman et al.	
	211	6119933		2000-09-19	Wong et al.	
	212	8694772		2014-04-08	Kao et al.	
	213	8719423		2014-05-06	Wyld, Jeremy	
	214	8347104		2013-01-01	Pathiyal, Krishna K.	
	215	7149229		2006-12-12	Leung, Kent K.	
	216	7242668		2007-07-10	Kan, Chao et al.	
	217	8095640		2012-01-10	Guingo, Pierrick et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	218	8780857		2014-07-15	Balasubramanian, Srinivasan et al.	
	219	8811991		2014-08-19	Jain, Nikhil et al.	
	220	7809351		2010-10-05	Panda et al.	
	221	8346210		2013-01-01	Balsan, Damien et al.	
	222	8355696		2013-01-15	Olding et al.	
	223	8422988		2013-04-16	Keshav, Srinivasan	
	224	8488597		2013-07-16	Nie et al.	
	225	6438575		2002-08-20	Khan et al.	
	226	7222304		2007-05-22	Beaton et al.	
	227	7561899		2009-07-14	Lee, Changseok	
	228	8200200		2012-06-12	Belser et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	229	8229914		2012-07-24	Ramer et al.	
	230	8522249		2013-08-27	Beaule, Stephane	
	231	8701015		2014-04-15	Bonnat, Pierre	
	232	6697821		2004-02-24	Ziff et al.	
	233	6763226		2004-07-13	McZeal Jr., Alfred	
	234	6982733		2006-01-03	McNally et al.	
	235	6983370		2006-01-03	Eaton, et al.	
	236	7318111		2008-01-08	Zhao, Wen	
	237	8064418		2011-11-22	Maki, Lasse	
	238	8249601		2012-08-21	Emberson et al.	
	239	8514927		2013-08-20	Sundararajan et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

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	1538730A	CN		2004-10-20	Zhongxing Communication Co., Ltd.		☐
	2	101115248A	CN		2008-01-30	Lenovo Beijing Ltd.		☐
	3	101341764A	CN		2009-01-07	Telefonaktiebolaget LM Ericsson		☐
	4	2007068288A1	WO		2007-06-21	Telefonaktiebolaget LM Ericsson		☐
	5	1802839A	CN		2006-07-12	Motorola Inc.		☐
	6	2004064306A2	WO		2004-07-29	Motorola Inc.		☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	7	101123553A	CN		2007-09-11	SouTheast University		☐
	8	1937511A	CN		2007-03-28	ZTE		☐
	9	1999027723 A1	WO		1999-06-03	Telefonaktiebolaget LM Ericsson		☐
	10	2007133844	WO		2007-11-22	Camiant, Inc.		☐
	11	101183958A	CN		2008-05-21	Huawei Tech. Co. Ltd.		☐
	12	1801829A	CN		2006-07-12	Kunda Computer Technology (Kunshan) Co., Ltd.		☐
	13	1867024A	CN		2006-11-22	Huawei Technologies Co., Ltd.		☐
	14	101815275A	CN		2010-08-25	Yang, Liu		☐

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	VerizonWireless.com news, "Verizon Wireless Adds to Portfolio of Cosumer-Friendly Tools With Introduction of Usage Controls, Usage Controls and Chaperone 2.0 Offer Parents Full Family Security Solution," August 18, 2008	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	2	"The Construction of Intelligent Residential District in Use of Cable Television Network," Shandong Science, Vol. 13, No. 2, June 2000	☐
	3	"Communication Concepts for Mobile Agent Systems," by Joachim Baumann et al.; Inst. Of Parallel and Distributed High-Performance Systems, Univ. of Stuttgart, Germany, pp. 123-135, 1997	☐
	4	"End to End QoS Solution for Real-time Multimedia Application;" Computer Engineering and Applications, 2007, 43 (4): 155-159, by Tan Zu-guo, Wang Wen-juan; Information and Science School, Zhanjian Normal College, Zhan jiang, Guangdong 524048, China	☐
	5	"ASA/PIX: Allow Split Tunneling for VPN Clients on the ASA Configuration Example," Document ID 70917, January 10, 2008	☐

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	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

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.

☐ Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ None

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	/James E. Harris/	Date (YYYY-MM-DD)	2015-04-29
Name/Print	James E. Harris	Registration Number	40013

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.

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	14667516
Filing Date	2015-03-24
First Named Inventor	Raleigh
Art Unit	2431
Examiner Name	not yet assigned
Attorney Docket Number	RALEP007C11C4

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	20100030890		2010-02-04	Dutta, Satadip et al.	
	2	20080025230		2008-01-31	Patel, Alpesh et al.	
	3	20040170191		2004-09-02	Guo, Zihua et al.	
	4	20020188732		2002-12-12	Buckman, Charles R. et al.	
	5	20080034419		2008-02-07	Mullick, Amarnath et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	6	20080010379		2008-01-10	Zhao, Hang	
	7	20080139210		2008-06-12	Gisby, Doug et al.	
	8	20040243992		2004-12-02	Gustafson, James P. et al.	
	9	20070226775		2007-09-27	Andreasen, Flemming Stig et al.	
	10	20100235329		2010-09-16	Koren, David et al	
	11	20090254857		2009-10-08	Romine, Christopher et al.	
	12	20080166993		2008-07-10	Gautier et al.	
	13	20040137890		2004-07-15	Kalke, Catherine	
	14	20070143824		2007-06-21	Shahbazi, Majid	
	15	20070266422		2007-11-15	Germano et al.	
	16	20090044185		2009-02-12	Krivopaltsev, Eugene	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	17	20040039792		2004-02-26	Nakanishi, Tomoaki	
	18	20050075115		2005-04-07	Corneille et al.	
	19	20050239447		2005-10-27	Holzman et al.	
	20	20070213054		2007-09-13	Han, Seung-Wook	
	21	20080032715		2008-02-07	Jia et al.	
	22	20090163173		2009-06-25	Williams, Timothy D.	
	23	20100075666		2010-03-25	Garner, Neil Robert	
	24	20080293395		2008-11-27	Matthews, Ajit et al.	
	25	20050245241		2005-11-03	Durand, Terry et al.	
	26	20080125079		2008-05-29	O'Neil, Douglas et al.	
	27	20050135264		2005-06-23	Popoff, Jeff et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	28	20070165630		2007-07-19	Rasanen, Jorma	
	29	20100287599		2010-11-11	HE, Xianhui	
	30	20070060200		2007-03-15	Boris et al.	
	31	20060030306		2006-02-09	Kuhn, Brian Gerald	
	32	20060035631		2006-02-16	White et al.	
	33	20060206709		2006-09-14	Labrou et al.	
	34	20090046707		2009-02-19	Smires et al.	
	35	20100311402		2010-12-09	Srinivasan et al.	
	36	20110277019		2011-11-10	Pritchard Jr., John Russell	
	37	20050250536		2005-11-10	Deng et al.	
	38	20070192460		2007-08-16	Choi et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	39	20080080457		2008-04-03	Cole, Terry L.	
	40	20090049518		2009-02-19	Roman et al.	
	41	20100248719		2010-09-30	Scholaert, Hugh	

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] ¡	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	1310401A	CN		2000-02-22	Wang, Di Xing		☐
	2	1878160A	CN		2006-12-13	Jiang, Yong		☐
	3	101127988A	CN		2008-02-20	ZTE Corporation		☐
	4	1503548 A1	EP		2005-02-02	FG Microtec GmbH		☐
	5	3148713 B2	JP		2001-03-26	ATR Kankyo Tekio Tsushin Kenkyusho		☐
	6	2009-218773	JP		2009-09-24	Advanced Telecommunication Research Institute Inte		☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

	7	2006093961	WO		2006-09-08	Kyocera Wireless Corp.		☐
	8	2007-318354	JP		2007-12-06	Fujitsu Ten Ltd.		☐
	9	2007126352	WO		2007-11-08	Telefonaktiebolaget LM Ericsson		☐
	10	2009-212707	JP		2009-09-17	Fujitsu Ltd.		☐
	11	2008-301121	JP		2008-12-11	Kyocera Corp.		☐

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	Dixon et al., "Triple Play Digital Services: Comcast and Verizon (Digital Phone, Television, and Internet), August 2007	☐

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	14667516
	Filing Date	2015-03-24
	First Named Inventor	Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C4

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.

☐ Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ None

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	/James E. Harris/	Date (YYYY-MM-DD)	2015-04-29
Name/Print	James E. Harris	Registration Number	40013

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] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04M 1/00 (2006.01)
H04M 1/21 (2006.01)
G04G 5/00 (2006.01)

[12] 发明专利申请公开说明书

[21] 申请号 200410099356.1

[43] 公开日 2006 年 7 月 12 日

[11] 公开号 CN 1801829A

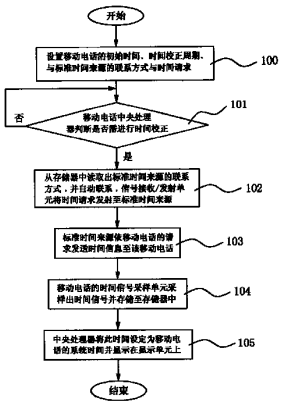
[22] 申请日 2004.12.30
[21] 申请号 200410099356.1
[71] 申请人 昆达电脑科技（昆山）有限公司
地址 215300 江苏省昆山市昆山出口加工区
[72] 发明人 许世法
权利要求书 1 页 说明书 3 页 附图 2 页

[54] 发明名称

移动电话时间自动校正方法

[57] 摘要

本发明揭示一种移动电话时间自动校正方法，该移动电话包括接收信号与发射信号的信号接收/发射单元、从接收到的信号中采样出时间信号的时间信号采样单元、存储时间信息与设定信息的存储器、中央处理器及显示单元，该方法主要通过设置移动电话的初始时间、时间校正周期、与标准时间来源的联系方式与时间请求，当需进行时间校正时，该移动电话自动将时间请求发送至标准时间来源，并取得标准时间，而后将该标准时间设定为移动电话的系统时间，从而令移动电话使用一般的石英振荡器亦可满足较高的时间精度，从而利于降低移动电话成本，并不影响移动电话的体积。



1、一种移动电话时间自动校正方法，该移动电话包括接收信号与发射信号的信号接收/发射单元、从接收到的信号中采样出时间信息的时间信号采样单元、存储时间信息与设定信息的存储器、中央处理器及显示单元，其特征在于该时间自动校正方法包括如下步骤：

设置移动电话的初始时间、时间校正周期、与标准时间来源的联系方式与时间请求，并将此些数据存储于移动电话的存储器中；

移动电话中央处理器判断是否需进行时间校正，如否则继续判断；

如需进行时间校正，则移动电话自动发射请求信号至标准时间来源；

标准时间来源依请求发送时间信息至该移动电话；

移动电话的时间信号采样单元采样出时间信号并存储至存储器中；

中央处理器将该时间设定为移动电话的系统时间。

2、如权利要求1所述的移动电话时间自动校正方法，其特征在于:该方法还包括将移动电话的系统时间显示在显示单元上的步骤。

3、如权利要求1或2所述的移动电话时间自动校正方法，其特征在于：该标准时间来源为声询台。

4、如权利要求3所述的移动电话时间自动校正方法，其特征在于：该移动电话内设有语音产生单元与语音辨识单元，行动电话中预先设有的时间询问请求为询问时间的声音信号。

5、如权利要求4所述的移动电话时间自动校正方法，其特征在于：当移动电话呼叫声询台后，移动电话通过语音产生单元提出时间询问请求。

6、如权利要求5所述的移动电话时间自动校正方法，其特征在于：声询台依请求发送的时间信号至移动电话，该信号经过移动电话的语音产生单元发出，并且移动电话的语音辨识单元采样出时间信号并存储至存储器中。

7、如权利要求1或2所述的移动电话时间自动校正方法，其特征在于：该标准时间来源为移动电话服务供应网络。

8、如权利要求7所述的移动电话时间自动校正方法，其特征在于：该移动电话中预先设有的时间询问请求为询问时间的短信。

9、如权利要求8所述的移动电话时间自动校正方法，其特征在于：移动电话从存储器中读取出标准时间来源的联系方式，并自动联系，信号接收/发射单元将询问时间的短信发射至移动电话服务供应纲络。

10、如权利要求9所述的移动电话时间自动校正方法，其特征在于：移动电话服务供应纲络以短信形式发送标准时间至该移动电话，移动电话的时间信号采样单元采样出时间信号并存储至存储器中。

移动电话时间自动校正方法

【技术领域】

本发明有关一种时间自动校正方法，尤其是应用于移动电话中的时间自动校正方法。

【背景技术】

随着通讯技术的发展，具有时钟功能的移动电话普及率日益提高，其中时钟的准确性在移动电话的实际使用中的重要性日益提高，如现在的备忘录、闹钟等功能的实现均依靠时钟的准确性。而目前时钟的精确性主要取决于时钟电路中使用的振荡器的精度，而目前多使用普通的石英振荡器，其频率误差在±20-50ppm（百万分之20-50），如以20ppm的误差为例，每天产生的时间误差将为1.728秒，而一年的时间误差则累积为630.72秒，将达10.5分钟之久，故会给使用者带来一定的不便。

针对该问题，业界采取使用较高精度的石英振荡器或使用微调电容或类似的元件对普通振荡器的频率进行微调的二种方法。第一种方法的不足在于：即使使用高精度的石英振荡器，振荡电路的负载电容依存在差别，所以实际上不可能得到与石英振荡器相同的高精度，因此无论使用多么昂贵的元件，也不可能得到高准确度的时间。第二种方法的不足之处在于：虽然使用一般的石英振荡器成本不会太高，但是需要频率调节装置，如微调电容器，这引起了部件成本增加和令频率调节过程较为繁琐的缺陷，特别是元件数量的增加会导致对移动电话小型化的妨碍。

有鉴于此，实有必要提供一种既不会增加移动电话成本，且不影响移动电话体积的移动电话时间自动校正方法。

【发明内容】

本发明目的在于提供一种既不会增加移动电话成本，且不影响移动电话体积的移动电话时间自动校正方法。

为实现上述目的，实施本发明的移动电话包括接收信号与发射信号的信号接收/发射单元、从接收到的信号中采样出时间信号的时间信号采样单元、存储时间信息与设定信息的存储器、中央处理器及显示单元，本发明移动电话时间的自动校正方法包括以下步骤：

设置移动电话的初始时间、时间校正周期、与标准时间来源的联系方式与时间请求，并将此些数据存储于移动电话的存储器中；

移动电话中央处理器判断是否需进行时间校正，如否则继续判断；

如需进行时间校正，则移动电话自动发射请求信号至标准时间来源；

标准时间来源依请求发送时间信息至该移动电话；

移动电话的时间信号采样单元采样出时间信号并存储至存储器中；

中央处理器将该时间设定为移动电话的系统时间。

较佳地，该标准时间来源为声询台，移动电话通过呼叫声询台提出时间请求，并且声询台发送的时间信号至移动电话，该信号经过移动电话的语音产生单元发出，并且移动电话的语音辨识单元采样出时间信号并存储至存储器中。

较佳地，该标准时间来源为移动电话服务供应网络，移动电话通过发送短信至移动电话服务供应纲络提出时间请求，并且移动电话服务供应纲络发送标准时间至该移动电话，移动电话的时间信号采样单元采样出时间信号并存储至存储器中。

与现有技术相比较，本发明利用移动电话联系外部的标准时间来源定期对移动电话的系统时间进行校正，从而可定期将时间误差及时消除，因此即使移动电话的时钟电路采用一般的石英振荡器，也不会给使用者造成不便，如此不需采用较为昂贵的石英振荡器或其它的微调电容器等，因此不会增加移动电话的成本，并且也不会对移动电话的小型化形成妨碍。

为对本发明的目的、构造特征及其功能有进一步的了解，兹配合附图详细说明如下：

【附图说明】

图 1 为本发明移动电话的组成框图。

图 2 为本发明移动电话时间自动校正方法的流程图。

【具体实施方式】

以下将结合图 1 与图 2 对本发明的进行详细说明，在以下说明中是以行动电话为例进行说明，该技术领域的普通技术人员应可理解，实施本发明的电子装置并不局限于移动电话，如具有无线通信功能的智能电话及个人数字助理（PDA）均可应用本发明。

请参阅图 1 所示，实施本发明的移动电话 1 包括：

信号接收/发射单元 10，用于发射与接收无线通讯信号；

时间信号采样单元 11，与信号接收/发射单元 10 耦接，用以将接收信号中的时间信号采样出；

存储器 12，用以存储移动电话 1 的系统程序、时间校正周期、标准时间来源的联系方式及移动电话 1 的最初设定时间；

显示单元 14，用以显示移动电话 1 的系统时间；

中央处理器 13，与上述各单元耦接，用以控制以上不同单元的运作。

请参阅图 2 所示，本发明的移动电话 1 的时间自动校正方法包括以下步骤：

设置移动电话的初始时间、时间校正周期、与标准时间来源的联系方式与时间请求，并将此些数据存储于移动电话 1 的存储器 12 中，其中时间校正周期可设定为一周或一个月，而标准时间来源可为声询台，如中国大陆的 114 查询台或中国台湾的 104 报时台（步骤 100）；

移动电话 1 中央处理器 13 判断是否需进行时间校正，即从最初设定的时间起，是否经过设定的时间校正周期的时间，如否则继续判断（步骤 101）；

如需进行时间校正，即从最初设定的时间起，已经过设定的时间校正周期的时间，则移动电话 1 的中央处理器 13 执行自动联系功能，即从存储器 12 中读取出标准时间来源的联系方式，并自动联系，信号接收/发射单元 10 将时间请求发射至标准时间来源（步骤 102）；

标准时间来源依移动电话 1 的请求发送时间信息至该移动电话 1(步骤 103）；

移动电话 1 的时间信号采样单元 11 采样出时间信号并存储至存储器 12 中（步骤 104）；

中央处理器 13 将此时间设定为移动电话 1 的系统时间并显示在显示单元 14 上（步骤 105)。

较佳地，当该标准时间来源为声询台时，而移动电话 1 内设有语音产生单元与语音辨识单元，步骤 100 中包括预先在移动电话 1 内设定时间询问请求，如可为询问时间的声音信号，步骤 102 具体包括以下步骤：当移动电话 1 呼叫声询台后，移动电话 1 通过语音产生单元提出时间询问请求，而步骤 103 相应包括以下步骤：声询台依次请求发送的时间信号至移动电话 1，该信号经过移动电话 1 的语音产生单元发出，并且移动电话 1 的语音辨识单元采样出时间信号并存储至存储器 12 中。

较佳地，当该标准时间来源为移动电话服务供应网络，步骤 100 中包括预先在移动电话 1 内设定时间询问请求，如可为询问时间的短信，步骤 102 具体包括以下步骤：移动电话 1 从存储器 12 中读取出标准时间来源的联系方式，并自动联系，信号接收/发射单元 10 将询问时间的短信发射至移动电话服务供应纲络，而步骤 103 相应包括以下步骤：移动电话服务供应纲络以短信形式发送标准时间至该移动电话 1，移动电话的时间信号采样单元 11 采样出时间信号并存储至存储器 12 中。

与现有技术相比较，本发明利用移动电话联系外部的标准时间来源定期对移动电话的系统时间进行校正，从而可定期将时间误差及时消除，因此即使移动电话的时钟电路采用一般的石英振荡器，也不会给使用者造成不便，如此不需采用较为昂贵的石英振荡器或其它的微调电容器等，因此不会增加移动电话的成本，并且也不会对移动电话的小型化形成妨碍。

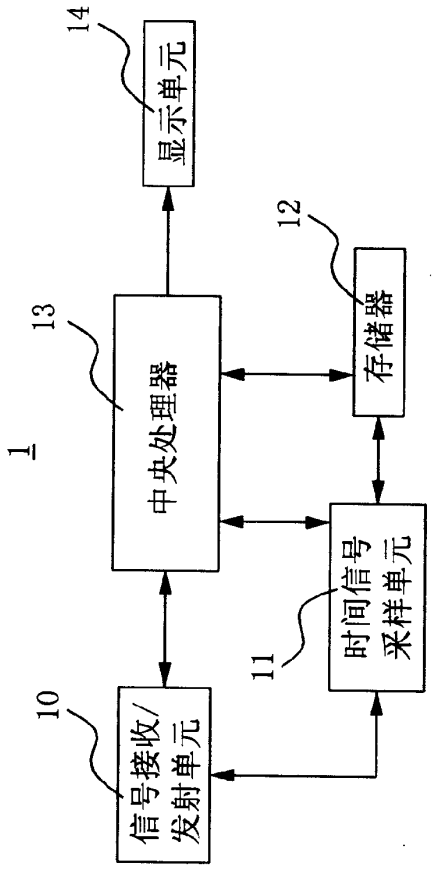


图1

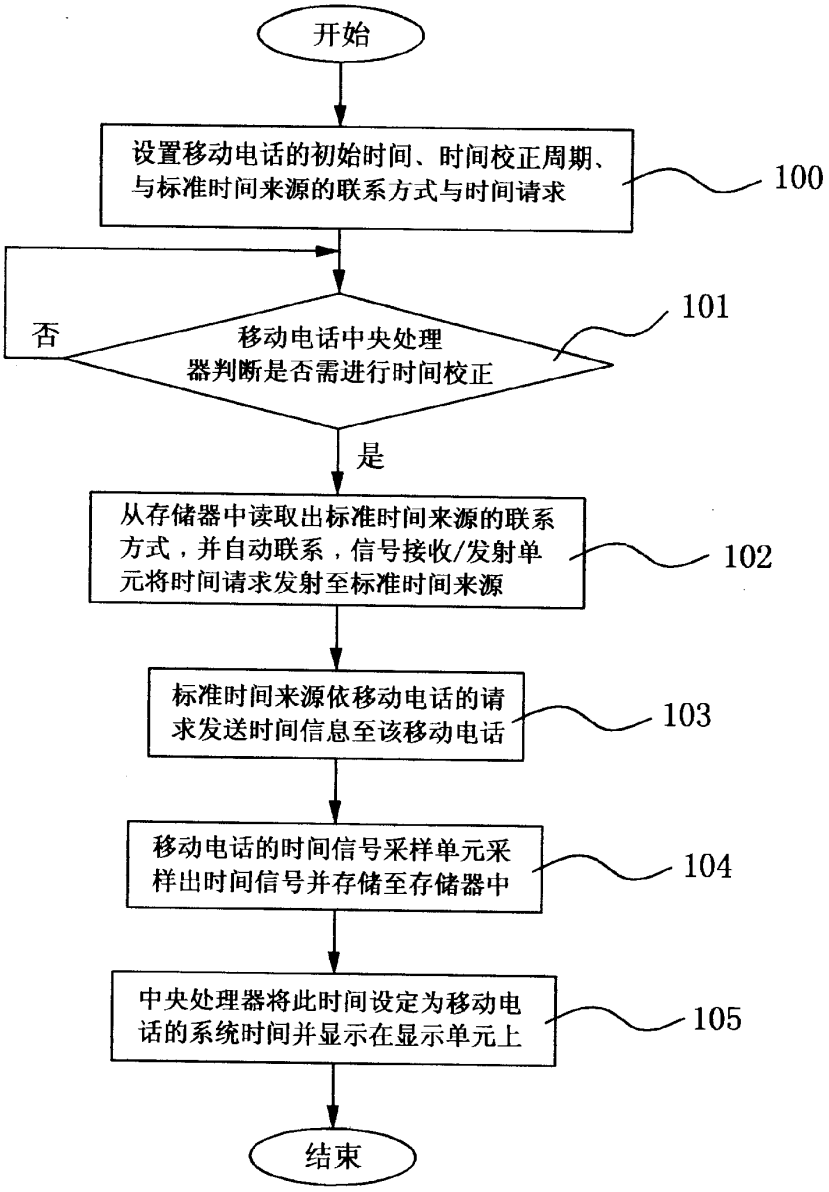

开始
设置移动电话的初始时间、时间校正周期、与标准时间来源的联系方式与时间请求
100
否
移动电话中央处理器判断是否需进行时间校正
101
是
从存储器中读取出标准时间来源的联系方式，并自动联系，信号接收/发射单元将时间请求发射至标准时间来源
102
标准时间来源依移动电话的请求发送时间信息至该移动电话
103
移动电话的时间信号采样单元采样出时间信号并存储至存储器中
104
中央处理器将此时间设定为移动电话的系统时间并显示在显示单元上
105
结束

图2

Sign in

Patents English Chinese Find prior art Discuss this application View PDF Download PDF

Mobile phone time automatic correction method

CN 1801829 A

Publication number	CN1801829 A
Publication type	Application
Application number	CN 200410099356
Publication date	Jul 12, 2006
Filing date	Dec 30, 2004
Priority date	Dec 30, 2004
Inventors	许世法
Applicant	昆达电脑科技(昆山)有限公司
Export Citation	BiBTeX, EndNote, RefMan

Classifications (3), Legal Events (3)

External Links: SIPO, Espacenet

ABSTRACT

Said invention provides a mobile telephone time autocorrection method. It contains signal reception / transmitting unit, time signal sampling unit memory unit, central processing unit and display unit, said method mainly setting mobile telephone initial time, time adjustment cycle, and standard time source connection mode and time request , when need proceeding time correction, said mobile telephone automatically transmitting time request to standard time source and taking standard time then configuring said standard time as system time of mobile telephone to reach higher time precision by using normal quartz oscillator.

DESCRIPTION translated from Chinese

Mobile phone time automatic calibration method

TECHNICAL FIELD The present invention relates to a method of automatic correction of the time, especially for mobile phones in the automatic time correction method.

BACKGROUND OF THE INVENTION With the development of communication technology, mobile phone penetration has a clock function increasing importance of the accuracy of the clock and the actual use of mobile phones increasing, as now realize memo, alarm clock and other functions both rely on the accuracy of the clock. At present, the accuracy of the clock depends on the accuracy of the clock oscillator used in the circuit, and the current multi-use ordinary quartz oscillator frequency error at ± 20-50ppm (20-50 ppm), as to 20ppm error, for example, the time error will be generated every 1.728 seconds, while the one-year time error accumulation is 630.72 seconds, to reach 10.5 minutes long, it will bring some inconvenience to users.

To solve this problem, the industry adopted the use of high precision quartz oscillator or use a trimmer capacitor or similar elements of the common oscillator frequency tuning of the two methods. The first method is inadequate: even when using high-precision quartz oscillator, the oscillation circuit of the load capacitance according to the presence of differences, so this is actually impossible to obtain the same high-precision crystal oscillator, and therefore regardless of 11 more expensive components, it is impossible to obtain a highly accurate time. Deficiencies of the second method comprising: using a general quartz oscillator although cost is not too high, but requires a frequency adjustment means, such as a trimmer capacitor, causing an increase in component cost and make the process more complicated frequency adjusting defects, particularly is an increase in the number of components will result in miniaturization of mobile phones interfere.

In view of this, there is a need to provide both a mobile phone without increasing the cost, and does not affect the time the mobile phone automatic calibration method for a mobile phone volume.

SUMMARY OF THE INVENTION The present invention aims to provide a mobile phone without increasing either the cost, and does not affect the time the mobile phone automatic calibration method for a mobile phone volume.

CLAIMS (10) translated from Chinese

A mobile phone automatic time correction method, the mobile phone includes a signal receiving / transmitting unit receives the signal and the transmitted signal, the received signal samples from the time information in the time signal sampling unit that stores the time information and the setting information memory, the central processor and display unit, characterized in that the automatic time correction method comprising the steps of: setting an initial time a mobile phone, the correction time period, and the contacts for the source of the standard time and time request, and such data is stored in memory of the mobile phone; mobile phone to determine whether the need for a central processor time correction, otherwise continue as judge; For the time correction, the mobile phone automatically transmit a request signal to the standard time source; transmission time information source standard time upon request to the mobile phone; mobile phone time signal sampling means sampling and storing the time signal into the memory; central processing time is set to the system time of the mobile phone.

The mobile phone automatic time correction method according to claim 1, characterized in that: the method further comprises the mobile telephone system time is displayed on the display unit in step.

Automatic time correction method for a mobile phone according to claim 1 or claim 2, wherein: the standard time for the sound source exercise station.

The mobile phone automatic time correction method according to claim 3, characterized in that: the mobile phone equipped with a voice generating unit and a voice recognition unit, the mobile phone has to call a pre-request signal into sound inquiry time .

The mobile phone automatic time correction method according to claim 4, wherein: when the mobile telephone calling sound exercise station, mobile phone unit made by voice time inquiry request is generated.

Identification of the mobile phone and the speech sound exercise station by a time request signal to the mobile phone, the mobile phone voice signal through generating unit issued: The mobile phone automatic time correction method according to claim 5, characterized in that means sampling and storing the time signal into the memory.

To achieve the above object, a mobile phone embodiment of the present invention includes a signal receiving / transmitting unit receives the signal and the transmitted signal, a time signal sampling time signal sampling unit from the received signal, the memory storing the time information and setting information, Automatic time correction method for a mobile phone central processor and a display unit, the present invention comprises the steps of: setting the mobile phone of the initial time, the correction time period, and the contacts for the source of the standard time and time request, and such data stored in the mobile phone memory; the central processor determines whether the mobile phone need to be time correction, otherwise continue as judge;

For a time correction, the mobile phone automatically transmit a request signal to the standard time source; Standard Time time information sources according to the request of the mobile phone; mobile phone signal sampling unit time sampling the time signal and storage to memory; a central processing The time is set to a mobile telephone system time.

Preferably, the standard time for the sound source exercise station, mobile telephone inquiry station calling sound made by the time the request, and the time the signal transmitted by the acoustic exercise station to the mobile phone, the signal through the mobile phone voice generating unit is issued, and the mobile phone sampling the speech recognition unit time signal and stores into the memory.

The mobile phone automatic time correction method according to claim 1 or claim 2, wherein: the standard time source for cellular phone service network.

Mobile phone time automatic calibration method according to claim 7, characterized in that: the mobile phone in advance of the time provided for the inquiry message query request time.

The mobile phone automatic time correction method according to claim 8, wherein: the mobile phone reads from the memory the standard time source contact, and automatic contact, signal receiving / transmitting unit transmitting the inquiry message time Mobile phone service providers to network in.

Mobile phone time automatic calibration method as claimed in claim 9, wherein: the mobile phone service provider network in order to send a message in the form of standard time to the mobile phone, mobile phone signal sampling unit time sampling the time signal and stores to memory.

Preferably, the standard time source for mobile phone service provider networks, mobile phone by sending an SMS to a mobile phone service network in time to make the request, and the mobile phone service provider network in standard time sent to the mobile phone, mobile phone time signal sampling means sampling the time signal and stores into the memory.

Compared with the prior art, the present invention is the use of a mobile phone outside the regular standard time source mobile phone system time is corrected, thereby periodically time error promptly eliminated so that even if the mobile phone is generally of a clock circuit using a quartz oscillator nor will cause inconvenience to the user, so the need to adopt a more expensive quartz oscillator or other fine-tuning capacitor, etc., it will not increase the cost of mobile phones, and nor will it interfere with the formation of the miniaturization of mobile phones.

For the purposes of this invention, the structural features and functions have a better understanding, with a detailed description of the drawings hereby follows: BRIEF DESCRIPTION Figure 1 is a block diagram of the invention of mobile phones.

Figure 2 is a schematic flow chart of a mobile phone automatic time correction method.

[DETAILED DESCRIPTION] Hereinafter, in conjunction with Figure 1 and Figure 2 the present invention will be described in detail, based on the mobile phone as an example in the following description, one of ordinary skill in the art will appreciate, electronic embodiment of the electronic apparatus of the present invention is not limited to a mobile phone, having a wireless communication function such as smart phones and personal digital assistants (PDA) can be applied to the present invention.

See Figure 1, the embodiment of the present invention, a mobile phone 1 includes: a signal receiving / transmitting unit 10 for transmitting and receiving wireless communication signals; time signal sampling unit 11, and the signal receiving / transmitting unit 10 is coupled to the received signal in the time signal samples; a memory 12 for storing a system program of the mobile telephone, the time correction period, the standard time source contacts and the mobile phone 1 of the first setting time; a display unit 14 for displaying the system time of the mobile phone 1; central processor 13, and each of the unit is coupled to the control over the operation of the different units.

See Figure 2, the mobile phone 1 of the present invention, the automatic time correction method comprising the steps of:

Setting the mobile phone of the initial time, the time correction cycle, and the standard time source contact and time of the request, and such data is stored in a memory of the mobile phone 12, wherein the time correction period can be set to one week or one month, The standard time for the sound source can exercise stations, a query such as 114 Chinese mainland China Taiwan 104 repeater stations or station (step 100); mobile phone a central processor 13 determines whether the need for time correction, that is, from the initial set time Since, if after a set time correction cycle time, as otherwise continue to determine (step 101); For the time correction, that is, from the initial set time has been set time correction cycle time, the move The central processor 13 performs an automatic telephone contact function, reads the standard time source contacts from the memory 12, and automatically links, signal receiving / transmitting unit 10 transmit a request to the time the standard time source (step 102); standard time sent by the source of the mobile phone 1 requests the time information to the mobile phone 1 (step 103); time signal sampling unit 11 of the mobile phone 1 and the sampling time for

the signal stored to the memory 12 (step 104); a central processor 13 This time is set to the system time of the mobile phone 1 and displayed on (step 105) the display unit 14.

Preferably, when the standard time for the sound source exercise station, and the mobile phone 1 is equipped with a voice generating unit and a voice recognition unit, step 100 includes a pre-set time in the mobile phone 1 inquiry request, such as may be inquired time sound signal, step 102 includes the following steps: When a mobile phone call sound exercise stations, a mobile phone made by voice generating unit time inquiry request, and the corresponding step 103 includes the following steps: Time sound exercise station in turn request sent signal to the mobile telephone 1, the signal through the mobile phone voice generating unit 1 to issue, and the speech recognition unit of the mobile phone 1 and the sampling time for the signal stored to the memory 12.

Preferably, the standard time when the source is a mobile telephone service provider network, step 100 comprises a pre-set time in the mobile phone 1 inquiry request, such as SMS for inquiry time, step 102 includes the following steps: the mobile phone 1 read from the memory 12 times the standard source of contact information, and automatically links the signal receiver / transmitter unit 10 will ask for time to transmit messages to the mobile phone service provider network in, while the corresponding step 103 includes the following steps: mobile phone service providers network in order to send a text message to the mobile phone standard time a mobile phone signal sampling unit 11 hours a time signal sampling and storage to memory 12.

Compared with the prior art, the present invention is the use of a mobile phone outside the regular standard time source mobile phone system time is corrected, thereby periodically time error promptly eliminated so that even if the mobile phone is generally of a clock circuit using a quartz oscillator nor will cause inconvenience to the user, so the need to adopt a more expensive quartz oscillator or other fine-tuning capacitor, etc., it will not increase the cost of mobile phones, and nor will it interfere with the formation of the miniaturization of mobile phones.

CLASSIFICATIONS

International Classification	G04R20/00, H04M1/21, H04M1/00

LEGAL EVENTS

Date	Code	Event	Description
Nov 26, 2008	C02	Deemed withdrawal of patent application after publication (patent law 2001)	
Sep 6, 2006	C10	Request of examination as to substance	
Jul 12, 2006	C06	Publication	

Google Home - Sitemap - USPTO Bulk Downloads - Privacy Policy - Terms of Service - About Google Patents - Send Feedback

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04M 17/00 (2006.01)
H04Q 7/22 (2006.01)
H04L 12/14 (2006.01)

[12] 发明专利申请公开说明书

[21] 申请号 200510070958.9

[43] 公开日 2006 年 11 月 22 日

[11] 公开号 CN 1867024A

[22] 申请日 2005.5.19

[21] 申请号 200510070958.9

[71] 申请人 华为技术有限公司

地址 518129 广东省深圳市龙岗区坂田华为总部办公楼

[72] 发明人 申 海 孙 谦

[74] 专利代理机构 北京同达信恒知识产权代理有限公司

代理人 郭润湘

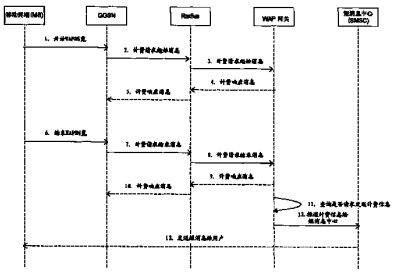
权利要求书 3 页 说明书 9 页 附图 2 页

[54] 发明名称

一种计费信息发送方法

[57] 摘要

本发明公开了一种计费信息发送方法，应用于无线应用协议(WAP)业务，该方法包括：移动终端经 WAP 网关使用 WAP 业务，WAP 网关对移动终端进行计费，WAP 网关发送计费信息给移动终端。本发明方法能实现由 WAP 网关将用户使用 WAP 业务的计费信息即时发送给用户终端，方便用户控制和使用 WAP 业务。



1、一种计费信息发送方法，应用于无线应用协议（WAP）业务，该方法包括：移动终端经 WAP 网关使用 WAP 业务，WAP 网关对移动终端进行计费，WAP 网关发送计费信息给移动终端。

2、如权利要求 1 所述的方法，其特征在于，在 WAP 网关中预先设置计费信息发送方式，在移动终端使用 WAP 业务过程中或使用 WAP 业务结束后 WAP 网关根据设置的计费信息发送方式发送计费信息给移动终端。

3、如权利要求 2 所述的方法，其特征在于，所述 WAP 网关中预先设置的计费信息发送方式与移动终端对应，在移动终端使用 WAP 业务过程中或使用 WAP 业务完成后 WAP 网关采用移动终端对应的计费信息发送方式发送计费信息给该移动终端。

4、如权利要求 2 或 3 所述的方法，其特征在于，所述计费信息发送方式为短消息发送；WAP 网关通过 WAP 推送方式发送移动终端使用 WAP 业务的计费信息给短消息中心；短消息中心以短消息方式将所述计费信息下发给移动终端。

5、如权利要求 4 所述的方法，其特征在于，所述计费信息发送方式中还包括设定的时间间隔，在移动终端使用 WAP 业务过程中，WAP 网关按所述设定的时间间隔发送所述计费信息给短消息中心。

6、如权利要求 4 所述的方法，其特征在于，所述计费信息发送方式中还包括设定的余额阈值、流量阈值或费用阈值，在移动终端使用 WAP 业务过程中，当 WAP 网关检测到预付费移动终端的余额小于设定的余额阈值、移动终端使用 WAP 业务流量超过设定的流量阈值或移动终端使用 WAP 业务费用超过设定的费用阈值时，WAP 网关发送计费信息给短消息中心。

7、如权利要求 2 或 3 所述的方法，其特征在于，所述计费信息发送方式为 WAP 网页；具体包括：在移动终端使用 WAP 业务过程中，WAP 网关为该

移动终端产生一个包含计费信息的临时 WAP 网页，并将该临时 WAP 网页的超链接地址以及超链接的显示文字插入到移动终端当前请求浏览的网页中，移动终端通过访问所述超链接地址获取计费信息；并在 WAP 业务结束后，删除所述临时 WAP 网页。

8、如权利要求 2 或 3 所述的方法，其特征在于，所述计费信息发送方式为 WAP 网页；具体包括：在移动终端使用 WAP 业务过程中，WAP 网关将指向一个即时计费单元的超链接插入到移动终端当前请求浏览的网页中，移动终端访问所述超链接时，即时计费单元从 WAP 网关中获取该移动终端的计费信息，并生成 WAP 网页返回给移动终端。

9、如权利要求 2 或 3 所述的方法，其特征在于，所述计费信息发送方式为 WAP 网页；具体包括：设定一个用于发送计费信息的固定超链接地址，当 WAP 网关检测到移动终端请求该固定超链接地址时将该移动终端的计费信息以 WAP 网页方式发送给移动终端。

10、如权利要求 9 所述的方法，其特征在于，所述固定超链接地址预置在所述移动终端中。

11、如权利要求 2 或 3 所述的方法，其特征在于，所述计费信息发送方式为 IP 数据包发送，WAP 网关接收到移动终端的计费信息请求或根据设定的时间间隔将包含计费信息的数据包按照 IP 协议格式发送给移动终端对应的 IP 地址，由移动终端显示出计费信息。

12、如权利要求 11 所述的方法，其特征在于，在移动终端 WAP 浏览器界面的固定位置显示所述计费信息。

13、如权利要求 1 所述的方法，其特征在于，当移动终端为预付费终端，还包括 WAP 网关在该移动终端请求 WAP 业务时，查询其预付费余额的步骤；若预付费余额不足，则 WAP 网关通知该移动终端，并拒绝其使用请求的 WAP 业务，否则移动终端正常使用 WAP 业务。

14、如权利要求 1 所述的方法，其特征在于，所述 WAP 业务为 WAP 浏览

类业务或 WAP 流媒体业务。

15、如权利要求 1 所述的方法，其特征在于，所述计费信息为移动终端本次使用 WAP 业务流量、累计使用 WAP 业务流量、本次使用 WAP 业务费用、累计使用 WAP 业务费用、本次业务使用时长、本次业务费率和预付费余额其中之一或任意多个的组合信息。

16、如权利要求 15 所述的方法，其特征在于，若 WAP 网关发送的计费信息包括累计使用 WAP 业务流量、累计使用 WAP 业务费用、本次业务费率或预付费余额中至少其中之一时，还包括 WAP 网关向数据业务管理平台发送请求消息，获取上述计费信息的步骤。

17、如权利要求 16 所述的方法，其特征在于，若数据业务管理平台没有保存相应请求的计费信息，则由数据业务管理平台到智能网的业务控制点（SCP）上获取。

一种计费信息发送方法

技术领域

本发明涉及无线通信领域，尤其涉及无线应用协议（Wireless Application Protocol，WAP）业务的计费信息发送方法。

背景技术

WAP技术目前已成为移动通信网络中终端访问无线信息服务的全球主要标准，也是实现现有移动数据及增值业务的技术基础。WAP浏览类业务是最普通和常用的移动数据业务，用户通过终端的浏览器查看从服务器收到的WAP网页信息，作为移动数据业务的一种基础业务，WAP浏览类业务正被越来越多的移动用户所使用并接受。另外基于WAP的移动流媒体业务，也将成为3G通信网络中的主流应用。开放移动联盟（Open Mobile Alliance，OMA）在WAP业务具体计费实现上并没有做出限定，而现有技术中也还没有一种将WAP业务计费信息即时传送给移动终端的方法。移动终端的计费信息只能在话费月结时由计费系统如BOSS对从WAP网关采集来的话单进行统计批价，然后打印出来提供给用户，而且通常还没有费用的明细记录。由于WAP网关很多情况都是按流量进行计费，这样对于预付费和后付费用户，都存在一个同样的问题：用户在使用WAP业务中或进行一次WAP业务后，不知道产生了多少流量，也不知道本月累计使用了多少流量，使得用户无法及时掌握或控制WAP业务的使用情况；特别是对于预付费用户，当预付费用用完时，在用户无法事先获知的情况下WAP网关会强行中断业务，给用户使用WAP业务造成困扰。

发明内容

本发明提供一种计费信息发送方法，用以解决现有技术中存在的 WAP 业

务不能即时提供计费信息的问题。

本发明方法包括：移动终端经 WAP 网关使用 WAP 业务，WAP 网关对移动终端进行计费，WAP 网关发送计费信息给移动终端。

根据本发明的上述方法，在 WAP 网关中预先设置计费信息发送方式，在移动终端使用 WAP 业务过程中或使用 WAP 业务结束后 WAP 网关根据设置的计费信息发送方式发送计费信息给移动终端。

所述 WAP 网关中预先设置的计费信息发送方式与移动终端对应，在移动终端使用 WAP 业务过程中或使用 WAP 业务完成后 WAP 网关采用移动终端对应的计费信息发送方式发送计费信息给该移动终端。

所述计费信息发送方式为短消息发送；WAP 网关通过 WAP 推送方式发送移动终端使用 WAP 业务的计费信息给短消息中心；短消息中心以短消息方式将所述计费信息下发给移动终端。

所述计费信息发送方式中还包括设定的时间间隔，在移动终端使用 WAP 业务过程中，WAP 网关按所述设定的时间间隔发送所述计费信息给短消息中心。

所述计费信息发送方式中还包括设定的余额阈值、流量阈值或费用阈值，在移动终端使用 WAP 业务过程中，当 WAP 网关检测到预付费移动终端的余额小于设定的余额阈值、移动终端使用 WAP 业务流量超过设定的流量阈值或移动终端使用 WAP 业务费用超过设定的费用阈值时，WAP 网关发送计费信息给短消息中心。

所述计费信息发送方式为 WAP 网页；具体包括：在移动终端使用 WAP 业务过程中，WAP 网关为该移动终端产生一个包含计费信息的临时 WAP 网页，并将该临时 WAP 网页的超链接地址以及超链接的显示文字插入到移动终端当前请求浏览的网页中，移动终端通过访问所述超链接地址获取计费信息；并在 WAP 业务结束后，删除所述临时 WAP 网页。

所述计费信息发送方式为 WAP 网页；具体包括：在移动终端使用 WAP

业务过程中，WAP 网关将指向一个即时计费单元的超链接插入到移动终端当前请求浏览的网页中，移动终端访问所述超链接时，即时计费单元从 WAP 网关中获取该移动终端的计费信息，并生成 WAP 网页返回给移动终端。

所述计费信息发送方式为 WAP 网页；具体包括：设定一个用于发送计费信息的固定超链接地址，当 WAP 网关检测到移动终端请求该固定超链接地址时将该移动终端的计费信息以 WAP 网页方式发送给移动终端。

所述固定超链接地址预置在所述移动终端中。

所述计费信息发送方式为 IP 数据包发送，WAP 网关接收到移动终端的计费信息请求或根据设定的时间间隔将包含计费信息的数据包按照 IP 协议格式发送给移动终端对应的 IP 地址，由移动终端显示出计费信息。

在移动终端 WAP 浏览器界面的固定位置显示所述计费信息。

当移动终端为预付费终端，还包括 WAP 网关在该移动终端请求 WAP 业务时，查询其预付费余额的步骤；若预付费余额不足，则 WAP 网关通知该移动终端，并拒绝其使用请求的 WAP 业务，否则移动终端正常使用 WAP 业务。

所述 WAP 业务为 WAP 浏览类业务或 WAP 流媒体业务。

所述计费信息为移动终端本次使用 WAP 业务流量、累计使用 WAP 业务流量、本次使用 WAP 业务费用、累计使用 WAP 业务费用、本次业务使用时长、本次业务费率和预付费余额其中之一或任意多个的组合信息。

若 WAP 网关发送的计费信息包括累计使用 WAP 业务流量、累计使用 WAP 业务费用、本次业务费率或预付费余额中至少其中之一时，还包括 WAP 网关向数据业务管理平台发送请求消息，获取上述计费信息的步骤。

若数据业务管理平台没有保存相应请求的计费信息，则由数据业务管理平台到智能网的业务控制点（SCP）上获取。

本发明有益效果如下：

（1）本发明通过利用 WAP 网关向终端发送计费信息，实现了用户在使用 WAP 业务过程中或刚刚使用 WAP 业务完成后的时间内能够即时获取计费信

息，方便用户控制和使用 WAP 业务。

（2）本发明提供了多种计费信息发送方式的实现方案，包括：短消息方式、WAP 网页方式和 IP 数据包方式，WAP 网关可以根据网络状况和能力选择其中至少一种计费信息发送的实现方案将计费信息即时发送给用户终端；而对于同时提供了多种计费信息发送方式的 WAP 网关，用户也可以灵活设置计费信息发送方式，充分满足用户的个性化需求和使用习惯。

（3）本发明可以对需要 WAP 业务计费信息即时发送的用户预先进行登记，系统只对登记的用户按默认或设置的计费信息发送方式发送计费信息，在充分满足用户需求的同时，减少系统负荷。

附图说明

图 1 为计费信息下发所涉及的系统结构示意图；

图 2 为本发明实施例中 WAP 浏览业务计费过程及通过短消息下发计费信息的信令流程图；

图 3 为本发明实施例中 WAP 流媒体业务计费过程及通过短消息下发计费信息的信令流程图。

具体实施方式

本发明方法是由 WAP 网关在移动终端使用 WAP 业务过程中或使用 WAP 业务结束后发送计费信息给移动终端。而 WAP 网关发送计费信息的方式可以是短消息，WAP 网页等，具体实施中可以在 WAP 网关中实现一种或同时实现多种计费信息发送方式。

对于不同的移动终端，通过预先在 WAP 网关存储对应的计费信息发送方式，在移动终端使用 WAP 业务过程中或使用 WAP 业务完成后 WAP 网关采用移动终端对应的计费信息发送方式发送计费信息给该移动终端。

在实际应用中，可以将计费信息发送作为一个新的 WAP 业务功能，由用

户进行登记。对于登记使用该业务功能的用户，在使用 WAP 业务过程中或业务结束后，WAP 网关采用该移动终端对应的计费信息发送方式发送计费信息给该移动终端，如果 WAP 网关不允许用户设置自己的计费信息发送方式或者用户没有设置自己的计费信息发送方式则 WAP 网关采用系统默认的计费信息发送方式发送计费信息给移动终端；对于没有登记该业务功能的用户，则可以不发送计费信息。

具体实施方法包括：在 WAP 网关的用户信息数据库中添加表明用户希望使用 WAP 计费信息即时发送标识（为描述方便，称之为第一标识），当用户申请 WAP 计费信息即时发送这项业务功能时，给该移动用户的第一标识赋值为“1”；否则，赋值为“0”表示该用户不使用 WAP 业务计费信息即时发送业务功能。同时，需要添加计费信息发送方式标识（为描述方便，称之为第二标识）；在第二标识中可以用不同的值代表不同的发送方式，如：“0”表示以短消息方式发送，“1”表示以 WAP 网页方式发送，“2”表示以 IP 数据包方式发送等；同种方式还可以衍生出多种子类型，如按时间间隔周期性发送，超过设定的流量阈值或费用阈值时发送等。还可以将其中一种发送方式作为系统默认的发送方式，如第二标识为“0”的短消息方式发送方式。

当移动用户请求 WAP 业务时，WAP 网关查询存储的用户信息数据库，若检测到该移动用户已申请 WAP 计费信息即时发送业务功能，则将其计费信息按照设置的发送方式发送给移动终端。

发送的计费信息包括至少下列之一：本次或累计流量，本次或累计费用，业务使用时长，业务费率，预付费余额等。WAP 网关一般只有当前流量信息，累计流量以及费率等需要从数据业务管理平台（DSMP）和业务控制点（SCP）上获取，如图 1 所示，WAP 网关向 DSMP 发送请求，如果 DSMP 上没有相应信息，则 DSMP 向 SCP 请求信息，获取业务相关的费率、预付费余额以及终端累计费用信息等，然后发送给移动终端。一般情况下，WAP 网关不直接与 SCP 相连，而是通过 DSMP 连接 SCP 获取计费信息。

若移动终端对应的计费信息发送方式为短消息发送，则 WAP 网关通过 WAP 推送方式发送计费信息给短消息中心；短消息中心以短消息方式将计费信息下发给移动终端。

如图 2 所示，为 WAP 浏览业务计费过程及通过短消息下发计费信息的信令流程图，包括如下流程：

1、移动用户通过移动终端发起 WAP 浏览；

2、网关 GPRS 支持节点（GGSN）为移动终端（MS）分配了 IP 地址后向远程身份验证拨入用户服务（RADIUS）服务器发送计费请求起始消息，在该消息中包含分配给 MS 的 IP 地址和手机号码；

3、RADIUS 服务器向 WAP 网关转发计费请求起始消息；

4、WAP 网关收到计费请求起始消息后，向 RADIUS 服务器发送计费响应消息；

5、RADIUS 服务器收到计费响应消息后转发给 GGSN，若 GGSN 未收到计费响应消息，应向 RADIUS 服务器重新发送计费请求起始消息；

6、移动用户结束此次 WAP 浏览；

7、GGSN 向 RADIUS 服务器发送计费请求结束消息；

8、RADIUS 服务器向 WAP 网关转发计费请求结束消息；

9、WAP 网关收到计费请求结束消息后，向 RADIUS 服务器发送计费响应消息；

10、RADIUS 服务器收到计费响应消息后转发给 GGSN，若 GGSN 未收到计费响应消息，应重新发送计费请求结束消息；

11、WAP 网关发送计费响应后，判断该移动用户的第一标识，如果第一标识为“0”，则结束；如果第一标识为“1”，且第二标识为通过短消息方式发送计费信息，则执行步骤 12；

12、WAP 网关通过推送代理网关（Push Proxy GateWay，PPG）向短消息中心（SMSC）推送用户本次使用流量（费用）以及累计流量（费用）等信息；

13、SMSC 以短消息方式将接收的计费信息发送到移动终端上。

图 3 为 WAP 流媒体业务计费过程及通过短消息下发计费信息的信令流程图。WAP 网关收到 MS 发出的访问请求后，对访问请求的统一定位资源（URL）进行解析，判断为流媒体业务后将相关业务的提供商标识信息（SPID）、业务标识信息（ServiceID）以及用户的 IP 地址等与计费相关的信息上报给 DSMP 进行业务鉴权批价。流媒体业务计费同时支持预付费用户和后付费用户。对于预付费用户，DSMP 通过与 SCP 的交互完成实时扣费。具体信令交互流程如图 3 所示，包括:

1、MS 向 WAP 网关发起流媒体业务访问请求。

2、WAP 网关收到访问请求后，判断是否对用户请求进行转发，如果满足转发条件，则继续处理；否则，拒绝此次访问请求。

在该步骤中，是否对用户的业务请求进行前转或拒绝，是根据系统数据库中的一个“转发控制表”来执行的，该表存储有不可访问某项业务的 MS 的 IP 地址或终端号码，比如，在用户欠费或余额不足的情况下，将对其禁用某些类型的业务请求；当 MS 请求业务时，WAP 网关将查找“转发控制表”，如果发送业务请求的 MS 包含在“转发控制表”中，则确定所请求此项业务是否为不可访问业务，如果是，则对此 MS 禁用该项业务，并将用户的欠费信息发送给 MS；如果发送业务请求的 MS 不在转发控制表中，则说明此 MS 是合法的，WAP 网关则将该请求透传给业务提供商（SP），并进行内容计费或流量计费，在业务使用过程中或使用后将计费信息发给 MS。为了防止用户在已经充值的情况下，仍然无法使用某项业务，转发控制表中的用户信息是实时更新的。

3、WAP 网关将业务请求转发给相应的业务提供商或内容提供商（SP/CP）。

4、SP/CP 返回访问请求应答消息给 WAP 网关。

5、WAP 网关把请求应答消息下发给终端 MS。

6、WAP 网关记录或查询用户在线信息，并判断用户类型（根据 MSISDN 号段或 IMSI 号段区分用户类型，如预付费用户、后付费用户），如果是后付费

用户，业务使用结束后直接跳转到第 11 步；如果是预付费用户，根据请求的 URL 采集 SPID、ServiceID 以及用户 IP 地址等计费相关信息。

7、WAP 网关将采集到的计费相关信息上报 DSMP，进行鉴权批价。

8、DSMP 到 SCP 申请费用预扣。

9、SCP 向 DSMP 返回费用预扣应答消息。

10、DSMP 向 WAP 网关返回鉴权批价应答消息。

11、MS 向 WAP 网关发出断连请求。

12、WAP 网关把断连请求转发给 SP/CP。

13、SP/CP 向 WAP 网关返回断连请求应答消息。

14、WAP 网关把断连请求应答消息下发给终端 MS。

15、WAP 网关生成话单记录（Call Detail Record ，CDR），包括业务开始时间，结束时间，终端号码，业务类型等。

16、WAP 网关将 CDR 话单中的计费信息通过 WAP PUSH 短消息发给 MS。

以上用 WAP 浏览业务和流媒体业务的计费过程为例，对本发明采用短消息方式发送 WAP 业务计费信息进行了详细描述。其中，短消息发送方式可以是在移动终端使用 WAP 业务过程中，由 WAP 网关按设定的时间间隔发送；或在移动终端使用 WAP 业务过程中，当预付费移动终端的余额小于设定的余额阈值、移动终端使用 WAP 业务流量超过设定的流量阈值或移动终端使用 WAP 业务费用超过设定的费用阈值时，在 WAP 浏览业务的第 5 步与第 6 步之间或在 WAP 流媒体业务的第 10 步与第 11 步之间，由 WAP 网关发送计费信息给短消息中心。另外对于流媒体业务与浏览业务同时使用的情形，如 WAP 浏览时打开了一个流媒体，这样 WAP 网关同时将两个业务的计费信息分别或合并在一起发送给 MS。

对于计费信息的发送，除了采用短消息方式发送外，还可以采用 WAP 网页方式发送，包括下列具体方法：

方法一：在移动终端使用 WAP 业务过程中，WAP 网关为该移动终端产生

一个包含计费信息的临时 WAP 网页，并将该临时 WAP 网页的超链接地址插入到移动终端当前浏览的网页中，移动终端通过访问所述超链接地址获取计费信息；并在 WAP 业务结束后，删除产生的临时 WAP 网页。

方法二：在移动终端使用 WAP 业务过程中，WAP 网关将指向一个即时计费单元的超链接插入到移动终端当前请求浏览的网页中，移动终端访问所述超链接时，即时计费单元从 WAP 网关中获取该移动终端的计费信息，并生成包含计费信息的 WAP 网页由 WAP 网关返回给移动终端。

方法三：将移动终端使用 WAP 业务的计费信息存储到一个固定超链接地址的 WAP 网页中，当移动终端访问该固定超链接地址时，WAP 网关获取相应的计费信息并更新到上述 WAP 网页然后返回给移动终端。为用户使用方便，可以将上述固定超链接地址预先存储到移动终端中，用户可以随时通过访问该超链接地址获取计费信息。

计费信息发送方式还可以为 IP 数据包发送，可以设置为当 WAP 网关接收到移动终端的计费信息请求时，将包含计费信息的数据包按照 IP 协议格式发送给移动终端对应的 IP 地址，或 WAP 网关按照设定的时间间隔将包含计费信息的数据包按照 IP 协议格式发送给移动终端对应的 IP 地址，由移动终端显示出计费信息。同时改进 WAP 浏览器，使之在终端浏览器界面的固定位置显示 WAP 网关发送的计费信息（流量或费用信息）。

显然，本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样，倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。

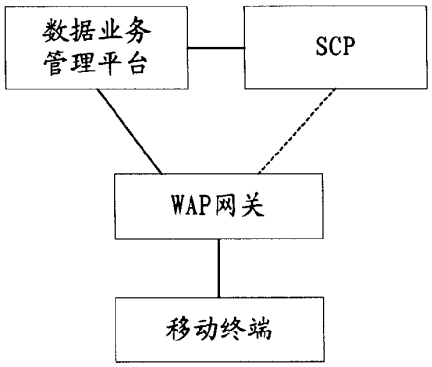

数据业务
管理平台
SCP
WAP网关
移动终端

图 1

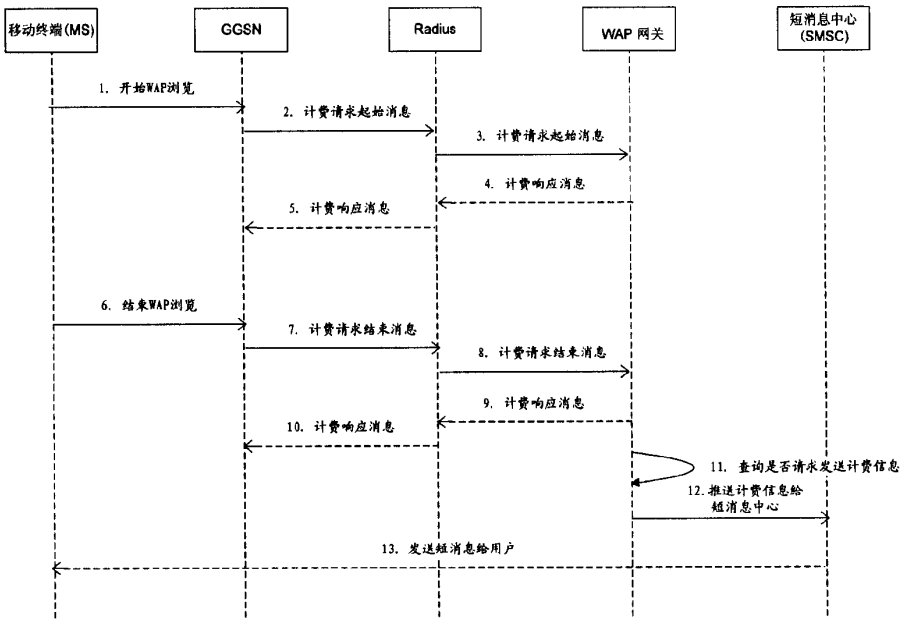

移动终端(MS)
GGSN
Radius
WAP 网关
短消息中心
(SMSC)
1. 开始WAP浏览
2. 计费请求起始消息
3. 计费请求起始消息
4. 计费响应消息
5. 计费响应消息
6. 结束WAP浏览
7. 计费请求结束消息
8. 计费请求结束消息
9. 计费响应消息
10. 计费响应消息
11. 查询是否请求发送计费信息
12. 推送计费信息给
短消息中心
13. 发送短消息给用户

图 2

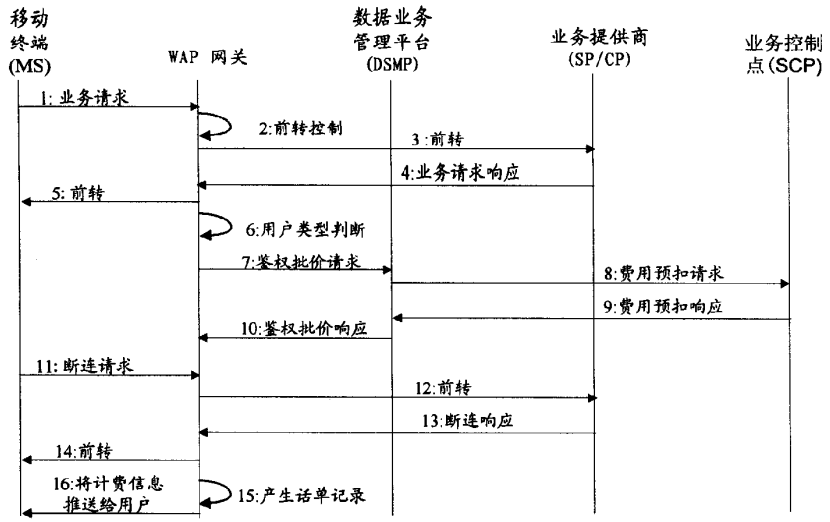

移动
终端
(MS)
WAP 网关
数据业务
管理平台
(DSMP)
业务提供商
(SP/CP)
业务控制
点(SCP)
1: 业务请求
2:前转控制
3 :前转
4:业务请求响应
5: 前转
6:用户类型判断
7:鉴权批价请求
8:费用预扣请求
9:费用预扣响应
10:鉴权批价响应
11: 断连请求
12:前转
13:断连响应
14:前转
16:将计费信息
推送给用户
15:产生话单记录

图 3

Sign in

Patents Application Grant English Chinese

Find prior art Discuss this application View PDF Download PDF

Charging information transmitting method

CN 1867024 A

Publication number	CN1867024 A
Publication type	Application
Application number	CN 200510070958
Publication date	22 Nov 2006
Filing date	19 May 2005
Priority date	19 May 2005
Also published as	CN1867024B
Inventors	申商, 孙豫
Applicant	华为技术有限公司
Export Citation	BiBTeX, EndNote, RefMan

Referenced by (6), Classifications (3), Legal Events (3)

External Links: SIPO, Espacenet

ABSTRACT

The invention relates to a charge information sending method, used in wireless application protocol (WAP) service, which comprises: the mobile terminal via WAP gateway uses WAP service; the WAP gateway charges the mobile terminal and sends the charge information to the mobile terminal. The invention can make the WAP gateway instantly send the charge information of consumed WAP service to the user terminal, to support the control and application of WAP service.

DESCRIPTION translated from Chinese

An information transmission method accounting

FIELD

The present invention relates to the field of wireless communications, and more particularly to a wireless application protocol (Wireless ApplicationProtocol, WAP) service charging information transmission method.

BACKGROUND

WAP technology has become a major global standard for mobile communications network terminal access wireless information services, as well as the technical foundation of existing mobile data and value-added services. WAP browser is the most common class of business and popular mobile data services, the user terminal via a browser to view WAP pages of information received from the server, as a basis for business mobile data services, WAP browsing class of business is being more and more Mobile users are using and accepted. Also WAP-based mobile streaming media business, will become the mainstream of 3G communication network applications. Open Mobile Alliance (Open Mobile Alliance, OMA) on WAP service specific implementation does not make a limited charging, while the prior art has not yet a WAP service billing information to a method for real time transmission to the mobile terminal. Billing information of the mobile terminal only when such calls monthly billing system by BOSS collected from the WAP gateway to the words of a single statistical rating, then print it out to users, but usually no expense detail records. Many cases are due to a WAP gateway billing by traffic, so for prepaid and postpaid users, there is a similar problem: the user in the use of WAP services, or conduct a WAP service, I do not know how much traffic generated, but also I do not know how much traffic this month cumulative use, so users can not grasp or control the use of WAP services; especially for prepaid subscribers, prepaid expenses when exhausted, in case the user can not be informed in advance of the WAP gateway will be forced to interrupt business users to use WAP services to cause trouble.

SUMMARY

The present invention provides a method for transmitting charging information to solve the prior art are not readily available WAP service charging information problems.

CLAIMS (17) translated from Chinese

A charging information transmission method, applied to a wireless application protocol (WAP) service, the method comprising: a mobile terminal using WAP services via the WAP gateway, WAP gateway of the mobile terminal for billing, WAP gateway sends accounting information to the mobile terminal.

2. The method according to claim 1, characterized in that the WAP gateway is preset in the charging information transmission method, in a mobile terminal using the WAP services used during or after the WAP gateway WAP service charging information according to the transmission setting Billing information is sent to the mobile terminal.

3. The method according to claim 2, characterized in that the charging information transmission method with the mobile terminal of the WAP gateway preset correspondence, using WAP service in a mobile terminal during or after completion of the WAP gateway WAP services using accounting information corresponding to the mobile terminal sending to send accounting information to the mobile terminal.

4. A method as claimed in claim 2 or claim 3, characterized in that the charging information transmission method for transmitting a short message, WAP gateway sends the mobile terminal using the WAP service charging information via WAP push mode to the short message center; SMS short message center to the next billing information to the mobile terminal.

5. The method according to claim 4, characterized in that the charging information transmission mode further includes setting the time interval, the mobile terminal using WAP in the course of business, WAP gateway according to the set time intervals sending the accounting information to the short message center.

6. The method of claim 4 when the WAP gateway detection claim, characterized in that the charging information transmission mode further includes setting a threshold value of the balance, the flow rate threshold or cost threshold, the mobile terminal using WAP in the course of business, When the prepaid balance of the mobile terminal is less than a set threshold balance value, the mobile terminal uses the mobile terminal traffic threshold or WAP traffic exceeds the costs of the use of WAP services cost more than the set threshold value, WAP

The method of the present invention includes: a mobile terminal via WAP gateway using WAP services, WAP gateway for mobile terminals for billing, WAP gateway sends billing information to the mobile terminal.

The above-described method according to the invention, the WAP gateway preset charging information transmission method, the business process using WAP or WAP gateway used to send accounting information to the accounting information based on the transmission method set by the mobile terminal after the WAP service in a mobile terminal .

Billing information transmitting manner with the WAP gateway of the mobile terminal set in advance corresponding to, in a mobile terminal using the WAP services used during or after completion of WAP gateway WAP services using the mobile terminal corresponding to the charging information sending to send accounting information to the mobile terminal.

The charging information transmission method for sending short messages; WAP gateway sends the mobile terminal using the WAP service billing information via WAP push mode to the short message center; short message center to a mobile short message will be sent to the billing information under terminal.

Information transmission mode further includes setting the charging time interval, using the WAP service in a mobile terminal during, WAP gateway according to the preset time interval to transmit the accounting information to the short message center.

The billing information transmitting mode further includes setting a threshold value of the balance, the flow rate threshold or cost threshold, the mobile terminal using WAP in the course of business, when the WAP gateway detects that the mobile terminal prepaid balance is less than the set threshold balance, moving When the end-use flow threshold or WAP mobile terminal traffic exceeds the cost of using WAP services exceeds the cost threshold, WAP gateway sends billing information to the short message center.

The charging information transmission method for WAP pages; including: the mobile terminal business processes using WAP, WAP gateway WAP page that contains the provisional billing information for the mobile terminal, and the temporary WAP page hyperlink address and display text hyperlinks inserted in the mobile terminal is currently viewed page request, the mobile terminal acquires the billing information by accessing the hyperlink address; and after the WAP service, deleting the temporary WAP page.

The charging information transmission method as WAP pages; specifically include: the mobile terminal using the WAP business process, WAP gateway will point to an immediate hyperlink accounting unit is inserted into the mobile terminal is currently viewed page request, the mobile terminal accesses when said hyperlink, immediate accounting unit receives charging information of the mobile terminal from the WAP gateway, and generates WAP pages returned to the mobile terminal.

The charging information transmission method as WAP pages; specifically includes: setting a fixed address hyperlink for transmitting the charging information, when the WAP gateway detects that the mobile terminal requests the fixed address of the mobile terminal hyperlink billing Information sent to the WAP pages to the mobile terminal.

Said fixed hyperlink address preset in the mobile terminal.

The charging information transmission method for transmitting IP packets, WAP gateway receives the charging information to the mobile terminal or a request intervals containing charging information according to the set time of the data packet transmitted to the mobile terminal corresponding to the IP protocol in accordance with the format of IP address, the mobile terminal displays the charging information.

gateway sends accounting information to the short message center.

7. The method according to claim 2 or claim 3, characterized in that the charging information transmission method as WAP pages; specifically include: the mobile terminal using the WAP business process, WAP gateway generates a count for the mobile terminal comprising Temporary fee WAP pages of information, and the temporary WAP page hyperlink address and hyperlink display text is inserted into the mobile terminal is currently viewed page request, the mobile terminal to obtain billing information by accessing the hyperlink address; and After the WAP service, delete the temporary WAP pages.

8. The method according to claim 2 or claim 3, characterized in that the charging information transmission method as WAP pages; specifically include: the mobile terminal using the WAP service process, WAP gateway will point to a real-time accounting unit hyperlink into the mobile terminal is currently viewed web page request, the mobile terminal to access the hyperlink, the accounting unit immediately obtain charge information of the mobile terminal from the WAP gateway, and generates WAP pages returned to the mobile terminal.

When the WAP gateway detection setting a fixed hyperlink address for sending billing information: including; 9. The method of claim 2 or claim 3, wherein the charging information transmission method for WAP pages to the mobile terminal requests the address of the hyperlink fixed charge information to the mobile terminal WAP page sent to the mobile terminal.

10. The method according to claim 9, characterized in that the fixed hyperlink address preset in the mobile terminal.

11. The method according to claim 2 or claim 3, characterized in that the charging information transmission method for transmitting IP packets, WAP gateway receives the charging information to the mobile terminal according to a request or set time interval will contain packet transmission according to the charging information to the mobile terminal IP protocol format corresponding to the IP address, the mobile terminal displays the charging information.

12. The method according to claim 11, characterized in that the charging information is displayed in a fixed position of the mobile terminal WAP browser interface.

13. The method of claim 1, wherein, when the mobile terminal is a prepaid terminal, further comprising the WAP gateway when the mobile terminal requests the WAP service, its pre-paid balance inquiry step; if insufficient pre-paid balance, the WAP gateway informs the mobile terminal, and reject the use of WAP service request, otherwise normal use of WAP mobile terminal business.

14. A method as claimed in claim 1, characterized in that the WAP service for WAP browsing WAP class of business or streaming media services.

15. A method as claimed in claim 1, characterized in that the billing information for mobile terminal using WAP traffic in this, the cumulative use of WAP traffic, this time using WAP operating expenses, total operating expenses using WAP, this When using a long time business, this business combination and prepaid tariff information which one or any number of balance.

16. The right to at least one of the times when business rates or prepaid balance method of claim 15, wherein if the WAP gateway sends billing information, including cumulative use WAP traffic, total

In the fixed position of the mobile terminal WAP browser interface displays the charging information.

When the mobile terminal for prepaid terminals, including WAP gateway when the mobile terminal requests WAP services, check their prepaid balance steps; pre-paid balance if less, the WAP gateway informs the mobile terminal, and reject the use of the requested WAP business, otherwise normal use of WAP mobile terminal business.

The WAP service for WAP Browser WAP class of business or streaming media services.

operating expenses using WAP, further comprising a WAP gateway to the data service management platform sends a request message, the charge information acquisition step.

17. The method of claim 16, wherein, if the data service management platform does not save the corresponding charging information requested by the data service management platform to a service control point (SCP) of the intelligent network on the acquisition.

The charging information for the mobile terminal using WAP traffic in this, the cumulative use of WAP traffic, this time using WAP operating expenses, total operating expenses using WAP, use a long time in this business, this business rates and pre-paid balance among One or a combination of any number of information.

If the WAP gateway sends billing information, including cumulative use WAP traffic, the cumulative cost of using WAP services, at least one of the times when business rates or pre-paid balance, which also includes a WAP gateway to the data service management platform sends a request message to get said step of charging information.

If the data is not saved billing service management platform information corresponding request by the data service management platform to the service control point (SCP) on the acquisition of the intelligent network.

Beneficial effects of the present invention is as follows: (1) The present invention utilizing WAP gateway sends billing information to the terminals, the user in the course of business using WAP or just use the time after the completion of WAP services can instantly obtain billing information, user-friendly control and use WAP services.

(2) The present invention provides a variety of billing information transmission method implementations, including: short message, WAP page mode and IP packet mode, WAP gateway can select at least one of the charging information is sent according to the network status and the ability realization of the program will immediately send the charging information to the user terminal; and for a variety of billing information while providing a way to send a WAP gateway, users can flexibly set billing information transmission mode, fully meet the user's individual needs and habits .

(3) The present invention may require the user to send instant WAP service billing information pre-registration, the system only to registered users by default or set of accounting information send send billing information, while fully meet user demand, reduce system load.

Brief Description

Figure 1 is a schematic structural view of the system under the charging information issued involved; Fig. 2 embodiment of the present invention, WAP browse service billing process and the short message sent by a flowchart of charging information at a signaling; Figure 3 embodiment of the present invention example WAP streaming service billing process and issued the flow chart via SMS billing information signaling.

DETAILED DESCRIPTION

The method of the present invention is a mobile terminal using the WAP gateway WAP in the course of business or accounting information sent to the mobile terminal after the end of the use of WAP services. The WAP gateway sends billing information can be a way SMS, WAP pages, the specific implementation can be achieved in a WAP gateway or billing information is sent simultaneously to achieve a variety ways.

For different mobile terminal via the WAP gateway is stored in advance in the charging information corresponding to the transmission method, in a mobile terminal during use or after use WAP services complete WAP gateway WAP services using the mobile terminal corresponding to the charging information sending to send accounting information to the mobile terminal.

In practice, the charging information may be sent as a new WAP service function registration by the user. For registered users to use the business functions, after or during the use of the WAP service end of the business, WAP gateway uses the mobile terminal corresponding billing information send billing information is sent to the mobile terminal, if the WAP gateway does not allow users to set their own billing information is sent way or you do not set your own way billing information is sent using the default WAP gateway sends billing information send billing information to the mobile terminal; for there is no registration of the business functions of the user, you can not send billing information.

DETAILED DESCRIPTION The method comprises: a WAP gateway in the user information database indicates that the user wishes to add in a WAP charging information sent immediately identified (for convenience of description, referred to the first identification), when the user applies the charging information immediately send the WAP service When the function assigned to the first identification of the mobile subscriber is "1"; otherwise, the value "0" indicates that the user

does not immediately send a service function using the WAP service billing information. Meanwhile, the need to add the accounting information identifies the transmission mode (for convenience of description, referred to the second identification); in the second identification can be different values represent different transmission methods, such as: "0" indicates that a short message sent "1" means to send WAP pages, "2" to send IP packets, etc; the same way many seeds can also be derived types, such as by sending periodic intervals, the flow exceeds the set threshold value or cost of When the threshold is sent and the like. Wherein a further short message transmission mode as the default transmission mode, such as the second identifier is "0" may be input mode.

When the mobile user requests a WAP service, the WAP gateway queries the user information database stored, if it is detected that the mobile user has applied charging information sent immediately WAP service function, it is the accounting information sent to the mobile terminal according to the transmission mode set.

Billing information sent includes at least one of the following: The total flow or that this or cumulative cost, long-time business use, business rates, and other pre-paid balance. WAP gateway generally only current traffic information, as well as cumulative flow rate, etc. need to obtain from the data service management platform (DSMP) and a service control point (SCP), as shown in Figure 1, WAP gateway sends a request to DSMP, if on no DSMP appropriate information, then DSMP to SCP request information, access to business-related rates, pre-paid balance and terminal cumulative cost information, and then sent to the mobile terminal. Generally, WAP gateway not directly connected with the SCP, but is connected SCP receives charging information DSMP.

If the mobile terminal corresponding to the charging information transmission method for sending short messages, the WAP gateway sends billing information via WAP push mode to the short message center; short message center to short message will be sent to the mobile terminal next billing information.

2, the billing process for the WAP browsing service by sending the next charging information and a signaling message flow diagram, comprises the following processes: 1, the mobile terminal through the mobile user initiates a WAP browser; 2, Gateway GPRS Support Node (After GGSN) for the mobile terminal (MS) is assigned an IP address to the Remote Authentication Dial-In User Service (RADIUS) server sends an accounting request start message containing the IP address assigned to the MS, and phone number in the message; 3, RADIUS server forwards the request to start charging WAP gateway message; 4, WAP gateway billing request after receiving the initial message, send a response message to the RADIUS accounting server; 5, RADIUS server receives the forwarded after charging response message to the GGSN If the GGSN charging response message is not received, the RADIUS server should start charging request to resend the message; 6, the end of the WAP mobile users browse; 7, GGSN sends an accounting request to the RADIUS server end of the message; 8, RADIUS WAP billing gateway server forwards the request to the end of the message; 9, WAP gateway charging request received after the end of the message, send a response message to the RADIUS accounting server; 10, RADIUS server receives forwarded to the GGSN after charging response message, if the GGSN charging response message is not received, the end should resend the charging request message; 11, WAP gateway after sending charging response, determines the first identification of the mobile user, if the first identifier is "0", the end; if the first one identified as "1", and the second is identified as sending billing information via short message, proceed to Step 12; 12, WAP Push Proxy Gateway gateway (Push Proxy GateWay, PPG) to the Short Message Service Center (SMSC) to push users The use of flow (expense) and total flow (expense) and other information;

13, SMSC to send billing information received short message to the mobile terminal.

Figure 3 WAP streaming service billing process and issued the flow chart via SMS billing information signaling. After the WAP gateway receives an access request issued by MS, unified resource location (URL) access request is parsed to determine the identification information for the provider of streaming media services-related business will (SPID), business identification information (ServiceID) and user The IP address and billing-related information reported to the grant price DSMP authorization to conduct business. Streaming service billing support prepaid and postpaid users users. For prepaid subscribers, DSMP through real-time interaction with the completion of the SCP deductions. Specific signaling interaction process shown in Figure 3, including: 1, MS initiates streaming service access request to the WAP gateway.

2, after the WAP gateway receives an access request to determine whether the request is forwarded to the user, if the forwarding condition, then continue processing; otherwise, reject the access request.

In this step, the front of the user's service request is transposed or rejected based on the system database in a "forwarding control table" to be executed, the table stores a business of MS is not accessible IP address or a station number , for example, in the user arrears or insufficient balance situation, which will be disable certain types of service requests; "Forward Control Table" When MS requests a service, WAP gateway will find, MS If you send a service request is contained in " forwarding control table ", it is determined whether the requested service is inaccessible to this service, if yes, the service is disabled for this MS, and the information is sent to the user arrears MS; if the MS is not transmitting a service request forwarding control table, the description for this MS is legitimate, WAP gateway through the request is passed to the service provider (SP), and content-based billing or traffic accounting, business use during or after the use of accounting information sent to MS. To prevent the user has to recharge the case is still unable to use certain services,

forwarding control table user information is updated in real time.

3, WAP gateway service request will be forwarded to the appropriate service provider or content provider (SP / CP).

4, SP / CP returns an access request response message to the WAP gateway.

5, WAP gateway to request a response message to the terminal MS under.

6, WAP gateway records or query the user online information, and determine the type of user (based on MSISDN or IMSI number section number section all types of users, such as pre-paid subscribers, post-paid subscribers), if it is post-paid users to jump directly after the end of the business use Go to Step 11; if it is a pre-paid subscribers, collecting SPID, ServiceID as well as the user's IP address and other billing related information according to the requested URL.

7, WAP gateway will be collected charging related information reporting DSMP, authenticate the grant price.

8, DSMP to SCP application fee withholding.

9, SCP DSMP return costs to withhold a response message.

10, DSMP grant price return authorization response message to the WAP gateway.

11, MS issued a disconnection request to the WAP gateway.

12, WAP gateway forwards the request to put off even the SP / CP.

13, SP / CP returns to the WAP gateway disconnection request response message.

14, WAP gateway to the disconnection request response message to the terminal under MS.

15, WAP gateway CDR record generation (Call Detail Record, CDR), including business start time, end time, terminal number, type of service.

16, WAP gateway bill in the CDR billing information to the MS via WAP PUSH short message.

WAP browser with more services and streaming services billing process, for example, the present invention uses the short message sent WAP service billing information described in detail. Wherein, the short message transmission mode in the mobile terminal may be a business process using the WAP, the WAP gateway send at set time intervals; or in the mobile terminal using the WAP service process, when the prepaid balance of the mobile terminal is less than the set balance threshold, the mobile terminal using flow threshold or mobile terminal WAP traffic exceeds the use of WAP service fee exceeds the cost threshold between Step 5 WAP browsing services with step 6 or WAP streaming media business section 10 steps between step 11 and sent by the WAP gateway billing information to the short message center. In addition to the case of streaming services and browse business use, such as the WAP browser to open a streaming media, such WAP gateway billing information while the two businesses separately or combined to the MS.

For sending billing information, in addition to the short message sent, but also can be sent using WAP pages, including the following specific methods: Method One: In the mobile terminal business process using WAP, WAP gateway generates a count for the mobile terminal contains Temporary fee WAP pages of information, and the temporary WAP page hyperlink address into the mobile terminal while browsing the mobile terminal to obtain billing information by accessing the hyperlink address; and after the WAP service, delete produce Temporary WAP pages.

Method 2: In the mobile terminal business process using WAP, WAP gateway will instantly hyperlink pointing to a billing unit is inserted into the mobile terminal is currently viewed web page request, the mobile terminal to access the hyperlink, instant charging unit from WAP gateway acquires accounting information of the mobile terminal, and generates charging information WAP page containing the return by the WAP gateway to the mobile terminal.

Method three: the mobile terminal using the WAP service billing information is stored to a fixed address hyperlink WAP pages, when the mobile terminal to access the fixed hyperlink addresses, WAP gateway obtains the corresponding charging information and updates to said WAP page then returned to the mobile terminal. The user easy to use, can be a hyperlink to the fixed address previously stored in the mobile terminal, the user can obtain billing information at any time by visiting the hyperlink address.

Accounting information packet transmission method can also transmit IP packets, may be provided to the WAP gateway when the mobile terminal receives the request for charging information, the charging information contains the mobile terminal transmits the corresponding IP address according to the IP protocol format , or a WAP gateway according to the set time interval will contain data packets transmitted to the accounting information corresponding to the IP address of the mobile terminal according to IP protocol format, the mobile terminal displays the charging information. While improving the WAP browser that displays the charging information (traffic or cost information) WAP gateway sends the location of the terminal in a fixed browser interface.

Obviously, those skilled in the art may make various modifications of the present invention and modifications without departing from the spirit and scope of the invention. Thus, if such modifications and variations of the present invention and the claims of the invention belongs to the technical scope of equivalents, the present invention is also intended to include these changes and modifications included.

REFERENCED BY

Citing Patent	Filing date	Publication date	Applicant	Title
CN100450130C	21 Dec 2005	7 Jan 2009	中兴通讯股份有限公司	System and method for realizing intermediately informing user telephone fee
CN101286858B	12 Apr 2007	8 Dec 2010	中兴通讯股份有限公司	Method and system for charging of WAP gateway for mobile terminal
CN101287161B	14 May 2008	20 Apr 2011	华为软件技术有限公司	Service request forwarding method, gateway for wireless application protocol and communication system
CN101583095B	3 Jun 2009	8 May 2013	中兴通讯股份有限公司	Telephone charge prewarning method and prewarning system
CN101674561B	15 Jan 2009	4 Jul 2012	华为技术有限公司	Subscriber arrearage treatment method, device and system
WO2010028556A1 *	10 Jul 2009	18 Mar 2010	Huawei Technologies Co., Ltd.	Method for processing user debt, mobile management entity and network system

* Cited by examiner

CLASSIFICATIONS

International Classification	H04Q7/22, H04L12/14, H04M17/00

LEGAL EVENTS

Date	Code	Event	Description
6 Oct 2010	C14	Granted	
17 Jan 2007	C10	Request of examination as to substance	
22 Nov 2006	C06	Publication	

Google Home - Sitemap - USPTO Bulk Downloads - Privacy Policy - Terms of Service - About Google Patents - Send Feedback

(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 101815275 A
(43)申请公布日 2010.08.25

(21)申请号 201010143134.0

(22)申请日 2010.04.09

(71)申请人 刘泱
地址 100190 北京市海淀区知春路 63 号卫星大厦 6 层 604 单元

(72)发明人 梁秋实 袁彬

(74)专利代理机构 北京联创佳为专利事务所（普通合伙） 11362
代理人 郭防

(51)Int.Cl.
H04W 4/24(2009.01)
H04W 88/02(2009.01)

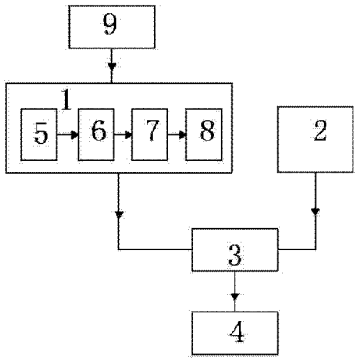
权利要求书 1 页 说明书 4 页 附图 2 页

(54)发明名称

一种手机话费计算装置

(57)摘要

本发明公开了一种手机话费计算装置，其特征在于：包括无线网络、业务支撑服务器(9)和手机；还包括设置在手机上的同步用户的话费计费规则到手机的网络同步模块(1)，记录用户通话详情的监控模块(2)，使用网络同步模块(1)上的话费计费规则对监控模块(2)记录的用户通话详情进行批价的批价模块(3)和将批价后的账单存储在手机上的存储模块(4)。本发明计算话费时的实时性和准确性高，并且可直接在手机上查询，话费详单数据量小，无需密码，更加方便快捷，同时存储的账单也便于用户对话费的核对。



CN 101815275 A

1. 一种手机话费计算装置，其特征在于：包括无线网络、业务支撑服务器(9)和手机；还包括设置在手机上的

网络同步模块(1)，用于同步用户的话费计费规则到手机上，通过无线网络与业务支撑服务器(9)相连；

监控模块(2)，用于记录用户通话详情；

批价模块(3)，用于将网络同步模块(1)上的话费计费规则对监控模块(2)记录的用户通话详情进行批价；

存储模块(4)，用于将批价后的账单存储在手机上，并与手机的显示设备相连；

监控模块(2)和网络同步模块(1)与批价模块(3)相连，批价模块(3)与存储模块(4)相连。

2. 根据权利要求1所述的手机话费计算装置，其特征在于：所述网络同步模块(1)包括获取手机的运营商、归属地和品牌信息的用户信息模块(5)，根据获取的用户信息从业务支撑服务器(9)下载运营商该品牌下所有的套餐列表的列表下载模块(6)、用于用户选择所用套餐的选择模块(7)和根据用户所选套餐从业务支撑服务器(9)获取该套餐计费规则的规则下载模块(8)。

3. 根据权利要求2所述的手机话费计算装置，其特征在于：所述用户信息模块(5)为人工输入或选择运营商、手机卡归属地、手机卡品牌和用户所在地信息的模块。

4. 根据权利要求2所述的手机话费计算装置，其特征在于：所述用户信息模块(5)为通过手机的短信中心号来判断用户的运营商和归属省份，通过手机当前的基站信息来辅助确定用户所在地的模块。

5. 根据权利要求4所述的手机话费计算装置，其特征在于：所述短信中心号与运营商、省份的对应关系从业务支撑服务器(9)下载，或预先存储在手机上。

6. 根据权利要求2所述的手机话费计算装置，其特征在于：所述规则下载模块(8)下载的套餐计费规则包括通话话费计费规则、短信计费规则、短信增值业务号码、GRPS上网费用计费规则、月租费、套餐费和手机号段。

7. 根据权利要求1所述的手机话费计算装置，其特征在于：所述监控模块(2)在手机端监控用户的通话、发送短信、通过GPRS联网的行为作为通话详情，并将此行为存为详细日志，或直接调用手机通话记录作为通话详情。

8. 根据权利要求7所述的手机话费计算装置，其特征在于：所述通话详情包括用户的通话、发送短信和通过GPRS联网行为的发话时间、结束时间、被叫方、主叫方、发话地点和流量。

9. 根据权利要求1、2或5所述的手机话费计算装置，其特征在于：所述业务支撑服务器(9)是储存套餐列表、套餐计费规则和短信中心号与运营商、省份的对应关系的服务器。

一种手机话费计算装置

技术领域

[0001] 本发明涉及一种手机话费计算装置，特别是一种手机上使用的手机话费计算装置。

背景技术

[0002] 一个典型的电信运营商所使用的计费系统中，业务网元是电信运营商提供基础服务的系统，电信的核心服务包括通话、短信、GPRS(GeneralPacketRadioService)等，每个服务对应一组业务网元。CDR(calldetailrecord)是业务详情记录，记录业务网元向用户提供的每次服务的详情。CDR40不仅仅指通话详情记录，也包括短信或GPRS的使用详情记录。每条CDR中包含发话时间、结束时间、主叫、被叫、发话地点等信息。系统向业务网元查询CDR40，然后对CDR40批价，得到账单详情，并将账单详情存入账单数据库。

[0003] 而现有的话费计算系统存在下述问题：

首先，现有的话费计算系统是在各电信运营商内部运作，且因为一些技术原因容易出现话费错算、误算的情况，手机用户很难清楚的了解自己每笔话费的产生原因，进而无法确定自己话费的准确性、正确性。

[0004] 其次，因为话单的数量巨大，一些电信运营商并不对全部用户提供话费详单查询服务。即便某些电信运营商对于部分用户开放了详单查询的业务，也存在使用不便(比如要输入服务密码、或者到移动营业厅现场办理)、实时性不强(比如只能查上月的话费详单、或几天前的话费详单)等问题。

[0005] 再次，即便用户拿到了话费详单，也会因为各运营商、各种套餐的计算规则各异，如存在优惠时段、赠送通话分钟数等特殊规则，导致用户对话费的核对非常困难。

发明内容

[0006] 本发明的目的在于，提供一种手机话费计算装置。它是一种便于用户查看和理解，具有高实时性、准确性的手机话费计算装置。

[0007] 本发明的技术方案：一种手机话费计算装置，其特征在于：包括无线网络、业务支撑服务器和手机；还包括设置在手机上的

网络同步模块，用于同步用户的话费计费规则到手机上，通过无线网络与业务支撑服务器相连；

监控模块，用于记录用户通话详情；

批价模块，用于将网络同步模块上的话费计费规则对监控模块记录的用户通话详情进行批价；

存储模块，用于将批价后的账单存储在手机上，并与手机的显示设备相连；

监控模块和网络同步模块与批价模块相连，批价模块与存储模块相连。

[0008] 上述的手机话费计算装置中，所述网络同步模块包括获取手机的运营商、归属地

和品牌信息的用户信息模块，根据获取的用户信息从业务支撑服务器下载运营商该品牌下所有的套餐列表的列表下载模块、用于用户选择所用套餐的选择模块和根据用户所选套餐从业务支撑服务器获取该套餐计费规则的规则下载模块。

[0009] 前述的手机话费计算装置中，所述用户信息模块为人工输入或选择运营商、手机卡归属地、手机卡品牌和用户所在地信息的模块。

[0010] 前述的手机话费计算装置中，所述用户信息模块为通过手机的短信中心号来判断用户的运营商和归属省份，通过手机当前的基站信息来辅助确定用户所在地的模块。

[0011] 前述的手机话费计算装置中，所述短信中心号与运营商、省份的对应关系从业务支撑服务器下载，或预先存储在手机上。

[0012] 前述的手机话费计算装置中，所述规则下载模块下载的套餐计费规则包括通话话费计费规则、短信计费规则、短信增值业务号码、GRPS 上网费用计费规则、月租费、套餐费和手机号段。

[0013] 前述的手机话费计算装置中，所述监控模块在手机端监控用户的通话、发送短信、通过 GPRS 联网的行为作为通话详情，并将此行为存为详细日志，或直接调用手机通话记录作为通话详情。

[0014] 前述的手机话费计算装置中，所述通话详情包括用户的通话、发送短信和通过 GPRS 联网行为的发话时间、结束时间、被叫方、主叫方、发话地点和流量。

[0015] 前述的手机话费计算装置中，所述业务支撑服务器是储存套餐列表、套餐计费规则和短信中心号与运营商、省份的对应关系的服务器。

[0016] 与现有技术相比，本发明由于使用了无线网络、业务支撑服务器和手机组成的基本构架，并在手机上结合了用于同步用户的话费计费规则到手机上的网络同步模块、用于记录用户通话详情的监控模块和用于将网络同步模块上的话费计费规则对监控模块记录的用户通话详情进行批价的批价模块。这种结合方式可以使计算话费时的实时性和准确性高，并且可直接在手机上查询，无需密码，更加方便快捷，同时存储的账单也便于用户对话费的核对。本发明所提供的手机话费计算装置，针对特定用户计算他自身的手机话费，话费详单数据量小，使用户可以很方便、快捷的查看、汇总自己以往的话费使用情况，并且可以在通话结束后立刻看到通话费用的变化。同时利用了电信运营商的话费计算规则，保证了话费计算的准确性，透明性。又因为计费规则存储在手机上，所以无需等待一次通话、联网结束即可实时计算当前通话、联网所产生的费用，更可以在拨出、接听一个电话之前预估本次通话每分钟的费用。现有的计费装置是在电信端计算，这套装置要对一个地市或一省的所有用户提供计费服务，其计算、存储的数据量相当庞大，因此也造成了计算的实时性较差，准确度不高，查询不便的问题。而本装置只针对特定用户计算，数据量、运算量只有电信计费装置的数百万至数千万分之一。对于正常使用的用户，每个月的数据存储只消耗数百 K，每天需要计费的电话、短信、上网等次数也只有数百次以内，完全可以做到实时准确的计算。

附图说明

[0017] 图 1 是本发明的结构示意图；

图 2 是本发明实施例的工作流程图；

图 3 是图 2 中步骤 S10 的工作流程图。

[0018] 附图中的标记：1- 网络同步模块，2- 监控模块，3- 批价模块，4- 存储模块，5- 用户信息模块，6- 列表下载模块，7- 选择模块，8- 规则下载模块，9- 业务支撑服务器。

具体实施方式

[0019] 下面结合附图和实施例对本发明作进一步的说明，但并不作为对本发明限制的依据。

实施例

[0020] 一种手机话费计算装置，结构如图 1 所示，包括无线网络、业务支撑服务器 3 和手机；还包括设置在手机上的

网络同步模块 1，用于同步用户的话费计费规则到手机上，通过无线网络与业务支撑服务器 9 相连；

监控模块 2，用于记录用户通话详情；

批价模块 3，用于将网络同步模块 1 上的话费计费规则对监控模块 2 记录的用户通话详情进行批价；

存储模块 4，用于将批价后的账单存储在手机上，并与手机的显示设备相连；

监控模块 2 和网络同步模块 1 与批价模块 3 相连，批价模块 3 与存储模块 4 相连。

[0021] 网络同步模块 1 包括获取手机的运营商、归属地和品牌信息的用户信息模块 5，根据获取的用户信息从业务支撑服务器 9 下载运营商该品牌下所有的套餐列表的列表下载模块 6、用于用户选择所用套餐的选择模块 7 和根据用户所选套餐从业务支撑服务器 9 获取该套餐计费规则的规则下载模块 8。

[0022] 用户信息模块 5 为人工输入或选择运营商、手机卡归属地、手机卡品牌和用户所在地信息的模块。

[0023] 用户信息模块 5 也为通过手机的短信中心号来判断用户的运营商和归属省份，通过手机当前的基站信息来辅助确定用户所在地的模块。

[0024] 短信中心号与运营商、省份的对应关系从业务支撑服务器 9 下载，或预先存储在手机上。

[0025] 规则下载模块 8 下载的套餐计费规则包括通话话费计费规则、短信计费规则、短信增值业务号码、GRPS 上网费用计费规则、月租费、套餐费和手机号段。

[0026] 监控模块 2 在手机端监控用户的通话、发送短信、通过 GPRS 联网的行为作为通话详情，并将此行为存为详细日志，或直接调用手机通话记录作为通话详情。

[0027] 通话详情包括用户的通话、发送短信和通过 GPRS 联网行为的发话时间、结束时间、被叫方、主叫方、发话地点和流量。

[0028] 业务支撑服务器 9 是储存套餐列表、套餐计费规则和短信中心号与运营商、省份的对应关系的服务器。

[0029] 本发明的工作流程(如图 2)：

步骤 S10，通过网络同步模块 1 同步该用户的话费计费规则到手机；

步骤 S20，在手机端通过监控模块 2 监控用户的通话、发送短信、通过 GPRS 联网的行为，

并将此行为存为详细日志；

步骤 S30，在批价模块 3 上，使用该用户的话费计费规则对详细日志进行批价；

步骤 S50，用存储模块 4 将批价后的账单存储在手机上。并通过手机显示设备（可为手机显示屏）展现给用户。

[0030] 其中步骤 S10 还包括以下步骤（如图 3）：

步骤 S101，通过用户信息模块 5，用户选择所用手机的运营商、归属地和品牌；

步骤 S102，通过列表下载模块 6，手机从支撑服务器获取该运营商该品牌下所有的套餐列表；

步骤 S103，通过选择模块 7，用户从列表中选择自己采用的套餐；

步骤 S104，通过规则下载模块 8，手机从支撑服务器获取该套餐的计费规则。

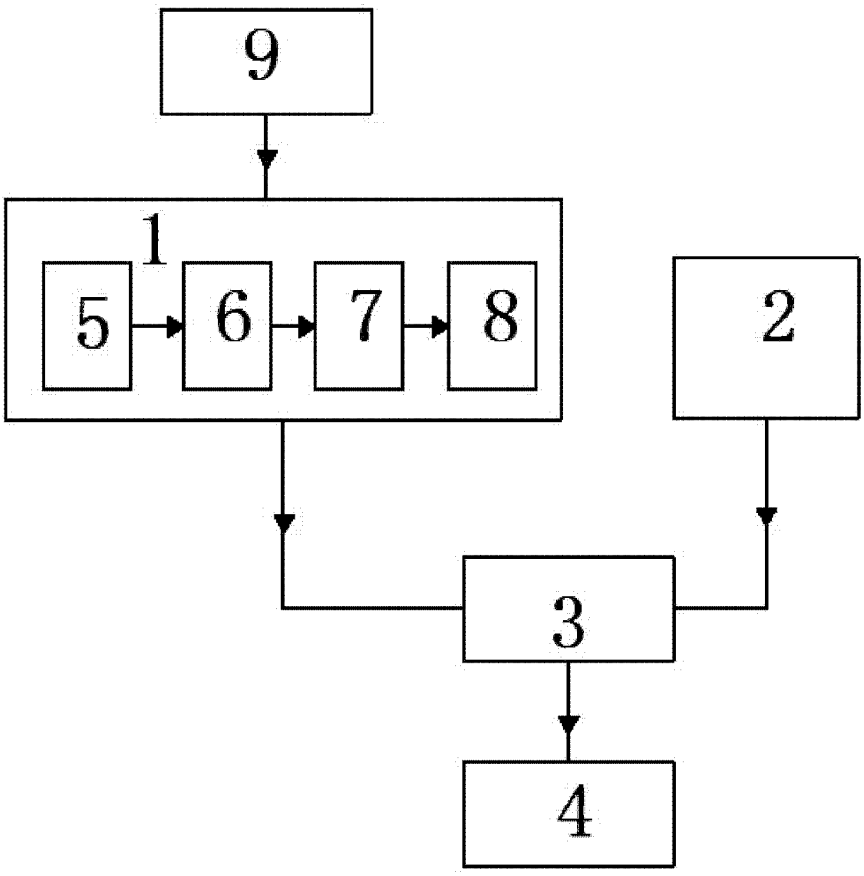


图 1

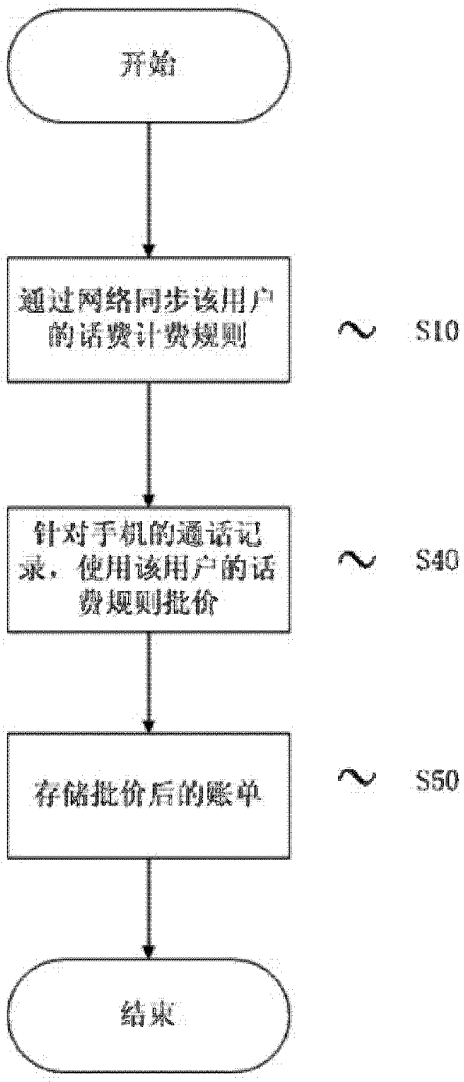

开始
通过网络同步该用户的话费计费规则
S10
针对手机的通话记录，使用该用户的话费规则批价
S40
存储批价后的账单
S50
结束

图 2

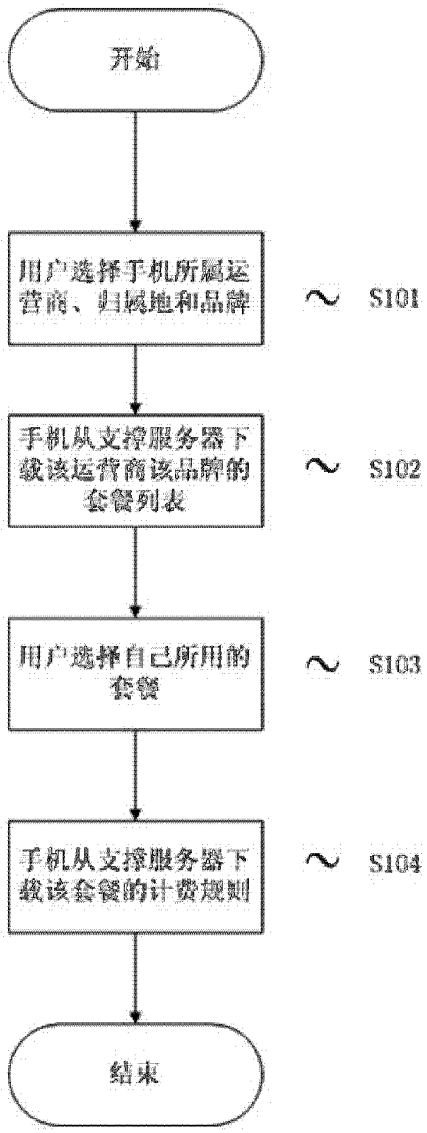

开始
用户选择手机所属运营商、归属地和品牌
S101
手机从支撑服务器下载该运营商该品牌的套餐列表
S102
用户选择自己所用的套餐
S103
手机从支撑服务器下载该套餐的计费规则
S104
结束

图 3

Sign in

Patents English Chinese Find prior art Discuss this application View PDF Download PDF

Mobile phone charge calculating device

CN 101815275 A

Publication number	CN101815275 A
Publication type	Application
Application number	CN 201010143134
Publication date	Aug 25, 2010
Filing date	Apr 9, 2010
Priority date	Apr 9, 2010
Inventors	樊秋实, 袁彬
Applicant	刘涉
Export Citation	BiBTeX, EndNote, RefMan

Referenced by (2), Classifications (2), Legal Events (5)

External Links: SIPO, Espacenet

ABSTRACT

The invention discloses a mobile phone charge calculating device, which is characterized by comprising a wireless network, a service support server (9), a mobile phone, a network synchronization module (1), a monitoring module (2), a pricing module (3) and a storage module (4), wherein the network synchronization module (1) is arranged on the mobile phone and is used for synchronizing a charge billing rule of a user to the mobile phone; the monitoring module (2) is used for recording user conversation details; the pricing module (3) is used for pricing the user conversation details recorded by the monitoring module (2) by using the charge billing rule on the network synchronization module (1); and the storage module (4) is used for storing a bill after pricing in the mobile phone. The calculating device has high real-time performance and accuracy during charge calculation, can query the charge on the mobile phone directly, has a small charge detail record data volume, needs no password and is more convenient and efficient, and simultaneously the stored bill is convenient for a user to check the charge.

DESCRIPTION translated from Chinese

One kind of phone calls computing device

Art

[0001] The present invention relates to a phone bill computing devices, especially cell phone calls on a computing device to use the phone.

BACKGROUND

[0002] A typical billing system used by telecom operators, the business NE telecommunications operators to provide basic services systems, telecommunications core services include calls, SMS, GPRS (GeneralPacketRadioService), etc., each service corresponds to a Group business NE. ③R (calldetailrecord) is the business details of the recording, the details of each service provided to the user NE business records. CDR40 not only refers to the call detail records, including SMS or GPRS usage detail records. Each CDR contains the utterance time, end time, caller, callee, caller location and other information. Systems to business NE query CDR40, then CDR40 grant price, get bill details and billing details stored in the billing database.

[0003] and the existing computing system calls the following problems:

First, the existing computing system calls in the inner workings of the telecom operators, and prone to technical reasons because some calls wrong calculation, miscalculation of the situation, the mobile phone user is difficult to clearly understand the causes of their own each bill, and thus can not be determine their own phone bill accuracy, correctness.

[0004] Second, because of the huge number of single words, some carriers do not bill for all users with details of a single query service. Even some telecom operators for some users open the details of a single query of business, there are also inconvenient to use (for example, to enter the service password, or to apply for Business Hall site), real-time is not strong (such as last month's bill can only check single detail, or details of a single bill a few days ago) and other

CLAIMS (9) translated from Chinese

1. A phone bill computing device, comprising: a wireless network, business support server (9) and mobile phones; also includes network settings on the phone synchronization module (1), is used to synchronize the user's calls to a cell phone charging rules connected through a wireless network and business support server (9); monitoring module (2) for recording call details of the user; grant price module (3) for network synchronization module calls accounting rules (1), for monitoring Module User Call Details (2) batch record price; memory module (4) for the phone, and connected storage bills after the grant price and the phone's display equipment; monitoring module (2) and network synchronization module (1) the approved price module (3) is connected, (4) is connected to the grant price module (3) and memory modules.

2. The phone calls computing device of claim 1, wherein, wherein: said network synchronization module (1) including access to mobile phone operators, attribution and brand information subscriber information module (5), according to the obtained user information from the business support server (9) Downloads operators under the brand list download module lists all the packages (6) for the user to select the choice with our subscription module (7) and based on user selected business support package from the server (9) to get the package charging rules rules download module (8).

3. 3. Phone calls computing device according to claim 2, wherein, wherein: said subscriber information module (5) for manual input or select the module carrier, phone cards attribution, phone card brand and user location information.

4. The phone calls computing device according to claim 2, wherein, wherein: said subscriber information module (5) through the phone's SMS center number to determine the user's operators and the home provinces, through the mobile phone base station information to the current assist in determining the

issues.

[0005] Once again, even if the user got the details of a single bill, also because the calculation rules for each operator, a variety of different packages, such as the existence of preferential period, giving the number of calls and other special rules minute, causing the user to check the phone bill is very difficult .

SUMMARY

The purpose of [0006] The present invention is to provide a phone bill computing device. It is a user-friendly viewing and understanding, with a high real-time accuracy of phone calls computing device.

[0007] aspect of the present invention: a phone bill computing device, comprising: a wireless network, business support servers and mobile phones; also includes setting on the phone

Network synchronization module for synchronizing user charging rules to the phone calls connected through a wireless network and business support server;

Monitoring module for recording user call details;

Grant price module for network synchronization module calls on the accounting rules for the monitoring module records the user calls the details were approved price;

Storage module for on the phone, and connected storage bills after the grant price and the phone's display device; connected monitoring module and network synchronization module and the grant price of the module, the module is connected to the grant price and the storage module.

[0008] The computing device of phone calls, the network synchronization module includes access to mobile phone operators, attribution and subscriber information module brand of information, access to information based on user downloads carriers under the brand all the support from the business server Package list List Download module for the user to select the package selection module and access rules of the charging rules package downloaded from the service module supporting server based on user-selected packages.

[0009] The aforementioned phone bill computing device, wherein the user information module for manual input or select the module carrier, phone cards attribution, phone card brand and user location information.

[0010] The foregoing phone calls computing device, the mobile phone subscriber information module for SMS center number to determine the user's operators and the home provinces, the current through the mobile phone base station information to assist in determining the location of the user module.

[0011] The foregoing phone calls computing device, the message center number correspondence between operators, provinces and downloaded from the service support server or stored on the phone.

[0012] The foregoing phone calls computing device, the rules of the download module download package billing rules include rules call toll billing, SMS billing rules, SMS value-added service numbers, costs GRPS Internet billing rules, monthly fees, Package fee and phone number section.

[0013] The aforementioned phone bill computing device, wherein the monitoring module to monitor the end user in the mobile phone calls, send text messages through GPRS network acts as the call details, and this behavior is saved as a detailed log, or directly call phone call records As the call details.

[0014] The foregoing calculation means phone calls, the call details including the user's calls, send text messages and through the GPRS network behavior utterance time, end time, the called party, the caller, the caller location and traffic.

[0015] The foregoing phone calls computing device, the storage server is a business support package lists, correspondence between server packages billing rules and message center number with operators, provinces.

[0016] Compared with the prior art, the basic framework of the present invention is the use of a wireless network, composed of business support servers and mobile phones, combined with a bill charging rules for synchronizing user on the phone to the network synchronization module on your phone record the call details of the user for the monitoring module and charging rules calls for network synchronization module for monitoring module records the user's call details were awarded the grant price price module. This combination can make calls when calculating real-time and high

location of the user module.

5. 5. phone calls computing device according to claim 4, wherein, characterized in that: the SMS center number correspondence between operators, provinces and from business support server (9) download, or stored on the phone.

6. 6. phone calls computing device according to claim 2, wherein, wherein: said rules download module (8) Download the package billing rules include rules call toll billing, SMS billing rules, SMS value-added service numbers, GRPS Charging Rules Internet access charges, monthly fees, course fees and phone number section.

7. 7. The phone calls computing device according to claim 1, characterized in that: the monitoring module (2) monitor the user's end of the phone call, send SMS, via GPRS network acts as the call details, and keep this behavior for detailed logging, or directly call phone call records as a call for more information.

8. 8. phone calls computing device according to claim 7, wherein, wherein: said call details including the user's calls, send SMS and GPRS network behavior by utterance time, ending time, the called party, the caller, the caller Location and traffic.

9. 9. phone calls, 2 or computing device according to claim 5, characterized in that: the business support server (9) is a storage package list, the corresponding charging rule packages and SMS center number and operators, provinces server relationship.

accuracy, and can query directly on the phone without a password, faster and more convenient, but also easy for users to store bills for calls reconciliation. Phone calls computing device of the present invention provides, calculated for a particular user's phone bill of his own, a small amount of data calls single detail, so that users can easily and quickly view, summarizing his past calls usage, and can end in a call After seeing changes in the cost of calls immediately. While taking advantage of the service provider's bill calculation rules to ensure that the bill calculation accuracy, transparency. And because the accounting rules are stored on the phone, so no need to wait for a call, the networking end the current call to real-time computing, networking costs arising, more can be set aside, before answering a phone call estimate this cost per minute . Existing billing system is to calculate the telecommunications side, this device is to provide billing services for all users by one city or a province, which is calculated, the amount of data storage is quite large, and therefore resulted in the more real-time computing poor accuracy is not high, the query inconvenient questions. And this is only for a specific user computing device, the amount of data, computation device only telecommunications billing millions to thousands of parts per million. For normal use, the monthly data storage consumes only several hundred K, daily need billing telephone, text messaging, Internet and other times only within hundreds of times, can be done in real-time and accurate count Da Bian.

Brief Description

[0017] Figure 1 is a schematic structural view of the present invention; FIG. 2 is a flowchart of an embodiment of the present invention; FIG. 3 is a flowchart of step SIO of Figure 2.

[0018] The drawings mark: 1- network synchronization module, 2-monitoring module, 3 grant price module, 4 storage modules, user information module 5-, 6- List Download module, 7-selection module, 8 Rules download module, 9-business support server.

Specific embodiments

[0019] accompanying drawings and the following embodiment of the present invention will be further illustrated by, but not as a basis for limiting the present invention.

Example

[0020] A computing device phone calls, the structure shown in Figure 1, including Wi-Fi, business support server 3 and mobile phones; also includes setting on the phone

Network synchronization module 1, calls for synchronizing user charging rules to the phone, connected through a wireless network and business support server 9;

Monitoring Module 2, is used to record the call details of the user;

Module 3 approved price for network synchronization module Call Details user charging rule calls for a monitoring module 2 on the batch record price;

Storage Module 4 for the bill after the grant price of storage on the phone, and the phone is connected to a display device; monitoring module 2 and network synchronization module 1 module 3 is connected with the grant price, grant price of module 3 is connected with the storage module 4.

[0021] network synchronization module 1 includes access to mobile phone operators, attribution and brand information user information module 5, download carriers under the brand list all the packages to download the module from the list of six business support server 9 based on user access to information for the user to select the package selection module download module with 7 and rules based on user-selected packages to get the package from the service support server charging rules 9 8.

[0022] The user information module 5 for manual input or select the module carrier, phone cards attribution, phone card brand and user location information.

[0023] The user information module 5 also via mobile phone SMS center number to determine the user's operators and the home provinces, the current through the mobile phone base station information to assist in determining the location of the user module.

[0024] SMS center number corresponds to the relationship operators, provinces and downloaded from the service support server 9, or stored on the phone.

[0025] Rule 8 download download module packages billing rules include rules call toll billing, SMS billing rules, SMS value-added service numbers, costs GRPS Internet billing rules, monthly fees, package costs and phone number section.

[0026] 2 at the end of the phone monitoring module to monitor the user's call, send SMS, via GPRS network acts as the call details, and keep a detailed log of this behavior, or directly call phone call records as a call for more information.

[0027] Call details include the user's calls, send text messages and through the GPRS network behavior utterance time,

end time, the called party, the caller, the caller location and traffic.

[0028] 9 is a storage server business support package lists, correspondence between server packages billing rules and message center number with operators, provinces.

[0029] The workflow of the invention (Figure 2):

Step S10, the synchronous network synchronization module 1 through the user's calls to the phone charging rules; step S20, the mobile terminal 2 through the monitoring module to monitor users' calls, send text messages through GPRS network behavior, and this behavior is saved for details logs;

Step S30, the grant price Module 3, using the user's calls for a detailed log accounting rules grant price; step S50, with a storage module 4 will grant price after the bill is stored on the phone. And through mobile display devices (for mobile phone display) presented to the user.

[0030] wherein step further comprises the step SIO (Figure 3):

Step S101, the user information module 5, the user selects the mobile phone operators, attribution and brand; step S102, 6, cell phones get packages list of all under the carrier of the brand from the supporting server list download module; step S103, 7, users choose their own package by selecting the modules used from the list; step S104, the adoption of the rules download module 8, cell phone charging rules to get the package from the support server.

REFERENCED BY

Citing Patent	Filing date	Publication date	Applicant	Title
CN102711076B *	May 24, 2012	Feb 11, 2015	武汉诚迈科技有限公司	一种实时预测手机通话余额的方法
WO2012171369A1 *	Mar 15, 2012	Dec 20, 2012	Zte Corporation	Method and system for calculating call charge of terminal

* Cited by examiner

CLASSIFICATIONS

International Classification	H04W4/24, H04W88/02

LEGAL EVENTS

Date	Code	Event	Description
Oct 30, 2013	C12	Rejection of an application for a patent	
Jun 1, 2011	C41	Transfer of the right of patent application or the patent right	
Jun 1, 2011	ASS	Succession or assignment of patent right	**Effective date:** 20110421 **Free format text:** FORMER OWNER: LIU YANG **Owner name:** BEIJING WALI NETWORK TECHNOLOGY CO., LTD.
Jun 1, 2011	COR	Bibliographic change or correction in the description	**Free format text:** CORRECT: ADDRESS; FROM: 100190 UNIT 604, 6/F, SATELLITE BUILDING, NO. 63, ZHICHUN ROAD, HAIDIAN DISTRICT, BEIJING TO: 100114 ROOM 2533, BUILDING 3, NO. 3, XIJING ROAD, BADACHU HIGH-TECH. PARK, SHIJINGSHAN DISTRICT, BEIJING
Aug 25, 2010	C06	Publication	

Google Home - Sitemap - USPTO Bulk Downloads - Privacy Policy - Terms of Service - About Google Patents - Send Feedback

Electronic Acknowledgement Receipt

EFS ID:	22208879
Application Number:	14667516
International Application Number:	
Confirmation Number:	5348
Title of Invention:	Network System With Common Secure Wireless Message Service Serving Multiple Applications on Multiple Wireless Devices
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	James E. Harris/Ann Taylor
Filer Authorized By:	James E. Harris
Attorney Docket Number:	RALEP007C11C4
Receipt Date:	29-APR-2015
Filing Date:	24-MAR-2015
Time Stamp:	17:25:49
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Assignee showing of ownership per 37 CFR 3.73	P007C11C4_Statement.pdf	118463 2c16be60cb0f45b80b12dc2989d410b42fdb0742	no	3

Warnings:	
Information:	

2	Transmittal Letter	P007C11C4_IDSTransLtr.pdf	59085 e129ac49242ed5a29dc8bb6a457a49acd03f2530	no	2
Warnings:					
Information:					
3	Information Disclosure Statement (IDS) Form (SB08)	IDS1.pdf	622621 f061852db8b8c9122830628a29cd82bdfc4eda87	no	36
Warnings:					
Information:					
4	Information Disclosure Statement (IDS) Form (SB08)	IDS2.pdf	619447 07c4fd81141fce37b65bc2e4a84fbe2b30c4ab75	no	27
Warnings:					
Information:					
5	Information Disclosure Statement (IDS) Form (SB08)	IDS3.pdf	619080 7b2cc0ce738642f6b6d3a97074a9168d41d8818f	no	31
Warnings:					
Information:					
6	Information Disclosure Statement (IDS) Form (SB08)	IDS4.pdf	613710 bba0bfe383db9b43f7ea95b43143ccbd34a7bb8d	no	8
Warnings:					
Information:					
7	Foreign Reference	2060.pdf	1082588 d731de97188a46d46fa00f136f87db05a28d9044	no	10
Warnings:					
Information:					
8	Foreign Reference	2061.pdf	2061940 86232d632925d26176ca285a7928e3c5a3f21baa	no	21
Warnings:					
Information:					
9	Foreign Reference	2062.pdf	907410 8e1e1537e7aa0c658cd339f06c2b1b63ab448ad0	no	12
Warnings:					
Information:					
10	Non Patent Literature	3039.pdf	1271520 5ff7631e8a8dfa2c00f75e44b77d86a2e9719407	no	12
Warnings:					
Information:					

Total Files Size (in bytes):	7975864

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

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

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

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

PTO/AIA/96 (08-12)
Approved for use through 01/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office;U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of1995, no persons arerequired to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

Applicant/Patent Owner: Gregory G. Raleigh

Application No./Patent No.: 14/667,516 Filed/Issue Date: March 24, 2015

Titled: Network System With Common Secure Wireless Message Service Serving Multiple Applications on Multiple Wireless Devices

Headwater Partners I LLC, a Limited Liability Company

(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

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

1. ☑ The assignee of the entire right, title, and interest.

2. ☐ An assignee of less than the entire right, title, and interest (check applicable box):

   ☐ The extent (by percentage) of its ownership interest is _____%. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.

   ☐ There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

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

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

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

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

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

A. ☑ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel 035246, Frame 0168, or for which a copy thereof is attached.

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

   1. From: _____ To: _____

      The document was recorded in the United States Patent and Trademark Office at

      Reel _____, Frame _____, or for which a copy thereof is attached.

   2. From: _____ To: _____

      The document was recorded in the United States Patent and Trademark Office at

      Reel _____, Frame _____, or for which a copy thereof is attached.

This collection of information is required by37 CFR3.73(b). The information is required toobtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentialityis governed by35 U.S.C. 122and 37 CFR1.11 and1.14. Thiscollection is estimated to take 12 minutes to complete, including gathering, preparing, and submittingthe 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 tothe Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS.**SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450**

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

PTO/AIA/96 (08-12)
Approved for use through 01/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

3. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

4. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

5. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

6. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

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

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

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

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

/James E. Harris/	April 29, 2015
Signature	Date
James E. Harris	40013
Printed or Typed Name	Title or Registration Number

[Page 2 of 2]

Privacy Act Statement

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

The informationprovided 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 informationin 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 InternationalApplication 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, arecord 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 thissystem 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.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Raleigh	Examiner:	not yet assigned
Serial No.:	14/667,516	Art Unit:	2431
Filed:	March 24, 2015	Conf. No.:	5348
Title:	Network System With Common Secure Wireless Message Service Serving Multiple Applications on Multiple Wireless Devices		

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

INFORMATION DISCLOSURE STATEMENT

The references cited on attached form PTO/SB/08A are being called to the attention of the Examiner. Copies of the references are not enclosed.

In accordance with 37 CFR §1.98(d), copies of the references can be found in related U.S. Patent Application No. 14/263,604 filed April 28, 2014, of which the instant application is a continuation. Any foreign or non-patent references not submitted in that parent application are transmitted herewith.

It is respectfully requested that the cited references be expressly considered during the prosecution of this application, and the references be made of record therein and appear among the "references cited" on any patent to issue therefrom.

As provided for by 37 CFR § 1.97(g) and (h), no inference should be made that the information and references cited are prior art merely because they are in this statement and no

representation is being made that a search has been conducted or that this statement encompasses all the possible relevant information.

Applicant believes that no fee is required for submission of this statement, but if for any reason an insufficient fee has been paid, please charge the insufficiency to Deposit Account No. **50-5876**.

Respectfully submitted,

Date: April 29, 2015

By: /James E. Harris/
James E. Harris
Reg. No. 40,013
Headwater Partners I LLC
555 Twin Dolphin Dr., Suite 310
Redwood City, CA 94065
(650) 517-2798

CERTIFICATE OF ELECTRONIC TRANSMISSION

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being filed electronically via EFS-Web addressed to the Commissioner for Patents on:

Date: April 29, 2015 By: /Ann Taylor/
Ann Taylor

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 14/667,516

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))	18 minus 20 =	*	x 40 =	0.00	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	1 minus 3 =	*	x 210 =	0.00			
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).			800			
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	1530		TOTAL	

APPLICATION AS AMENDED - PART II

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

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)	OR	RATE($)	ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							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
14/667,516	03/24/2015	2652	1530	RALEP007C11C4	18	1

CONFIRMATION NO. 5348

106963
Headwater Partners I LLC
555 Twin Dolphin Drive, Suite 310
Redwood Shores, CA 94065

FILING RECEIPT

OC000000074404379

Date Mailed: 04/06/2015

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)

Gregory G. Raleigh, Woodside, CA;

Applicant(s)

Headwater Partners I LLC, Redwood City, CA

Power of Attorney: The patent practitioners associated with Customer Number 106963

Domestic Priority data as claimed by applicant

This application is a CON of 14/263,604 04/28/2014
which is a CON of 12/380,780 03/02/2009 PAT 8839388
which claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009

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 - A proper **Authorization to Permit Access to Application by Participating Offices** (PTO/SB/39 or its equivalent) has been received by the USPTO.

If Required, Foreign Filing License Granted: 04/02/2015
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 14/667,516**

Projected Publication Date: 07/16/2015

Non-Publication Request: No

Early Publication Request: Yes
**** SMALL ENTITY ****
Title

Network System With Common Secure Wireless Message Service Serving Multiple Applications on Multiple Wireless Devices

Preliminary Class

379

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.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Raleigh		Examiner:	not yet assigned
Serial No.:	14/667,516	Art Unit:	2652
Filed:	March 24, 2015	Conf. No.:	5348
Title:	Automated Device Provisioning and Activation		

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

PRELIMINARY AMENDMENT

Prior to examination on the merits, please amend the above-identified application as follows:

Amendments to the Specification begin on page 2.

Amendments to the Claims begin on page 3.

Remarks begin on page 7.

AMENDMENTS TO THE SPECIFICATION

Please amend the **Application Title** as follows:

Network System With Common Secure Wireless Message Service Serving Multiple Applications on Multiple Wireless Devices

Please replace the **Abstract** with the following:

Each of several mobile end-user devices contains a device messaging agent that securely communicates with a network message server over a wireless network. The network message server delivers messages to the device messaging agent on behalf of a plurality of network application servers. Each network application server supplies the network message server with application data and an indication of a device and an application on the device to which the application data should be delivered. The network message server securely passes the data and an application identifier to the device messaging agent on the appropriate mobile end-user device. The device messaging agent maps the application identifier to a software process corresponding to the application, and a secure interprocess communication service delivers the application data to that software process.

AMENDMENTS TO THE CLAIMS

Please amend the claims as follows:

1. (Canceled).

2. (New) A network system comprising:

a plurality of device messaging agents, each executable on a respective one of a plurality of mobile end-user devices configured to exchange Internet data via a data connection to a wireless network; and

a network message server

supporting a plurality of secure Internet data connections, each secure Internet data connection between the network message server and a respective one of the mobile end-user devices via a device data connection to a wireless network,

the network message server configured to receive, from each of a plurality of network application servers, multiple requests to transmit application data, each such request indicating a corresponding one of the mobile end-user devices and one of a plurality of applications,

the network message server to generate corresponding Internet data messages based on the requests, each such message containing at least one application identifier for an indicated application and application data corresponding to one of the requests, and

the network message server to transmit each of the generated Internet data messages to the device messaging agent located on the device indicated in the corresponding request, using the corresponding secure Internet data connection for the device indicated in the corresponding request;

each device messaging agent, when executing,

to receive the Internet data messages from the secure Internet data connection corresponding to the device executing the device messaging agent, and

to, for each received message, map the application identifier in the message to a software process corresponding to the application

identifier, and forward the application data in the message to the software process via a secure interprocess communication service.

3. (New) The network system of claim 2, wherein the plurality of applications include a first application that receives the application data in a first format, and a second application that receives the application data in a second format different than the first format.

4. (New) The network system of claim 2, the network message server further to encrypt the secure Internet data messages, the device messaging agents further to decrypt each received message to obtain the corresponding application identifier and application data.

5. (New) The network system of claim 4, wherein the secure Internet data messages are transported to the device messaging agent on each device using one or more of encryption on a transport services stack, IP (Internet Protocol) layer encryption, and tunneling.

6. (New) The network system of claim 2, wherein the device messaging agent executes in a secure execution environment on at least one of the devices, and at least one of the applications executes outside of the secure execution environment on that device.

7. (New) The network system of claim 2, wherein:
at least a subset of the device messaging agents, when respectively executing on their respective devices, are each further to
receive, from each of multiple applications executing on the corresponding device, at least one corresponding request to transmit application data, each such request indicating a corresponding one of the network application servers,
generate corresponding upload Internet data messages based on the requests, each such message containing at least one server identifier for an indicated application server and application data corresponding to one of the requests, and

transmit each of the generated upload Internet data messages to the network message server, using the corresponding secure Internet data connection for the device; and

the network message server is further to

receive the upload Internet data messages over the respective secure Internet data connections, and

for each received upload Internet data message, map the server identifier in that message to a corresponding one of the network application servers, and transmit the application data from that message to the corresponding network application server, together with an indication of the device from which that message was received.

8. (New) The network system of claim 7, wherein at least one of the upload Internet data messages comprises a key for the network application server corresponding to the requesting application.

9. (New) The network system of claim 2, further comprising, on at least one of the devices, the secure interprocess communication service, and wherein the secure interprocess communication service and the secure Internet data connection from that device to the network message server are separately secured.

10. (New) The network system of claim 2, wherein at least one of the secure Internet data messages comprises multiple identifier/data pairs.

11. (New) The network system of claim 2, wherein the secure interprocess communication service forwards the application data to at least one of the software processes in an encrypted format.

12. (New) The network system of claim 2, the device messaging agent on at least one of the devices further to initiate the secure connection to the network message server.

13. (New) The network system of claim 2, at least one of the devices having a network stack in communication with the device messaging agent, wherein the secure

connection between the network message server and that device is terminated within the network stack.

14. (New) The network system of claim 2, wherein at least one of the applications on at least one of the devices and the network application server corresponding to that application authenticate with each other prior to passing application data via the device messaging agent on that device and the network message server.

15. (New) The network system of claim 2, further comprising a secure server to store a secure authorization list, the secure authorization list indicating the applications and network application servers that are allowed to communicate using the network message server.

16. (New) The network system of claim 2, the network message server further to collect and buffer multiple requests to transmit application data to a particular one of the devices.

17. (New) The network system of claim 16, wherein the network message server transmits the collected and buffered requests to the particular device upon the occurrence of a transmission trigger.

18. (New) The network system of claim 17, wherein the transmission trigger is the receipt of a transmission from the device messaging agent of the particular device.

19. (New) The network system of claim 17, wherein the transmission trigger is the expiration of a periodic timer.

REMARKS

Applicant respectfully requests entry of the amendments provided herein. This preliminary amendment is presented before any office action. Claim 1 has been cancelled, and new claims 2-19 have been added. No new matter has been added. If the Examiner has any questions or needs any additional information, the Examiner is invited to contact the undersigned.

The Commissioner is authorized to charge any fee deficiency or credit any overpayment to Deposit Account 50-5876.

Respectfully submitted,

Date: March 25, 2015

By: /James E. Harris/

James E. Harris
Reg. No. 40,013
Patent Counsel
Headwater Partners I LLC
555 Twin Dolphin Dr., Suite 310
Redwood Shores, CA 94065
(650) 517-2798

CERTIFICATE OF ELECTRONIC TRANSMISSION

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being filed electronically via EFS-Web addressed to the Commissioner for Patents on:

Date: March 25, 2015 By: /Ann Taylor/
Ann Taylor

PTO/AIA/80 (07-12)
Approved for use through 11/30/2014. OMB 0651-0035
U.S. Patent and Trademark Office; U.S DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO

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

I hereby appoint:

☒ Practitioners associated with Customer Number: 106963

OR

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

Name	Registration Number	Name	Registration Number

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

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

☒ The address associated with Customer Number: 106963

OR

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

Assignee Name and Address: Headwater Partners I LLC
555 Twin Dolphin Drive, Suite 310
Redwood City, CA 94065 U.S.A.

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

SIGNATURE of Assignee of Record

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

Signature		Date	25 June 2014
Name	David R. Johnson	Telephone	650-517-2782
Title	Chief Financial Officer		

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

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.

Electronic Acknowledgement Receipt

EFS ID:	21875748
Application Number:	14667516
International Application Number:	
Confirmation Number:	5348
Title of Invention:	Automated Device Provisioning and Activation
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	James E. Harris/Ann Taylor
Filer Authorized By:	James E. Harris
Attorney Docket Number:	RALEP007C11C4
Receipt Date:	25-MAR-2015
Filing Date:	
Time Stamp:	15:34:14
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		P007C11C4_PreliminaryAmendment.pdf	82438 057a5f7cadec1b589182c2f825b14115ceedbc53	yes	7

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Preliminary Amendment	1	1
	Specification	2	2
	Claims	3	6
	Amendment/Req. Reconsideration-After Non-Final Reject	7	7

Warnings:					
Information:					
2	Power of Attorney	POA.pdf	645382 515a132f61663477437881ed77cd308133200ab1	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	727820		

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

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

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

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

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	RALEP007C11C4
	Application Number	
Title of Invention	Automated Device Provisioning and Activation	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor 1 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Gregory	G.	Raleigh	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Woodside	State/Province	CA	Country of Residence i	US

Mailing Address of Inventor:

Address 1	555 Twin Dolphin Dr., Suite 310		
Address 2			
City	Redwood City	State/Province	CA
Postal Code	94065	Country i	US

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

☐ **An Address is being provided for the correspondence Information of this application.**

Customer Number	106963		
Email Address	patent@headwaterllc.com	Add Email	Remove Email

Application Information:

Title of the Invention	Automated Device Provisioning and Activation		
Attorney Docket Number	RALEP007C11C4	Small Entity Status Claimed	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	106	Suggested Figure for Publication (if any)	

Filing By Reference :

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	RALEP007C11C4
	Application Number	
Title of Invention	Automated Device Provisioning and Activation	

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

Publication Information:

☒ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	106963		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.
When referring to the current application, please leave the application number blank.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
notyetassigned	Continuation of	14263604	2014-04-28
Prior Application Status	Patented		Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
14/263604	Continuation of	12380780	2009-03-02	8839388	2014-09-16
Prior Application Status	Expired				Remove

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	RALEP007C11C4
	Application Number	
Title of Invention	Automated Device Provisioning and Activation	

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
12/380780	Claims benefit of provisional	61206354	2009-01-28
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
12/380780	Claims benefit of provisional	61206944	2009-02-04
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
12/380780	Claims benefit of provisional	61207393	2009-02-10
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
12/380780	Claims benefit of provisional	61207739	2009-02-13
Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button.			Add

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(d). When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX) [i] the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(h)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

			Remove
Application Number	Country [i]	Filing Date (YYYY-MM-DD)	Access Code [i] (if applicable)
Additional Foreign Priority Data may be generated within this form by selecting the **Add** button.			Add

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	RALEP007C11C4
	Application Number	
Title of Invention	Automated Device Provisioning and Activation	

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Authorization to Permit Access:

☒ Authorization to Permit Access to the Instant Application by the Participating Offices

If checked, the undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the instant patent application is filed access to the instant patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the instant patent application is filed to have access to the instant patent application.

In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the instant patent application with respect to: 1) the instant patent application-as-filed; 2) any foreign application to which the instant patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the instant patent application; and 3) any U.S. application-as-filed from which benefit is sought in the instant patent application.

In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date of filing this Authorization.

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	RALEP007C11C4
	Application Number	
Title of Invention	Automated Device Provisioning and Activation	

Applicant 1 Remove

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

◉ Assignee	○ Legal Representative under 35 U.S.C. 117	○ Joint Inventor
○ Person to whom the inventor is obligated to assign.	○ Person who shows sufficient proprietary interest	

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor :

If the Applicant is an Organization check here. ☒

Organization Name	Headwater Partners I LLC		
Mailing Address Information:			
Address 1	555 Twin Dolphin Dr., Suite 310		
Address 2			
City	Redwood City	**State/Province**	CA
Country [i]	US	Postal Code	94065
Phone Number	650-517-2798	Fax Number	
Email Address	patent@headwaterllc.com		

Additional Applicant Data may be generated within this form by selecting the Add button. Add

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not subsitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Assignee 1

Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication . An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.

Remove

If the Assignee or Non-Applicant Assignee is an Organization check here. ☐

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	RALEP007C11C4
	Application Number	
Title of Invention	Automated Device Provisioning and Activation	

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1			
Address 2			
City		**State/Province**	
Country i		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button. Add

Signature:

Remove

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

Signature	/James E. Harris/			Date (YYYY-MM-DD)	2015-03-24
First Name	James E.	Last Name	Harris	Registration Number	40013

Additional Signature may be generated within this form by selecting the Add button. Add

This collection of information is required by 37 CFR 1.76. 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 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet 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 records.

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

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

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

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

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

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

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

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

AUTOMATED DEVICE PROVISIONING AND ACTIVATION

CROSS REFERENCE TO OTHER APPLICATIONS

[0001] This application is a continuation of Application No. 14/263,604 entitled DEVICE AGENT FOR REMOTE USER CONFIGURATION OF WIRELESS NETWORK ACCESS, filed April 28, 2014, which is a continuation of Application No. 12/380,780 entitled AUTOMATED DEVICE PROVISIONING AND ACTIVATION, filed March 2, 2009, which is hereby incorporated by reference for all purposes. Application No. 12/380,780 entitled AUTOMATED DEVICE PROVISIONING AND ACTIVATION, filed March 2, 2009, claims the benefit of provisional Application No. 61/206,354 entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD, filed January 28, 2009; provisional Application No. 61/206,944 entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD, filed February 4, 2009; provisional Application No. 61/207,393 entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD filed February 10, 2009; and provisional Application No. 61/207,739 entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD filed February 13, 2009, all of which are hereby incorporated by reference for all purposes.

BACKGROUND OF THE INVENTION

[0002] With the advent of mass market digital communications and content distribution, many access networks such as wireless networks, cable networks and DSL (Digital Subscriber Line) networks are pressed for user capacity, with, for example, EVDO (Evolution-Data Optimized), HSPA (High Speed Packet Access), LTE (Long Term Evolution), WiMax (Worldwide Interoperability for Microwave Access), and Wi-Fi (Wireless Fidelity) wireless networks increasingly becoming user capacity constrained. Although wireless network capacity will increase with new higher capacity wireless radio access technologies, such as MIMO (Multiple-Input Multiple-Output), and with more frequency spectrum being deployed in the future, these capacity gains are likely to be less than what is required to meet growing digital networking demand.

[0003] Similarly, although wire line access networks, such as cable and DSL, can have higher average capacity per user, wire line user service consumption habits are trending toward very high bandwidth applications that can quickly consume the available capacity and degrade overall network service experience. Because some components of service provider costs go up with increasing bandwidth, this trend will also negatively impact service provider profits.

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] Various embodiments of the invention are disclosed in the following detailed description and the accompanying drawings.

[0005] FIG. 1 illustrates a simplified (e.g., "flattened") network architecture in accordance with some embodiments.

[0006] FIG. 2 illustrates another simplified (e.g., "flattened") network architecture including an MVNO (Mobile Virtual Network Operator) relationship in accordance with some embodiments.

[0007] FIG. 3 illustrates another simplified (e.g., "flattened") network architecture including two central providers in accordance with some embodiments.

[0008] FIG. 4 illustrates a network architecture including a Universal Mobile Telecommunications System (UMTS) overlay configuration in accordance with some embodiments.

[0009] FIG. 5 illustrates a network architecture including an Evolution Data Optimized (EVDO) overlay configuration in accordance with some embodiments.

[0010] FIG. 6 illustrates a network architecture including a 4G LTE and Wi-Fi overlay configuration in accordance with some embodiments.

[0011] FIG. 7 illustrates a network architecture including a WiMax and Wi-Fi overlay configuration in accordance with some embodiments.

[0012] FIG. 8 illustrates another simplified (e.g., "flattened") network architecture including multiple wireless access networks (e.g., 3G and 4G Wireless Wide Area Networks (WWANs)) and multiple wire line networks (e.g., Data Over Cable Service Interface Specification (DOCSIS) and Digital Subscriber Line Access Multiplexer (DSLAM) wire line networks) in accordance with some embodiments.

[0013] FIG. 9 illustrates a hardware diagram of a device that includes a service processor in accordance with some embodiments.

[0014] FIG. 10 illustrates another hardware diagram of a device that includes a service processor in accordance with some embodiments.

[0015] FIG. 11 illustrates another hardware diagram of a device that includes a service processor in accordance with some embodiments.

[0016] FIG. 12 illustrates another hardware diagram of a device that includes a service processor in accordance with some embodiments.

[0017] FIG. 13 illustrates another hardware diagram of a device that includes a service processor implemented in external memory of a System On Chip (SOC) in accordance with some embodiments.

[0018] FIG. 14 illustrates another hardware diagram of a device that includes a service processor implemented in external memory of a System On Chip (SOC) in accordance with some embodiments.

[0019] FIGS. 15A through 15F illustrate hardware diagrams of a device that include a service processor and a bus structure extension using intermediate modem or networking device combinations in accordance with various embodiments.

[0020] FIG. 16 is a functional diagram illustrating a device based service processor and a service controller in accordance with some embodiments.

[0021] FIG. 17 is another functional diagram illustrating the device based service processor and the service controller in accordance with some embodiments.

[0022] FIG. 18 is another functional diagram illustrating the device based service processor and the service controller in which the service processor controls the policy implementation for multiple access network modems and technologies in accordance with some embodiments.

[0023] FIG. 19 is another functional diagram illustrating the service processor and the service controller in accordance with some embodiments.

[0024] FIG. 20 is another functional diagram illustrating the service processor and the service controller in accordance with some embodiments.

[0025] FIG. 21 is another functional diagram illustrating the service processor and the service controller in accordance with some embodiments.

[0026] FIGS. 22A and 22B provide tables summarizing various service processor agents (and/or components/functions implemented in software and/or hardware) in accordance with some embodiments.

[0027] FIG. 23 provides a table summarizing various service controller server elements (and/or components/functions implemented in software and/or hardware) in accordance with some embodiments.

[0028] FIG. 24 is a functional diagram illustrating the service control device link of the service processor and the service control service link of the service controller in accordance with some embodiments.

[0029] FIG. 25 is a functional diagram illustrating framing structure of a service processor communication frame and a service controller communication frame in accordance with some embodiments.

[0030] FIGS. 26A through 26H provide tables summarizing various service processor heartbeat functions and parameters in accordance with some embodiments.

[0031] FIGS. 27A through 27P provide tables summarizing various device based service policy implementation verification techniques in accordance with some embodiments.

[0032] FIGS. 28A through 28E provide tables summarizing various techniques for protecting the device based service policy from compromise in accordance with some embodiments.

[0033] FIG. 29 is a functional diagram illustrating a device communications stack that allows for implementing verifiable traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments.

[0034] FIG. 30 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments.

[0035] FIG. 31 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments.

[0036] FIG. 32 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments.

[0037] FIG. 33 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments.

[0038] FIG. 34 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments.

[0039] FIG. 35 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments.

[0040] FIG. 36 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments.

[0041] FIG. 37 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments.

[0042] FIG. 38 is a functional diagram illustrating a device service processor packet processing flow in accordance with some embodiments.

[0043] FIG. 39 is another functional diagram illustrating the device service processor packet processing flow in accordance with some embodiments.

[0044] FIG. 40 is another functional diagram illustrating the device service processor packet processing flow in accordance with some embodiments.

[0045] FIG. 41 provides a table summarizing various privacy levels for service history reporting in accordance with some embodiments.

[0046] FIGS. 42A through 42J provide tables summarizing various service policy control commands in accordance with some embodiments.

[0047] FIGS. 43A through 43B are flow diagrams illustrating a flow diagram for a service processor authorization sequence as shown in FIG. 43A and a flow diagram for a service controller authorization sequence as shown in FIG. 43B in accordance with some embodiments.

[0048] FIGS. 44A through 44B are flow diagrams illustrating a flow diagram for a service processor activation sequence as shown in FIG. 44A and a flow diagram for a service controller activation sequence as shown in FIG. 44B in accordance with some embodiments.

[0049] FIGS. 45A through 45B are flow diagrams illustrating a flow diagram for a service processor access control sequence as shown in FIG. 45A and a flow diagram for a service controller access control sequence as shown in FIG. 45B in accordance with some embodiments.

[0050] FIG. 46 is a functional diagram illustrating open, decentralized, device based mobile commerce transactions in accordance with some embodiments.

[0051] FIGS. 47A through 47B are transactional diagrams illustrating open, decentralized, device based mobile commerce transactions in accordance with some embodiments.

[0052] FIG. 48 illustrates a network architecture including a service controller device control system and a service controller analysis and management system in accordance with some embodiments.

[0053] FIG. 49 illustrates a network architecture for an open developer platform for virtual service provider (VSP) partitioning in accordance with some embodiments.

[0054] FIG. 50 illustrates a network architecture including a billing to service controller interface for accommodating minimum changes in existing central billing, AAA and/or other network components in accordance with some embodiments.

[0055] FIG. 51 illustrates a network architecture for locating service controller device control functions with AAA and network service usage functions in accordance with some embodiments.

[0056] FIG. 52 illustrates a network architecture for locating service controller device control functions in the access transport network in accordance with some embodiments.

[0057] FIG. 53 illustrates a network architecture for locating service controller device control functions in the radio access network in accordance with some embodiments.

[0058] FIG. 54 illustrates a network architecture for locating service controller device control functions with AAA and network service usage including deep packet inspection functions in accordance with some embodiments.

[0059] FIG. 55 illustrates another network architecture for locating service controller device control functions with AAA and network service usage including deep packet inspection functions in accordance with some embodiments.

[0060] FIG. 56 illustrates a 4G/3G/2G DPI/DPC enabled gateway in accordance with some embodiments.

[0061] FIG. 57 illustrates a network architecture including the VSP workstation server in communication with the 4G/3G/2G DPI/DPC gateways in accordance with some embodiments.

[0062] FIG. 58 illustrates another 4G/3G/2G DPI/DPC enabled gateway in accordance with some embodiments.

[0063] FIG. 59 illustrates another network architecture including the VSP workstation server in communication with the 4G/3G/2G DPI/DPC gateways in accordance with some embodiments.

[0064] FIG. 60 illustrates a 4G/3G/2G DPI/DPC enabled gateway and service controller device control system in accordance with some embodiments.

[0065] FIG. 61 illustrates another network architecture including the VSP workstation server in communication with the 4G/3G/2G DPI/DPC gateways in accordance with some embodiments.

[0066] FIG. 62 illustrates another 4G/3G/2G DPI/DPC enabled gateway and service controller device control system in accordance with some embodiments.

[0067] FIG. 63 illustrates another network architecture including the VSP workstation server in communication with the 4G/3G/2G DPI/DPC gateways in accordance with some embodiments.

[0068] FIG. 64 illustrates another network architecture including a system located in the manufacturing or distribution chain for the device that provides the device provisioning or partial provisioning, and any pre-activation required for the device to later activate on the network in accordance with some embodiments.

DETAILED DESCRIPTION

[0069] The invention can be implemented in numerous ways, including as a process; an apparatus; a system; a composition of matter; a computer program product embodied on a computer readable storage medium; and/or a processor, such as a processor configured to execute instructions stored on and/or provided by a memory coupled to the processor. In this specification, these implementations, or any other form that the invention may take, may be referred to as techniques. In general, the order of the steps of disclosed processes may be altered within the scope of the invention. Unless stated otherwise, a component such as a processor or a memory described as being configured to perform a task may be implemented as a general component that is temporarily configured to perform the task at a given time or a specific component that is manufactured to perform the task. As used herein, the term "processor" refers to one or more devices, circuits, and/or processing cores configured to process data, such as computer program instructions.

[0070] A detailed description of one or more embodiments of the invention is provided below along with accompanying figures that illustrate the principles of the invention. The invention is described in connection with such embodiments, but the invention is not limited to any embodiment. The scope of the invention is limited only by the claims and the invention encompasses numerous alternatives, modifications and equivalents. Numerous specific details are set forth in the following description in order to provide a thorough understanding of the invention. These details are provided for the purpose of example and the invention may be practiced according to the claims without some or all of these specific details. For the purpose of clarity, technical material that is known in the technical fields related to the invention has not been described in detail so that the invention is not unnecessarily obscured.

[0071] With the development and increasing proliferation of mass market digital communications and content distribution, communication network capacity gains are being outpaced by growing digital networking demand. For example, some industry experts project average wireless device usage of four devices per subscriber, with a mixture of general purpose devices like smart phones and computers along with special purpose devices like music players, electronic readers, connected (e.g., networked) cameras and connected gaming devices. In

addition, wire line user service consumption habits are trending toward very high bandwidth applications that can quickly consume the available capacity and degrade overall network service experience if not efficiently managed. Because some components of service provider costs go up with increasing bandwidth, this trend will also negatively impact service provider profits.

[0072] There is a need for a communication system and method that provides for flexible service plans and management of user network services to provide consumer choice of more refined service plan offerings and efficient management of network capacity.

[0073] Also, it is becoming increasingly important to more deeply manage the level of services delivered to networked devices to provide cost effective services that match growing digital networking usage patterns. For example, access providers can move away from only billing for basic access and move toward billing for higher level service delivery with example services including rich Internet access and email, application based billing, content distribution, entertainment activities, information or content subscription or gaming. In addition, a growing number of new special purpose and general purpose networked devices are fueling demand for new service plans, for example, tailored to the new device usage models (e.g., a special service plan for an e-book reader device).

[0074] As network capabilities grow and new networked device offerings grow, access network service providers will realize increasing value in opening up their networks to allow innovation and expanded offerings for network service consumers. However, opening up the networks to provide efficient third party definition of alternative service and billing models requires more flexible service and billing policy management solutions. For example, machine to machine applications such as telemetry, surveillance, shipment tracking and two way power control systems are example new applications that would require new offerings to make such available to network service customers. The need to customize service offerings for these new applications requires more efficient methods for defining, testing and launching new services with more refined control of service functions and service costs. In some embodiments, this means billing for different types of service elements, such as total traffic, content downloads, application usage, information or content subscription services, people or asset tracking services, real time machine to machine information or electronic commerce transactions.

[0075] In some embodiments, network user capacity is increased and user service costs are reduced by managing and billing for service consumption in a more refined manner (e.g., to satisfy network neutrality requirements). By managing service consumption in a user friendly manner, the overall service capacity required to satisfy the user device needs can be tailored more closely to the needs of a given user thereby reducing user service costs and increasing service provider profits. For example, managing service usage while maintaining user satisfaction includes service usage policy implementation and policy management to identify, manage and bill for service usage categories, such as total traffic consumption, content downloads, application usage, information or content subscription services, electronic commerce transactions, people or asset tracking services or machine to machine networking services. As described herein, service activity is used to refer to any service usage or traffic usage that can be associated with, for example, an application; a network communication end point, such as an address, uniform resource locator (URL) or other identifier with which the device is communicating; a traffic content type; a transaction where content or other material, information or goods are transacted, purchased, reserved, ordered or exchanged; a download, upload or file transfer; email, text, SMS, IMS or other messaging activity or usage; VOIP services; video services; a device usage event that generates a billing event; service usage associated with a bill by account activity (also referred to as billing by account) as described herein; device location; device service usage patterns, device user interface (UI) discovery patterns, content usage patterns or other characterizations of device usage; or other categories of user or device activity that can be identified, monitored, recorded, reported, controlled or processed in accordance with a set of verifiable service control policies. As will be apparent to one of ordinary skill in the art in view of the embodiments described herein, some embodiments identify various service activities for the purpose of decomposing overall service usage into finer sub-categories of activities that can be verifiably monitored, categorized, cataloged, reported, controlled, monetized and used for end user notification in a manner that results in superior optimization of the service capabilities for various levels of service cost or for various types of devices or groups. In some embodiments, it will be apparent to one of ordinary skill in the art that the terms service activity or service usage are associated with categorizing and possibly monitoring or controlling data traffic, application usage, communication with certain network end points, or transactions, and it will also be apparent that in some embodiments the term service activity is

intended to include one or more of the broader aspects listed above. The shortened term service usage can be used interchangeably with service activity, but neither term is intended in general to exclude any aspect of the other. In some cases, where the terms service usage or service activity are used, more specific descriptors such as traffic usage, application usage, website usage, and other service usage examples are also used to provide more specific examples or focus in on a particular element of the more encompassing terms.

[0076] In some embodiments, employing this level of service categorization and control is accomplished in a manner that satisfies user preferences. In some embodiments, employing this level of service categorization and control is accomplished in a manner that also satisfies government rules or regulations regarding open access, for example, network neutrality requirements. In some embodiments, service management solutions that also collect and/or report user or device service usage or service activity behavior to determine how best to meet the user's simultaneous desires for service quality and lower service costs are disclosed. For example, such monitoring and reporting are accomplished in a manner that includes approval by the user and in a manner that also protects the privacy of user information and service usage behavior or service activity history.

[0077] In some embodiments, a system and method is disclosed for increasing network user capacity for wireless networks in the face of increasing service demand per user by providing for a greater number of base stations, also sometimes referred to as access points, base terminals, terminal nodes or other well known acronyms, to be more easily and/or more cost effectively deployed. For example, to simplify the process of deploying base stations, the installation complexity and the network infrastructure required for the base station to obtain backhaul service to the various networks that users desire to connect with are reduced.

[0078] In some embodiments, dense base station deployments are simplified by reducing the requirement to aggregate or concentrate the base station traffic through a specific dedicated core network infrastructure, so that the base stations connect to the desired user networks through a more diverse set of local loop, back bone and core routing options. This approach also reduces network infrastructure equipment, installation and maintenance costs. In some embodiments, this is accomplished by distributing the network traffic policy implementation and

control away from the core network by providing for more control for service policy implementation and management on the end user device and, in some embodiments, in the end user device with respect to certain service policies and the network (e.g., control plane servers) with respect to other service policies. For example, this approach facilitates connecting the base stations directly to the local loop Internet with a minimum of specific dedicated networking infrastructure.

[0079] In some embodiments, service and transaction billing event capture and logging are distributed to the device. For example, providing service and transaction billing event capture and logging at the device provides a greater capability to monitor, classify and control deeper aspects of service usage or service activity at the device as compared to the relatively less capability for the same in the network infrastructure (e.g., for certain traffic flows, such as encrypted traffic flows). Furthermore, billing at the device provides for very specialized with many different billing and service plans for different device and service usage or service activity scenario combinations without the problem of attempting to propagate and manage many different deep packet inspection (DPI) and traffic shaping profiles in the networking equipment infrastructure. For example, service billing at the device can provide for more sophisticated, more specialized and more scalable billing and service plans.

[0080] Another form of billing that needs improvement is electronic commerce transaction billing with device assisted central billing. Today, most central billing and content distribution models require either centralized content distribution maintained by the central service provider or central billing authority, or a centralized ecommerce website or portal traffic aggregation system controlled by the central service provider or central billing provider, or both. In such systems, content and transaction providers such as media providers, application developers, entertainment providers, transaction website providers and others must adapt their mainstream electronic offering and commerce systems, such as shopping experience websites, to fit within the various proprietary customized infrastructure and content storage solutions for ecommerce markets, such as BREW® (Binary Runtime Environment for Wireless from Qualcomm® Inc.), Symbian OS (from Symbian Software Ltd) and Apple iPhone 3G App Store (from Apple Inc.). This approach requires a large amount of unnecessary custom interface development and stifles open market creativity for HTTP, WAP or portal/widget based shopping

destinations and experiences. As disclosed below, a superior approach includes device based transaction billing for an open ecosystem in which a central billing provider provides users and ecommerce transaction providers with a central billing solution and experience that does not require extensive custom development or ecommerce infrastructure interfacing.

[0081] In some embodiments, products that incorporate device assisted service policy implementation, network services and service profiles (e.g., a service profile includes a set of one or more service policy settings for the device for a service on the network) are disclosed, as described below. For example, aspects of the service policy (e.g., a set of policies/policy settings for the device for network services, typically referring to lower level settings, such as access control settings, traffic control settings, billing system settings, user notification settings, user privacy settings, user preference settings, authentication settings and admission control settings) that are moved out of the core network and into the end user device include, for example, certain lower level service policy implementations, service usage or service activity monitoring and reporting including, for example, privacy filtering, customer resource management monitoring and reporting including, for example, privacy filtering, adaptive service policy control, service network access control services, service network authentication services, service network admission control services, service billing, transaction billing, simplified service activation and sign up, user service usage or service activity notification and service preference feedback and other service capabilities.

[0082] As discussed below, product designs that move certain aspects of one or more of these service profile or service policy implementation elements into the device provide several advantageous solutions to the needs described above. For example, benefits of certain embodiments include the ability to manage or bill for a richer and more varied set of network services, better manage overall network capacity, better manage end user access costs, simplify user or new device service activation, simplify development and deployment of new devices with new service plans (e.g., service profile and billing/costs information associated with that service profile), equip central service providers with more effective open access networks for new third party solutions, simplify the equipment and processes necessary to deploy wireless base stations and simplify the core networking equipment required to deploy certain access networks.

[0083] As discussed below, there are two network types that are discussed: a central provider network and a service provider network. The central provider network generally refers to the access network required to connect the device to other networks. The central provider network generally includes the physical layer, the Media Access Control (MAC) and the various networking functions that can be implemented to perform authentication, authorization and access control, and to route traffic to a network that connects to the control plane servers, as discussed below. The service provider network generally refers to the network that includes the control plane servers. In some embodiments, a central provider network and a service provider network are the same, and in some embodiments, they are different. In some embodiments, the owner or manager of the central provider network and the owner or manager of the service provider network are the same, and in some embodiments, they are different.

[0084] In some embodiments, control of the device service policies is accomplished with a set of service control plane servers that reside in the access network or any network that can be reached by the device. This server based control plane architecture provides for a highly efficient means of enabling third party control of services and billing, such as for central carrier open development programs or Mobile Virtual Network Operator (MVNO) relationships. As device processing and memory capacity expands, moving to this distributed service policy processing architecture also becomes more efficient and economical. In some embodiments, several aspects of user privacy and desired network neutrality are provided by enabling user control of certain aspects of device based service usage or service activity reporting, traffic reporting, service policy control and customer resource management (CRM) reporting.

[0085] In many access networks, such as wireless access networks, bandwidth capacity is a valuable resource in the face of the increasing popularity of devices, applications and content types that consume more bandwidth. To maintain reasonable service profit margins, a typical present service provider practice is to charge enough per user for access to make service plans profitable for the higher bandwidth users. However, this is not an optimal situation for users who desire to pay less for lower bandwidth service usage or service activity scenarios.

[0086] Accordingly, in some embodiments, a range of service plan pricing can be enabled that also maintains service profitability for the service provider, for example, by

providing a more refined set of management and control capabilities for service profiles. For example, this approach generally leads to service management or traffic shaping where certain aspects of a service are controlled down based on service policies to lower levels of quality of service. Generally, there are three problems that arise when these techniques are implemented. The first problem is maintaining user privacy preferences in the reporting of service usage or service activity required to set, manage or verify service policy implementation. This problem is solved in a variety of ways by the embodiments described below with a combination of user notification, preference feedback and approval for the level of traffic information the user is comfortable or approves and the ability to filter service usage or service activity, in some embodiments, specifically traffic usage or CRM reports so that only the level of information the user prefers to share is communicated. The second problem is satisfying network neutrality requirements in the way that traffic is shaped or services are managed. This problem is solved in a variety of ways as described in the embodiments described below by empowering the user to make the choices on how service usage, service activity, traffic usage or CRM data is managed down to control costs, including embodiments on user notification and service policy preference feedback. By allowing the user to decide how they want to spend and manage their service allowance or resources, a more neutral or completely neutral approach to network usage can be maintained by the service provider. The third problem is to help the user have an acceptable and enjoyable service experience for the lower cost plans that will result in much wider scale adoption of connected devices and applications but are more constrained on service activity usage or options or bandwidth or traffic usage. As lower cost service plans are offered, including plans where the basic connection service may be free, these service plans will require service provider cost controls to maintain profitability or preserve network capacity that result in lower limits on service usage or service activity. These lower service usage or service activity limit plans will result in more users who are likely run over service usage limits and either experience service shutdown or service cost overages unless they are provided with more capable means for assistance on how to use and control usage for the lower cost services. This problem is solved in a variety of ways with a rich collection of embodiments on user notification, service usage and cost projection, user notification policy feedback, user service policy preference feedback, and adaptive traffic shaping or service policy implementation. As described herein, some embodiments allow a wide range of flexible and verifiable service plan and service profile

implementations ranging from examples such as free ambient services that are perhaps sponsored by transaction revenues and/or bill by account sponsored service partner revenues, to intermediately priced plans for basic access services for mass market user devices or machine to machine communication devices, to more expensive plans with very high levels of service usage or service activity limits or no limits at all. Several bill by account embodiments also provide for the cataloging of service usage that is not a direct benefit to end users but is needed for basic maintenance of the device control channels and access network connection, so that the maintenance traffic service cost can be removed from the user billing or billed to non-user accounts used to track or account for such service costs. These embodiments and others result in a service usage or service activity control capability that provides more attractive device and service alternatives to end users while maintaining profitability for service providers and their partners.

[0087] In some embodiments, the above described various embodiments for device based service policy and/or service profile communications control are implemented using network based service control, for example, for satisfying various network neutrality and/or privacy requirements, based on indication(s) received from the device (e.g., user input provided using the device UI using the service processor) and network based service control (e.g., using a DPI service monitor or DPC policy implementation and/or other network elements).

[0088] In some embodiments, a virtual network overlay includes a device service processor, a network service controller and a control plane communication link to manage various aspects of device based network service policy implementation. In some embodiments, the virtual network overlay networking solution is applied to an existing hierarchical network (e.g., for wireless services), and in some embodiments, is applied to simplify or flatten the network architecture as will be further described below. In some embodiments, the large majority of the complex data path network processing required to implement the richer service management objectives of existing hierarchical networks (e.g., for wireless services) are moved into the device, leaving less data path processing required in the edge network and in some cases even less in the core network. Because the control plane traffic between the service control servers and the device agents that implement service policies can be several orders of magnitude slower than the data plane traffic, service control server network placement and back-haul

infrastructure is much less performance sensitive than the data plane network. In some embodiments, as described further below, this architecture can be overlaid onto all the important existing access network architectures used today. In some embodiments, this architecture can be employed to greatly simplify core access network routing and data plane traffic forwarding and management. For example, in the case of wireless networks, the incorporation of device assisted service policy implementation architectures can result in base stations that directly connect to the Internet local loop and the data traffic does not need to be concentrated into a dedicated core network. This results, for example, in a large reduction in backhaul cost, core network cost and maintenance cost. These cost savings can be re-deployed to purchase and install more base stations with smaller cells, which results in higher data capacity for the access network leading to better user experience, more useful applications and lower service costs. This flattened networking architecture also results in latency reduction as fewer routes are needed to move traffic through the Internet. In some embodiments, the present invention provides the necessary teaching to enable this powerful transformation of centralized network service architectures to a more distributed device based service architectures.

[0089] Device based billing can be compromised, hacked and/or spoofed in many different ways. Merely determining that billing reports are being received from the device, that the device agent software is present and properly configured (e.g., the billing agent is present and properly configured) is insufficient and easily spoofed (e.g., by spoofing the agent itself, providing spoofed billing reports using a spoofed billing agent or providing spoofed agent configurations). Accordingly, in some embodiments, verifiable device assisted and/or network based service policy implementation is provided. For example, verifiable service usage and/or service usage billing can be provided as described herein with respect to various embodiments.

[0090] While much of the below discussion and embodiments described below focus on paid service networks, those of ordinary skill in the art will appreciate that many of the embodiments also apply to other networks, such as enterprise networks. For example, the same device assisted network services that create access control services, ambient activation services and other service profiles can be used by corporate IT managers to create a controlled cost service policy network for corporate mobile devices. As another example, embodiments described below for providing end user service control can also allow a service provider to offer

parental controls by providing parents with access to a website with a web page that controls the policy settings for the access control networking service for a child's device.

Network Architecture for Device Assisted/Based Service Control

[0091] FIG. 1 illustrates a simplified (e.g., "flattened") network architecture in accordance with some embodiments. As shown, this provides for a simplified service infrastructure that exemplifies a simplified and "flattened" network architecture in accordance with some embodiments that is advantageous for wireless network architectures. This also reduces the need for complex data path protocol interaction between the base station and network infrastructure. For example, in contrast to a complex edge and core network infrastructure connecting base stations to the central service provider network, as shown the base stations 125 are connected directly to the Internet 120 via firewalls 124 (in some embodiments, the base stations 125 include the firewall functionality 124). Accordingly, in some embodiments, a central provider network is no longer required to route, forward, inspect or manipulate data plane traffic, because data plane traffic policy implementation is conducted in the device 100 by the service processor 115. However, it is still an option, in some embodiments, to bring data plane traffic in from the base stations 125 to a central provider network using either open or secure Internet routing if desired. Base station control plane communication for access network AAA (Authentication, Authorization, and Accounting) server 121, DNS/DHCP (Domain Name System/Dynamic Host Configuration Protocol) server 126, mobile wireless center 132 (sometimes referenced to in part as a home location register (HLR) or other acronym) or other necessary functions are accomplished, for example, with a secure IP tunnel or TCP connection between the central provider network and the base stations. The base station 125 is used to refer to multiple base station embodiments where the base station itself is directly connected to the RAN, or where the base station connects to a base station controller or base station aggregator function that in turn connects to the RAN, and all such configurations are collectively referred to herein as base station 125 in FIG. 1 and most figures that follow that reference base station 125 as described below.

[0092] As shown, the central provider access network is both 3G and 4G capable, the devices 100 can be either 3G, 4G or multi-mode 3G and 4G. Those of ordinary skill in the art

will also appreciate that in the more general case, the network could be 2G, 3G and 4G capable, or the device could be 2G, 3G and 4G capable with all or a subset of Global System for Mobile (GSM), General Packet Radio Service (GPRS), Code Division Multiple Access (CDMA) 1X, High Speed Packet Access (HSPA), Evolution Data Optimized (EVDO), Long Term Evolution (LTE) and WiMax modem capability. If the devices are single mode, then the 3G devices 100 will be activated with a service profile applied to service processor 115 that is consistent with the 3G network capacity and speed, and the 4G devices will be activated with service profiles applied to service processor 115 that are consistent with 4G network capacity and speed. In both cases, the same service controller 122 manages services for both sets of devices in accordance with some embodiments. If the devices are multimode, then the service processor 115 can be activated with a dual mode service profile capability in which the service profile for 3G offers a similar rich set of services as the service profile for 4G but with, for example, scaled back bandwidth. For example, this approach is allows central providers to offer a richer set of service offerings with 3G and then migrate the same set of service offerings to 4G but with higher performance. In particular, this approach allows 3G to 4G rich service migration to occur, for example, with the only change being the increased bandwidth settings in the service profiles that will be available in 4G at the same cost as 3G with lower service profile bandwidth settings.

[0093] In some embodiments, if the devices are multimode, a network selection policy implementation within service processor 115 is provided, or in some embodiments, a network selection policy is driven by policy decisions made in service controller 122 based on service availability reports received from service processor 115. The network selection policy allows the selection of the network that corresponds to the most desirable service profile to meet the user's service preferences. For example, if the user specifies, within the framework of the service notification and user preference feedback embodiments described below, that maximum performance is the most important factor in selecting which access network to connect to, then the best profile is likely to be the 4G network as 4G is typically faster, except perhaps, for example, if the device 100 is closer to the 3G base station so that there is a much stronger signal or if the 4G network is much more heavily loaded than the 3G network. On the other hand, if the user preference set specifies cost as the most important factor, then depending on the central provider service costs the 3G network may prove to be the most desirable service profile. This is

a simple example and many other selection criteria are possible in the network selection embodiment as discussed further below.

Network Based Service Usage Monitoring for Verification and Other Purposes

[0094] In some embodiments, if the base station data plane traffic is transmitted via the Internet 120 as discussed above, then IPDRs (Internet Protocol Detail Records, also sometimes and interchangeably referred to herein as Charging Data Records or CDRs, which as used herein refer to any network measure of service usage or service activity for voice and/or data traffic (e.g., IPDRs can include a time stamp, a device ID, and various levels of network measures of service usage for the device associated with that device ID, such as perhaps total traffic usage, network destination, time of day or device location)) are generated by and collected from the access network equipment. Depending on the specific network configuration, as discussed herein, for a WWAN network the IPDRs can be generated by one or more of the following: base station 125, RAN or transport gateways and AAA 121. In some access network embodiments, the IPDRs are transmitted to equipment functions that aggregated the IPDRs for the purpose of service billing and other functions. Aggregation can occur in the AAA, the transport gateways or other functions including the billing system 123. As discussed below, it is often the case that the IPDRs is assumed to be obtained from the AAA server 121 and/or a service usage data store 118 (e.g., a real-time service usage collection stored in a database or a delayed feed service usage collection stored in a database), or some other network function. However, this does not imply that the IPDRs may not be obtained from a variety of other network functions, and in some embodiments, the IPDRs are obtained from other network functions as disclosed herein. In some embodiments, existing IPDR sources are utilized to obtain network based service usage measures for multiple purposes including but not limited to service policy or profile implementation verification, triggering service verification error responds actions, and service notification synchronization. Certain types of IPDRs can be based on, or based in part on, what are sometimes referred to as CDRs (Charging Data Records, which can track charges for voice and data usage) or modifications of CDRs. Although the capability to monitor, categorize, catalog, report and control service usage or service activity is in general higher on the device than it is in the network, and, as described herein, device based service monitoring or control assistance is in some ways desirable as compared to network based implementations, as described herein many

embodiments take advantage of network based service monitoring or control to augment device assisted service monitoring or control and vice versa. For example, even though many embodiments work very well with minimal IPDR service usage or service activity information that is already available in a network, deeper levels of IPDR packet inspection information in general enable deeper levels of service monitoring or service control verification, which can be desirable in some embodiments. As another example, deeper levels of network capability to control service usage or service activity can provide for more sophisticated error handling in some embodiments, for example, providing for more options of the Switched Port Analyzer (SPAN) and network quarantine embodiments as described herein. As another example, in some embodiments it is advantageous to take advantage of network based service monitoring or control for those service aspects the network is capable of supporting, while using device assisted service monitoring or control for the service aspects advantageously implemented on the device.

[0095] In some embodiments, where base station data plane traffic is backhauled and concentrated in a central provider core network 110, then the IPDRs can originate in the base stations or a router or gateway in the central provider network 110, and the IPDRs are collected at the AAA server 121 and stored in the service usage data store 118. In some embodiments, the central billing system 123 collects the IPDRs from the AAA server 121 for service billing accounting purposes. In some embodiments, a central billing system 123 collects the IPDRs directly from the initial IPDR source or some other aggregator. In some embodiments, outside partners like MVNOs gain access to the IPDRs from the central billing system 123. As discussed below, it is assumed that the IPDRs are obtained from the AAA server 121, and it is understood that the source of the IPDRs is interchangeable in the embodiments.

[0096] In some embodiments, the IPDR information is used by the service processor 115, the service controller 122 and/or other network apparatus or device apparatus to implement service control verification is provided as described below. In some embodiments, an IPDR feed (e.g., also referred to as a charging data record (CDR)) flows between network elements. For example, an IPDR feed can flow from the RAN gateway 410 (e.g., SGSN 410, BSC packet control 510 or RNC 512) and the transport gateway 420 (e.g., GGSN or PDSN). In other embodiments, the IPDRs originate and flow from the base station 125 or some other

component/element in the network. In some embodiments, one or more of these IPDR feeds is transmitted to an IPDR aggregation function (e.g., also referred to as a charging gateway). For example, this aggregation function can be located in the AAA 121, in the mobile wireless center 132 (and/or in the home location register (HLR) or other similar function referred to by other common industry names), in the transport gateway 420, or in some other network element. This aggregation function collects the IPDR feeds into a database with an entry for each device 100. In some embodiments, an intermediate aggregation function is provided that feeds a higher level aggregation function, for example, the transport gateway 420 can receive IPDR feeds from the RAN gateway 410 or the base station 125 before sending them to another aggregation function. At some point in time (e.g., at the end of a specified time period, at the end of a device network connection session and/or at a specified time of day), the IPDR aggregation function sends summary information or detailed information of the IPDRs for a given device or group of devices to the billing system for billing and/or reconciliation. In some embodiments, in which the IPDR aggregation feed to the billing system is frequent enough for one or more of the IPDR information purposes described herein, the IPDR feed for the service controller 122 is derived from the aggregated feed, either by having the billing system 123 transmit it to the service controller 122, or by copying it from the IPDR aggregation function.

[0097] In some embodiments, the IPDR feed is obtained from the network function that is generating or aggregating the IPDR feed as described herein. In some embodiments, the IPDR feed is copied from the aggregation function in a manner that does not interrupt the operation of the network. For example, a switch based port analysis function can be used to copy the traffic to a traffic analysis or server element that filters out the IPDR traffic and records it to a data base that is then either pushed to the service controller 122 (or any other network element that uses IPDR information as described herein), or is queried by the service controller 122 (or any other function that uses the IPDR information as described herein). In some embodiments, if the aggregated IPDR information transmitted to the billing system is delayed from real-time traffic usage events by an amount of time that is, for example, too long for desired operation, or for any other reason that makes it less desirable to obtain the IPDR information from the same aggregated feed used for the billing system 123, the IPDR information can be collected from one or more of the sources discussed above including, for example, from another aggregation point (e.g., the feed to the charging gateway, AAA server and/or mobile wireless center/HLR), one or

more of the gateways 410, 420, 508, 512, 520, 608, 612, 620, 708, 712, 720 the base station 125 and/or another network element. In some embodiments, the IPDR feeds from these or other network functions are copied to a database as described above, which is either pushed or queried to get the information to the service controller 122 or other network elements that request the IPDR information.

[0100] In some embodiments, the service processor 115 includes various components, such as device agents, that perform service policy implementation or management functions. In some embodiments, these functions include service policy or implementation verification, service policy implementation tamper prevention, service allowance or denial, application access control, traffic control, network access control services, various network authentication services, service control plane communication, device heartbeat services, service billing, transaction billing, simplified activation services and/or other service implementations or service policy implementations. It will be apparent to those of ordinary skill in the art that the division in functionality between one device agent and another is a design choice, that the functional lines can be re-drawn in any technically feasible way that the product designers see fit, and that the placing divisions on the naming and functional breakouts for device agents aids in understanding, although in more complex embodiments, for example, it can make sense to the product designer to break out device agent functionality specifications in some other manner in order to manage development specification and testing complexity and workflow.

[0101] In some embodiments, network control of the service policy settings and services as discussed above is accomplished with the service controller 122 which in various embodiments includes one or more server functions. As with the service processor 115 agent naming and functional break out, it is understood that service controller 122 server naming and functional breakout is also a design choice and is provided mainly to aid in the discussion. It will be apparent to those of ordinary skill in the art that the server names and functional breakouts do not imply that each name is an individual server, and, for example, a single named function in the various embodiments can be implemented on multiple servers, or multiple named functions in the various embodiments can be implemented on a single server.

[0102] As shown, there are multiple open content transaction partner sites 134 (e.g., open content transaction servers), which represent the websites or experience portals offered by content partners or ecommerce transaction partners of the service provider. For example, transaction servers 134 can provide an electronic commerce offering and transaction platform to the device. In some embodiments, the central provider has ownership and management of the service controller 122, so the central provider and the service provider are the same, but as discussed below the service provider that uses the service controller 122 to manage the device services by way of service processor 115 is not always the same as the central provider who provides the access network services.

[0103] In some embodiments, further distribution of central provider access networking functions such as access network AAA server 121, DNS/DHCP server 126, and other functions are provided in the base stations 125. In some embodiments, network based device service suspend/resume control are also provided in the base stations 125 (or in some embodiments, for hierarchical or overlay networks, this function is provided by one or more of the following: RAN gateways, transport gateways, AAA 121 or some other network function). As shown, the following are connected (e.g., in network communication with) the central provider network 110: central provider billing system 123, dedicated leased lines 128 (e.g., for other services/providers), central provider service controller 122, a content management (e.g., content switching, content billing, and content catching) system 130, central provider DNS/DHCP server 126, access network AAA server 121, service usage data store 118 and central provider mobile wireless center 132. These embodiments may be advantageous particularly for flat networks as that shown in FIG. 1 that are provided by the present invention.

[0104] In some embodiments, the base stations 125 implement a firewall function via firewall 124 and are placed directly onto the local loop Internet for backhaul. Voice traffic transport is provided with a secure protocol with Voice Over IP (VOIP) framing running over a secure IP session, for example, Virtual Private Network (VPN), IP Security (IPSEC) or another secure tunneling protocol. In some embodiments, the VOIP channel employs another layer of application level security on the aggregated VOIP traffic trunk before it is placed on the secure IP transport layer. Base station control traffic and other central provider traffic can be provided in a number of ways with secure transport protocols running over Transmission Control Protocol

(TCP), Internet Protocol (IP) or User Datagram Protocol (UDP), although TCP provides a more reliable delivery channel for control traffic that is not as sensitive to delay or jitter. One example embodiment for the control channel is a control link buffering, framing, encryption and secure transport protocol similar to that described below for the service control link between a device and the network. In some embodiments, a service control heartbeat function is provided to the base stations 125 similar to that implemented between the service controller 122 and the service processor 115 as described below. If the need to maintain a bandwidth efficient control plane channel between the base stations and the central provider base station control network is not as critical as it is in the case of access network connection to the device, then there are many other approaches for implementing a secure control channel over the Internet including, for example, one or more of various packet encryption protocols running at or just below the application layer, running TCP Transport Layer Security (TLS), and running IP level security or secure tunnels.

[0105] In some embodiments, the device based services control plane traffic channel between the service processor 115 and the service controller 122 is implemented over the same control plane channel used for the flat base station control architecture, or in some embodiments, over the Internet. As discussed below, it is assumed that the device bases services control plane channel for service processor 115 to service controller 122 communications is established through the Internet 120 or through the access network using IP protocols as this is the more general case and applies to overlay network applications for various embodiments as well as applications where various embodiments are used to enable flattened access networks.

[0106] In some embodiments, by enabling the device to verifiably implement a rich set of service features as described herein, and by enabling the base station 125 to connect directly to the Internet 120 with a local firewall for device data traffic, tunnel the voice to a voice network with VOIP and secure Internet protocols, and control the base station 125 over a secure control plane channel using base station control servers located in a central provider network, base stations 125 can be more efficiently provisioned and installed, because, for example, the base station 125 can accommodate a greater variety of local loop backhaul options. In such embodiments, it is advantageous to perform certain basic network functions in the base station 125 rather than the central provider network.

[0107] In some embodiments, a basic device suspend/resume function for allowing or disallowing the device Internet access is provided by the base stations 125 (or in some embodiments, for hierarchical or overlay networks in some embodiments this function is provided by one or more of the following: RAN gateways, transport gateways, AAA 121 or some other network function). This functionality, as will be discussed below, is important for certain embodiments involving taking action to resolve, for example, service policy verification errors. In some embodiments, this function is performed at the base station (e.g., base stations 125) thereby eliminating the need for a more complex networking equipment hierarchy and traffic concentration required to perform the suspend/resume function deeper in the network. Access network base stations control media access and are therefore designed with awareness of which device identification number a given traffic packet, group of packets, packet flow, voice connection or other traffic flow originates from and terminates to. In some embodiments, the suspend/resume function is implemented in the base station 125 by placing an access control function in the traffic path of each device traffic flow. The suspend resume function can be used by various network elements, and in the context of the present embodiment can be used by the service controller 122 (e.g., in some embodiments, access control integrity server 1654 (FIG. 16) of service controller 122 or other service controller elements) to suspend and resume device service based on the assessment of the service policy implementation verification status as described below.

[0108] In some embodiments, at least a basic traffic monitoring or service monitoring function is performed at the base station (e.g., base stations 125) similar to the service history records or IPDRs collected deeper in the network in more conventional hierarchical access network infrastructure architectures. For example, the service or traffic monitoring history records are advantageous for tracking device network service usage or service activity behavior and for certain verification methods for device based service policy implementation or higher device based services as discussed below. In some embodiments, a traffic monitoring function is provided in the base station 125 in which the traffic for each device is at least counted for total traffic usage and recorded. In some embodiments, traffic inspection beyond simply counting total traffic usage is provided. For example, the base station traffic monitor can record and report IP addresses or include a DNS lookup function to report IP addresses or IP addresses and associated Uniform Resource Locators (URLs). Another example allows the base station 125 to

attach location data to the IPDR to provide device location data in the records. In some embodiments, traffic inspection includes recording deeper levels of traffic or service monitoring.

[0109] In some embodiments, device traffic associated with service verification conditions indicating service usage is out of policy or profile limits or allowances is routed to a quarantine network rather than or as an initial alternative to a suspending service. For example, the advantages for this approach and a more detailed description of the quarantine network are discussed below. In some embodiments, the quarantine network capability is provided for in which rather than simply suspending device traffic completely from the network as described above, the base station 125 includes a firewall function (e.g., firewall 124) that is capable of passing device access traffic with the quarantine network destinations and blocking device access to all other destinations. In some embodiments, when it is discovered that service verification conditions indicate that service usage is out of policy or profile limits or allowances, then one or more of the following actions are taken: the user is notified of the overage condition, the user is required to acknowledge the overage condition, the user account is billed for the overage condition, and the device is flagged for further analysis by a network device analysis function or a network manager.

[0110] In some embodiments, network complexity is reduced using the device without moving completely to a flat base station network as described above. Device participation in the core network services implementation provides for numerous measures for simplifying or improving network architecture, functionality or performance. For example, two approaches are discussed below ranging from a simple overlay of the service processor 115 onto devices and the service controller 122 in a conventional hierarchical access network as illustrated in FIGS. 4 through 7, to a completely flat network as illustrated in FIGS. 1 through 3 and 8. Those of ordinary skill in the art will appreciate that the disclosed embodiments provided herein can be combined with the above embodiments and other embodiments involving flat network base stations to provide several advantages including, for example, richer service capability, less access network complexity, lower access network expenses, more flexible base station deployments, or less complex or less expensive base station back haul provisioning and service costs.

[0111] In most of the discussion that follows, the network based service history records and the network based suspend-resume functionality used in certain embodiments involving service implementation verification are assumed to be derived from the device service history 1618 (as shown in FIG. 16) central provider network element and the AAA server 121 central provider network element, and in some embodiments, working in conjunction with other central provider network elements. It is understood that these functions provided by the network can be rearranged to be provided by other networking equipment, including the base station as discussed above. It is also understood that the network based device traffic monitoring, recording and reporting to the device service history 1618 element can be accomplished at the base stations. Furthermore, it is understood that while the AAA server 121 is assumed to provide the suspend/resume functionality, quarantine network routing or limited network access called for in some embodiments, the AAA server 121 can be a management device in which the actual implementation of the traffic suspend/resume, firewall, routing, re-direction forwarding or traffic limiting mechanisms discussed in certain embodiments can be implemented in the base stations as discussed above or in another network element.

[0112] In some embodiments, an activation server 160 (or other activation sequencing apparatus) provides for provisioning, as described below, of the devices 100 and/or network elements in the central provider network so that, for example, the device credentials can be recognized for activation and/or service by the network. In some embodiments, the activation server 160 provides activation functions, as described below, so that, for example, the devices can be recognized by the network, gain access to the network, be provided with a service profile, be associated with a service account and/or be associated with a service plan. As shown in FIG. 1, the activation server 160 is connected to the central provider core network 110. In this configuration, the activation server 160 acts as, an over the network or over the air, activation function. In some embodiments, the activation server 160, or variations of the activation server 160 as described below, is connected to apparatus in the manufacturing or distribution channel, or over the Internet 120, or as part of the service controller 122 to service provisioning or activation functions. In some embodiments, the activation server 160 is connected to the central provider core network 110. In some embodiments, the activation server 160 is connected to other network extensions such as an MVNO network or the Internet 120 if, for example, the routers in the service gateways or base stations have the capability to direct traffic from devices

that are not fully activated or provisioned to an Internet destination, or if the service processor 115 is used for such direction. In some embodiments, the activation server 160 is included in the service controller 122.

[0113] FIG. 2 illustrates another simplified (e.g., "flattened") network architecture including an MVNO (Mobile Virtual Network Operator) relationship in accordance with some embodiments. As shown, an open MVNO configuration is provided in a simplified network as similarly described above with respect to FIG. 1. In some embodiments, the service provider (e.g., service owner) is defined by the entity that maintains and/or manages the service controller 122 associated with and controlling the service processors 115 that are inside the devices 100 using the service. In some embodiments, the service controller 122 requires only a non-real time relatively low data rate secure control plane communication link to the service processors 115. Accordingly, in some embodiments, the service controller 122 servers can reside in any network that can connect to (e.g., be in network communication with) the Internet 120. For example, this approach provides for a more efficient provisioning of the equipment used to set up an MVNO partnership between the central provider and the service provider, and as shown in FIG. 2, an MVNO network 210 is in network communication with the Internet 120 just as with the central provider network 110 is in network communication with the Internet 120. As shown, the following are connected to (e.g., in network communication with) the MVNO core network 210: MVNO billing system 123, MVNO service controller 122, MVNO content management system 130, MVNO DNS/DHCP server 126, MVNO AAA server 121, and MVNO mobile wireless center 132.

[0114] By showing two service controllers 122, one connected to (e.g., in network communication with) the MVNO network 210 and one connected to the central provider network 110, FIG. 2 also illustrates that some embodiments allow two entities on the same access network to each use the service controller 122 and service processor 115 to control different devices and offer different or similar services. As described below, the unique secure communication link pairing that exists between the two ends of the service control link, 1691 and 1638 (as shown in FIG. 16), ensure that the two service controllers 122 can only control the devices associated with the correct service provider service profiles.

[0115] FIG. 3 illustrates another simplified (e.g., "flattened") network architecture including two central providers in accordance with some embodiments. For example, this provides for roaming agreements while maintaining rich services across different networks with completely different access layers. As shown, the mobile devices 100 are assumed to have a dual mode wireless modem that will operate on both a 4G network, for example LTE or WiMax, and a 3G network, for example HSPA or EVDO. One example roaming condition would be both Central Provider #1 and Central Provider #2 providing 3G and 4G network resources. In this example, the mobile devices 100 can connect to both 3G and 4G base stations 125 owned and operated by the central provider with whom they have signed up for service, or when neither is available from the central provider the user signed up with the device can roam onto the other central provider access network and still potentially offer the same rich service set using the same service profiles provided, for example, the roaming service costs are reasonable. In some embodiments, if roaming service costs are significantly more expensive than home network service costs, then the service processor 115 is configured with a roaming service profile that reduces or tailors service usage or service activity through a combination of one or more of user notification, user preference feedback regarding traffic shaping or service policy management preference collected and acted on by service processor 115, adaptive policy control in service processor 115 that tracks increasing roaming service costs and scales back service, or recognition of the change in network that causes the service controller 122 to configure service processor 115 of device 100 with a roaming service profile. In some embodiments, in roaming situations, network selection can be based on an automatic network selection with network selection being determined, for example, by a combination of user service profile preferences, service provider roaming deals and/or available roaming network capabilities and cost, as discussed further below.

[0116] In some embodiments, the devices 100 are again assumed to be multimode 3G and 4G devices (e.g., the mobile devices 100 are assumed to have a dual mode wireless modem that will operate on both a 4G network, for example LTE, and a 3G network, for example HSPA or EVDO), with the devices 100 being billed for service by Central Provider #1 being, for example, EVDO and LTE capable, and the devices 100 being billed for service by Central Provider #2 being, for example, HSPA and LTE capable. For example, the devices 100 can roam using the 4G LTE network of the roaming central provider when neither the 3G nor 4G

networks are available with the home central provider. As similarly discussed above with respect to the above described roaming embodiments, the service processors 115 and service controllers 122 are capable of providing similar services on the 4G roaming network and the 3G home network as on the 4G home network, however, the varying costs and available network capacity and speed differences of 3G home, 4G roaming and 4G home may also encourage the use of different, such as three different, service profiles to allow for the most effective and efficient selection and control of services based on the current network.

[0117] FIG. 4 illustrates a network architecture including a Universal Mobile Telecommunications System (UMTS) overlay configuration in accordance with some embodiments. As shown, FIG. 4 includes a 4G/3G/2G HSPA/Transport access network operated by a central provider and two MVNO networks 210 operated by two MVNO partners. In some embodiments, the central provider can offer improved service capabilities using a conventional UMTS network. As shown, the base stations 125 do not connect directly to the Internet 120, and instead the base stations 125 connect to the conventional UMTS network. However, as in various previous embodiments, the service processor 115 still connects through the secure control plane link to service controller 122. In some embodiments, the data plane traffic is backhauled across the various UMTS network routers and gateways as is the control plane traffic, and the IPDRs are obtained from the access network AAA server 121. Referring now to the 4G/3G/2G HSPA/Transport access network as shown in FIG. 4, the LTE/HSPA and HSPA/GPRS base stations/nodes 125 are in communication with 4G/3G/2G Service/Serving GPRS Support Nodes (SGSNs) cluster 410 via a radio access network 405, which are in communication with 4G/3G/2G Gateway GPRS Support Nodes (GGSNs) cluster 420 via an access transport network 415 (e.g., a GPRS-IP network), which are then in communication with central provider core network 110.

[0118] As shown in FIG. 4, as discussed elsewhere, service usage data store 118 is a functional descriptor for a network level service usage information collection and reporting function located in one or more of the networking equipment boxes attached to one or more of the sub-networks in the figure (e.g., RAN, transport and/or core networks). As shown in FIG. 4, service usage 118 is shown as an isolated function connected to the central provider core network 110 and the intention of this depiction is to facilitate all the possible embodiments for

locating the service usage 118 function. In some UMTS network embodiments, the service usage 118 function is located or partially located in the GGSN gateway (or gateway cluster) 420. In some embodiments, service usage 118 functionality is located or partially located in the SGSN gateway (or gateway cluster) 410. In some embodiments, service usage 118 functionality is located or partially located in the equipment cluster that includes the AAA 121 and/or the mobile wireless center 132. In some embodiments, service usage 118 functionality is located or partially located in the base station, base station controller and/or base station aggregator, collectively referred to as base station 125 in FIG. 4 and many other figures described herein. In some embodiments, service usage 118 functionality is located or partially located in a networking component in the transport network 415, a networking component in the core network 110, the billing system 123 and/or in another network component or function. This discussion on the possible locations for the network based service usage history logging and reporting function can be easily generalized to all the other figures described herein by one of ordinary skill in the art (e.g., RAN Gateway 410 and/or Transport Gateway 420), and this background will be assumed even if not directly stated in all discussion above and below.

[0119] In some embodiments, a central provider provides open development services to MVNO, Master Value Added Reseller (MVAR) and/or Original Equipment Manufacturer (OEM) partners. In some embodiments, all three service providers, central provider service provider, MVNO #1 service provider and MVNO #2 service provider have service control and billing control of their own respective devices 100 through the unique pairing of the service processors 115 and service controllers 122. For example, MVNO #1 and MVNO #2 can each have open development billing agreements with the central provider and each can own their respective billing systems 123. As shown in FIG. 4, MVNO #1 core network 210 is in communication with the central provider core network 110 via the Internet 120, and MVNO #2 core network 210 is in communication with the central provider core network 110 via an alternate landline(LL)/VPN connection 425. In some embodiments, the two MVNOs each offer completely different devices and/or services, and the devices and/or services also differ significantly from those offered by the central provider, and the service profiles are adapted as required to service the different devices and respective service offerings. In addition, the central billing system 123 allows all three service provider user populations to access ecommerce experiences from transaction provider partners operating transaction servers 134, to choose

central provider billing options that combine their third party transaction bills on their service provider bill, and each subscriber population can experience a service provider specified look and feel that is unique to the respective service provider even though the different user populations are interfacing to the same transaction servers and the transaction partners do not need to require significant custom development to provide the unique central billing and unique consistent user experience look and feel.

[0120] In some embodiments, a central provider offers open network device and service developer services using one service controller server 122 (e.g., a service controller server farm) and allows the open development partners to lease server time and server tools to build their own service profiles. The central provider also provides service billing on behalf of services to the open development partners. For example, this reduces costs associated with setting up an MVNO network for the open development partners and does not require the partners to give up significant control or flexibility in device and/or service control.

[0121] FIG. 5 illustrates a network architecture including an Evolution Data Optimized (EVDO) overlay configuration in accordance with some embodiments. This figure is similar to FIG. 4 except for the various particular variations of the EVDO network architecture as compared to the HSPA/GPRS wireless access network architecture as will be apparent to one of ordinary skill in the art. As shown, FIG. 5 includes an EVDO access network operated by a central provider and two MVNO networks 210 operated by two MVNO partners. The EVDO access network includes LTE/EVDO and EVDO/1xRTT base stations 125 in communication with Base Station Controller (BSC) packet control 508 and radio network controller 512 via a radio access network (RAN) 505, which are in communication with packet data service node 520 via an access transport network 515, which is in communication with central provider core network 110. As shown, a RAN AAA server 521 is also in communication with the access transport network 515.

[0122] In some embodiments, the central provider can offer improved service capabilities using a wireless access network. As shown, the base stations 125 do not connect directly to the Internet 120, and instead the base stations 125 connect to the wireless access network. However, as in various previous embodiments, the service processor 115 still connects through the secure

control plane link to service controller 122. In some embodiments, the data plane traffic is backhauled as shown across the various network routers and gateways as is the control plane traffic, and the IPDRs are obtained from the access network AAA server 121.

[0123] FIG. 6 illustrates a network architecture including a 4G LTE and Wi-Fi overlay configuration in accordance with some embodiments. This figure is also similar to FIG. 4 except for the various particular variations of the 4G LTE/Wi-Fi network architecture as compared to the HSPA/GPRS wireless access network architecture as will be apparent to one of ordinary skill. As shown, FIG. 6 includes a 4G LTE and Wi-Fi access network operated by a central provider and two MVNO networks 210 operated by two MVNO partners. The 4G LTE/Wi-Fi access network as shown includes LTE eNodeB and HSPA/EVDO base stations 125 in communication with Base Station Controller (BSC) packet control (EVDO & 1xRTT) 608 and SGSN (HSPA & GPRS) 612 via a radio access network (RAN) 605, which are in communication with System Architecture Evolution (SAE) Gateway (GW) 620 via an access transport network 615, which is then in communication with central provider (core) network 110. As shown, a Mobile Management Entity (MME) server 619 is also in communication with the access transport network 615. Also as shown, a Wi-Fi Access Point (AP) 602 is also in communication with the access transport network 615 via Wi-Fi Access Customer Premises Equipment (CPE) 604. As will be apparent to those of ordinary skill in the art, the embodiments of network architectures shown, for example, in FIGS. 1-8 are exemplary network architecture embodiments in which one or more of the shown network elements may not be required or included, alternative network elements included, and/or additional network elements included based on network design choices, network standards and/or other functional/design considerations and choices.

[0124] In some embodiments, the central provider can offer improved service capabilities using the wireless access network as depicted in FIG. 6. As shown, the base stations 125 do not connect directly to the Internet 120, and instead the base stations 125 connect to the wireless access network. However, as in various previous embodiments, the service processor 115 still connects through the secure control plane link to service controller 122. In some embodiments, the data plane traffic is backhauled as shown across the various network routers and gateways as is the control plane traffic, and the IPDRs are obtained from the access network AAA server 121.

Accordingly, as shown in FIGS. 4 through 6, various embodiments can be implemented independent of the wireless access network technology, and for example, can be implemented in 3G, 4G and any other wireless access network technology.

[0125] FIG. 7 illustrates a network architecture including a WiMax and Wi-Fi overlay configuration in accordance with some embodiments. This figure is also similar to FIG. 4 except for the various particular variations of a combined WiMax/Wi-Fi network as compared to the HSPA/GPRS wireless access network architecture as will be apparent to one of ordinary skill in the art. As shown, FIG. 7 includes both a WiMax and Wi-Fi network (e.g., a combined WiMax/Wi-Fi network) operated by a central provider and two MVNO networks 210 operated by two MVNO partners. Although the Wi-Fi and WiMax access technologies are different wireless access networking technologies, with WiMax providing a wide area networking technology and Wi-Fi providing a local area networking technology, which efficiently operates using the two wireless access networking capabilities. As similarly discussed above with respect to the switching between 3G and 4G networks, some embodiments employ the automatic network selection capability as described above to choose the best available network service profile, and, for example, the user can force the decision or the service controller can make the decision. For example, if free Wi-Fi services have adequate coverage, in most cases, the decision criteria programmed into the automatic network selection algorithm will select Wi-Fi as long as the Wi-Fi access points are associated with a known and trusted provider. In some embodiments, transaction billing from central provider billing system 123 or MVNO #1 or MVNO #2 billing systems 123 will work with the transaction servers when connected over Wi-Fi just as when connected over any other access technology (including wire line based connections). The WiMax/Wi-Fi access network as shown includes WiMax base stations 125, Wi-Fi access points/hotspots 702 and/or Wi-Fi mesh access networks 702 (in some embodiments, femto cells can be used in addition to and/or as an alternative to Wi-Fi), and Wi-Fi access customer-premises equipment (CPE) 704 in communication with WiMax service controller 708 and Wi-Fi service controller 712 via a radio access network 705, which are in communication with WiMax core gateway 720 via an access transport network 715, which is then in communication with central provider (core) network 110.

[0126] In some embodiments, the central provider can offer improved service capabilities using the wireless access network as depicted in FIG. 7. As shown, the base stations 125 do not connect directly to the Internet 120, and instead the base stations 125 connect to the wireless access network. However, as in various previous embodiments, the service processor 115 still connects through the secure control plane link to service controller 122. In some embodiments, the data plane traffic is backhauled as shown across the various network routers and gateways as is the control plane traffic, and the IPDRs are obtained from the access network AAA server 121.

[0127] Referring to FIG. 7, the Wi-Fi connection can be replaced with a femto cell (and the Wi-Fi modem shown in FIGS. 15D and 15E can be replaced with a femto cell modem (base station side functionality)). In some embodiments, the service processor 115 is provided on the femto cell to control subscriber access in a verifiable manner as similarly described herein with respect to various embodiments (e.g., the Wi-Fi related embodiments). For example, the femto cell service provider (e.g., the entity that owns the spectrum the femto cell is using) can operate the femto cell as a local access mechanism for the home subscriber (or other who purchased or installed the femto cell), and then also use it to provide pay-for-service or additional free services, with controlled access and/or traffic control and/or service control and/or billing control performed locally or in combination with network equipment as described herein. In some embodiments, the WWAN devices being used at home or work with the femto cell include a portion of the service processor functionality. For example, this allows the service provider for femto cells to provide service and monetize service in a controlled way even though the femto cell is not connected to the service provider network the way conventional base stations are connected to the service provider network, but is connected through the Internet 120. For example, the secure heartbeat function can be extended to include data traffic so that it is encrypted and secured along with the control plane traffic. The decision of whether or not to admit a device onto the femto cell can be made through the service processor 115 connection to the service controller 122 and subsequent look up of the credentials for the device and the associated service plan and service profile that is then programmed into the service processor on the femto cell and/or the device itself. The femto cell can also offer a landing page to devices through the service processor so that devices that do not belong to the network can gain access to the network by signing up over the femto cell. For example, the intermediate device embodiments for Wi-Fi on one end and WWAN on the other can be accomplished by using the

Wi-Fi connection in the cell phone in AP mode so that it becomes the intermediate device. The service processor 115 on the cell phone can then act in the same manner as described for the intermediate device as described herein.

[0128] FIG. 8 illustrates another simplified (e.g., "flattened") network architecture including multiple wireless access networks (e.g., 3G and 4G Wireless Wide Area Networks (WWANs)) and multiple wire line networks (e.g., Data Over Cable Service Interface Specification (DOCSIS) and Digital Subscriber Line Access Multiplexer (DSLAM) wire line networks) in accordance with some embodiments. It is a common network architecture for multi-access central providers to have one or more wired access networks and one or more wireless access networks. As shown, FIG. 8 includes both 3G and 4G wireless access networks, including a 4G base station 125 and a 3G base station 125, and both DOCSIS and DSLAM wire line networks (e.g., a combined WWAN/wire line network), including DOCSIS Head End 125 and DSLAM 125, operated by a central provider via central provider (core) network 110 and an MVNO partner via MVNO network 210 via the Internet 120.

[0129] As shown, the service processor 115 can reside on a number of different types of devices 100 that work on 3G or 4G wireless, DSL or DOCSIS, and the service controller 122 is capable of controlling each of these types of devices with a consistent service experience, for example, using different service profiles, service capabilities and service profile cost options depending on which network the device is connected to and/or other criteria. For example, a download of a High Definition (HD) movie can be allowed when the service controller 122 is managing service profile policies for a service processor 115 residing on a DOCSIS device 100 (e.g., a computer or laptop connected to a cable modem), but not when the same service controller 122 is managing service profile policies for a service processor 115 residing on a 3G device 100 (e.g., a smart phone connected to a mobile 3G network).

[0130] As will now be apparent to one of ordinary skill in the art in view of the above description of FIGS. 1 through 8, the present invention can be provided across any access network and a set of service profiles can be defined in a variety of ways including, for example, to user preference feedback, access network performance, access network cost, access network central provider partnership status with the service provider central provider and roaming deals

and costs. For example, as discussed below, various embodiments allow for users to have superior service experiences based on the ability to control certain of their service settings, and service providers can also more efficiently deploy a greater variety of services/service plans to users.

[0131] In some embodiments, the service processor 115 and the service controller 122 provide an overlay for existing networks without significantly changing the billing system 123, gateways/routers or other network components/elements, and also provide verifiable service monitoring to control services and/or service usage/costs without involving, for example, a service provider or MVNO (e.g., for smart phone devices and/or laptops or netbooks (or any other network accessible device) with an unlimited data plan or any other service plan). For example, applications that are deployed by device owners or service subscribers (e.g., an IT manager) and do not involve a service provider include roaming services provided as an after-market product without carrier/service provider involvement. In this example, device activity is recorded by the service processor 115 and transmitted to the service controller 122 (e.g., the IT manager controls the service controller 122). In another example, a third party after-market product is provided in which the service controller 122 is hosted by the third party and the device management entity (e.g., the IT manager or parents of the device user for parental controls) uses a secure Virtual Service Provider (VSP) website to control the devices that belong to that management entity's device partition (e.g., VSP partitions and techniques are described below with respect to FIG. 49). The VSP secure website techniques described herein can also be applied to service provider owned servers with device partitions for the purpose of controlling, for example, Deep Packet Inspection (DPI) controllers (e.g., DPC policy implementation 5402 as shown in FIG. 54) to provide similar or substantially equivalent service usage/control capabilities using network based service control techniques, as similarly described in detail below with respect to FIGS. 49 and 54 (e.g., IT manager VSP control of a group partition and/or MVNO VSP control of a group partition).

Service Processor Configurations for Devices

[0132] FIG. 9 illustrates a hardware diagram of a device 100 that includes a service processor 115 in accordance with some embodiments. As shown in FIG. 9, the service processor

115 is stored in a non volatile memory 910 and a memory 920 of the device 100. As will be appreciated by those of ordinary skill in the art, the present invention can operate with virtually any device architecture, and the device architectures discussed herein (e.g., with respect to FIGS. 9-14 and 15A-15F) are examples of various implementations on certain devices (e.g., of different representations of device 100).

[0133] As shown in FIG. 9, device 100 also includes a processor 930, sometimes referred to as a CPU or central processor unit, an APU or application processor unit, a core processor, a computing device, or many other well known terms. In some embodiments, device 100 includes one or more processors and/or a multicore processor. As shown, processor 930 includes a sub-processor 935. In some embodiments, processor 930 and/or sub-processor 935 are based on an architecture sometimes referred to as a complex instruction set computer or CISC, a reduced instruction set computer or RISC, a parallel processor, a combination of two or more architectures or any other processor architecture. In some embodiments, processor 930 has a design that is based on logic and circuitry from one or more standard design library or published architecture, or includes specialized logic and circuitry designed for a given device 100 or collection of such devices. In some embodiments, a device includes more than one processor and/or sub-processor, and in such a device, one processor and/or sub-processor can have one architecture while another may have a somewhat different or completely different architecture. In some embodiments, one or more of the processors and/or sub-processors can have a general purpose architecture or instruction set, can have an architecture or instruction set that is partially general or partially specialized, or can have an instruction set or architecture that is entirely specialized. In some embodiments, a device includes more than one processor and/or sub-processor, and in such a device, there can be a division of the functionality for one or more processors and/or sub-processors. For example, one or more processors and/or sub-processors can perform general operating system or application program execution functions, while one or more others can perform communication modem functions, input/output functions, user interface functions, graphics or multimedia functions, communication stack functions, security functions, memory management or direct memory access functions, computing functions, and/or can share in these or other specialized or partially specialized functions. In some embodiments, any processor 930 and/or any sub-processor 935 can run a low level operating system, a high level operating system, a combination of low level and high level operating systems, or can include

logic implemented in hardware and/or software that does not depend on the divisions of functionality or hierarchy of processing functionality common to operating systems.

[0134] As shown in FIG. 9, device 100 also includes non-volatile memory 910, memory 920, graphics memory 950 and/or other memory used for general and/or specialized purposes. As shown, device 100 also includes a graphics processor 938 (e.g., for graphics processing functions). In some embodiments, graphics processing functions are performed by processor 930 and/or sub-processor 935, and a separate graphics process 938 is not included in device 100. As shown in FIG. 9, device 100 includes the following modems: wire line modem 940, WWAN modem 942, USB modem 944, Wi-Fi modem 946, Bluetooth modem 948, and Ethernet modem 949. In some embodiments, device 100 includes one or more of these modems and/or other modems (e.g., for other networking/access technologies). In some embodiments, some or all of the functions performed by one or more of these modems are performed by the processor 930 and/or sub processor 935. For example, processor 930 can implement some or all of certain WWAN functional aspects, such as the modem management, modem physical layer and/or MAC layer DSP, modem I/O, modem radio circuit interface, or other aspects of modem operation. In some embodiments, processor 930 as functionality discussed above is provided in a separate specialized processor as similarly shown with respect to the graphics and/or multimedia processor 938.

[0135] As also shown in FIG. 9, device 100 includes an internal (or external) communication bus structure 960. The internal communication bus structure 960 generally connects the components in the device 100 to one another (e.g., allows for intercommunication). In some embodiments, the internal communication bus structure 960 is based on one or more general purpose buses, such as AMBA, AHP, USB, PCIe, GPIO, UART, SPI, I^2C, Fire wire, DisplayPort, Ethernet, Wi-Fi, Bluetooth, Zigbee, IRDA, and/or any other bus and/or I/O standards (open or proprietary). In some embodiments, the bus structure is constructed with one or more custom serial or parallel interconnect logic or protocol schemes. As will be apparent to one of ordinary skill in the art, any of these or other bus schemes can be used in isolation and/or in combination for various interconnections between device 100 components.

[0136] In some embodiments, all or a portion of the service processor 115 functions disclosed herein are implemented in software. In some embodiments, all or a portion of the service processor 115 functions are implemented in hardware. In some embodiments, all or substantially all of the service processor 115 functionality (as discussed herein) is implemented and stored in software that can be performed on (e.g., executed by) various components in device 100. FIG. 9 illustrates an embodiment in which service processor 115 is stored in device memory, as shown, in memory 920 and/or non-volatile memory 910, or a combination of both. In some embodiments, it is advantageous to store or implement certain portions or all of service processor 115 in protected or secure memory so that other undesired programs (and/or unauthorized users) have difficulty accessing the functions or software in service processor 115. In some embodiments, service processor 115, at least in part, is implemented in and/or stored on secure non-volatile memory (e.g., non volatile memory 930 can be secure non-volatile memory) that is not accessible without pass keys and/or other security mechanisms. In some embodiments, the ability to load at least a portion of service processor 115 software into protected non-volatile memory also requires a secure key and/or signature and/or requires that the service processor 115 software components being loaded into non-volatile memory are also securely encrypted and appropriately signed by an authority that is trusted by a secure software downloader function, such as service downloader 1663 as discussed below (and as shown in FIG. 16). In some embodiments, a secure software download embodiment also uses a secure non-volatile memory. Those of ordinary skill in the art will also appreciate that all memory can be on-chip, off-chip, on-board and/or off-board. In some embodiments, the service processor 115 which as shown in FIG. 9 is stored or implemented in non volatile memory 910 and memory 920, can be implemented in part on other components in device 100.

[0137] As shown, device 100 also includes a user interfaces device component 980 for communicating with user interface devices (e.g., keyboards, displays and/or other interface devices) and other I/O devices component 985 for communicating with other I/O devices. User interface devices, such as keyboards, display screens, touch screens, specialized buttons or switches, speakers, and/or other user interface devices provide various interfaces for allowing one or more users to use the device 100.

[0138] FIG. 10 illustrates another hardware diagram of a device 100 that includes a service processor 115 in accordance with some embodiments. As shown in FIG. 10, the service processor 115 is implemented on the processor 930 of the device 100. In some embodiments, this implementation can be in part or whole accomplished in software stored, implemented and/or executed on the processor 930. In some embodiments, the implementation and/or execution can be in part or whole accomplished in hardware that is on the processor 930. While the service processor 115 is shown in FIG. 10 as stored, implemented and/or executed on the processor 930, in other embodiments, the service processor 115 is implemented in part on other components in device 100, for example, as discussed below.

Service Processor Implemented on a Communications Modem

[0139] FIG. 11 illustrates another hardware diagram of a device 100 that includes a service processor 115 in accordance with some embodiments. As shown in FIG. 11, the service processor 115 is implemented on the WWAN modem 942 of the device 100. In some embodiments, this implementation can be in part or whole accomplished in software stored, implemented and/or executed on the WWAN modem 942. In some embodiments, the implementation and/or execution can be in part or whole accomplished in hardware that is on the WWAN modem 942. In some embodiments, service process 115 is implemented on another modem component of device 100 and/or one or more of the modem components of device 100.

[0140] In some embodiments, the service processor 115 is implemented on a modem processor (e.g., WWAN modem 942 or WWAN/Wi-Fi modem), and the service processor 115 can be installed and/or executed in protected and/or secure memory or processor hardware on the modem. The modem memory can be made robust to hacking or tampering and, in some embodiments, is only accessible from a secure network management channel or secure device management port and not by most end users. In some embodiments, a portion of the service processor 115 is implemented on a modem processor (e.g., WWAN modem 942 hardware or software), and a portion of the service processor 115 is implemented on another device 100 processor 930. For example, the device service monitor agent 1696 and one or more service usage measurement points (see discussion associated with FIG. 21) can be implemented on a modem processor, and other service processor 115 elements can be implemented in the main

device operating system processor 930. As another example, a second (or first) service monitor agent 1696 and one or more service usage measurement points can be implemented on a modem processor, and a first (or second) service monitor 1696 with one or more service measurement points can be implemented on the main operating system processor 930 for device 100. For example, such embodiments can be configured to provide a service usage measurement and reporting system that offers a diversified countermeasure to protect against hacking, tampering or other errors for device based service usage measurements that can be made harder to hack or tamper with than certain software embodiments on the processor 930. For example, such embodiments can be employed when one or more of the following capabilities are not available: network based service usage measures, network based service profile or policy implementation verification measures, and network based service usage verification error response action capabilities.

[0141] In some embodiments, certain portions of the service processor 115 that deal with application layer service monitoring or traffic flow identification (e.g., tagging or traffic flow shaping as disclosed elsewhere) are implemented on a main processor 930, and other portions of the service processor 115 are implemented on a modem processor (e.g., WWAN modem 942).

[0142] In some embodiments, the WWAN modem is a wide area access technology modem such as 2G, 2.5G, 3G or 4G. As discussed above and below, the connection to the WWAN modem 942 can be a connection internal to device 100, for example a USB, GPIO, AMBA or other bus, or can be a connection that extends external to the device such as for example a USB, Ethernet, Wi-Fi, Bluetooth or other LAN or PAN connection. Three example embodiments in which the bus is internal to the device are as follows: a PCIe modem card running over USB or PCIe, a GPIO connection running from a processor 930 chipset to a modem chipset inside a mobile device, or a Wi-Fi connection running from a Wi-Fi modem inside of device 100 to an intermediate modem or networking device combination that forwards the access network traffic between the access network connection and the device via the Wi-Fi connection. In some embodiments, in addition to the service processor 115 being implemented on the WWAN modem 942 either internal or external to the device 100, similarly service processor 115 can be implemented on a wire line modem 940, such as DSL, Cable or fiber, another wireless LAN or PAN modem, such as Wi-Fi, Zigbee, Bluetooth modem 948, White Space, or some other

modem, connected internal to device 100 or external to device 100 via a LAN or PAN extension of internal or external communications bus structure 960.

[0143] In some embodiments, a complete turn-key reference design product for the device modem (one or more of 942, 946, 948, 949, 944, 940) combined with a built-in service processor 115, possibly with a well defined and documented application interface and a well defined and documented service processor developers kit (SPDK) provides for a powerful product embodiment for the purpose of achieving mass market distribution and usage for the modem with service processor 115 and associated service controller 122 features. For example, embodiments that include the WWAN modem 942, possibly in combination with one or more additional modems including Wi-Fi modem 946, bluetooth modem 948, USB modem 944 and Ethernet modem 949, can be combined with a pre-tested or pre-certified integrated embodiment of the service processor 115, possibly in combination with a well defined API for writing software applications that interface to, reside on or communicate with this turn-key modem embodiment. As disclosed herein, the advantageous capabilities of the service processor 115, possibly in conjunction with the service controller 122, to assist in monitoring, control, billing and verification for services is made more available for device 100 manufacturers in such a form, because the manufacturers do not need to spend as much time and resources to develop a custom modem only for a subset of devices that the turn-key modem can be used to support. In some embodiments, the service processor 115, as discussed herein, can be configured to provide device assisted service monitoring, control, billing and/or verification across not just when connected to the WWAN network via the WWAN modem, but also when connected to the other networks corresponding to the other access modems included in the turn-key combined module plus service processor 115 (or SPDK or chipset plus service processor 115) design. The pre-integrated service processor 115 and API possibly in combination with testing and certification can be packaged in a small form factor that may have standardized interfaces such as USB, PCIe, firewire, Display Port, GPIO, or other interface. The form factor may be miniaturized into standard configurations such as minicard, half minicard or even smaller form factors, or it can be designed into a non-standard or proprietary form factor. The module form factor can be well documented to simplify integration into various device 100 designs. The SPDK embodiments can be designed to contain one or more of the following: hardware integration and use documentation, software integration documentation, software programming documentation,

application interface documentation, service controller documentation, overall testing guidelines and overall use guidelines. In some embodiments, the modem module can be integrated with the service processor 115 functionality as a combined chipset, firmware and/or software product, with other SPDK features very similar to those listed above. The service controller programming guide for these turn-key embodiments can also be documented for the SPDK service processor 115 software, turn-key module with service processor 115 or integrated chipset with service processor 115. Accordingly, these embodiments provide various solutions to simplify the OEM task of integrating, developing, testing and shipping device 100 products (or integrated networking device products) with any of the device assisted service monitoring, control, billing or verification capabilities disclosed herein.

[0144] FIG. 12 illustrates another hardware diagram of a device 100 that includes a service processor 115 in accordance with some embodiments. As shown in FIG. 12, the service processor 115 is implemented on the other I/O devices component 980 of the device 100. In some embodiments, this implementation can be in part or whole accomplished in software stored, implemented and/or executed on the other I/O devices component 980 (e.g., a SIM/USIM card or other secure hardware I/O device). In some embodiments, the implementation and/or execution can be in part or whole accomplished in hardware that is on the other I/O devices component 980.

[0145] As discussed above, various embodiments include product designs in which the service processor 115 resides on device volatile or non-volatile memory (see FIG. 9), the device application processor or CPU (see FIG. 10), the wireless access modem (see FIG. 11) (or any other modem), or another I/O device (see FIG. 12). While these are just a few of the example service processor 115 placement embodiments, these embodiments show that the placement of where the software or hardware for implementing the service processor 115 can reside in the device 100 is very flexible and can be implemented in a myriad of places and ways depending on the device and/or other technical design choices.

[0146] FIG. 13 illustrates another hardware diagram of a device 100 that includes a service processor 115 implemented in external memory of a System On Chip (SOC) 1310 in accordance with some embodiments. As shown in FIG. 13, the service processor 115 is

implemented on the external memory 1320 of the device 100. In some embodiments, this implementation can be in part or whole accomplished in software stored, implemented and/or executed on the external memory 1320. In some embodiments, the implementation and/or execution can be in part or whole accomplished in hardware that is on the external memory 1320. In some embodiments, SOC chipset 1310 and external memory 1320 provide a portion or all of the hardware of device 100.

[0147] FIG. 14 illustrates another hardware diagram of a device 100 that includes a service processor 115 implemented in external memory of a System On Chip (SOC) 1310 in accordance with some embodiments. As shown, the service processor 115 is stored in a non volatile memory 910 and a memory 920 of the SOC chipset 1310, as similarly discussed above with respect to FIG. 9. In some embodiments, SOC chipset 1310 and external memory 1320 provide a portion or all of the hardware of device 100.

[0148] As similarly discussed above with respect to FIGS. 9 through 12, various embodiments include product designs including the SOC chipset 1310 in which the service processor 115 resides on internal volatile or non-volatile memory 910 of the SOC chipset 1310 (see FIG. 14), the device application processor or CPU 930 and/or sub processor 935, the modems 940, 942, 944, 946, 948, and/or 949 (or any other modem), another I/O device 985, and/or external memory 1320 (see FIG. 13) (and/or any combinations thereof). While these are just a few of the example service processor 115 placement embodiments, these embodiments show that the placement of where the software or hardware for implementing the service processor 115 can reside in the SOC chipset 1310 and/or the external memory 1320 of the device 100 is very flexible and can be implemented in a myriad of places and ways depending on the device and/or other technical design choices.

[0149] The above discussion with respect to FIGS. 9 through 14 illustrating various internal hardware embodiments for device 100 applies equally to this partitioning of device functionality or any other partitioning of how the components in device 100 are configured, whether they are all separate components, some of the components are combined into a single chipset but there are still multiple chipsets, or all of the components are combined into a chipset. For example, FIGS. 9 through 14 illustrating various internal hardware embodiments for device

100 show several access modem components including the wire line modem 940, wireless wide area network (WWAN) modem 942, USB modem 944, Wi-Fi modem 946, Bluetooth modem 948, and Ethernet modem 949. In some embodiments, wire line modem 940 is a DSL or cable modem such as DOCSIS, or some other modem with a hard connection such as fiber. In some embodiments, as discussed above and below, connection to the wire line or wireless access network is accomplished through an extension of the internal or external communications bus structure 960. For example, such an extension is accomplished using one or the other modems, such as Wi-Fi modem 946 or Ethernet modem 949, connecting to a local area network that in turn connects to the access network via a device that bridges the local area network to the access network. One of ordinary skill in the art will appreciate that when discussing device connection to any access network the connection can be via a direct connection to the network, such as a 3G or 4G WWAN modem 942 connection to a 3G or 4G WWAN network, or can be a connection to the access network through an intermediate connection, such as a Wi-Fi modem 946 connection to a modem or networking device combination that has a Wi-Fi LAN connection and a 3G or 4G network access network connection. Another example of an extended modem connection embodiment includes a Wi-Fi modem 946 device connection to a modem or networking device combination that includes a Wi-Fi LAN connection and a DOCSIS or DSL network access connection. Other examples of such combinations will be readily apparent to one of ordinary skill in the art.

Service Processor Configurations for Intermediate Networking Devices

[0150] FIGS. 15A through 15F illustrate hardware diagrams of a device 100 that include a service processor 115 and a bus structure extension 1510 using intermediate modem or networking device combinations in accordance with various embodiments . For example, FIGS. 15A through 15E illustrate various extended modem alternatives for access network connection through an intermediate modem or networking device combination that has a connection (e.g., LAN connection) to one or more devices 100.

[0151] In some embodiments, device 100 includes a 3G and/or 4G network access connection in combination with the Wi-Fi LAN connection to the device 100. For example, the intermediate device or networking device combination can be a device that simply translates the

Wi-Fi data to the WWAN access network without implementing any portion of the service processor 115 as shown in FIG. 15B. In some embodiments, an intermediate device or networking device combination includes a more sophisticated implementation including a networking stack and some embodiments a processor, as is the case for example if the intermediate networking device or networking device combination includes a router function, in which case the service processor 115 can be implemented in part or entirely on the intermediate modem or networking device combination. The intermediate modem or networking device combination can also be a multi-user device in which more than one user is gaining access to the 3G or 4G access network via the Wi-Fi LAN connection. In the case of such a multi-user network, the access network connection can include several managed service links using multiple instantiations of service processor 115, each instantiation, for example, being implemented in whole or in part on device 100 with the intermediate modem or networking device combination only providing the translation services from the Wi-Fi LAN to the WWAN access network.

[0152] Referring now to FIGS. 15A, 15C, 15D, and 15E, in some embodiments, the service processors 115 are implemented in part or in whole on the intermediate modem or networking device combination. In the case where the service processor 115 is implemented in part or in whole on the intermediate modem or networking device combination, the service processor 115 can be implemented for each device or each user in the network so that there are multiple managed service provider accounts all gaining access through the same intermediate modem or networking device combination. In some embodiments, the functions of service processor 115 are implemented on an aggregate account that includes the WWAN access network traffic for all of the users or devices connected to the Wi-Fi LAN serviced by the intermediate modem or networking device combination. In some embodiments, the central provider can also provide an aggregated account service plan, such as a family plan, a corporate user group plan and/or an instant hotspot plan. In the case where there is one account for the intermediate modem or networking device combination, the intermediate modem or networking device combination can implement a local division of services to one or more devices 100 or users in which the services are controlled or managed by the intermediate modem or networking device combination or the device 100, but the management is not subject to service provider control and is auxiliary to the service management or service policy implementation performed

by service processors 115. In some embodiments, another service model can also be supported in which there is an aggregate service provider plan associated with one intermediate modem or networking device combination, or a group of intermediate modems or networking device combinations but where each user or device still has its own service plan that is a sub-plan under the aggregate plan so that each user or device has independent service policy implementation with a unique instantiation of service processor 115 rather than aggregate service policy implementation across multiple users in the group with a single instantiation of service processor 115.

[0153] As shown in FIGS. 15A and 15C, in some embodiments, device 100 includes a Wi-Fi modem 946, a Wi-Fi modem 946 combined with a 3G and/or 4G WWAN modem 1530 on intermediate modem or networking device combination 1510, and the intermediate modem or networking device combination forwards WWAN access network traffic to and from device 100 via the Wi-Fi link. For example, the service processor 115 can be implemented in its entirety on device 100 and the service provider account can be associated exclusively with one device. This is an embodiment associated with one or more of FIGS. 29, 31, 32 or 34 discussed below, in which the modem bus represents the Wi-Fi LAN connection via the Wi-Fi modem 946. Similarly, as shown in FIGS. 15A and 15D, such an implementation can be provided using a different access modem and access network, such as a 2G and/or 3G WWAN, DSL wire line, cable DOCSIS wire line or fiber wire line configuration in place of the 3G and/or 4G access network connection to the intermediate modem or networking device combination 1510. In addition, various other embodiments similarly use DSL as shown in FIGS. 15A and 15E, USB, Ethernet, Bluetooth, or another LAN or point to point connection from device 100 to the intermediate modem or networking device combination 1510.

[0154] In some embodiments, a portion of the service processor 115 is implemented on the device 100, such as the application interface agent 1693 and other supporting agents (see FIG. 16), and another portion of the service provider 115 is implemented on the intermediate modem or networking device combination, such as policy implementation agent 1690 or possibly modem firewall 1655 as well as other agents (see FIG. 16). This is an embodiment associated with one or more of FIGS. 30 or 36 discussed below, in which the modem bus in the figure represents the Wi-Fi LAN connection via the Wi-Fi modem 946. In this example, the

service provider 115 can still offer individual service plans associated exclusively with one device, or can offer an aggregate plan in which the portion of the service processor 115 located on the intermediate modem or networking device combination 1510 aggregates service plans into one WWAN connection but each individual device 100 has a unique service interface via the application interface agents and associated agents located on device 100. Similarly, such an implementation can be provided using a different access modem and access network, for example a 2G and/or 3G WWAN, DSL wire line, cable DOCSIS wire line or fiber wire line configuration in place of the 3G and/or 4G access network connection to the intermediate modem or networking device combination 1510. In addition, various other embodiments similarly use USB, Ethernet, Bluetooth, or another LAN or point to point connection from device 100 to the intermediate modem or networking device combination 1510.

[0155] In some embodiments, all of the service processor 115 is implemented on the intermediate modem or networking device combination 1510 and the aggregate device or user traffic demand from the LAN port is serviced through one service provider service plan account. This is an embodiment associated with FIG. 35 in which as discussed below the modem bus in the figure represents the Wi-Fi LAN connection via the Wi-Fi modem 946. Similarly, such an implementation can be provided using a different access modem and access network, for example a 2G and/or 3G WWAN, DSL wire line, cable DOCSIS wire line or fiber wire line configuration in place of the 3G and/or 4G access network connection to the intermediate modem or networking device combination 1510. In addition, various other embodiments similarly use USB, Ethernet, Bluetooth, or another LAN or point to point connection from device 100 to the intermediate modem or networking device combination 1510.

[0156] In some embodiments, the device 100 uses the on-board WWAN modem 942 when it is outside of Wi-Fi LAN coverage area for one or more trusted access networks for the device, and when the device comes within range of a Wi-Fi network associated with a intermediate modem or networking device combination connected to a trusted wire line access network, the device can switch to the Wi-Fi link service to connect service processor 115 to the trusted wire line access network. In some embodiments, the decision to switch to the Wi-Fi LAN associated with a trusted wire line access network can be made automatically by the device based on the policy implementation rules settings for the modem selection and control 1811

and/or the policy control agent 1692, can be made by the user, or can be made by the service controller 122 (see FIG. 18). In addition, various other embodiments similarly use USB, Ethernet, Bluetooth, or another LAN or point to point connection from device 100 to the intermediate modem or networking device combination 1510.

[0157] FIG. 15F illustrates another hardware diagram of a device 100 that includes a service processor 115 and a bus structure extension 1510 using intermediate modem or networking device combinations in accordance with various embodiments . In some embodiments, more than one access network connection is implemented in the intermediate modem or networking device combination 1510. This allows the device 100 to potentially connect through the intermediate modem or networking device combination with a choice of access network services. An example of such an embodiment is illustrated in FIG. 15F in which an access network router (e.g., an enterprise router) connected to a LAN with a wire line primary backhaul connection and a back up WWAN connection, for example 3G or 4G, to provide access services when the primary wire line connection fails. As discussed above, the service provider service profile for service processor 115 and the service plan account can be set up as an aggregate account with multiple users connected to the LAN. The service provider can elect to use an embodiment that includes a portion of the service processor 115 on each device 100 so that the account can be managed for each user or each device, or the service provider can elect to implement all of the necessary features in the service processor 115 on the intermediate modem or networking device combination so that there is no visibility to the individual devices 100 or users.

[0158] As described herein, various embodiments provide many service policy implementation options that can enhance the service provider control of the service experience and cost, or enhance the user control of the service experience and cost by providing a verifiable or compromise resistant solutions to manage service policy implementation on the intermediate modem or networking device combination, for one or both of the WWAN or wire line access networks, when the WWAN access network is active, or when the WWAN access network is inactive. The level of service control, user preference feedback and service policy implementation verification or compromise resistance enabled by these embodiments improves the offered back up services and primary wire line services. One of ordinary skill in the art will

also now appreciate that any number of wire line and/or wireless network access connections can be supported by the various embodiments as described herein, with any number of device architectures and architectures for intermediate modem or networking device combinations bridging the device to the access network of choice. Accordingly, various embodiments provide a verifiable managed service architecture, design and implementation for any number of single access and/or multi-access networks in which the service account can be consistent across multiple networks, and the service policies can be changed from network to network as deemed appropriate by the service provider with service notification, service cost control and privacy preference inputs from the user.

[0159] In various embodiments, the verification embodiments discussed herein for service policy implementation verification or service policy implementation compromise protection can be applied. In some embodiments, rather than attaching a service provider service plan account to a single device, it is attached to (e.g., associated with) a user. For example, when the user logs onto an access network with a service controller controlled by a service provider, regardless of what device the user logs onto with the user's service plan profile can be automatically looked up in the central billing system 123 and dynamically loaded (e.g., downloaded) onto the device 100 from the service controller 122 (e.g., a service profile provided on demand based on the user's identity). In some embodiments, in addition to dynamically loading the user's service policy implementation and control settings, one or more of the user's preferences including notification, service control, traffic monitor reporting privacy and Customer Relationship Management (CRM) reporting privacy are also dynamically loaded. For example, this allows the user to have the same service settings, performance and experience regardless of the device the user is logged into and using on the network. In addition, as discussed herein, in the various embodiments that call for roaming from one type of access network to another, the user service plan profile, that includes all of the above in addition to the service plan profile changes that take effect between different types of access network, can be used on any device and on any network, providing the user with a verifiable or compromise resistant, consistent service experience regardless of network or device.

[0160] Many of the embodiments described herein refer to a user using device 100. It is understood that there are also applications for these various embodiments that do not involve

user interfaces. Examples of such applications include equipment, apparatus or devices for automation, telemetry, sensors, security or surveillance, appliance control, remote machine to machine data connections, certain remote access configurations, two way power metering or control, asset tracking, people tracking or other applications in which a human user interface is not required for device 100.

[0161] Various embodiments of the device 100 described above include other I/O devices 985. In some embodiments, these other devices include other modems, other special purpose hardware components, and/or other I/O devices or drivers or modems to connect to other I/O devices. In some embodiments, these other devices include a Subscriber Identity Module (SIM) or Universal Subscriber Identity Module (USIM) device. In some embodiments, it is advantageous to implement some or all of the service processor 115 functions on an embodiment of device 100 that includes a SIM and/or a USIM. In some embodiments, the other I/O devices 985 include a hardware device designed to implement a portion or all of the service processor 115 functions. For example, this is advantageous in cases in which the original device 100 was not manufactured with the service processor 115; in cases in which dedicated hardware is desired to improve one or more aspects of service processor 115 performance; allowing users, for example, to have the same service settings, performance and experience regardless of the device the user is using on the network by using such a SIM and/or USIM (e.g., or implemented as a type of dongle); and/or in cases in which a separate component is desired to assist in compromise protection for one or more aspects of service processor 115.

[0162] As discussed above, some embodiments described herein provide for billing of certain access services. In some embodiments, various applications do not require or involve billing of certain services. For example, applications like enterprise IT (Information Technology) group management of enterprise workforce access policy implementation or access cost control or access security policy, privacy control, parental control, network quality of service control or enhancement, private network services, free access services, publicly funded access services, flat rate no-options service and other services, or other examples that will be apparent to one of ordinary skill in the art do not require billing functionality but benefit from many other aspects of various embodiments.

[0163] **Service Processor and Service Controller for Verifiable Service Monitoring, Notification and Control**

[0164] FIG. 16 is a functional diagram illustrating a device based service processor 115 and a service controller 122 in accordance with some embodiments. For example, this provides relatively full featured device based service processor implementation and service controller implementation. As shown, this corresponds to a networking configuration in which the service controller 122 is connected to the Internet 120 and not directly to the access network 1610. As shown, a data plane (e.g., service traffic plane) communication path is shown in solid line connections and control plane (e.g., service control plane) communication path is shown in dashed line connections. As previously discussed, it is understood that the division in functionality between one device agent and another is based on, for example, design choices, networking environments, devices and/or services/applications, and various different combinations can be used in various different implementations. For example, the functional lines can be re-drawn in any way that the product designers see fit. As shown, this includes certain divisions and functional breakouts for device agents as an illustrative implementation, although other, potentially more complex, embodiments can include different divisions and functional breakouts for device agent functionality specifications, for example, in order to manage development specification and testing complexity and workflow. In addition, the placement of the agents that operate, interact with or monitor the data path can be moved or re-ordered in various embodiments. For example, as discussed below in some embodiments, one or more of the policy implementation or service monitoring functions can be placed on one of the access modems located below the modem driver and modem bus in the communication stack as illustrated in certain figures and described herein. As discussed below, some simplified embodiment figures illustrate that not all the functions illustrated in all the figures are necessary for many designs, so a product/service designer can choose to implement those functions believed to be most advantageous or sufficient for the desired purposes and/or environment. The functional elements shown in FIG. 16 are described below.

[0165] As shown, service processor 115 includes a service control device link 1691. For example, as device based service control techniques involving supervision across a network become more sophisticated, it becomes increasingly important to have an efficient and flexible

control plane communication link between the device agents and the network elements communicating with, controlling, monitoring, or verifying service policy. In some embodiments, the service control device link 1691 provides the device side of a system for transmission and reception of service agent to/from network element functions. In some embodiments, the traffic efficiency of this link is enhanced by buffering and framing multiple agent messages in the transmissions. In some embodiments, the traffic efficiency is further improved by controlling the transmission frequency or linking the transmission frequency to the rate of service usage or traffic usage. In some embodiments, one or more levels of security or encryption are used to make the link robust to discovery, eavesdropping or compromise. In some embodiments, the service control device link 1691 also provides the communications link and heartbeat timing for the agent heartbeat function. As discussed below, various embodiments disclosed herein for the service control device link 1691 provide an efficient and secure solution for transmitting and receiving service policy implementation, control, monitoring and verification information with other network elements.

[0166] In some embodiments, the service control device link 1691 agent messages are transmitted asynchronously as they are generated by one or more of the service agents. In some embodiments, the service control device link 1691 performs collection or buffering of agent messages between transmissions. In some embodiments, the service control device link 1691 determines when to transmit based potentially on several parameters including, for example, one or more of the following parameters: periodic timer trigger, waiting until a certain amount of service usage or traffic usage has occurred, responding to a service controller message, responding to a service controller request, initiated by one or more agents, initiated by a verification error condition, initiated by some other error or status condition. In some embodiments, once a transmission trigger has occurred, the service control device link 1691 assembles all buffered agent communications and frames the communications.

[0167] In some embodiments, the transmission trigger is controlled by waiting for an amount of service usage, such as waiting until a certain amount of data traffic has passed, which reduces the control plane communication channel traffic usage to a fraction of the data plane traffic. For example, this approach preserves network capacity and reduces service cost even in traffic scenarios in which data traffic is light.

[0168] In some embodiments, the transmission trigger is based on waiting for an amount of service usage, and also including a minimum transmission rate that triggers a transmission according to one or more of the following parameters: a maximum time between transmissions clock to keep the service processor 115 in communication with the service controller 122 when little or no service usage is occurring, a polling request of some kind from the service controller 122, a response to a service controller heartbeat, a transmission generated by a service verification error event, or a transmission generated by some other asynchronous event with time critical service processor 115 (or service controller 122) messaging needs, such as a transaction or service billing event or a user request. For example, service control plane traffic down is reduced to a relatively inexpensive and capacity conserving trickle when device 100 data traffic is not significant. At the same time, this approach also provides an effective flow of real time or near real-time service control plane traffic that is both cost and capacity efficient, because the service control plane traffic is a relatively small percentage of the data plane traffic when data plane traffic usage is heavy. For example, when data plane traffic usage is heavy is generally the time when close monitoring of service policy implementation verification or compromise prevention can be particularly important and by keeping the control plane overhead to a fraction of data plane traffic close monitoring and control of services are maintained at a reasonable cost in terms of percentage of both bandwidth used and network capacity. In some embodiments, the service usage or service activity trigger occurs based on some other measure than traffic usage, such as a number of messages transacted, one or more billing events, number of files downloaded, number of applications run or time that an application has been running, usage of one or more specified applications, GPS coordinate changes, roaming event, an event related to another network connection to the device and/or other service related measures.

[0169] In some embodiments, the service control device link 1691 provides for securing, signing, encrypting or otherwise protecting communications before sending. For example, the service control device link 1691 can send to the transport layer or directly to the link layer for transmission. In some embodiments, the communications are further secured with transport layer encryption, such as TCP TLS (Transport Control Protocol Transport Layer Security) or another secure transport layer protocol. In some embodiments, communications are encrypted at the link layer, such as IPSEC (Internet Protocol Security), various VPN (Virtual Private

Network) services, other forms of IP layer encryption and/or another link layer encryption technique.

[0170] In some embodiments, the service control link 1691 includes the above discussed agent heartbeat function in which the agents provide certain required reports to the service controller 122 for the purpose of service policy implementation verification (e.g., verification related reports on certain aspects of the service processor 115) or for other purposes. For example, such agent heartbeat messages can be in the open/clear (unencrypted) or encrypted, signed and/or otherwise secured. In some embodiments, these messages include one or more of the below described types of messages: an agent information message, an agent check-in message and/or agent cross check message.

[0171] In some embodiments, an agent information message is included in the agent heartbeat service policy implementation verification message, which includes, for example, any information the agent needs to communicate to the service controller 122 as part of the operation of the service policy implementation system. For example, an agent response to a service controller challenge, as described below, can be included in the agent heartbeat service policy implementation verification message.

[0172] In some embodiments, an agent check-in message is included in an agent heartbeat service policy implementation verification message, which includes, for example, a transmission of a unique agent identifier, secure unique identifier, and/or hashed encrypted and signed message beginning with some shared secret or state variable for the hash. For example, an agent self-check can be included in the agent heartbeat service policy implementation verification message, which includes reporting on agent configuration, agent operation, agent code status, agent communication log, agent error flags, and/or other agent associated information potentially hashed, encrypted, signed or otherwise secured in the message (e.g., using a shared secret unique to that agent).

[0173] In some embodiments, an agent cross-check message is included in the agent heartbeat service policy implementation verification message, which includes, for example, reports on the status, configuration, operation observations, communication log or other aspects of another agent. For example, agent environment reports can be included in the agent heartbeat

service policy implementation verification message, which includes, for example, reports on certain aspects of the service processor 115 operating environment, such as software presence (e.g., installation status of certain operating system and/or application software and/or components thereof), observed communication with agents or communication attempts, memory accesses or access attempts, network accesses or access attempts, software downloads or attempted downloads, software removal or download blocking, service policy implementation verification or compromise event error conditions with respect to the operating environment for the service processor 115, and/or other messages regarding the verification or possibility of compromise associated with the service processor 115 operating environment or agents.

[0174] In some embodiments, the agent heartbeat function also provides regular updates for information important to user service notification services. For example, the network based elements can provide regular synchronization updates for the device based service usage or service activity counters in which service usage or service activity measures available from one or more network service history elements is transmitted to the device 100. This allows the service usage counter errors between the device service counter and the counters used for central billing to be minimized. A common service usage or service activity measure is total traffic usage measured to date within a time frame over which a service limit is applicable. Other service usage or service activity measures can also be tracked and reconciled in a similar manner.

[0175] In some embodiments for the heartbeat function, the service controller 122 verifies that the scheduled agent reports are being received and that the reports are within expected parameters. In some embodiments, the access control integrity server 1654 issues signed challenge/response sequences to the policy implementation agent 1690. For example, the challenges can be asynchronous, issued when an event or error condition occurs, issued on a schedule or issued when a certain amount of data has passed. This approach, for example, provides a second layer of service policy implementation verification that strengthens the service usage or service activity measurement verification. For example, a challenge/response can be sent over the heartbeat link for the purpose of verifying device agent integrity. Various challenge/response related verification embodiments are described below.

[0176] In some embodiments, the challenge/response heartbeat message can include sending any kind of command or query, secure or transmitted in the open, receiving a response from the agent and then evaluating the response to determine if the response is within a range of parameters expected for a correctly configured agent, an agent that is operating properly, an agent that is not partially compromised or an agent that is not entirely compromised. In some embodiments, the agent is only required to respond with a simple acknowledgement of the challenge. In some embodiments, the agent is required to respond with a message or piece of information that is known by the agent. In some embodiments, the agent is required to respond with a message or piece of information that is difficult for the agent to respond correctly with if it were to be partially or entirely compromised. In some embodiments, the agent is required to respond back with information regarding the operation or configuration of the agent that is difficult for the agent to respond properly with if the agent is not properly configured, not operating properly, is partially compromised or is entirely compromised. In some embodiments, the first agent is required to respond back with information regarding the operation, configuration, status or behavior of a second agent that is difficult for the first or second agent to respond properly with if the first or second agent is not properly configured, not operating properly, is partially compromised or is entirely compromised. In some embodiments, the agent is required to respond with a response that includes a shared secret. In some embodiments, the agent is required to respond with information regarding the presence, configuration, operating characteristics or other information regarding other programs in the operating environment of the agent. In some embodiments, the agent is required to respond with hashed information to be portions of code or a code sample (e.g., the code portion or code sample can be specified by the service controller 122).

[0177] In some embodiments, the information the agent responds with is a response to a signed or encrypted message from the service controller 122 in which the agent must know how to decode the encrypted controller message in order to respond correctly or it would be difficult for the agent to respond properly if the agent is not configured properly, is not operating within appropriate limits, is partially compromised or is entirely compromised. In some embodiments, the agent signs or encrypts information in such a manner that it is difficult to respond correctly when the message is decoded by the service controller 122 unless the agent is configured properly, is operating within appropriate limits, is not partially compromised and is not entirely

compromised. In some embodiments, the agent is required to respond with a signed or encrypted hash of information that is difficult for the agent to generate unless the agent is configured properly, is operating within appropriate limits, is not partially compromised and is not entirely compromised. For example, the hashed information can be local device configuration information, portions of code or all of the code, and/or the code portion to be used in the response can be specified by the service controller. In another example, the hashed information the agent responds with can include a shared secret, and/or the hashed information can be information regarding the presence, configuration, operating characteristics or other information regarding other programs in the operating environment of the agent.

[0178] Accordingly, as described above, the agent heartbeat function provides an important and efficient system in some embodiments for verifying the service policy implementation or protecting against compromise events. For example, there are many other functions the agent heartbeat service can perform and some are described herein while others will be apparent to one of ordinary skill in the art given the principles, design background and various embodiments provided herein.

[0179] In some embodiments, the service control device link 1691 facilitates another important function, which is the download of new service processor software elements, revisions of service processor software elements, and/or dynamic refreshes of service processor software elements. There are many embodiments for such operations. In some embodiments, the software is received as a single file over the service control device link 1691. For example, the file can have encryption or signed encryption beyond any provided by the communication link protocol itself. In some embodiments, the software files are segmented into smaller packets that are communicated in multiple messages sent over the service control device link 1691. In some embodiments, once the file(s) are received, or the segmented portions of the file(s) are received, they are communicated to a service downloader 1663 for file aggregation and installation, which, in some embodiments, is performed after further measures to verify the service processor software are completed. In some embodiments, the files are sent using other delivery means, such a direct TCP socket connection to the service downloader 1663 or some other software installer, which can also involve secure transport and additional levels of encryption.

[0180] As shown in FIG. 16, an agent communication bus 1630 represents a functional description for providing communication for the various service processor 115 agents and functions. In some embodiments, as represented in the functional diagram illustrated in FIG. 16, the architecture of the bus is generally multipoint to multipoint so that any agent can communicate with any other agent, the service controller or in some cases other components of the device, such user interface 1697 and/or modem components. As described below, the architecture can also be point to point for certain agents or communication transactions, or point to multipoint within the agent framework so that all agent communication can be concentrated, or secured, or controlled, or restricted, or logged or reported. In some embodiments, the agent communication bus is secured, signed, encrypted, hidden, partitioned and/or otherwise protected from unauthorized monitoring or usage.

[0181] In some embodiments, as described below, there are multiple layers of security applied to the agent communication bus 1630 communication protocols, such as including one or more of the following: point to point message exchange encryption using one or more keys that are partially shared or shared within the service processor 115 agent group and/or the service controller 122, point to point message exchange that using one or more keys that are private to the two endpoints of the communication, a bus-level message exchange encryption that can be in place of or in addition to other encryption or security, or using one or more keys that are partially shared or shared within the service processor 115 agent group and/or the service controller 122, a set of secure messages that can only be decoded or observed by the agents they are intended for, a set of secure messages that allow communication between certain agents or service processor functions and entities outside of the service processor operating environment. In some embodiments, and as described herein, the service control device link 1691 is assumed to be equivalent to an agent for communication purposes, and, in the case of the service control device link 1691, the communication is not restricted to the agent communication bus 1630 but also extends to the service control communications link 1653. In some embodiments, the system has the capability to replace keys or signatures on occasion or on a regular basis to further secure against monitoring, eavesdropping or compromise of the agent communication system.

[0182] For example, various forms of message encryption and security framework techniques can be applied to encrypt and/or secure the agent communication bus 1630, including

one or more of the following: agent bus encryption using shared key for all agents provided and updated by the secure server; agent bus encryption using point to point keys in which the secure server informs the bus and agents of keys and updates as appropriate; agent level encryption using agent to agent shared keys in which the secure server informs agents of the key and updates the key as appropriate; agent level encryption using agent to agent point to point key in which the secure server informs agent of the point to point keys that are required and updates the keys as appropriate; agent level access authorization, which only allows access to the agents that are on the secure authorization list and in which the list is provided by the secure server and signatures are provided by the secure server; UI messages are only analyzed and passed, in which the UI cannot have access to configuration information and cannot issue challenges; agent level heartbeat encryption, which can be point to point or shared key for that agent; control link level heartbeat encryption; TLS (Transport Layer Security) communication protocols; server level heartbeat encryption, which can be point to point or shared key for that secure server; and/or the access control integrity agent 1694 or heartbeat function can become point to multipoint secure communications hubs.

[0183] In some embodiments of the agent communication bus 1630, the design of the agent communication bus depends on the nature of the design embodiments for the agents and/or other functions. For example, if the agents are implemented largely or entirely in software, then the agent communication bus can be implemented as an inter-process software communication bus. In some embodiments, such an inter-process software communication bus is a variant of D-bus (e.g., a message bus system for inter-process software communication that, for example, helps applications/agents to talk to one another), or another inter-process communication protocol or system, running a session bus in which all communications over the session bus can be secured, signed, encrypted or otherwise protected. For example, the session bus can be further protected by storing all software (e.g., software components, applications and/or agents) in secure memory, storing all software in encrypted form in secure memory, and/or executing all software and communications within a secure execution environment, hardware environment and/or protected memory space. In some embodiments, if the agents and other functions are designed with a mixture of software and hardware, or primarily with hardware, then the implementation of the bus design will vary, and the principles and embodiments described herein

will enable one of ordinary skill in the art to design the specifics of the agent communication bus 1630 to meet a particular set of product and desired functional requirements.

[0184] As shown in FIG. 16, an access control integrity agent 1694 collects device information on service policy, service usage or service activity, agent configuration and agent behavior. In some embodiments, the access control integrity agent 1694 also cross checks this information to identify integrity breaches in the service policy implementation and control system. In some embodiments, the access control integrity agent 1694 also initiates action when a service policy violation or a system integrity breach is suspected. In some embodiments, the access control integrity agent 1694 also performs asynchronous or periodic agent checks to verify presence, configuration or proper operation of other agents. In some embodiments, the access control integrity agent 1694 also performs challenge-response sequence verification of other agents.

[0185] In some embodiments, the access control integrity agent 1694 obtains service usage or service activity measures from a service monitor agent 1696 and compares one or more first service usage measurement points against one or more second service usage measurement points to verify service policy implementation. For example, as shown in FIG. 21, if the service usage at measurement point IV is inconsistent with measurement point III, which, for example, can indicate, for example, that an unauthorized or unmonitored usage of the access modem (e.g., modems 2122, 2123, 2124, 2125 or 2141) is taking place. As another example, as also shown in FIG. 21, if one or more aspects of upstream traffic usage measurement point II, which represents the upstream demand side of policy implementation agent 1690, is inconsistent with upstream traffic measurement point III, which represents delivered traffic from the policy implementation agent 1690, then the policy implementation agent 1690 may not be operating properly. As another example, as also shown in FIG. 21, if service measurement point III and IV indicate that firewall agent 1655 is passing traffic to URLs or IP addresses that are in the blocked policy settings, then a verification error condition can be set for the access control policy. As another example, if the policy controller reports traffic usage statistics that are inconsistent with traffic usage policy settings, then a traffic usage policy verification error may have occurred. As another example, if the service usage counter synchronization information received from the service controller 122, the device service history 1618 and/or the central billing system 1619, is

compared to the service usage history reported by the service monitor agent and the two are found to be outside of acceptable tolerance limits for the comparison, then there may be a verification error in the service monitor service usage or service activity accounting. There are numerous additional embodiments of such comparisons as described herein and others as will be readily apparent to one of ordinary skill in the art given the principles, design background and specific examples and various embodiments described herein.

[0186] In some embodiments, device service policy implementations are verified by comparing various service usage measures used at the device against expected service usage or service activity behavior given the policies (e.g., one or more service policy settings, service profile or service profile settings for network based access/services, and/or service plan or service plan for network based access/services). For example, verification is performed based on a measure of total data passed at the device as compared to the service policy for total data usage. For example, verification is performed based on a measure of data passed in a period of time at the device as compared to the service policy for data passed in such a period of time. For example, verification is performed based on a monitoring of communications from the device based on IP addresses as compared to the policy for permissible IP addresses. For example, verification is performed based on a measure of total data passed from the device per IP address as compared to the policy for total data usage per IP address. Other examples include such actual versus policy comparisons based on other measures at/from/to the device, such as location, downloads, email accessed, URLs, and/or any other data, location, application, time or other criteria or any combination of criteria that can be measured for comparing with various policy settings and/or restrictions.

[0187] In some embodiments, the access control integrity agent 1694 monitors agent self-check reports to verify that agents are properly configured. In some embodiments, the access control integrity agent 1694 reports the agent self check reports to the service controller 122. In some embodiments, the access control integrity agent 1694 performs a role in service usage test transmission, reception and/or monitoring, with the usage test being tailored to test monitoring or control aspects for any subset of service activities. In some embodiments, the access control integrity agent 1694 performs a role in billing test event generation and/or monitoring. In some embodiments, the access control integrity agent 1694 checks and reports the result of service

usage monitoring verification tests, service usage billing verification tests and/or transaction billing verification tests.

[0188] In some embodiments, the access control integrity agent 1694 receives agent access attempt reports to determine if unauthorized agent access attempts are occurring. In some embodiments, the access control integrity agent 1694 acts as a central secure communications hub for agent to agent or service controller 122 to agent communication. For example, the access control integrity agent 1694 can be used so that no other software or function can access other agents or so that agents cannot access other agents except through the secure point to multipoint communications hub. In some embodiments, this approach further enhances compromise resistance for the agents. In some embodiments, some or all of the agent communications, including agent to agent or service controller 122 to agent communications, and possibly including unauthorized attempts to communication with agents, are monitored and logged so that a trace log of some or all agent communications can be maintained. For example, the agent communication trace log can be summarized and/or compressed for transmission efficiency or regularly reported, such as through the heartbeat function, or the agent communication trace log can be reported only when the service controller 122 requests the agent communication trace log or when there is a verification error event. As similarly described above, the partitioning of agent functions and server functions is provided herein mainly to aid in disclosing various embodiments but those of ordinary skill in the art will appreciate that other partitioning of agent functions and server functions can be used based on different design choices. For example, the central agent communication hub function is performed in some embodiments by the access control integrity agent 1694, however, in other embodiments that function is performed by the service control device link 1691. For example, when the central agent communication hub function is located in the service control device link 1691, then architecturally the device link can be a single point to multipoint secure communications hub for all agent to agent and service controller 122 to agent communications. In some embodiments, this approach has certain advantages from a service policy implementation verification or compromise protection robustness perspective, or has certain advantages from a communications protocol efficiency perspective, or simply can be more efficient to implement. It should be noted that in other embodiments described herein the agent to agent and agent to service controller 122 communications can be multipoint to multipoint, with each agent having the capability to

communicate with other agents or the service controller, this communication can be secure, signed or otherwise encrypted or protected in some embodiments and in the open/clear in others. Also, as discussed in some embodiments, the agents can maintain their own communications or attempted communications log, which can then be reported to the service controller 122. In some embodiments, the agents implement restrictions on which device components or agents the agents will conduct communications with so that only agents that need to communicate with one another can do so.

[0189] In some embodiments, the service control device link 1691 reviews local billing event history and compares such history to billing event reports to verify that a billing agent 1695 is functioning properly (e.g., has not been tampered with or compromised). In some embodiments, the service control device link 1691cross-checks service usage or service activity against billing event reports from the billing agent 1695 to verify that billing events are properly billing for service usage or service activity. In some embodiments, the service control device link 1691cross-checks transaction billing process or records against transaction billing reports to ensure that transaction billing events are being properly reported by the billing agent 1695. In some embodiments, the service control device link 1691 determines if one or more agents have been compromised, and if so, initiates a dynamic agent download process to replace any such potentially compromised agent.

[0190] In some embodiments, the access control integrity agent 1694 verifies that the service usage counter is reporting service usage or service cost to the user within acceptable limits of accuracy when compared to the service usage reports obtained from the service monitor agent 1696, the service controller 122, the device service history 1618 and/or the central billing system 1619. In some embodiments, the access control integrity agent 1694 checks to verify that user privacy filter preferences are being properly implemented. In some embodiments, the access control integrity agent 1694 checks to verify that the user is properly receiving UI warnings regarding service usage or roaming service usage conditions.

[0191] In some embodiments, the access control integrity agent 1694 checks to verify that the device is not beginning service usage until it has been authenticated, authorized or granted access to the network. In some embodiments, access control integrity agent 1694 checks

with the service controller 122 or the billing system 1619 to verify that the user or device has a valid service standing and should be admitted to access on the network.

[0192] In some embodiments, an Activation Tracking Service (ATS) is provided in which the service monitoring function (e.g., performed by the service monitor agent 1696 and/or some other agent/component or combinations thereof on the device) is used in part to determine which access networks are being connected to and to record and/or report this information. In some embodiments, the ATS is only enabled if the device user approves reporting of access networks connected to by the user device. In some embodiments, the ATS is protected from tampering. For example, the ATS can be hardened, that is, to be more tamper resistant, using a variety of techniques, including any of the following: the ATS can be located (e.g., stored) in secure memory and/or secure hardware; the ATS can be implemented in the system BIOS, the access modem and/or another hard to access portion of the device; a second device agent can confirm the presence of the ATS with a report to a network based server; the second agent or the network server can initiate a reinstall of the ATS if it is missing or is found to be operating improperly; and/or the ATS can be placed in a secure area of the OS so that it cannot be removed or if removed must be replaced for proper device operation to resume. A variety of other tamper resistance techniques can also be used to protect the ATS from tampering as similarly described herein with respect to other device based functions/software components/agents.

[0193] In some embodiments, the access control integrity agent 1694 verifies that ATS software or hardware is present, properly configured or operating properly. In some embodiments, the access control integrity agent 1694 reviews network connection or activity history and compares such to ATS reports to verify activation tracking service reports are occurring properly. In some embodiments, the access control integrity agent 1694 replaces ATS software if it has been removed. In some embodiments, the access control integrity agent 1694 monitors access or compromise of ATS software to determine if it may have been compromised. In some embodiments, the access control integrity agent 1694 reports status of ATS functions.

[0194] In some embodiments, the access control integrity agent 1694 scans the local agent execution environment to determine if there are unauthorized accesses to service processor functions, settings or code. In some embodiments, the access control integrity agent 1694

monitors software loading activity, protected memory access or communication with service processor 115 agents to detect unauthorized changes to service processor software or configuration. For example, the access control integrity agent 1694 can have a local database of potentially malicious elements and compare entries in the database against the elements detected locally. As another example, the access control integrity agent 1694 can communicate a list of some or all of the elements detected locally to the service controller 122 to augment or take the place of the database comparison function that may be performed locally. In some embodiments, the access control integrity agent 1694 detects new software downloads, installs or invocations and immediately issues an error flag report when potentially malicious software is downloaded, installed or invoked. In some embodiments, the access control integrity agent 1694 scans the local software loading and invocation activity along with a log of other software runtime events and regularly reports this trace so that when an error or compromise event occurs the trace preceding the event can be analyzed to determine the offending software or activity trace that took place to cause the compromise or error. Once the software or activity that caused the compromise is known, it can be entered into a refreshed version of the database that the device and other devices use to detect potentially malicious pre-cursor conditions. Examples of such pre-cursor events include software invocations, software downloads, attempts to uninstall certain agent and/or application software/components or OS components, a sequence of memory I/O events, a sequence of software access events, a sequence of network address or URL communications or downloads or a sequence of access modem I/O activity. In various other embodiments of the access control integrity agent 1694, the agent performs or (securely) communicates with other software/hardware device/network components that perform other well known signature, behavior blocking and/or intrusion detection identification/detection and/or blocking techniques based on the presence of potentially unwanted and/or potentially or known malicious software and/or intrusion attempts by unauthorized software and/or unauthorized users, using, for example, real-time, on access, periodic, and/or on demand scanning.

[0195] In some embodiments, the access control integrity agent 1694 detects or blocks potentially compromising behavior of other software programs/users attempting unauthorized behavior in the service processor 115 operating environment. In some embodiments, the access control integrity agent 1694 detects software that is being loaded that has the same or similar name, identification, memory location or function as one or more of the service processor 115

agents. In some embodiments, the access control integrity agent 1694 blocks operation or loading of such software. In some embodiments, the access control integrity agent 1694 detects or blocks unauthorized access of service processor 115 protected memory. In some embodiments, the access control integrity agent 1694 verifies configuration and operation of secure service downloader 1663. In some embodiments, the access control integrity agent 1694 monitors network and I/O activity to detect potentially compromising events, such as a program that is downloaded from known detrimental or potentially suspect IP addresses or URLs or a program that accesses certain IP addresses or URLs. In some embodiments, the access control integrity agent 1694 scans of the service processor operating environment are recorded and kept for a period of time, and if a service policy verification error occurs, then the scans immediately prior to the error are analyzed or reported to the service controller 122 for analysis. In some embodiments, such scans are regularly reported to the service controller 122 without the presence of service policy verification error conditions.

[0196] In some embodiments, the access control integrity agent 1694 requests a dynamic agent download of certain critical service processor functions, including in some cases the access control integrity agent 1694 on a periodic basis, or on a periodic basis when network access activity is not required or minimal.

[0197] In some embodiments, the access control integrity agent 1694 determines if a threshold has been surpassed for a max usage trigger for ambient and/or other services that should not be using significant amounts of data (e.g., based on the type of device and/or service profile settings).

[0198] In some embodiments, the access control integrity agent 1694 determines if verification errors exist in one or more of the verification process embodiments and, in some embodiments, reports errors immediately or in the next agent heartbeat to the service controller 122. In some embodiments, any number of results from the above checks, monitoring activities, reports or tests are reported to the service controller 122.

[0199] In some embodiments, a policy control agent 1692 receives policy instructions from the service controller 122 and/or the user via the billing agent 1695 and adapts device service policy settings (e.g., instantaneous device service policy settings) in one or more of the

following agents/components: a policy implementation agent 1690, the modem firewall 1655 and/or an application interface agent 1693. As shown in FIG. 16, the modem firewall 1655 is in communication with a modem driver 1640, which is in communication with the agent communication bus 1630 and access network 1610. As shown with respect to access network 1610, a central billing server 1619, an access network AAA server 1621 and device server history 1618 are also provided. As shown, the Internet 120 is accessible via the access network 1610 and firewall 124, from which device 100 can then access various Internet services 1615.

[0200] In some embodiments, the policy control agent 1692 adapts low level service policy rules/settings to perform one or more of the following objectives: achieve higher level service usage or cost objectives, reduce network control channel capacity drain, reduce network control plane server processing bandwidth, and/or provide a higher level of user privacy or network neutrality while satisfying service usage or service activity objectives. In some embodiments, the policy control agent 1692 performs a policy control function to adapt instantaneous service policies to achieve a service usage objective. In some embodiments, the policy control agent 1692 receives service usage information from the service monitor agent 1696 to evaluate service usage history as compared to service usage goals. In some embodiments, the policy control agent 1692 uses service monitor 1696 service usage or service activity history and various possible algorithm embodiments to create an estimate of the future projected service usage. In some embodiments, the policy control agent 1692 uses a future projection of service usage to determine what service usage or service activity controls need to be changed to maintain service usage goals. In some embodiments, the policy control agent 1692 uses service usage history to perform a service usage or service activity analysis to determine the distribution of service usage across service usage elements within categories, such as usage by application, usage by URL, usage by address, usage by content type, usage by time of day, usage by access network, usage by location, and/or any other categories for classifying service usage. In some embodiments, the policy control agent 1692 uses the service usage distribution analysis to determine which service usage elements or service activities are creating the largest service usage (e.g., if e-mail, social networking, or multimedia/online video application categories are creating the largest service usage).

[0201] In some embodiments, the policy control agent 1692 is instructed, for example, by the user, through billing agent 1695 to perform a service control algorithm, such as traffic shaping or download management, to manage service usage or service activities to assist the user in controlling service costs. As a basic example of such a traffic shaping algorithm, the traffic shaping algorithm can simply reduce traffic speed for all applications and traffic types successively until the service usage projections are within service usage limits for the present service billing period. To illustrate an algorithm that is more sophisticated and provides the advantage of leaving many service usage elements or service activities unaffected while only controlling down usage on the most aggressive service usage elements or service activities, the traffic shaping algorithm can identify the highest traffic usage applications and/or websites and successively reduce traffic speed just for the highest usage applications and/or websites until the service usage projections are within service usage limits for the present service billing period. These examples thereby reduce network traffic for the user in accordance with the user's service usage objectives while maintaining overall satisfactory service usage experience for the user in a manner that satisfies various net neutrality requirements (e.g., the traffic throttling of certain applications/websites based on user input in which categories based on service usage history are selected by the user, for example, a certain application may be using 90% of the aggregate traffic usage). For example, adaptive throttling algorithms can be used to throttle application traffic that the user requests throttling, such as recursively throttling of the specified application traffic (e.g., to denigrate the traffic usage associated with that application and thereby reduce overall service data usage).

[0202] In some embodiments, the policy control agent 1692 adjusts service policy based on time of day. In some embodiments, the policy control agent 1692 obtains a measure of network availability and adjusts traffic shaping policy settings based on available network capacity. In some embodiments, the policy control agent 1692 automatically and dynamically adjusts service policy based on one or more other service policy settings, the service profile and/or the service plan associated with the device and/or user of the device.

[0203] In some embodiments, various lower level service policy implementation embodiments are combined with a higher level set of service policy supervision functions to

provide device assisted verifiable network access control, authentication and authorization services.

[0204] In some embodiments, device based access control services are extended and combined with other policy design techniques to create a simplified device activation process and connected user experience referred to herein as ambient activation. In some embodiments, ambient access generally refers to an initial service access in which such service access is in some manner limited, such as where service options are significantly limited (e.g., low bandwidth network browsing and/or access to a specific transactional service), limited bandwidth, limited duration access before which a service plan must be purchased to maintain service or have service suspended/disabled or throttled or otherwise limited/reduced/downgraded, and/or any other time based, quality based, scope of service limited initial access for the network enabled device. In some embodiments, ambient activation is provided by setting access control to a fixed destination (e.g., providing access to a portal, such as a web page (e.g., for a hotspot) or WAP (Wireless Application Protocol) page, that provides the user with service plan options for obtaining a service plan for the user desired access, such as the service plan options for data usage, service types, time period for access (e.g., a day pass, a week pass or some other duration), and costs of service plan(s)). In some embodiments, service data usage of the ambient activated device is verified using IPDRs (e.g., using the device ID/device number for the device 100 to determine if the device has been used in a manner that is out of plan for the service plan associated with the device 100, such as based on the amount of data usage exceeding the service plan's service data usage limits, out of plan/unauthorized access to certain websites, and/or out of plan/unauthorized transactions). In some embodiments, service data usage of the ambient activated device is verified by setting a maximum data rate in the policy control agent 1692 and if/when it is determined that the device is exceeding a specified data rate/data usage, then the service data usage is throttled accordingly. In some embodiments, various other verification approaches are used for ambient activation purposes.

[0205] In some embodiments, the policy control agent 1692 (and/or another agent/component of the service processor 115 and/or service controller 122) performs a service control algorithm to assist in managing overall network capacity or application QoS (Quality of Service). In some embodiments, the policy control agent 1692 (and/or another agent/component

of the service processor 115) performs an access network selection algorithm to determine which access network to connect to based on connection options and determined strengths of available wireless networks, network preference or security settings, service usage cost based network preferences, and/or any other criteria.

[0206] Accordingly, as described herein with respect to various embodiments, service usage or service activities can be measured by various agents at various different measurement points, which provides for a more robust verification and integrity of device based services communication. For example, it is much less likely and more difficult to compromise and/or spoof multiple agents. As described herein, various verification and integrity checks are performed, including, for example, network based service usage measurement (e.g., using IPDRs); heartbeat monitoring; agent based heartbeat (e.g., challenge/response queries); agent operating environment protection; monitoring agent communications; agent cross-checks; comparing device based and network based measures (e.g., service usage measures); dynamic software/agent download; and/or any combination of these and various other verification/integrity check techniques described herein and/or apparent from the various embodiments described herein.

[0207] In some embodiments, the device 100 is capable of connecting to more than one network and device service policies are potentially changed based on which network the device is connected to at the time. In some embodiments, the network control plane servers detect a network connection change and initiate the service policy implementation established for the second network. In some embodiments, the device based adaptive policy control agent, as described herein (e.g., policy control agent 1692), detects network connection changes and implements the service policies established for the second network.

[0208] In some embodiments, when more than one access network is available, the network is chosen based on which network is most preferred according to a network preference list or according to which network that optimizes a network cost function. For example, the network preference list can be pre-established by the service provide and/or the user and/or later modified/adjusted by either the service provider and/or the user. For example, the cost function can be based on determining a minimum service cost, maximum network performance, whether

or not the user or device has access to the network, maximizing service provider connection benefit, reducing connections to alternative paid service providers, and/or any other cost related criteria for network selection purposes.

[0209] In some embodiments, the device 100 detects when one or more preferred networks are not available, implements a network selection function or intercepts other network selection functions, and offers a connection to the available service network that is highest on a preference list. For example, the preference list can be set by the service provider, the user and/or the service subscriber. In some embodiments, a notification is provided to the device/user when the device is not connected to a network (e.g., indicating in a pop-up/bubble or other UI based display a notification, such as "You are not connected to the network. Click here to learn more, get free trial, use a session, sign-up for service"). In some embodiments, the notification content can be determined based on usage service patterns, locally stored and/or programmable logic on the device and/or a server (e.g., device reports that user is not connected and WWAN is available). Decisions on what bubble to present when may be in pre-stored logic on device.

[0210] In some embodiments, service policies are automatically adapted based on the network to which device 100 is connected. For example, the device can be a cellular communication based device connected to a macrocell, a microcell, a picocell, or a femtocell (e.g., femto cells generally provide a low power, small area cellular network used, for example, in homes or offices, which, for example, can be used as an alternative to Wi-Fi access). In some embodiments, service monitoring agent 1696 and/or billing agent 1695 modify service usage counting and/or billing based on whether the device is connected to a macrocell, microcell, picocell or femtocell. In some embodiments, the device recognizes which type of network it is currently connecting to (e.g., looking up in a local or network table for the current base station connected to, and/or the information is broadcast to the device upon the connection with the base station), that is, whether it is a macrocell, microcell, picocell or femtocell. In other embodiments, the device does not recognize which type of network it is currently connected to, but reports its current base station, and the network uses a network lookup function to determine which type of network it is connected to. In some embodiments, the device adjusts the billing based on the type of network it is connected to, or in other embodiments, the device calculates an offset to such billing based on the type of network it is connected to, and/or in other

embodiments, the device records such service usage associated with the type of network it is connected to and the network billing can adjust the billing accordingly. For example, the billing can be lower for service data usage over a femtocell versus a macrocell. In some embodiments, service policies are adjusted based on the type of network that the device is connected, such as billing, user notification, data usage/bandwidth, throttling, time of day, who owns the cellular network connection (e.g., user's home femtocell, or user's work femtocell, or a commercial business's femtocell like a coffee shop or any other common area like an airport) and/or any other service policy can be different for a femtocell connection (or for any other type of connection, such as a macrocell, microcell, or picocell). In some embodiments, the local service usage counter is adjusted based on the type of network (and/or based on the time of day of such service activity) that the device is connected, such as billing, user notification, data usage/bandwidth, and/or any other service policy can be different for a femtocell connection (or for any other type of connection, such as a macrocell, microcell, or picocell). In some embodiments, the service policies and/or billing policies are adjusted based on network congestion.

[0211] In some embodiments, if adaptive service policy control is not required, then the policy control agent 1692 can simply pass instantaneous service policy settings directly to the agents responsible for implementing instantaneous service policies.

[0212] In some embodiments, a policy implementation agent 1690 implements traffic shaping and QoS policy rules for the device 100. In some embodiments, the policy implementation agent 1690 provides a firewall function. In some embodiments, the policy implementation agent 1690 performs traffic inspection and characterization. In some embodiments, packet inspection is aided by literal or virtual application layer tagging while in other embodiments packet inspection is performed entirely in/by the policy implementation agent 1690. In some embodiments, the policy implementation agent 1690 accepts service policy implementation settings from the policy control agent 1692 or directly from the service controller 122. More detail on specific embodiments for the policy implementation agent 1690 is provided below with respect to the figures associated with communication stack and communication protocol flow.

[0213] In some embodiments, the burst size, buffer delay, acknowledgement delay and drop rate used in upstream and downstream traffic shaping are optimized with the goal of reducing access network traffic overhead, and excess capacity usage that can result from mismatches in traffic transmission parameters with the access network MAC and PHY or from excess network level packet delivery protocol re-transmissions. In some embodiments, the application interface agent 1693 is used to literally tag or virtually tag application layer traffic so that the policy implementation agent(s) 1690 has the necessary information to implement selected traffic shaping solutions. As shown in FIG. 16, the application interface agent 1693 is in communication with various applications, including a TCP application 1604, an IP application 1605, and a voice application 1602.

[0214] In some embodiments, downstream literal or virtual application tagging are delayed until a traffic flow passes through the service policy implementation functions and to the application interface function where the service flow is then identified and associated with the underlying traffic and application parameters, and the literal or virtual tag is then communicated to the first policy implementation function or service monitoring function in the downstream traffic processing stack. In some embodiments, prior to being associated with a literal or virtual tag, the traffic flow is allowed to pass with no traffic shaping, and once the traffic flow is identified and tagged, the appropriate traffic shaping is applied. In some embodiments, a set of traffic shaping policy parameters are applied to the unidentified traffic flow before the flow is identified, and then the traffic shaping policy for the flow is updated when the flow is tagged. In some embodiments, the traffic flow can be blocked at the application interface agent even before the tag is passed to the policy implementation functions if it is found to be associated with traffic parameters that are blocked by policy once packet processing, framing and encryption are removed.

[0215] In some embodiments, a service monitor agent 1696 records and reports device service usage or service activities of device 100. In some embodiments, service usage history is verified by a number of techniques including verifying against network based service usage history (e.g., device service history 1618) and the various service policy implementation techniques as described herein.

[0216] In some embodiments, the service monitor agent 1696 includes the capability to filter service usage history reporting with the decision on which aspects of service history to report being determined by policies including possibly privacy policies defined by the device user or control plane servers in the network. In some embodiments, the service monitor agent 1696 monitors and possibly records or reports Customer Resource Management (CRM) information such as websites visited, time spent per website, interest indications based on website viewing, advertisements served to the device, advertisements opened by the user, location of the user, searches conducted by the user, application usage profile, device user interface usage history, electronic commerce transactions, music or video files played, applications on device, and/or when the user is actively working or playing or inactive. In some embodiments, to protect the privacy of this user CRM information, the user is provided with options on how much of the information to share and the user's response to the options are recorded and used to determine the filtering policy for how much of the CRM data to report (e.g., CRM filter level options selected by the user via the device UI and/or via various service plan or service profile or service policy options) and how much to suppress or to not even monitor/record/store in the first place. In some embodiments, to protect the privacy of this user's GPS/location tracking related information, the user is provided with options on how much of the information to share and the user's response to the options are recorded and used to determine the filtering policy for how much of the GPS/location tracking related data to report (e.g., GPS/location tracking filter level options) and how much to suppress or to not even monitor/record/store in the first place. In some embodiments, the service processor 115 allows the user to provide feedback on the user's preferences, such as for privacy/CRM data to report. In some embodiments, the user can also specify their preference(s) for notification (e.g., related to service usage/cost, traffic reporting and other service usage/monitored information) and/or service controls. In some embodiments, the service monitor agent 1696 observes and possibly records or reports service usage categorized by network possibly including roaming networks, paid service networks or free service networks. In some embodiments, the service monitor agent 1696 observes and possibly records or reports service usage categorized by sub-accounts for various types of traffic or various types of network.

[0217] For example, service monitor reports can be provided to the service controller 122. Service is monitored through various embodiments that can involve service usage logging

or traffic inspection and usage logging at the application level, various levels in the networking communication stack or the access modem. Some embodiments involve multiple levels of service or traffic measurement at various levels in the communications stack as described further below.

[0218] In some embodiments, service or traffic monitoring includes monitoring one or more of the following: traffic associated with one or more users; traffic downstream and/or upstream data rate; total traffic received and/or transmitted over a period of time; traffic transmitted and/or received by IP addresses, domain names, URLs or other network address identifiers; traffic transmitted and/or received by email downloads or uploads; traffic transmitted and/or received by an application; traffic transmitted and/or received by network file transfers; traffic transmitted and/or received by file download or upload content types; traffic transmitted and/or received by mobile commerce transactions; traffic transmitted and/or received by one or more time periods; traffic transmitted and/or received by differing levels of network activity and network capacity availability; traffic transmitted and/or received by one or more delivered levels of quality of service; traffic transmitted and/or received by software downloads; traffic transmitted and/or received by application downloads; traffic transmitted and/or received by one or more activities associated with the service control plane link or other network related functions, or traffic that may not directly result in service usage or service activity that the user values or desires; traffic transmitted and/or received to support one or more service provider third party service partner offerings; software usage history; application usage history; device discovery history for UI components, applications, settings, tutorials; ads served history; ads visited history; and/or device location history.

[0219] In some embodiments, some or all of the service usage monitoring occurs at the application layer. In some embodiments, the service monitor agent 1696 implements traffic inspection points between the applications and the networking stack application interface, such as the sockets API. In other embodiments, the application interface agent 1693 performs traffic inspection and reports the results to the service monitor agent 1696. Traffic inspection can be accomplished in several ways, including, for example, implementing a T-buffer at each socket connection and feeding the side traffic into a traffic flow analyzer, which in combination with a mapping of application to socket provides much of the information listed above. In cases in

which it is necessary to obtain traffic information from the application itself, some embodiments call for the application to be adapted to provide the information to either the application interface agent 1693 or the service monitor agent 1696. As an example, the application interface agent 1693 or the service monitor agent 1696 can monitor and decode advertisements downloaded via HTTP, but if the browser and HTTP server employ security above the sockets protocol stack layer then the application interface agent can communicate with the browser via a java applet or some other inter-process communication method. In some embodiments, the service monitor agent 1696, the billing agent 1695 and/or the policy control agent 1692 (or some other software or hardware function on the device) can monitor and/or control (e.g., allow, block and/or replace) advertisement traffic flow into the device. In some embodiments, the monitoring and control of advertisement traffic flow into the device is also used for bill by account purposes (e.g., charges, such as service charges, billed to the advertiser, sponsor, and/or service or transactional service provider).

[0220] In some embodiments, some or all of the service usage monitoring occurs below the application interface for the networking stack. In this case, some portion of the information listed above may not always be available due to encryption applied at the higher layers and/or the computational costs associated with performing deep packet inspection on mobile devices.

[0221] In some embodiments, the service monitor agent 1696 is also monitors the operating software install or loading systems, and/or otherwise monitors software installs or loads and/or software uninstalls/deinstallations.

[0222] Some of the information above may be considered by some users, advocacy groups or agencies as customer sensitive personal information. Simply sending the above information to the network for unspecified purposes may not, therefore, be acceptable for some service providers. However, if the user provides specific approval (e.g., informed consent) for the device, network or service provider to use some or all of the information that may be sensitive for specified purposes, then the user can control the level of information that is used and the purpose the information is used for. Accordingly, various embodiments described herein provide the user with control of what information is used and the purposes it is used for thereby allowing the user adequate control of any such sensitive information. In some embodiments,

information that is thought to perhaps be sensitive and is reported to the network must first receive user approval for the reporting. Some basic information is generally not considered sensitive and is necessary for certain basic service provider needs. For example, total data transmitted and/or received, traffic downstream and/or upstream speed, overall traffic usage by time of day are generally not considered private from the service provider's perspective and are necessary in many basic service policy implementations. As additional examples, perhaps other service usage history, such as total traffic email downloads and uploads but not the type of files or any specifics about the email traffic, the total web browsing traffic but nothing specific about the sites visited or content viewed, total file transfer traffic but not the type of files transferred or the addresses involved in the transfer, and other examples may not be viewed as private and, in some embodiments, provide valuable information for the service provider to manage services. Conversely, information such as websites visited, content viewed, mobile commerce transactions completed, advertisements visited, GPS location history and other service usage history the service monitor is capable of recording may be sensitive or private for some users and would thereby benefit from the various embodiments that provide enhanced user control of the reporting of such potentially sensitive or private data. It should also be appreciated that there is an inherent advantage to implementing traffic monitoring, traffic, service monitoring or service control on a device, because it is not necessary to report sensitive information to the network to accomplish many of these service policy implementation objectives.

[0223] In some embodiments, the service monitor agent 1696 assists in virtual application tagging of traffic flows through the networking stack policy implementation by tracking the virtually tagged packets through the stack processing and communicating the flow tags to the service policy implementation agent(s) 1690. In some embodiments, the service monitor agent 1696 maintains a history and provides reports or summary reports of which networks in addition to the networks controlled by the service controller 122 to which the device has connected. In some embodiments, this network activity summary includes a summary of the networks accessed, activity versus time per connection, and/or traffic versus time per connection. In some embodiments, the traffic reports that go to the network, possibly to service controller 122, billing system 1619 and/or device service history 1618, are first filtered according to rules defined by user preference selection at the time of service activation (e.g., service plan/service plan option selection), time of first device use, at a time the user selected the option on the

service UI or at a time the user chose to change the option on the service UI or some other time/mechanism allowing for user preference selection.

[0224] In some embodiments, the service monitor agent 1696 monitors application usage (e.g., which application the user executes on the device 100, such as e-mail applications, web browsing applications and/or media content streaming applications). In some embodiments, the service monitor agent 1696 monitors multimedia file usage (e.g., based on multimedia file type and/or based on specific multimedia files, such as specific movies and/or songs). In some embodiments, the service monitor agent 1696 monitors the device user interface, application, and content discovery history (e.g., monitoring which applications/content the user accesses from the device, including monitoring the pattern by which the user accesses such applications/content, such as how the user navigates the user interface on the device to access such applications/content and maintaining such patterns and history, such as which icons the user access on a home page, secondary or other portion/mechanism on the device for accessing various applications/content). In some embodiments, the service monitor agent 1696 monitors advertisements provided to the user on the device 100. In some embodiments, the service monitor agent 1696 monitors advertisements viewed (e.g., accessed, such as by clicking on a web advertisement) by the user on the device 100. In some embodiments, the service monitor agent 1696 monitors GPS/location information for the device 100. As will be appreciated by those of ordinary skill in the art, the service monitor agent 1696 can monitor a wide variety of activities performed by the device/user of the device and/or based on other information related to the device 100 such as GPS/location information. As described herein, in some embodiments, the user of the device 100 can also specify which activities that the user authorizes for such monitoring (e.g., the user may prefer to not allow for such GPS/location monitoring).

[0225] In some embodiments, the application interface agent 1693 provides an interface for device application programs. In some embodiments, the application interface agent 1693 identifies application level traffic, reports virtual service identification tags or appends literal service identification tags to assist service policy implementation, such as access control, traffic shaping QoS control, service type dependent billing or other service control or implementation functions. In some embodiments, the application interface agent 1693 assists with application layer service usage monitoring by, for example, passively inspecting and logging traffic or

service characteristics at a point in the software stack between the applications and the standard networking stack application interface, such as the sockets API. In some embodiments, the application interface agent 1693 intercepts traffic between the applications and the standard network stack interface API in order to more deeply inspect the traffic, modify the traffic or shape the traffic (e.g., thereby not requiring any modification of the device networking/communication stack of the device OS). In some embodiments, the application interface agent 1693 implements certain aspects of service policies, such as application level access control, application associated billing, application layer service monitoring or reporting, application layer based traffic shaping, service type dependent billing, or other service control or implementation functions.

[0226] In some embodiments, application layer based traffic monitoring and shaping can be performed as described below. The traffic from each application can be divided into one or more traffic flows that each flow through a traffic queue, with each queue being associated with one or more additional classifications for that application (e.g., the application can be a browser that is associated with multiple queues representing different destinations or groups of destinations it is connected to, with each destination or group of destinations having potentially different access control or traffic control policies, or the application can be associated with different content types or groups of content types with each content type having different queues, the application might be an email program with email text traffic going to one queue and downloads going to another with different policies for each). In some embodiments, queues are formed for all applications or groups of applications that are associated with one or more traffic parameters such as destination, content type, time of day or groups of applications can be similarly assigned to different queues. The functions performed by the application layer queues can be similar to the functions described for the policy implementation agent, such as pass, block, buffer, delay, burst in order to control the traffic or network access associated with the queue. The drop function can also be implemented, such as for application layer protocols that include reliable transmission methods, but if the application layer protocol does not involve reliable retransmission of lost information this can result in lost data or unreliable communication which may be acceptable in some cases. The manner in which the queues are controlled can be constructed to result in a similar approach for controlling services or implementing service activity control similar to the other embodiments described herein,

including, for example, the policy control agent 1692 implementing an higher layer of service control to achieve a higher level objective as discussed herein.

[0227] In some embodiments, the application interface agent 1693 interacts with application programs to arrange application settings to aid in implementing application level service policy implementation or billing, such as email file transfer options, peer to peer networking file transfer options, media content resolution or compression settings and/or inserting or modifying browser headers. In some embodiments, the application interface agent 1693 intercepts certain application traffic to modify traffic application layer parameters, such as email file transfer options or browser headers. In some embodiments, the application interface agent 1693 transmits or receives a service usage test element to aid in verifying service policy implementation, service monitoring or service billing. In some embodiments, the application interface agent 1693 performs a transaction billing intercept function to aid the billing agent 1695 in transaction billing. In some embodiments, the application interface agent 1693 transmits or receives a billing test element to aid in verifying transaction billing or service billing.

[0228] In some embodiments, a modem firewall 1655 blocks or passes traffic based on service policies and traffic attributes. In some embodiments, the modem firewall 1655 assists in virtual or literal upstream traffic flow tagging. Although not shown in FIG. 16, in some embodiments, the modem firewall 1655 is located on either side of the modem bus and in some embodiments it is advantageous to locate it on the modem itself.

[0229] In some embodiments, the billing agent 1695 detects and reports service billing events. In some embodiments, the billing agent 1695 plays a key role in transaction billing. In some embodiments, the billing agent 1695 performs one or more of the following functions: provides the user with service plan options, accepts service plan selections, provides options on service usage notification policies, accepts user preference specifications on service usage notification policies, provides notification on service usage levels, provides alerts when service usage threatens to go over plan limits or to generate excess cost, provides options on service usage control policy, accepts choices on service usage control policy, informs policy control agent 1692 of user preference on service usage control policy, provides billing transaction options and/or accepts billing transaction choices. In some embodiments, the billing agent 1695

interacts with transaction servers (e.g., open content transaction partner sites 134) to conduct ecommerce transactions with central billing 1619.

[0230] In some embodiments, service processor 115 includes one or more service usage or service activity counters. For example, the service monitor agent 1696, billing agent 1695 or a combination of these agents and/or other agents/components of service processor 115 can include such a local service usage counter(s) for the device 100. In some embodiments, a service usage counter monitors service usage including data usage to/from the device 100 with the access network 1610. In some embodiments, the service usage counter periodically, in response to a user request, in response to a service processor 115 agent's request (e.g., the billing agent 1695, the policy control agent 1692, or another agent of service processor 115), in response to the service controller 122, and/or in response to the central billing 1619 (e.g., for billing purposes and/or for storing in the device service history 1618), provides a service usage report, including monitored service usage for the device 100. In some embodiments, the service usage counter periodically, or in response to a request, synchronizes the service usage counter on the device 100 with a network (and/or billing) service usage counter, such as that maintained potentially at central billing 1619. In some embodiments, service processor 115 utilizes the service usage counter to provide a service usage projection. In some embodiments, service processor 115 utilizes the service usage counter to provide a service usage cost estimate. In some embodiments, service usage projections from policy control agent 1692 are used to estimate the projected future service usage if user service usage behavior remains consistent. In some embodiments, service processor 115 utilizes the service usage counter to provide a cost of service usage, and the service processor 115 then periodically, or in response to a request, synchronizes the cost of service usage with, for example, the central billing 1619. In some embodiments, the service processor 115 utilizes the service usage counter to determine whether the user is exceeding and/or is projected to exceed their current service plan for data usage, and then various actions can be performed as similarly described herein to allow the user to modify their service plan and/or modify (e.g., throttle) their network data usage. In some embodiments, the service usage counter can support providing to the user the following service usage related data/reports: service usage, known usage and estimated usage, projected usage, present costs, projected costs, cost to roam, cost to roam options, and/or projected roaming costs. For example, including a local service data usage counter on the device 100 allows the service processor 115

to more accurately monitor service data usage, because, for example, network (and/or billing) service usage counters may not accurately also include, for example, control plane data traffic sent to/from the device 100 in their monitored service data usage count.

[0231] In some embodiments, verifiable device based service billing solutions are provided. For example, as described herein, various device based service billing solutions can include a wide range of verification techniques to ensure that the device is properly reporting service billing events (e.g., to verify/ensure that the service billing is not malfunctioning and/or has not been tampered with/compromised such that it is not accurately or timely providing service billing information). As described herein, service billing generally refers the billing for one or more services for a device, such as device 100 (e.g., email service billing for data usage associated with received/sent email related data over the access network 1610, web browsing service billing for data usage associated with received/sent web browsing related data over the access network 1610 and/or any other network based service, and/or any transactional based services, such as for multimedia content purchases or other transactions).

[0232] In some embodiments, verifiable device based service billing is provided by sending dummy(/test) billing events, such as having an access control integrity server 1654 of the service controller 122 instruct the access control integrity agent 1694 to send a dummy(/test) billing event to the billing agent 1695. If the billing agent does not then send the expected report, which should reflect the dummy(/test) (or fails to timely send any report), then the system can verify whether the billing process is working properly. In addition, a dummy (/test) transaction can be used to verify transaction based billing through a variety of approaches (e.g., the access control integrity agent 1694 can similarly send a dummy(/test) transactional billing event to the billing agent 1695 as a test to determine whether the billing agent 1695 then provides the expected report reflecting that dummy(/test) transaction). For example, the test billing events can be trapped by a device assisted billing mediation server and removed from the user account billing.

[0233] In some embodiments, verifiable device based service billing is provided by sending one or more data bursts to the device to confirm that data was received and to confirm that the service monitor agent 1696 properly logged the data burst(s) in the local service usage or

service activity counter. In some embodiments, data bursts can be used to verify data throttling (e.g., if the device has exceeded service data usage limits and/or is approaching such limits such that service data usage should be throttled, then sending data bursts can be used to verify whether the expected throttling is properly being performed on the device). In some embodiments, verifiable device based service billing is provided by submitting requests to connect to an unauthorized service/website to verify if that unauthorized service usage is properly blocked. In some embodiments, verifiable device based service billing is provided by submitting requests to perform an unauthorized transaction to verify if that unauthorized transaction is properly blocked.

[0234] In some embodiments, verifiable device based service billing is provided by verifying device service activities relative to IPDRs for the device. In some embodiments, the IPDRs for the device (possibly in a modified format) are periodically and/or upon request sent to the device, as described herein. For example, IPDRs for the device can be compared to the device's local service data usage counter and/or to the service plan for the device to determine if the overall service data usage limit has been exceeded, whether out of plan/unauthorized/unrecorded websites/other services have been performed by the device, whether service plan/profile bandwidth limits have been exceeded, whether out of plan/unauthorized/unrecorded transactions have been performed (e.g., verifying IPDR transaction logs, assuming such are included in the IPDRs, with the local transaction logs of the device to determine, for example, whether the local device records indicate that fewer than the network recorded number of content downloads, such as downloaded songs, were purchased), and/or whether any other activities verifiable based on a comparison of IPDRs indicate that the device has been used in any manner that is out of or exceeds the service plan/profile for the device.

[0235] In some embodiments, device based service billing includes recording billing option response history. For example, this approach can be particularly important for service plan overage conditions (e.g., when the use of the device is exceeding the service plan associated with the device in some manner, such as service data usage, bandwidth, service or transaction access and/or in some other manner). In some embodiments, in a service plan overage condition, the user is requested to confirm that user has acknowledged notification of service plan overage,

such as via the user interface 1697. In some embodiments, such service plan overage acknowledgements require that the user enter a unique identification to validate authorization by the user identity associated with the device (e.g., another type of verification mechanism, in the event a device is stolen or being used by someone other than the authorized user of the device, then that unauthorized user would not be able to confirm the service plan overage acknowledgement, and appropriate actions can then be taken, such as throttling, quarantining or (temporarily) suspending service/network access). In some embodiments, if the device is compromised/hacked (e.g., by the user of the device), and the device is used in a manner that results in a service usage overage (e.g., determined based on device assisted service usage monitoring, and/or network based service usage monitoring using IPDRs/CDRs), then the billing system determines billing for such service usage overage costs. This overage billing can be initiated by the device 100 (e.g., service processor 115), the service controller 122, the billing system 123, the AAA 121, or some other network function. In some embodiments, if the device is compromised/hacked (e.g., by a user of the device), and the device is used in a manner that results in a service usage overage, one or more of the following actions is taken: the user is notified, the user is required to acknowledge the notification, the device traffic is sent to SPAN (or similar traffic sampling and analysis function), and/or the device is flagged for further analysis.

[0236] In some embodiments, device based service billing includes an option to bill by account, such as to bill different service activities and/or transactions to a specified account (e.g., other than the user's account associated with the general service plan for the device). For example, bill by account can provide for billing according to application, content type, website, transaction, network chatter (e.g., heartbeat communications and/or other network traffic that is used by, for example, the central/service provider to generally maintain network access for the device), and/or transaction partner sponsored activities and then report such bill by account information for billing mediation/reconciliation. For example, a bill by account report can be sent by billing agent 1695 from the device to central billing 1619 (e.g., as a billing event); or alternatively, sent to an intermediate server/aggregator, which can then reformat and send the reformatted report to central billing 1619 (e.g., providing the billing report in a format required by central billing 1619); or alternatively, sent to a mediation server, which can re-compute the billing based on the bill by account report (e.g., offset the bill based on network chatter,

transaction based billing, transaction partner sponsored activities, content providers, website providers and/or advertising providers) and then send the recomputed (and potentially reformatted) report to central billing 1619.

[0237] In some embodiments, one or more of the mediation/reconciliation functions for device assisted billing, device generated billing events, device generated bill by account events and device generated open transaction billing events can be implemented in the service controller 122 (e.g., the billing event server 1662) or in another function located in the billing system 123 or elsewhere. This billing mediation server function accepts the device based billing events discussed immediately above, reformats the billing events into a format accepted and recognized by the billing system, mediates the billing event information to remove service usage billing from the user account and place it in other bill by account categories as appropriate according to the bill by account mediation rules, adds other billing events for service usage or transactions to the user account as appropriate according to the device based billing rules, and then applies the information to the billing information the user account to correct or update the account.

[0238] For example, a bill by account can allow for a website provider, such as Google or Yahoo, to pay for or offset certain account usage for web browsing, web based searching, web based email, or any other web based or other service usage activities, which may also be based (in whole or in part) on the activities performed by the user on such transactional services (e.g., based on advertisement viewing/accessing or click-through activities by the user, by which an advertisement business model used by such website providers directly or indirectly supports such service account subsidies). As another example, a bill by account can allow for an advertiser to pay for or offset certain account usage for viewing and/or accessing (e.g., clicking through) a web placed advertisement or other advertisement sent via the network to the device. As yet another example, various network chatter (e.g., heartbeat related network and other network chatter related service data usage) can be assigned to a dummy account and such can be used to offset the bill and/or used for tracking the data usage for such activities for the device. In another example, service data usage for access to a transactional service, such as a multimedia content download service (e.g., music, eBook, music/video streaming, and/or movie or other multimedia content download service), or an online shopping site (e.g., Amazon, eBay or another online shopping site), can be billed to a transactional service account assigned to a transactional

service partner that sponsors access to that sponsor's transactional service, thereby allowing that transactional service partner to pays for or offset (e.g., subsidize) the account usage for such activities, which may also be based (in whole or in part) on the transactions actually performed by the user on such transactional services (e.g., based on the volume/cost of the multimedia service download purchases by the user and/or online activities).

[0239] In some embodiments, device based service billing includes recording billing events on the device and then reporting such billing to the network (e.g., central billing 1619). In some embodiments, device based service billing includes reporting service usage events and/or applying cost look-up and logging/reporting service billing updates. For example, this allows for reporting not only service usage but also cost of such service usage to the user via the user interface of device 100. Also, for example, the cost of such service usage can also be reported to the billing server. In some embodiments, device based service billing includes reporting service usage to the network, and the network determines the cost for such service usage.

[0240] In some embodiments, billing information for roaming partners is provided. For example, a roaming server can include a roaming service cost data table for roaming service partners. In this example, when the device (e.g., device 100) connects to a roaming network provided by a roaming service partner, then the device can also receive the roaming service data rate based on the roaming service cost data table provided by the roaming server. Alternatively, the roaming server can send the roaming service cost data table (or a modified format of the same) to the device thereby allowing the device to determine the costs for such roaming network service usage or service activity. As described herein, the device can also automatically use a roaming service profile when connecting to the roaming network service and/or the user can be notified of the roaming service profile options based on the roaming service data costs and then select the desired roaming service profile accordingly.

[0241] In some embodiments, the user is provided with a list of service costs based on locally stored roaming table and a search of available roaming partners that the device 100 detects and can connect to. In some embodiments, the user is provided with a projected cost per day for one or more roaming service provider options based on typical service usage history and the cost for each service provider. In some embodiments, the user is provided with a set of

options for service usage notification, controlling or throttling service usage and/or cost while roaming (e.g., using the service notification and cost control techniques as similarly discussed herein but applied to the roaming network). In some embodiments, these controls are set by a VSP (or, e.g., an IT manager using VSP functions). In some embodiments, roaming tables are updated periodically in the background while on a home network (or other low cost network) and cached. In some embodiments, cache updates occur based on fixed time period (e.g., late at night when updates are less expensive due to network inactivity). In some embodiments, the roaming partner cost table cache updates are done whenever connected to a desirable network that is not as expensive or bandwidth constrained (e.g., at home, work, or off the WWAN). In some embodiments, updates occur at time of day that network is not busy. In some embodiments, updates occur based on network push when roaming table is changed (e.g., one or more of the roaming partners changes the rate). In some embodiments, the service cost to update the roaming service cost table is charged to bill by account and possibly not charged to end user. In some embodiments, the roaming service center is provided as a service that is paid for (e.g., potentially bill by account tracks all related costs). For example, this type of roaming cost control can be provided as a service through central provider, MVNO, roaming partner provider, VSP or as a third party application not associated with any service provider (e.g., IT manager). For example, the controls for how to update cache, set service control policies, and other controls can be defined by any number of VSP entities including the user through a website service.

[0242] In some embodiments, a roaming service center is provided as a service in which, for example, the user is provided with a list of service costs based on a locally stored (or remotely accessed) roaming table. In some embodiments, the roaming service center provides the user with a projected cost per day for one or more roaming service provider options based on typical service usage history and the cost for each service provider. In some embodiments, the roaming service center provides the user with a set of options for controlling/throttling usage and/or cost while roaming. In some embodiments, these controls are set by a VSP (e.g., an IT manager using VSP functions). For example, roaming tables can be updated periodically in the background while on a home network and cached. In some embodiments, cache updates occur based on a fixed time period. In some embodiments, the roaming partner cost table cache updates are done whenever the device is connected to a desirable network that is not as

expensive or bandwidth constrained (e.g., at home, work and/or off the WWAN). In some embodiments, updates occur at time of day that network is not busy. In some embodiments, updates occur based on a network push when a roaming table is changed (e.g., one or more of the roaming partners changes the rate). In some embodiments, the service cost to update the roaming service cost table is charged to bill by account and possibly not charged to the user. In some embodiments, the roaming service center is provided as a service that is paid for by the user and/or part of a service plan. In some embodiments, a bill by account function tracks all related costs. For example, the roaming service center can be provided as a service through central provider, MVNO, roaming partner provider, VSP or as a third party application not associated with any service provider (e.g., IT manager).

[0243] In some embodiments, a synchronized local service usage counter based on time stamped central billing information is provided. For example, the local service usage counter, as similarly described above, can also be synchronized to past service usage records (e.g., time stamped central billing records of service usage for the device) and use local estimates for current/present service usage estimates for the device. In this example, the central billing system (e.g., central billing 1619) can push the time stamped central billing information to the device (e.g., device 100), the device can pull the time stamped central billing information, and/or an intermediate server can provide a mediated push or pull process. In some embodiments, synchronization is performing periodically based on service usage levels with free-running estimates between synchronizations.

[0244] In some embodiments, service usage is projected based on calculated estimates of service usage based on synchronized service usage and local service usage count information. For example, projected service usage can be calculated on the device or calculated on a server (e.g., a billing server or an intermediate billing server), which provides the calculated projected service usage information to the device, such as using various adaptive algorithms for service usage projections. For example, an adaptive algorithm can use historical/past synchronized network service usage information (e.g., synchronized with local service usage data based on time stamps associated with IPDRs) to assist in service usage projections, based on, for example, total service usage count, service usage count by certain service related criteria (e.g., application, content, service type, website and/or time of day). In another example, an adaptive algorithm

synchronizes to past service usage data (e.g., the local estimate of past service usage data is updated to be synchronized up through the point in time associated with the latest IPDR time stamp that has been received) and current local estimates of service usage collected since the latest time stamp are then added to the time stamped IPDR service usage counter to minimize the service usage counter offset so that it is no greater than the difference between the network service usage measure and the local service usage measure since the latest IPDR time stamp. In some embodiments, these adaptive algorithm techniques are performed on the device and/or performed on the network (e.g., on a network server) for processing. In some embodiments, if there is an offset in the local device based service usage count between IPDR synchronization events and the IPDR service usage count between IPDR synchronization events, then an algorithm can be employed to estimate any systematic sources for the offset and correct the local service usage count to minimize the offsets. As an example, if the IPDR service usage count is typically off by a fixed percentage, either high or low, then an algorithm can be employed to estimate a multiplier that is applied to the local service usage count to minimize the offset between IPDR service usage synchronization events. In another example, there can be a consistent constant offset and a multiplier offset, both of which can be estimated and corrected for. Those of ordinary skill in the art will appreciate that more sophisticated algorithms can be employed to estimate the nature of any systematic offsets, including, for example, offsets that occur due to specific service usage activities or network chatter to manage the device, and such offsets can then be minimized between IPDR service synchronization events. In some embodiments, synchronized service usage data is used to create an improved analysis of the statistical patterns of service usage to provide more accurate service usage projections. Those of ordinary skill in the art will also appreciate that a variety of additional adaptive algorithm techniques can be used including those that provide for various statistical analysis techniques and/or other techniques.

[0245] In some embodiments, service usage is projected for the end of a billing/service period for a service plan versus the service usage allowed under the service plan for that billing/service period. A display of excess charges is also provided for the projected rate of service usage based on the monitored service usage behavior through the end of the billing/service period (e.g., this can be zero if the service usage is projected to be less than that allowed under the service plan and a positive cost number if it is projected to be more than the

service plan). For example, this can be implemented in numerous ways, such as on a server in the network, on a gateway/router/switch in the network, and/or on the device, as discussed below and generally described herein with respect to other service/cost usage monitoring and notification embodiments. If implemented in the network server or gateway/router/switch, then the service/cost usage projections and related information can be pushed to the device, or the device can be notified that such information is available to pull and/or periodically pushed/pulled. The service usage information/estimates can be collected from the device, the network or both (e.g., reconciled and/or synchronized) as similarly described herein. The service usage information/estimates are then analyzed to determine service usage/cost projects as similarly described herein and compared to the service plan for the device to determine the projected service/cost usage overage (if any). In some embodiments, one or more of the following are determined by, reported to and/or displayed on the device: service usage value, projected service usage value, service usage plan limit, projected service usage overage, projected service cost overage, service plan period time duration, service plan time remaining before end of period and/or other pertinent information.

[0246] In some embodiments, the device also determines service costs based on the synchronized service usage count thereby allowing the device to also report the service cost information to the user. For example, the device can locally store a service cost look-up table(s), locally store different service cost look-up tables for different networks and/or for roaming networks, and/or request such information from a billing or intermediate billing server (and/or a roaming server) on the network. As another example, the device can obtain the calculated service costs based on the synchronized local service usage count and/or network service usage count from an intermediate server (e.g., a billing or intermediate billing server) thereby offloading the computational costs associated with calculated these projections and the data storage for service cost lookup tables onto the intermediate server on the network using the network service usage counter with or, alternatively, without the synchronized local service usage counter.

[0247] In some embodiments, service usage count categorization by network (e.g., a home network (such as a Wi-Fi, WAN, femtocell or other home network) versus a roaming network) is provided. Similarly, the synchronized local service usage counter can be

synchronized by network. Also, a synchronized local service usage count for networks controlled by a central provider, for networks controlled by other providers (e.g., MVNO), and/or free networks can similarly be provided.

[0248] In some embodiments, a service notification and billing interface is provided. For example, service usage and projected service usage, such as described herein, can be displayed to the user of the device (e.g., via user interface 1697). Similarly, expected/projected service or cost overrun/overage, such as described herein, can also be displayed to the user. As another example, a most cost effective plan can be determined/projected based on historical and/or projected service usage, and this determined/projected most cost effective plan can be displayed to the user. In yet another example, a list of available networks accessible by the device can be displayed to the user. In this example, one or more undesired available networks can also be blocked from display thereby only displaying to the user desired and/or preferred available networks. In this example, service usage plans and/or service usage plan option comparison for one or more alternative networks or roaming networks can also be displayed to the user. Similarly, service cost plans and/or service/cost plan option comparison for one or more alternative networks or roaming networks can also be displayed to the user. In addition, roaming service usage, projected roaming service usage, estimated roaming service cost, and/or projected estimated roaming service cost can also be displayed to the user. These roaming service usage/costs can also be displayed to the user so that the user can utilize this information for selecting various roaming service billing options. In another example, alternative and/or least cost networks are determined and displayed to the user. In another example, alternative warnings are displayed to the user for any or specified roaming networks.

[0249] In some embodiments, the service notification and billing interface notifies the user of expected network coverage (e.g., based on the device's current geography/location and the accessible networks for the device from that current geography/location) and displays options to the user based on the expected network coverage information. In some embodiments, the service notification and billing interface notifies the user of their current service usage at specified service usage points and displays various options to the user (e.g., service usage options and/or billing options). For example, the user's responses to the presented options are recorded (e.g., stored locally on the device at least temporarily for reporting purposes or

permanently in a local configuration data store until such configuration settings are otherwise modified or reset) and reported, such as to the billing server (e.g., central billing 1619). For example, user input, such as selected options and/or corresponding policy settings, can be stored locally on the device via a cache system. As another example, the service notification and billing interface displays options to the user for how the user wants to be notified and how the user wants to control service usage costs, the user's input on such notification options is recorded, and the cost control options (e.g., and the billing agent 1695 and policy control agent 1692) are configured accordingly. Similarly, the user's input on service plan options/changes can be recorded, and the service plan options/changes (e.g., and the billing agent 1695 and policy control agent 1692) are configured/updated accordingly. In another example, the service notification and billing interface provides various traffic control profiles, such as for where the user requests assistance in controlling service usage costs (e.g., service data usage and/or transactional usage related activities/costs). Similarly, the service notification and billing interface can provide various notification options, such as for where the user wants advance warning on service coverage. In another example, the service notification and billing interface provides options for automatic pre-buy at a set point in service usage. In another example, the service notification and billing interface provides the option to choose different notification and cost control options for alternative networks or roaming networks.

[0250] In some embodiments, an online portal or web server is provided for allowing the user to select and/or update policy settings. For example, user input provided via the online portal/web server can be recorded and reported to the billing server (e.g., central billing 1619). In another example, the online portal/web server can display transaction billing information and/or accept input for a transaction billing request, which can then be reported to the billing server accordingly.

[0251] As shown in FIG. 16, the service processor 115 includes a service interface or user interface 1697. In some embodiments, the user interface 1697 provides the user with information and accepts user choices or preferences on one or more of the following: user service information, user billing information, service activation, service plan selection or change, service usage or service activity counters, remaining service status, service usage projections, service usage overage possibility warnings, service cost status, service cost projections, service

usage control policy options, privacy/CRM/GPS related options, and/or other service related information, settings, and/or options. For example, the user interface 1697 can collect service usage information from service monitor agent 1696 to update the local service usage counter (and/or, alternatively, the service usage information is obtained from the service controller 122) to update user interface service usage or service cost information for display to the user. As another example, service billing records obtained from central billing system 1619 can be used to synchronize local service usage counters and service monitor agent 1696 information to perform real-time updating of local service usage counters between billing system 1619 synchronizations. As another example, the user interface 1697 can display options and accept user preference feedback, such as similarly discussed above with respect to user privacy/CRM/GPS filtering, traffic monitoring and service controls. For example, the user interface 1697 can allow the user of the device to modify their privacy settings, provide user feedback on service preferences and/or service experiences, modify their service profiles (e.g., preferences, settings, configurations, and/or network settings and options), to review service usage data (e.g., based on local service usage counters and/or other data monitored by the service processor 115), to receive various events or triggers (e.g., based on projected service usage/costs), and/or the user interface 1697 can provide/support various other user input/output for service control and service usage.

[0252] In some embodiments, by providing the service policy implementation and the control of service policy implementation to the preferences of the user, and/or by providing the user with the option of specifying or influencing how the various service notification and control policies or control algorithms are implemented, the user is provided with options for how to control the service experience, the service cost, the capabilities of the service, the manner in which the user is notified regarding service usage or service cost, the level of sensitive user information that is shared with the network or service provider entity, and the manner in which certain service usage activities may or may not be throttled, accelerated, blocked, enabled and/or otherwise controlled. Accordingly, some embodiments provide the service control to beneficially optimize user cost versus service capabilities or capacities in a manner that facilitates an optimized user experience and does not violate network neutrality goals, regulations and/or requirements. For example, by offering the user with a set of choices, ranging from simple choices between two or more pre-packaged service control settings options to advanced user screens where more detailed level of user specification and control is made

available, some embodiments allow the service provider, device manufacturer, device distributor, MVNO, VSP, service provider partner, and/or other "entity" to implement valuable or necessary service controls while allowing the user to decide or influence the decision on which service usage activities are controlled, such as how they are controlled or throttled and which service usage activities may not be throttled or controlled in some manner. These various embodiments allow the service provider, device manufacturer, device distributor, MVNO, VSP, service provider partner, or other "entity" to assist the user in managing services in a manner that is network neutral with respect to their implementation and service control policies, because the user is making or influencing the decisions, for example, on cost versus service capabilities or quality. By further providing user control or influence on the filtering settings for the service usage reporting or CRM reporting, various levels of service usage and other user information associated with device usage can be transmitted to the network, service provider, device manufacturer, device distributor, MVNO, VSP, service provider partner, and/or other "entity" in a manner specified or influenced by the user to maintain the user's desired level of information privacy.

[0253] As shown in FIG. 16, the service processor 115 includes the service downloader 1663. In some embodiments, the service downloader 1663 provides a download function to install or update service software elements on the device. In some embodiments, the service downloader 1663 requires a secure signed version of software before a download is accepted. For example, the download can require a unique key for a particular service downloader 1663. As another example, the service downloader 1663 can be stored or execute in secure memory or execute a secure memory partition in the CPU memory space. Those of ordinary skill in the art will appreciate that there are a variety of other security techniques that can be used to ensure the integrity of the service downloader 1663.

[0254] As shown in FIG. 16, the service processor 115 includes a modem driver 1640. In some embodiments, the modem driver 1640 converts data traffic into modem bus (not shown) traffic for one or more modems via the modem firewall 1655. As shown in FIG. 18, in some embodiments, modem selection and control 1811 selects the access network connection and is in communication with the modem firewall 1655, and modem drivers 1831, 1815, 1814, 1813, 1812 convert data traffic into modem bus traffic for one or more modems and are in

communication with the modem selection and control 1811. As shown in FIG. 21, in some embodiments, modems 2141, 2125, 2124, 2123, 2122, which are in communication with the modem bus 2120, connect the device to one or more networks. In some embodiments, different profiles are selected based on the selected network connection (e.g., different service profiles/policies for WWAN, WLAN, WPAN, Ethernet and/or DSL network connections), which is also referred to herein as multimode profile setting. For example, service profile settings can be based on the actual access network (e.g., home DSL/cable or work network) behind the Wi-Fi not the fact that it is Wi-Fi (or any other network, such as DSL/cable, satellite, or T-1), which is viewed as different than accessing a Wi-Fi network at the coffee shop. For example, in a Wi-Fi hotspot situation in which there are a significant number of users on a DSL or T-1 backhaul, the service controller can sit in a service provider cloud or an MVNO cloud, the service controls can be provided by a VSP capability offered by the service provider (e.g., as described herein with respect to FIG. 49) or the service controller can be owned by the hotspot service provider that uses the service controller on their own without any association with an access network service provider. For example, the service processors can be controlled by the service controller to divide up the available bandwidth at the hotspot according to QoS or user sharing rules (e.g., with some users having higher differentiated priority (potentially for higher service payments) than other users). As another example, ambient services (as similarly described herein) can be provided for the hotspot for verified service processors.

[0255] In some embodiments, the service processor 115 and service controller 122 are capable of assigning multiple service profiles associated with multiple service plans that the user chooses individually or in combination as a package. For example, a device 100 starts with ambient services that include free transaction services wherein the user pays for transactions or events rather than the basic service (e.g., a news service, eReader, PND service, pay as you go session Internet) in which each service is supported with a bill by account capability to correctly account for any subsidized partner billing to provide the transaction services (e.g., Barnes and Noble may pay for the eReader service and offer a revenue share to the service provider for any book or magazine transactions purchased form the device 100). In some embodiments, the bill by account service can also track the transactions and, in some embodiments, advertisements for the purpose of revenue sharing, all using the service monitoring capabilities disclosed herein. After initiating services with the free ambient service discussed above, the user may later choose

a post-pay monthly Internet, email and SMS service. In this case, the service controller 122 would obtain from the billing system 123 in the case of network based billing (or in some embodiments the service controller 122 billing event server 1622 in the case of device based billing) the billing plan code for the new Internet, email and SMS service. In some embodiments, this code is cross referenced in a database (e.g., the policy management server 1652) to find the appropriate service profile for the new service in combination with the initial ambient service. The new superset service profile is then applied so that the user maintains free access to the ambient services, and the billing partners continue to subsidize those services, the user also gets access to Internet services and may choose the service control profile (e.g., from one of the embodiments disclosed herein). The superset profile is the profile that provides the combined capabilities of two or more service profiles when the profiles are applied to the same device 100 service processor. In some embodiments, the device 100 (service processor 115) can determine the superset profile rather than the service controller 122 when more than one "stackable" service is selected by the user or otherwise applied to the device. The flexibility of the service processor 115 and service controller 122 embodiments described herein allow for a large variety of service profiles to be defined and applied individually or as a superset to achieve the desired device 100 service features.

[0256] As shown in FIG. 16, the service controller 122 includes a service control server link 1638. In some embodiments, device based service control techniques involving supervision across a network (e.g., on the control plane) are more sophisticated, and for such it is increasingly important to have an efficient and flexible control plane communication link between the device agents (e.g., of the service processor 115) and the network elements (e.g., of the service controller 122) communicating with, controlling, monitoring, or verifying service policy. For example, the communication link between the service control server link 1638 of service controller 122 and the service control device link 1691 of the service processor 115 can provide an efficient and flexible control plane communication link, a service control link 1653 as shown in FIG. 16, and, in some embodiments, this control plane communication link provides for a secure (e.g., encrypted) communications link for providing secure, bidirectional communications between the service processor 115 and the service controller 122. In some embodiments, the service control server link 1638 provides the network side of a system for transmission and reception of service agent to/from network element functions. In some

embodiments, the traffic efficiency of this link is enhanced by buffering and framing multiple agent messages in the transmissions (e.g., thereby reducing network chatter). In some embodiments, the traffic efficiency is further improved by controlling the transmission frequency and/or linking the transmission frequency to the rate of service usage or traffic usage. In some embodiments, one or more levels of security and/or encryption are used to secure the link against potential discovery, eavesdropping or compromise of communications on the link. In some embodiments, the service control server link 1638 also provides the communications link and heartbeat timing for the agent heartbeat function. As discussed below, various embodiments described herein for the service control server link 1638 provide an efficient and secure mechanism for transmitting and receiving service policy implementation, control, monitoring and verification information between the device agents (e.g., service processor agents/components) and other network elements (e.g., service controller agents/components).

[0257] In some embodiments, the service control server link 1638 can employ the counterpart service control plane secure transmission methods discussed above with respect to the service control device link 1691. For example, one or more layers of security can be used to secure the communications link, including, for example, basic IP layer security, TCP layer security, service control link layer security, and/or security specific from service controller servers to service processor agents.

[0258] In some embodiments, the service control server link 1638 reduces network chatter by efficiently transmitting service control related communications over the link. For example, the service control server link 1638 can transmit server messages asynchronously as they arrive. As another example, the service control server link 1638 can perform collection or buffering of server messages between transmissions. As another example, the service control server link 1638 can determine when to transmit based potentially on several parameters, such as one or more of: periodic timer trigger, waiting until a certain amount of service usage or traffic usage has occurred, responding to a service agent message, responding to a service agent request, initiated by one or more servers, initiated by a verification error condition, and/or initiated by some other error condition. For example, once a transmission trigger has occurred, the service control server link 1638 can take all buffered agent communications and frame the communications. In addition, the service control server link 1638 can provide for an efficient

communication link based on various embodiments related to the timing of transmissions over the service control link, as similarly discussed above with respect to the service control device link 1691 description. For example, the timing functions, such as asynchronous messages or polling for messages, constant frequency transmission, transmission based on how much service usage or data traffic usage has taken place, transmission in response to device side control link message, service verification error events, other error events, and/or other message transmission trigger criteria can be determined, controlled and/or initiated by either the device side or the network side depending on the embodiment.

[0259] In some embodiments, the service control server link 1638 provides for securing, signing, encrypting and/or otherwise protecting the communications before sending such communications over the service control link 1653. For example, the service control server link 1638 can send to the transport layer or directly to the link layer for transmission. In another example, the service control server link 1638 further secures the communications with transport layer encryption, such as TCP TLS or another secure transport layer protocol. As another example, the service control server link 1638 can encrypt at the link layer, such as using IPSEC, various possible VPN services, other forms of IP layer encryption and/or another link layer encryption technique.

[0260] In some embodiments, the service control server link 1638 includes the agent heartbeat function in which the agents provide certain required reports to the service processor for the purpose of service policy implementation verification or for other purposes. For example, the heartbeat function can also be used to issue queries or challenges, messages, service settings, service control objectives, information requests or polling, error checks and/or other communications to the agents. As another example, agent heartbeat messages can be in the open or encrypted, signed and/or otherwise secured. Additional heartbeat function and the content of heartbeat messages can be provided as similarly described herein, such as described above with respect to the service control device link 1691 and the access control integrity agent 1694 and other sections. In some embodiments, the service controller 122 and/or agents of the service controller 122 are programmed to periodically provide reports, such as upon a heartbeat response (e.g., an agent can repeatedly send necessary reports each heartbeat), and appropriate actions can then be taken based upon such received reports. Accordingly, the heartbeat function

provides an important and efficient system in various embodiments described herein for verifying the service policy implementation and/or protecting against compromise events. There are many other functions the agent heartbeat service can perform many of which are discussed herein, while many others will be apparent to one of ordinary skill in the art given the principles, design background and various embodiments provided herein.

[0261] In some embodiments, the service control server link 1638 also provides a service control software download function for various embodiments, which, for example, can include a download of new service software elements, revisions of service software elements, and/or dynamic refreshes of service software elements of the service processor 115 on the device. In some embodiments, this function is performed by the service control server link 1638 transmitting the service control software as a single file over the service control link. For example, the file can have encryption or signed encryption beyond any provided by the communication link protocol itself for service control link 1653. In another example, the service control software files can be segmented/divided into smaller packets that are transmitted in multiple messages sent over the service control link 1653. In yet another example, the service control software files can be transmitted using other delivery mechanism, such as a direct TCP socket connection from a service download control server 1660, which can also involve secure transport and additional levels of encryption. In some embodiments, the service control server link 1638 and/or service download control server 1660 use(s) an agent serial number and/or a security key look up when agents are updated and/or when a dynamic agent download occurs.

[0262] As shown in FIG. 16, the service controller 122 includes an access control integrity server 1654. In some embodiments, the access control integrity server 1654 collects device information on service policy, service usage, agent configuration and/or agent behavior. For example, the access control integrity server 1654 can cross check this information to identify integrity breaches in the service policy implementation and control system. In another example, the access control integrity server 1654 can initiate action when a service policy violation or a system integrity breach is suspected.

[0263] In some embodiments, the access control integrity server 1654 (and/or some other agent of service controller 122) acts on access control integrity agent reports and error

conditions. Many of the access control integrity agent 1654 checks can be accomplished by the server. For example, the access control integrity agent 1654 checks include one or more of the following: service usage measure against usage range consistent with policies (e.g., usage measure from the network and/or from the device); configuration of agents; operation of the agents; and/or dynamic agent download.

[0264] In some embodiments, the access control integrity server 1654 (and/or some other agent of service controller 122) verifies device service policy implementations by comparing various service usage measures (e.g., based on network monitored information, such as by using IPDRs, and/or local service usage monitoring information) against expected service usage behavior given the policies that are intended to be in place. For example, device service policy implementations can include measuring total data passed, data passed in a period of time, IP addresses, data per IP address, and/or other measures such as location, downloads, email accessed, URLs, and comparing such measures expected service usage behavior given the policies that are intended to be in place.

[0265] In some embodiments, the access control integrity server 1654 (and/or some other agent of service controller 122) verifies device service policy, and the verification error conditions that can indicate a mismatch in service measure and service policy include one or more of the following: unauthorized network access (e.g., access beyond ambient service policy limits); unauthorized network speed (e.g., average speed beyond service policy limit); network data amount does not match policy limit (e.g., device not stop at limit without re-up/revising service policy); unauthorized network address; unauthorized service usage (e.g., VOIP, email, and/or web browsing); unauthorized application usage (e.g., email, VOIP, email, and/or web); service usage rate too high for plan, and policy controller not controlling/throttling it down; and/or any other mismatch in service measure and service policy.

[0266] In some embodiments, the access control integrity server 1654 (and/or some other agent of service controller 122) verifies device service policy based at least in part on, for example, various error conditions that indicate a mismatch in service measure and service policy. For example, various verification error conditions that can indicate a mismatch in service measure and service policy include one or more of the following: mismatch in one service

measure and another service measure; agent failure to report in; agent failure to respond to queries (e.g., challenge-response sequence and/or expected periodic agent reporting); agent failure to respond correctly to challenge/response sequence; agent improperly configured; agent failure in self checks; agent failure in cross-checks; unauthorized agent communication or attempted unauthorized communication; failure in service policy implementation test; failure in service usage reporting test; failure in service usage billing test; failure in transaction billing test; failure in download sequence; environment compromise event, such as unauthorized software load or execution (or attempt), unauthorized memory access (or attempt), unauthorized agent access (or attempt), known harmful software, and/or known harmful communications signature; and/or failure to respond to various messages, such as send message and suspend and/or send message and quarantine. In some embodiments, the access control integrity server 1654 (and/or some other agent of service controller 122) verifies device service policy by performing automated queries and analysis, which are then reported (e.g., anomalous/suspicious report results can be reported for further analysis by a person responsible for determining whether such activities indicate out of policy activities or to provide information to the user to inform the user of such anomalous/suspicious report results that may indicate out of policy activities). For example, the user can review the report to authorize whether such activities were performed by the user (e.g., website access requests, specific transactions, and/or phone calls) and/or indicate that such activities were not authorized by the user (e.g., indicate a potential compromise of the device, such as by malware or other unauthorized software/user use of the device). In another example, the user can also be connected to communicate with service support of the service provider regarding such reported activities (e.g., by text/chat, voice/phone, and/or video conference to a service support). Accordingly, in some embodiments, the access control integrity server 1654 (and/or some other agent of service controller 122) provides a policy/service control integrity service to continually (e.g., periodically and/or based on trigger events) verify that the service control of the device has not been compromised and/or is not behaving out of policy.

[0267] In some embodiments, upon detection of one or more service verification errors, such as the various service verification errors discussed above, the device is directed to a quarantine network status in which the device can, for example, only access network control plane functions, billing functions, and other functions generally controlled by the access network

service provider or the central service provider. For example, quarantine network access restrictions and routing can be accomplished with the access network AAA and routing system (e.g., access network AAA server 1621 and one or more of the gateways 410, 420, 508, 512, 520, 608, 612, 620, 708, 712, 720) or can be accomplished with device based access control or traffic control policy implementation. Quarantine network equipment or servers can, for example, be located within the access network or within another network with access to the access network. Communication with the quarantine network infrastructure can be accomplished, for example, with a secure link with one or more encryption levels or a dedicated private link. In some embodiments, quarantining a device includes, for example, a two step process for routing quarantine network device traffic, first, to a quarantine traffic handling router or server and, second, from there to the actual quarantine network infrastructure, with the route being determined by device parameters, user parameters, access service provider parameters or other parameters associated with the quarantine network routing. In some embodiments, the device is completely suspended from the network in which, for example, the device can first issue a user interface message to the user or issuing another form of a message to the user or service subscriber, such as via email, hard copy message and/or voice message. In some embodiments, the device network access, service capabilities and/or traffic shaping are limited, partially restricted or completely restricted, service capabilities. For example, these limitations and/or restrictions can be implemented in the device and/or in the network. For example, implementing a device quarantine (e.g., using a RADIUS server to quarantine the device) can involve assigning the device to a different billing profile.

[0268] In some embodiments, upon detection of one or more service verification errors, such as the various service verification errors discussed above, switch based port analysis is performed to further monitor the device (e.g., referred to as Switched Port Analyzer (SPAN) on Cisco switches, and various other vendors have different names for it, such as Roving Analysis Port (RAP) on 3Com switches). In some embodiments, the device service policy implementation behavior is monitored at a deeper level in the network by copying device traffic in the switch so that it goes to both an intended data path destination and to a specified port for switch based port analysis (e.g., the traffic content can be analyzed and recorded using deep packet inspection (DPI) techniques, which can provide a finer level of detail than the typical IPDR). For example, an advantage of performing a switch based port analysis function is that

the traffic need not be analyzed in real time, and a sample subset of the devices on the network can be selected for such analysis based on, for example, either identifying devices that have suspect service policy implementation behavior and/or a regular sampling algorithm that eventually samples all devices, or some other selection approaches. As another example, a scheduled switch based port analysis sampling can be applied that eventually rotates through all devices and designates a higher priority in the sampling queue for devices that are suspect.

[0269] In some embodiments, switch based port analysis allows for off-line sampled or non-real-time DPI, as described above, as a verification measure for the device based service control measures that are implemented. In some embodiments, sophisticated DPI techniques are used to enhance the content of the IPDRs so that they provide detailed information that can be made available in the network. For example, some of the DPI packet analysis may be redundant between the device and the network, but this approach provides for a much finer grain validation for the device based service and less reliance on the device for some of the service traffic analysis that service providers need. In some embodiments, the device control server functions and the service control policy verification functions are implemented in an integrated hardware/software system (e.g., a gateway, server, router, switch, base station, base station aggregator, AAA server cluster or any other hardware or hardware/software system) located in the network that the network level traffic inspection is accomplished in, or in one or more servers integrated to operate in a coordinated manner with the DPI boxes. In some embodiments, the device control server functions and the service control policy verification functions are implemented in an integrated hardware/software system (e.g., a gateway, server, router, switch, base station, base station aggregator, AAA server cluster or any other hardware or hardware/software system) located in the network that provides deep service control capability (e.g., using DPI techniques) for devices that have some or all of the service processor functions installed and, in some embodiments, also providing coarser network control of the basics for devices that do not have a service processor installed in the device (e.g., such coarser network control functions include max data rate and/or max total data).

[0270] In some embodiments, the SPAN function is used in a revolving periodic manner as well to augment CDR data with deeper packet information for the purpose of spot-checking device based service usage measures. Examples of where this can be beneficial include spot

checking network address access policies, spot checking ambient access policies, spot checking billing event reports, spot checking intermediate networking device/end point device count (via checking network source or destination addresses, token, cookies or other credentials, etc). For example, the periodic SPAN can be scheduled for all devices equally, for certain devices or users with higher priority, frequency or depth of SPAN than others, higher priority, higher frequency or immediate priority for devices with higher usage patterns or unusual usage patterns, immediate or very high priority for devices with a policy violation status.

[0271] In some embodiments, a combination traffic inspection and service control approach implements traffic and service control functions in the network that are conducive for a network based implementation and implements traffic and service control functions in the device that are either more conducive for performing in the device or can only be performed in the device (e.g., activities involving inspection of traffic that is encrypted once it is transmitted to the network). For example, using this approach, activities that can be done in the network are generally performed in the network and/or are more efficiently performed in the network than the device, and activities that are more efficiently performed in the device or can only be performed in the device are performed in the device (e.g., depending on device processing/storage capabilities and/or other design/security considerations). For example, the following are various traffic and service control functions that, in some embodiments, are preferably or can only be performed in the device: network based packet processing capability limitations (e.g., encrypted traffic, application layer information unavailable once the traffic goes into the networking stack, other application/usage context information available on the device but not in the network); information that is generally/preferably maintained and processed locally in the device for network neutrality reasons (e.g., network neutrality issues can generally be efficiently implemented by keeping all, substantially all or at least some aspect of decisions on how to implement algorithms to control traffic local to the device and under user decision control, and/or by providing the user with a set of pre-packaged choices on how to manage service usage or service activity usage or manage service usage versus service cost or price); information that is generally/preferably maintained and processed locally in the device for user privacy reasons (e.g., deeper levels of traffic monitoring and service usage monitoring data where it is available for assisting the user in achieving the best, lowest cost experience and implementing a CRM filter function to the user so that the user can control the level of CRM the network is allowed to

receive, such as with the higher levels of information being exchanged for something of value to the user, and/or user location information); information that is generally/preferably maintained and processed locally in the device for the purpose of informing the user of service control settings or service activity usage or to adjust service activity control settings or receive user feedback to choices regarding service usage policies or billing options (e.g., providing the user with a UI for the purpose of monitoring an estimate of service usage and/or notifying the user of at least some aspect of estimated service usage or projected service usage, providing the user with a UI for the purpose of monitoring an estimate of service cost and/or notifying the user of at least some aspect of estimated service cost or projected service cost, providing the user with a UI for the purpose of providing the user with one or more service usage and/or service cost notification messages that require user acknowledgement and/or a user decision and obtaining or reporting the user acknowledgements and/or decisions, providing the user with a UI for the purpose of providing the user with service options and/or service payment options, providing the user with a UI for the purpose of obtaining user choice for such options when service usage or cost estimates are about to run over limits or have run over limits or are projected to run over limits, providing the user with a UI for the purpose of monitoring or conducting open central billing transactions or other transactions, providing the user with a UI for the purpose of selecting the service control techniques and/or policies and/or algorithms and/or pre-packaged configurations that can be used to define or partially define the service activity usage control policies implemented in the device service processor or the network service control equipment/billing system or a combination of both); service control for roaming on different networks that typically do not have compatible DPI-type techniques with the home network; certain service notification and traffic control algorithms (e.g., stack-ranked activity statistical analysis and control of only the high usage activities); and/or a function for assigning a device to a service experience or ambient activation experience or virtual service provider (VSP) at various times from manufacturing to device distribution to a user of the device. In some embodiments, certain activities are implemented in the device as a solution for networks in which a new centralized DPI approach is not possible, not economically feasible, or for any number of reasons not an option or not a preferred option.

[0272] In some embodiments, a network based solution is provided for a more basic set of services for all devices that do not have service control capabilities, and a super-set of services

and/or additional services are provided for devices that include a service processor. As described herein, a service controller function can be located in various places in the network in accordance with various embodiments . It should also be noted that various other embodiments described herein also employ a hybrid service control function performing certain service control functions in the network (e.g., collecting network service usage information, such as IPDRs, and/or performing DPI related functions in the network for collecting network service usage information and/or throttling/shaping traffic) and service control functions in the device (e.g., service processor 115, which, for example, monitors service usage in the device and/or performs throttling or traffic shaping in the device and/or performs certain billing event recording and reporting functions that are aptly performed on the device).

[0273] In some embodiments, lower level service policy implementation embodiments are combined with a higher level set of service policy supervision functions to provide device assisted verifiable network access control, authentication and authorization services.

[0274] In some embodiments, device based access control services are extended and combined with other policy design techniques to create a simplified device activation process and connected user experience referred to herein as ambient activation. As similarly discussed above, ambient activation can be provided by setting access control to a fixed destination, verifying access with IPDRs, verifying access by setting a max data rate and triggering off in the network if it exceeds the max data rate, and/or by various other techniques.

[0275] As shown in FIG. 16, service controller 122 includes a service history server 1650. In some embodiments, the service history server 1650 collects and records service usage or service activity reports from the Access Network AAA Server 1621 and the Service Monitor Agent 1696. For example, although service usage history from the network elements can in certain embodiments be less detailed than service history from the device, the service history from the network can provide a valuable source for verification of device service policy implementation, because, for example, it is extremely difficult for a device error or compromise event on the device to compromise the network based equipment and software. For example, service history reports from the device can include various service tracking information, as similarly described above. In some embodiments, the service history server 1650 provides the

service history on request to other servers and/or one or more agents. In some embodiments, the service history server 1650 provides the service usage history to the device service history 1618. In some embodiments, for purposes of facilitating the activation tracking service functions (described below), the service history server 1650 maintains a history of which networks the device has connected to. For example, this network activity summary can include a summary of the networks accessed, activity versus time per connection, and/or traffic versus time per connection. As another example, this activity summary can further be analyzed or reported to estimate the type of service plan associated with the traffic activity for the purpose of bill sharing reconciliation.

[0276] As shown in FIG. 16, service controller 122 includes a policy management server 1652. In some embodiments, the policy management server 1652 transmits policies to the service processor 115 via the service control link 1653. In some embodiments, the policy management server 1652 manages policy settings on the device (e.g., various policy settings as described herein with respect to various embodiments) in accordance with a device service profile. In some embodiments, the policy management server 1652 sets instantaneous policies on policy implementation agents (e.g., policy implementation agent 1690). For example, the policy management server 1652 can issue policy settings, monitor service usage and, if necessary, modify policy settings. For example, in the case of a user who prefers for the network to manage their service usage costs, or in the case of any adaptive policy management needs, the policy management server 1652 can maintain a relatively high frequency of communication with the device to collect traffic and/or service measures and issue new policy settings. In this example, device monitored service measures and any user service policy preference changes are reported, periodically and/or based on various triggers/events/requests, to the policy management server 1652. In this example, user privacy settings generally require secure communication with the network (e.g., a secure service control link 1653), such as with the policy management server 1652, to ensure that various aspects of user privacy are properly maintained during such configuration requests/policy settings transmitted over the network. For example, information can be compartmentalized to service policy management and not communicated to other databases used for CRM for maintaining user privacy.

[0277] In some embodiments, the policy management server 1652 provides adaptive policy management on the device. For example, the policy management server 1652 can issue policy settings and objectives and rely on the device based policy management (e.g., service processor 115) for some or all of the policy adaptation. This approach can require less interaction with the device thereby reducing network chatter on service control link 1653 for purposes of device policy management (e.g., network chatter is reduced relative to various server/network based policy management approaches described above). This approach can also provide robust user privacy embodiments by allowing the user to configure the device policy for user privacy preferences/settings so that, for example, sensitive information (e.g., geo-location data, website history) is not communicated to the network without the user's approval. In some embodiments, the policy management server 1652 adjusts service policy based on time of day. In some embodiments, the policy management server 1652 receives, requests or otherwise obtains a measure of network availability and adjusts traffic shaping policy and/or other policy settings based on available network capacity.

[0278] In some embodiments, the policy management server 1652 performs a service control algorithm to assist in managing overall network capacity or application QoS. In some embodiments, the policy management server 1652 performs an algorithm to determine which access network is best to connect to, such as based on network capacity or application QoS, service usage costs, and/or any other criteria. In some embodiments, the device is capable of connecting to more than one network, and accordingly, device service policies can be selected/modified based on which network the device is connected to. In some embodiments, the network control plane servers detect a network connection change from a first network to a second network and initiate the service policy implementation established for the second network. In other embodiments, the device based adaptive policy control agent (e.g., policy control agent 1692 described herein) detects network connection changes from the first network to the second network and implements the service policies established for the second network.

[0279] In some embodiments, when more than one access network is available, the network is chosen based on which network is most preferred according to a network preference list or according to the network that optimizes a network cost function. For example, the preference list can be pre-established by the service provide and/or the user. For example, the

network cost function can be based on a minimum service cost, maximum network performance, determining whether or not the user or device has access to the network, maximizing service provider connection benefit, reducing connections to alternative paid service providers, and/or a variety of other network preference criteria. In other embodiments, the device detects when one or more preferred networks are not available, implements a network selection function or intercepts other network selection functions, and offers a connection to the available service network that is highest on a preference list. For example, the preference list can be set by the service provider, the user and/or the service subscriber.

[0280] As shown in FIG. 16, service controller 122 includes a network traffic analysis server 1656. In some embodiments, the network traffic analysis server 1656 collects/receives service usage history for devices and/or groups of devices and analyzes the service usage. In some embodiments, the network traffic analysis server 1656 presents service usage statistics in various formats to identify improvements in network service quality and/or service profitability. In other embodiments, the network traffic analysis server 1656 estimates the service quality and/or service usage for the network under variable settings on potential service policy. In other embodiments, the network traffic analysis server 1656 identifies actual or potential service behaviors by one or more devices that are causing problems for overall network service quality or service cost.

[0281] As shown in FIG. 16, service controller 122 includes a beta test server 1658. In some embodiments, the beta test server 1658 publishes candidate service plan policy settings to one or more devices. In some embodiments, the beta test server 1658 provides summary reports of network service usage or user feedback information for one or more candidate service plan policy settings. In some embodiments, the beta test server 1658 provides a mechanism to compare the beta test results for different candidate service plan policy settings or select the optimum candidates for further policy settings optimization.

[0282] As shown in FIG. 16, service controller 122 includes a service download control server 1660. In some embodiments, the service download control server 1660 provides a download function to install and/or update service software elements (e.g., the service processor 115 and/or agents/components of the service processor 115) on the device, as described herein.

[0283] As shown in FIG. 16, service controller 122 includes a billing event server 1662. In some embodiments, the billing event server 1662 collects billing events, provides service plan information to the service processor 115, provides service usage updates to the service processor 115, serves as interface between device and central billing server 1619, and/or provides trusted third party function for certain ecommerce billing transactions.

[0284] As shown in FIG. 16, the Access Network AAA server 1621 is in network communication with the access network 1610. In some embodiments, the Access Network AAA server 1621 provides the necessary access network AAA services (e.g., access control and authorization functions for the device access layer) to allow the devices onto the central provider access network and the service provider network. In some embodiments, another layer of access control is required for the device to gain access to other networks, such as the Internet, a corporate network and/or a machine to machine network. This additional layer of access control can be implemented, for example, by the service processor 115 on the device. In some embodiments, the Access Network AAA server 1621 also provides the ability to suspend service for a device and resume service for a device based on communications received from the service controller 122. In some embodiments, the Access Network AAA server 1621 also provides the ability to direct routing for device traffic to a quarantine network or to restrict or limit network access when a device quarantine condition is invoked. In some embodiments, the Access Network AAA server 1621 also records and reports device network service usage (e.g., device network service usage can be reported to device service history 1618).

[0285] As shown in FIG. 16, the device service history 1618 is in network communication with the access network 1610. In some embodiments, the device service history 1618 provides service usage data records used for various purposes in various embodiments. In some embodiments, the device service history 1618 is used to assist in verifying service policy implementation. In some embodiments, the device service history 1618 is used to verify service monitoring. In some embodiments, the device service history 1618 is used to verify billing records and/or billing policy implementation. In some embodiments, the device service history 1618 is used to synchronize and/or verify the local service usage counter.

[0286] As shown in FIG. 16, the central provider billing server 1619 is in network communication with the access network 1610. In some embodiments, the central provider billing server 1619 provides a mediation function for central provider billing events. For example, the central provider billing server 1619 can accept service plan changes. In some embodiments, the central provider billing server 1619 provides updates on device service usage, service plan limits and/or service policies. In some embodiments, the central provider billing server 1619 collects billing events, formulates bills, bills service users, provides certain billing event data and service plan information to the service controller 122 and/or device 100.

[0287] **Establishing Coordinated Service and Verification Policies for Service Processor, Service Controller and Network Functions**

[0288] In some embodiments, device and network apparatus coordinate one or more of the following: network service policy implementation settings, device service policy implementation settings, network service profile implementation settings, device service profile implementation settings, network service usage measures used for the purpose of verifying service policy implementation, device service usage measures used for the purpose of verifying service policy implementation, network actions taken upon detection of service usage policy violation and device actions taken upon detection of service usage policy violation. In some embodiments, local device settings for the service monitoring, usage and/or billing profile or policy settings used, for example, by a device service processor 115, are associated with corresponding records for the various network apparatus that also rely upon the service policy and profile settings to monitor, control and/or bill for services or to respond to out of policy service usage conditions. For example, such network apparatus include the service controller 122 or similar functions, the billing system 123 or similar functions, the network AAA 121, gateways 410, 420, 508, 512, 520, 608, 612, 620, 708, 712, 720, or other networking equipment. In some embodiments, the service profile or policy settings are associated between the device and network in a manner that allows for effective and coordinated operation between the device service processor 115 and the network apparatus, but does not require an explicit function that simultaneously controls/ coordinates the service policy or profile implementation and/or verification actions taken by the device 100 (e.g., the service processor 115) and the network

apparatus. As an example, such embodiments can be applied in overlay applications as discussed below.

[0289] In some embodiments, a network function (e.g., the service controller 122, and/or more specifically the policy management server 1652 function, or other similar function) obtain, derive or otherwise determine the association of the service profile or policy settings to program a device service processor 115 and the various network apparatus functions (e.g., possibly including but not limited to the service controller 122 or similar functions, the billing system 123 or similar functions, the network AAA 121, gateways 410, 420, 508, 512, 520, 608, 612, 620, 708, 712, 720, or other networking equipment) by reading, receiving, querying, pulling or otherwise obtaining the settings from one or more of the network apparatus functions or from a data base that stores the service policy or profile settings for one or more of the network apparatus functions. After obtaining one or more of the network apparatus settings, a mapping (e.g., an association) of the network apparatus settings to the appropriate device 100 (service processor 115) settings can be determined to advantageously support the service usage monitoring, service usage control, service usage billing or service usage verification objectives being addressed. The policy or profile settings for the device can be a direct translation of the policy or profile settings used for the network apparatus, or the device policy or profile settings can be less directly derived from the network apparatus policy or profile settings. For example, service usage limits contained in the billing system 123 service plan can be either directly mapped to usage limit settings on the device service processor 115 (e.g., service usage stops when the limit is hit or the user is notified or the user is billed), or the usage limits can be mapped to a number of service profiles the user may select from (e.g. , as discussed herein, the user can select from options involving various actual usage versus usage limit notification policies and/or service usage control, limitations or throttling policies).

[0290] For example, the service usage policy or profile limits or allowances maintained for the network apparatus functions (e.g., the service profile or service plan usage limits stored in the billing system 123 or AAA 121) can be read or queried by a network function (e.g., the service controller 122 or the service controller 122 through a second intermediary server connected to the billing system 123 and/or the AAA system 121), and the service usage limits stored in these networking apparatus can be either directly translated to the settings for the

service processor 115 or may need to be interpreted, expanded or otherwise modified to obtain the required service processor 115 policy and/or profile settings.

[0291] In some embodiments, the service usage limits set in the billing system 123 service plan record, and/or the service profile record stored in the AAA system 121 can be acquired (e.g., from the apparatus or from a database storing the settings for the apparatus) by the service controller (or another network function) and directly translated and used to program the settings in the service processor 123. In some embodiments, the service usage limits are determined or obtained by the activation server apparatus embodiments, other apparatus embodiments associated with service activation, or the virtual service provider embodiments, as described herein. In this manner, once the association of the service usage profile or policy settings used by a device service processor 115 and the profile or policy settings used by the various network apparatus functions is established, then the service policy or profile for service monitoring, control, billing, verification and/or actions taken on verification error can be coordinated between device and network even if some of the network functions act independent of some of the device functions.

[0292] For example, associating the service usage policies and/or profiles between the device service processor 115 and the various network apparatus functions, and then allowing for independent operation or action by the various functions in a manner that results in a coordinated outcome, facilitates an overlay of the device assisted services technology onto existing network equipment in a manner that results in reliable and verifiable service enhancements while minimizing the need for major existing network equipment upgrades.

[0293] In some embodiments, the association of the service profile or policy settings used by a device service processor 115 and the service profile or policy settings used by the various network apparatus functions can be provided by a centralized network function that determines the appropriate settings for the network apparatus and the service processor 115 and sets one or more settings to each function. In some embodiments, this networking function is provided by a centralized network management function or service account activation function (e.g., the activation server apparatus embodiments, one of the other disclosed apparatus

embodiments associated with service activation or the virtual service provider apparatus embodiments, as described herein).

[0294] In some embodiments, the association of the service profile or policy settings used by a device service processor 115 and the service profile or policy settings used by the various network apparatus functions can be provided by a network function that by reads, receives, queries, pulls or otherwise obtains the setting used by the service controller 122 or the service processor 115. The network function can then determine the association of the service profile or policy settings used by a device service processor 115 and the service profile or policy settings required by the various network apparatus functions before writing, transmitting, pushing, or otherwise recording the appropriate settings required by each of the other network apparatus functions. In some embodiments, this functionality can be implemented in the service controller (e.g., the policy management server, possibly acting in coordination with another network function or server), which then links into the databases used for storing the policy or profile settings for the other network apparatus.

[0295] In some embodiments, once the association is established between service policy or profile settings in the network apparatus and the service policy or profile settings in the service processor 115, then the network based service usage measures (e.g., IPDRs communicated to the billing system 123, the AAA 121, service controller 122 or other network functions used to verify service usage and/or take actions) used for verification of device 100 service usage versus service policy or profile can be monitored by the network apparatus (e.g., billing system 123 and AAA 121) independent of coordination with the service processor 115 and/or independent of the service controller 122. In some embodiments, in addition to independent monitoring and verification of service usage versus policy, independent service profile or policy verification error response actions can be taken by the network apparatus (e.g., suspend, quarantine, SPAN or flag device 100, notify the user and possibly require acknowledgement, or bill the user account for service usage overage) without direct involvement by the service processor 115 and/or the service controller 122.

[0296] Accordingly, the association between service profile and/or service policy that is implemented on the device 100 (e.g., service processor 115) and the service profile and/or policy

usage limits recorded in network apparatus can be associated with one another by one or more of the following: (A) implementing a function to read from the network database (e.g., the billing 123 data base, AAA 121 data base, service controller 122 data base, etc.) and mapping the network profiles and/or policies to device 100 (e.g., service processor 115) profiles and/or policies; (B) implementing a function that simultaneously sets the device profile and/or policy and the network equipment profile and/or policy recorded in the appropriate data base records; and (C) implementing a function that reads the profile and/or policy on the device 100 (e.g., service processor 115) or the service controller 122 and then sets the network equipment profile and/or policy recorded in the appropriate data base records. This allows for a simplified but coordinated response to monitoring, controlling and billing for service usage, for verifying service usage versus service usage profile or policy, and/or initiating or carrying out network actions in response to service usage versus profile or policy verification errors and/or device actions in response to service usage versus profile or policy verification errors.

[0297] FIG. 17 is another functional diagram illustrating the device based service processor 115 and the service controller 122 in accordance with some embodiments. FIG. 17 provides for various embodiments as similarly described above with respect to the various embodiments described above with respect to FIG. 16, with one of the differences being that the service controller 122 as shown in FIG. 17 is connected to the access network and not (directly) connected to the Internet. Accordingly, as shown in FIG. 17, in some embodiments, the service control link 1653 is a communications link between the service controller 122 and the service processor 115 over the access network 1610.

[0298] FIG. 18 is another functional diagram illustrating the device based service processor 115 and the service controller 122 in which the service processor controls the policy implementation for multiple access network modems and technologies in accordance with some embodiments. As shown, FIG. 18 provides for various embodiments as similarly described above with respect to the various embodiments described above with respect to FIG. 16, with one of the differences being that the service processor controls the policy implementation for multiple access network modems and technologies. Accordingly, as shown in FIG. 18, in some embodiments, a connection manager 1804, which as shown is in control plane communication with a modem selection and control 1811, provides a control and supervision function for one or

more modem drivers or modems that connect to an access network. In some embodiments, the modem selection and control 1811 selects the access network connection and is in communication with the modem firewall 1655, and modem drivers, which as shown include Dial/DSL modem driver 1831, Ethernet modem driver 1815, WPAN modem driver 1814, WLAN modem driver 1813, and WWAN modem driver 1812, convert data traffic into modem bus traffic for one or more modems and are in communication with the modem selection and control 1811.

[0299] FIG. 19 is another functional diagram illustrating the service processor 115 and the service controller 122 in accordance with some embodiments. As shown in FIG. 19, a stripped down (e.g., reduced set of agents/components/functionality) embodiment of the service processor 115 and the service controller 122 are provided in which service policy is not adaptive but rather is set by the service controller 122. In this example, the agent within the service processor 115 that implements service policy is the policy implementation agent 1690. Also, in this example, the service controller 122 is similarly stripped down to a simplified configuration (e.g., reduced set of agents/components/functionality).

[0300] Referring to FIG. 19, in some embodiments, many of the service policy implementation verification and compromise protection techniques are similarly provided using these simplified configurations of the service processor 115 and the service controller 122, as described above with respect to, for example, FIG. 16. For example, the service control device link 1691 and service control server link 1638 can be used for downloading service policies to the policy implementation agent 1690 (but, in some embodiments, cannot perform the heartbeat or authentication function).

[0301] For example, a basic service profile or service policy implementation verification technique for this reduced configuration calls for the access control integrity server 1654 to obtain IPDRs from access network AAA server 1621 (or 121) (e.g., or other network functions as described herein) and compare the service usage exhibited by device 100 with a range of expected service usage that would be expected if the intended service policies were in place on the device. In some embodiments, the access control integrity server 1654 initiates or carries out one or more of the service usage profile or policy verification error response actions disclosed

herein, including, for example, one or more of the following: notify the user of the out of policy or overage condition, require the user to acknowledge the condition and/or acknowledge a subsequent billing event to proceed, bill the user for service overage, suspend the device from the network, quarantine the device, SPAN the device, or notify a network manager or device management or error handling function.

[0302] In some embodiments, a service profile or service policy implementation verification technique for this reduced configuration calls for the billing system 123 to obtain IPDRs from access network AAA server 1621 (or 121) (or other network functions as discussed herein) and compare the service usage exhibited by device 100 with a range of expected service usage that would be expected if the intended service policies were in place on the device. In some embodiments, the billing system 123 initiates or carries out one or more of the service usage profile or policy verification error response actions disclosed herein, including, for example, one or more of the following: notify the user of the out of policy or overage condition, require the user to acknowledge the condition and/or acknowledge a subsequent billing event to proceed, bill the user for service overage, suspend the device from the network, quarantine the device, SPAN the device, or notify a network manager or device management or error handling function.

[0303] In some embodiments, a service profile or service policy implementation verification technique for this reduced configuration calls for the AAA server 1621 (or 121) itself to compare the service usage exhibited by device 100 with a range of expected service usage that would be expected if the intended service policies were in place on the device. In some embodiments, the AAA server 1621 (or 121) initiates or carries out one or more of the service usage profile or policy verification error response actions disclosed herein, including, for example, one or more of the following: notify the user of the out of policy or overage condition, require the user to acknowledge the condition and/or acknowledge a subsequent billing event to proceed, bill the user for service overage, suspend the device from the network, quarantine the device, SPAN the device, or notify a network manager or device management or error handling function.

[0304] Accordingly, this approach provides a basic first layer of service policy implementation verification that does not depend on device based agent behavior for the verification. If the service policy is in error in a way that violates the expected service policy usage limits, then the access control integrity server 1654 will detect this condition and appropriate action can be taken. In some embodiments, if one or more service policy integrity verification tests fail, the appropriate responsive actions can include routing the device to quarantine status, sending an error message to the device or device user interface and then suspend access for the device, and/or limiting access in some way without completely suspending access, as similarly described above. In some embodiments, if one or more service policy integrity verification tests fail, the appropriate responsive actions can include logging excess service usage above the intended service policy limits and billing the user for some or all of the excess usage, sending the user a notification and/or acknowledgement response request (possibly including a simple keystroke acknowledgement, or a password, a biometric signature or other secure response), and/or limiting access in some way without completely suspending access, as similarly described above.

[0305] In some embodiments, a billing system technique provides another verification overlay. For example, the service processor 115 can have a set of service policy implementations (or service profile) that calls for maintaining service usage within a certain limit, or assisting the user or network to maintain service usage to that limit. The billing system 123 can be implemented in a way to provide a "back stop" to the service usage controls or limits provided for by the service processor 115, so that even if the service processor 115 is compromised, hacked, spoofed or is otherwise in error, the billing system 123 protects the service provider, "service owner", carrier, VSP or network operator from unpaid access beyond the service limits. This can be accomplished, for example, by assigning a service usage limit within the billing system 123 so that if the service processor 115 is compromised and the service usage runs over the desired limit, the billing system 123 automatically charges the user account for the overage. The billing system 123 can receive service usage information from the IPDRs that are aggregated in the network as in the case of a conventional billing system, and because these network based measures are independent from the device agent operation, they cannot be spoofed by merely spoofing something on the device or service processor 115. In this manner, defeating the service processor 115 service agent control mechanisms described herein simply

results in a billing charge and not free service. In some embodiments, if the service usage runs over the service usage limit specified in the service profile, the user can be notified as discussed herein, and the user can be required to acknowledge the overage and approve a billing charge for the overage as also discussed herein, with the acknowledgement being communicated back to the network in some embodiments. This positive acknowledgement also provides a layer of protection and verification of the service control and usage limit control for the device service processor 115. In some embodiment also discussed herein, the user is requested to input a password, biometric or other secure response to the usage overage notification, providing yet another layer of protection to verify that the user intends to pay for the service usage overage. In these embodiments taken individually or in combination, the service processor 115 assistance for service usage control can be verified and/or protected from compromise.

[0306] In some embodiments, the service control device link 1691 and service control server link 1638 are used to implement the service processor 115 heartbeat authentication and communication functions to strengthen the verification of a proper service policy implementation of the embodiments of FIG. 19. For example, the heartbeat function can be used as authentication for service monitoring versus network reports. In addition, the heartbeat function can be used as authentication for challenge/response queries of agents. Also, the heartbeat function can be used as authentication for access control. In some embodiments, to strengthen verification of the basic system illustrated in FIG. 19, the communication access to the policy implementation agent 1690 is restricted so that software or hardware on device 100 and/or on a network cannot have authorized access to the policy implementation agent 1690. For example, authorized access to the policy implementation agent 1690 can be restricted to include only the service controller 122 through the service control device link 1691 and the service control server link 1638. For example, the agent control bus 1630 can be secured with encryption and/or other security techniques so that only the service control device link 1691 can have authorized access to the policy implementation agent 1690. As another example, the agent level message encryption can be used as described herein.

[0307] In some embodiments, the service policy implementation agent 1690 of the embodiments of FIG. 19 can be further strengthened against errors, intrusion, tampering, hacking and/or other inadvertent or intentional integrity degradation by using various other techniques.

For example, the dynamic agent download feature of the service controller 122 can download a new version of the policy implementation agent 1690. In this example, the new agent code can be identical in functionality and also hashed, obfuscated or ordered differently before signing and encryption so that any hacking attempt must be reinitiated, and this process can be periodically repeated or repeated upon a triggering event. Additionally, once the new dynamically loaded agent is in place, it can be required to perform an environment scan to determine if the system configuration or operation are as expected, and/or it can seek to detect elements in the execution environment that can be harmful or threatening to the integrity of the policy implementation. The agent can also be required to report back on the scan within a relatively short period of time so that any attempt to compromise the agent does not have sufficient time to be effective.

[0308] In some embodiments, the service policy implementation agent 1690 of the embodiments of FIG. 19 can be further strengthened to protect the policy implementation from compromise attempts by locating the software and/or hardware used onto an access modem associated with the service. For example, the modem can make it difficult to get access to the policy implementation agent 1690 by employing one or more security elements on one or more access ports into the modem, such as the device bus, an I/O port, a network connection or the debug port. The modem can also store and/or execute the policy implementation agent in secure memory. The modem can also require a secure download key or a secure software signature to accept any updates to the agent software.

[0309] In some embodiments, the service policy implementation agent 1690 of the embodiments of FIG. 19 can be further strengthened against compromise attempts by performing scans of the device 100 code execution environment and/or code storage environment to identify potentially malicious and/or unwanted/untrusted software or hardware. For example, this function can be performed by the policy implementation agent 1690. The agent can have a local database of potentially malicious elements and compare the entries in the database against the elements detected locally using various malicious code, behavior blocking, intrusion detection, and/or other well known techniques for security analysis. Alternatively or in addition, the agent can communicate a list of some or all of the elements detected locally to the service controller 122 to augment or take the place of the database comparison function that can be performed locally, thereby performing such or further such security analysis on the network (e.g., by the

service controller 122), and, in some embodiments, if not automatically detected, such elements detected locally (e.g., and/or samples of such detected potentially malicious code or logs of potentially malicious/suspicious behavior/intrusions) forwarded to security analysts for the service provider for further security analysis (e.g., service provider security analysts and/or an outside security vendor engaged to protect the service provider's network and supported devices). In some embodiments, the agent detects new software downloads, installs and/or invocations and immediately issues an error flag report when potentially malicious software is downloaded, installed or invoked (e.g., file and network based on access security detection techniques). In some embodiments, the agent scans the local software loading and invocation activity along with a log of other software runtime events and regularly reports this trace so that when an error or compromise event occurs the trace preceding the event can be analyzed to determine the offending software or activity trace that took place to cause the compromise or error. For example, once the software or activity that caused the compromise is known or otherwise detected, it can be entered into a refreshed version of the database that the device and other devices use to detect potentially malicious precursor conditions. Examples of such precursor events can include software invocations, software downloads, a sequence of memory I/O events, a sequence of software access events, a sequence of network address or URL communications or downloads, or a sequence of access modem I/O activity.

[0310] FIG. 20 is another functional diagram illustrating the service processor 115 and the service controller 122 in accordance with some embodiments. As shown in FIG. 20, the modem firewall 1655 has been removed, and firewall and access control and traffic shaping functions are performed in these embodiments by the policy implementation agent 1690 and application interface agent 1693.

[0311] FIG. 21 is another functional diagram illustrating the service processor 115 and the service controller 122 in accordance with some embodiments. FIG. 21 illustrates the various modem drivers and modems 2122 through 2125 and 2141. In some embodiments, the modems, which include WWAN modem 2122, WLAN modem 2123, WPAN modem 2124, Ethernet modem 2125, and Dial/DSL modem 2141, which are in communication with the modem bus 2120, connect the device to one or more networks. As shown, the service measurement points labeled I through VI represent various service measurement points for service monitor agent

1696 and/or other agents to perform various service monitoring activities. Each of these measurement points can have a useful purpose in various embodiments described herein. For example, each of the traffic measurement points that is employed in a given design can be used by a monitoring agent to track application layer traffic through the communication stack to assist policy implementation functions, such as the policy implementation agent 1690, or, in some embodiments, the modem firewall agent 1655 or the application interface agent 1693, in making a determination regarding the traffic parameters or type once the traffic is farther down in the communication stack where it is sometimes difficult or impossible to make a complete determination of traffic parameters. It should be noted that although the present invention does not need to implement any or all of the measurement points illustrated in FIG. 21 to have an effective implementation as was similarly shown with respect to FIG. 19, various embodiments benefit from these and/or similar measurement points. It should also be noted that the exact measurement points can be moved to different locations in the traffic processing stack, just as the various embodiments described herein can have the agents affecting policy implementation moved to different points in the traffic processing stack while still maintaining effective operation.

[0312] As shown in FIG. 21, measurement point I occurs at the application interface agent 1693 interface to the applications. At this measurement point, the application traffic can be monitored before it is framed, packetized or encrypted by the lower layers of the networking stack. For example, this allows inspection, characterization, tagging (literal or virtual) and, in some embodiments, shaping or control of services or traffic. At this measurement point, traffic can be more readily associated with applications, URLs or IP addresses, content type, service type, and other higher level parameters. For example, at this level email traffic and downloads, web browser applications and end points, media file transfers, application traffic demand, URL traffic demand and other such service monitoring parameters are more readily observed (e.g., accessible in the clear without the need for deep packet inspection and/or decryption), recorded and possibly shaped or controlled. As described herein, it is also possible to monitor upstream traffic demand at this point and compare it to the other measurement points to determine if the traffic policies in place are meeting overall traffic control policy objectives or to determine if traffic policy implementation is operating properly. For example, the downstream delivered traffic can be optimally observed at this measurement point.

[0313] As shown in FIG. 21, traffic measurement points II and III are situated on the upstream and downstream sides of policy implementation agent 1690. As described herein, these two locations allow potential tracking of upstream and downstream traffic through the stack portions associated with the policy implementation agent 1690. These two locations also provide for potential cross-checking of how the policy implementation agent 1690 is impacting the demand and delivery of traffic. In a similar manner, measurement point III in connection with measurement point IV provide an opportunity for packet tracing through the stack components associated with the modem firewall 1655 and provide for the opportunity to observe the demand and delivery sides of the modem firewall 1655. Traffic measurement point V provides the potential for observing the traffic at the modem bus drivers for each of the modems.

[0314] As shown in FIG. 21, traffic measurement point VI provides, in some embodiments, the ultimate measure of access traffic, for example, the traffic that actually transacts over the access network through the modem. As shown, measurement point VI is at the modem side of the internal or external communications bus 1630, and it will be appreciated that, in some embodiments, this measurement point can be further down the modem stack closer to the MAC or physical layer (e.g., at the designer's discretion). An advantage of having a measurement point deep in the modem is, for example, that if the software or hardware that implements the measurement and reporting is well secured against compromise, then this measure can be almost as strong from a verification perspective as the measure that comes from the network (e.g., from the network elements). Accordingly, this makes it possible to compare this measure against the other measures to determine if there is a traffic path that is leaking past the other measurement point or one or more policy implementation points.

[0315] FIGS. 22A and 22B provide tables summarizing various service processor 115 agents (and/or components/functions implemented in software and/or hardware) in accordance with some embodiments. Many of these agents are similarly described above, and the tables shown in FIGS. 22A and 22B are not intended to be an exhaustive summary of these agents, nor an exhaustive description of all functions that the agents perform or are described herein, but rather FIGS. 22A and 22B are provided as a summary aid in understanding the basic functions of each agent in accordance with some embodiments and how the agents interact with one another,

with the service controller server elements, and/or with other network functions in certain embodiments to form a reliable device based service delivery solution and/or platform.

[0316] FIG. 23 provides a table summarizing various service controller 122 server elements (and/or components/functions implemented in software and/or hardware) in accordance with some embodiments. Many of these agents are similarly described above, and the table shown in FIG. 23 is not intended to be an exhaustive summary of these server elements, nor an exhaustive description of all functions that the elements perform or are described herein, but rather FIG. 23 is provided as a summary aid in understanding the basic functions of each element in accordance with some embodiments and how the elements interact with one another, certain network elements, and/or the service processor agents in certain embodiments to form a reliable device based service delivery solution and/or platform.

[0317] In some embodiments, it is desirable to provide a control plane between the service processor and the service controller using a flexible connection or communication path that, for example, will work between virtually any two network connection endpoints, one being the service controller and one being the device, in a secure yet scalable manner. In view of the embodiments described herein, one of ordinary skill in the art will recognize that it is possible to achieve such features with a variety of different embodiments that share similar core features to the embodiments described herein.

Service Control Device Link and Continuous Heartbeat Authentication

[0318] As described herein, there are numerous ways to implement the control plane communication channel between the service processor 115 and the service controller 122. Various embodiments described herein disclose a secure and bandwidth efficient control plane that is compatible with any IP based network (including the ability to locate the service controller 122 over the Internet); provides for consistent device assisted service monitoring, control, verification and/or billing while roaming across multiple networks with different access technologies; and allows continuous device assisted service control verification and/or authentication with a variety of mechanisms for setting the transmission heartbeat frequency. Other techniques that could be used for this function include, for example, encapsulating the control plane in the access network control plane channel, encapsulating the control plane in IP

or data packet framing mechanisms (e.g., IPV6), running a more conventional VPN or IPSEC channel, and/or using an independent access network connection.

[0319] FIG. 24 is a functional diagram illustrating the service control device link 1691 of the service processor 115 and the service control service link 1638 of the service controller 122 in accordance with some embodiments. In particular, the service control device link 1691 of the service processor 115 and the service control service link 1638 of the service controller 122 as shown in FIG. 24 provide for secure control plane communication over the service control link 1653 between the service processor 115 and the service controller 122 in accordance with some embodiments. Various embodiments include two or three layers of encryption in the service control link, with one embodiment or layer being implemented in the encrypt functions (2408, 2428) and decode functions (2412, 2422), and another embodiment or layer implemented in the transport services stack (2410, 2420). An optional third embodiment or layer of encryption is implemented below the transport services stack, for example, with IPSEC or another IP layer encryption, VPN or tunneling scheme. For example, various known security encryption techniques can be implemented in the encrypt functions (2408, 2428), with public/private or completely private keys and/or signatures so that very strong levels of security for service processor control plane traffic can be achieved even through the basic transport services (2410, 2420) implemented with standard secure or open Internet networking protocols, such as TLS or TCP. For example, the service processor agent communications local to the device can be conducted to and from the service controller elements via the service control device link 1691 connection to the agent communication bus 1630. The combination of the service control device link 1691 and the agent communication bus 1630, which in some embodiments is also securely encrypted or signed, provides a seamless, highly secure, asynchronous control plane connection between the service processor and service controller server elements and the service controller and service controller agents that works over a wide range of access networks, such as any access network that has the capability to connect IP or TCP traffic to another TCP or IP endpoint on the access network, another private network or over the Internet 120. As described herein, in some embodiments, the agent communication bus 1630 also provides a fourth level of encrypted or signed communication to form a secure closed system on the device for agent to agent communication, for example, making it very difficult or practically impossible for software or applications to gain access to one or more of the a service processor agents on the device in any

way other than the service control device link 1691. In this way, in some embodiments, the agent communication bus 1630 and the service processor agents can only be accessed by one another as necessary or permitted by agent communication policies, or by the service controller or other authorized network function with proper security credentials communicating over the service control device link 1691. Additionally, in some embodiments, communications between a subset of two or more agents, or between one or more agents and one or more service controller server elements are encrypted with unique keys or signatures in such a way that a fourth level of security providing private point to point, point to multipoint, or multipoint to multipoint secure communication lines is provided.

[0320] In some embodiments, all of the service control device link 1691 communications are transformed into a continuous control plane connection, with a frequency based on the rate of service usage, a minimum set period between connections, and/or other methods for establishing communication frequency. In some embodiments, this heartbeat function provides a continuous verification link by which the service controller verifies that the service processor and/or device are operating properly with the correct service policies being implemented. In view of the following heartbeat function embodiments described herein, it will be apparent to one of ordinary skill in the art that different approaches for implementing the various heartbeat embodiments are possible, and it will be clear that there are many ways to achieve the essential features enabling a reliable, sometimes continuous control link and verification function for the purpose of assisting control of service usage in a verifiable manner. As shown, inside the service processor 115, the service control device link 1691 includes a heartbeat send counter 2402 in communication with the agent communication bus 1630. For example, the heartbeat send counter 2402 can provide a count for triggering when a service processor 115 communication (e.g., periodic communication based on a heartbeat mechanism) should be sent to the service controller 122, and a heartbeat buffer 2404, also in communication with the agent communication bus 1630, buffers any such information for the next service processor 115 communication, in accordance with various heartbeat based embodiments, as similarly described herein. The heartbeat buffer 2404 is in communication with a framing element 2406 and an encrypt element 2408 for framing and encrypting any service processor 115 communications transmitted to the service controller 122 by a transport services stack 2410 over the service control link 1653. Similarly, as shown inside the service controller 122, the service control

server link 1638 includes a heartbeat send counter 2434 in communication with a service controller network 2440, a heartbeat buffer 2432, also in communication with the service controller network 2440, buffers any such information for the next service controller 122 communication, in accordance with various heartbeat based embodiments, as similarly described herein. The heartbeat buffer 2432 is in communication with a framing element 2430 and an encrypt element 2428 for framing and encrypting any such service controller 122 communications transmitted to the service processor 115 by a transport services stack 2420 over the service control link 1653.

[0321] As also shown inside the service processor 115 of FIG. 24, the service control device link 1691 includes a decode element 2412 for decoding any received service controller 122 communications (e.g., decrypting encrypted communications), an unpack element 2414 for unpacking the received service controller 122 communications (e.g., assembling packetized communications), and an agent route 2416 for routing the received service controller 122 communications (e.g., commands, instructions, heartbeat related information or status reports, policy related information or configuration settings and/or updates, challenge/response queries, agent refreshes and/or new software for installation) to the appropriate agent of the service processor 115. Similarly, as shown inside the service controller 122, the service control server link 1638 also includes a decode element 2422 for decoding any received service processor 115 communications (e.g., decrypting encrypted communications), an unpack element 2424 for unpacking the received service processor 115 communications (e.g., assembling packetized communications), and an agent route 2426 for routing the received service processor 115 communications (e.g., responses to instructions and/or commands, heartbeat related information or status reports, policy related information or configuration settings and/or updates, challenge/response queries, agent status information, network service/cost usage and/or any other reporting related information) to the appropriate agent of the service controller 122. Accordingly, as described herein with respect to various embodiments, the various secure communications between the service controller 122 and the service processor 115 can be performed using the embodiment as shown in FIG. 24, and those of ordinary skill in the art will also appreciate that a variety of other embodiments can be used to similarly provide the various secure communications between the service controller 122 and the service processor 115 (e.g., using different software and/or hardware architectures to provide secure communications, such

as using additional and/or fewer elements/functions or other design choices for providing such secure communications).

[0322] In some embodiments, an efficient and effective communication framing structure between the service processor and service controller is provided, and the following embodiments (e.g., as shown and described with respect to FIG. 25) teach such a structure that packs the various service processor agent control plane communications and the various service controller element control plane connections into a format that does not consume excessive bandwidth to enable a continuous control plane connection between the device and service controller. In some embodiments, an efficient and effective communication framing structure between the service processor and service controller is provided to buffer such communication messages for some period of time before framing and transmitting, such as in a heartbeat frequency that is based on rate of service usage. In some embodiments, an efficient and effective communication framing structure between the service processor and service controller is provided to allow for the frame to be easily packed, encrypted, decoded, unpacked and the messages distributed. In view of the various embodiments described herein, it will be apparent to one of ordinary skill in the art that many framing structures will work for the intended purpose of organizing or framing agent communications and the uniqueness and importance of combining such a system element with the device service controller functions, the service processor functions, the service control verification functions and/or the other purposes.

[0323] FIG. 25 is a functional diagram illustrating a framing structure of a service processor communication frame 2502 and a service controller communication frame 2522 in accordance with some embodiments. In particular, the service control device link 1691 of the service processor 115 and the service control service link 1638 of the service controller 122 (e.g., as shown in FIG. 24) provide for secure control plane communication over the service control link 1653 between the service processor 115 and the service controller 122 using communication frames in the format of the service processor communication frame 2502 and the service controller communication frame 2522 as shown in FIG. 25 in accordance with some embodiments. As shown, the service processor communication frame 2502 includes a service processor framing sequence number 2504, a time stamp 2506, an agent first function ID 2508, an agent first function message length 2510, an agent first function message 2512, and assuming

more than one message is being transmitted in this frame, an agent Nth function ID 2514, an agent Nth function message length 2516, and an agent Nth function message 2518. Accordingly, the service processor communication frame 2502 can include one or more messages as shown in FIG. 25, which can depend on networking frame length requirements and/or other design choices. Similarly, as shown, the service controller communication frame 2522 includes a service controller framing sequence number 2524, a time stamp 2526, an agent first function ID 2528, an agent first function message length 2530, an agent first function message 2532, and assuming more than one message is being transmitted in this frame, an agent Nth function ID 2534, an agent Nth function message length 2536, and an agent Nth function message 2538. Accordingly, the service controller communication frame 2522 can include one or more messages as shown in FIG. 25, which can depend on networking frame length requirements and/or other design choices.

[0324] FIGS. 26A through 26H provide tables summarizing various service processor heartbeat functions and parameters (e.g., implemented by various agents, components, and/or functions implemented in software and/or hardware) in accordance with some embodiments. Many of these heartbeat functions and parameters are similarly described above, and the tables shown in FIGS. 26A-26H are not intended to be an exhaustive summary of these heartbeat functions and parameters, but rather are provided as an aid in understanding these functions and parameters in accordance with some heartbeat based embodiments described herein.

[0325] FIGS. 27A through 27P provide tables summarizing various device based service policy implementation verification techniques in accordance with some embodiments. Many of these device based service policy implementation verification techniques are similarly described above, and the tables shown in FIGS. 27A-27P are not intended to be an exhaustive summary of these device based service policy implementation verification techniques, but rather are provided as an aid in understanding these techniques in accordance with some device based service policy embodiments described herein.

[0326] FIGS. 28A through 28E provide tables summarizing various techniques for protecting the device based service policy from compromise in accordance with some embodiments. Many of these techniques for protecting the device based service policy from

compromise are similarly described above, and the tables shown in FIGS. 28A-28E are not intended to be an exhaustive summary of these techniques for protecting the device based service policy from compromise, but rather are provided as an aid in understanding these techniques in accordance with some device based service policy embodiments described herein.

Device Assisted Service Control and Traffic Control

[0327] As described below, various techniques are disclosed for implementing device assisted traffic shaping and service control at the lower levels of service usage policy implementation.

[0328] FIG. 29 is a functional diagram illustrating a device communications stack that allows for implementing verifiable traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments. As shown, several service agents take part in data path operations to achieve various data path improvements, and, for example, several other service agents can manage the policy settings for the data path service, implement billing for the data path service, manage one or more modem selection and settings for access network connection, interface with the user and/or provide service policy implementation verification. Additionally, in some embodiments, several agents perform functions to assist in verifying that the service control or monitoring policies intended to be in place are properly implemented, the service control or monitoring policies are being properly adhered to, that the service processor or one or more service agents are operating properly, to prevent unintended errors in policy implementation or control, and/or to prevent tampering with the service policies or control. As shown, the service measurement points labeled I through VI represent various service measurement points for service monitor agent 1696 and/or other agents to perform various service monitoring activities. Each of these measurement points can have a useful purpose in various embodiments described herein. For example, each of the traffic measurement points that is employed in a given design can be used by a monitoring agent to track application layer traffic through the communication stack to assist policy implementation functions, such as the policy implementation agent 1690, or in some embodiments the modem firewall agent 1655 or the application interface agent 1693, in making a determination regarding the traffic parameters or type once the traffic is farther down in the communication stack where it is sometimes difficult

or impossible to make a complete determination of traffic parameters. For example, a detailed set of embodiments describing how the various measurement points can be used to help strengthen the verification of the service control implementation are described herein, including, for example, the embodiments described with respect to FIG. 16 and FIG. 21. The particular locations for the measurement points provided in these figures are intended as instructional examples, and other measurement points can be used for different embodiments, as will be apparent to one of ordinary skill in the art in view of the embodiments described herein. Generally, in some embodiments, one or more measurement points within the device can be used to assist in service control verification and/or device or service troubleshooting.

[0329] In some embodiments, the service monitor agent and/or other agents implement virtual traffic tagging by tracking or tracing packet flows through the various communication stack formatting, processing and encryption steps, and providing the virtual tag information to the various agents that monitor, control, shape, throttle or otherwise observe, manipulate or modify the traffic. This tagging approach is referred to herein as virtual tagging, because there is not a literal data flow, traffic flow or packet tag that is attached to flows or packets, and the book-keeping to tag the packet is done through tracking or tracing the flow or packet through the stack instead. In some embodiments, the application interface and/or other agents identify a traffic flow, associate it with a service usage activity and cause a literal tag to be attached to the traffic or packets associated with the activity. This tagging approach is referred to herein as literal tagging. There are various advantages with both the virtual tagging and the literal tagging approaches. For example, it can be preferable in some embodiments to reduce the inter-agent communication required to track or trace a packet through the stack processing by assigning a literal tag so that each flow or packet has its own activity association embedded in the data. As another example, it can be preferable in some embodiments to re-use portions of standard communication stack software or components, enhancing the verifiable traffic control or service control capabilities of the standard stack by inserting additional processing steps associated with the various service agents and monitoring points rather than re-writing the entire stack to correctly process literal tagging information, and in such cases, a virtual tagging scheme may be desired. As yet another example, some standard communication stacks provide for unused, unspecified or otherwise available bit fields in a packet frame or flow, and these unused, unspecified or otherwise available bit fields can be used to literally tag traffic without the need to

re-write all of the standard communication stack software, with only the portions of the stack that are added to enhance the verifiable traffic control or service control capabilities of the standard stack needing to decode and use the literal tagging information encapsulated in the available bit fields. In the case of literal tagging, in some embodiments, the tags are removed prior to passing the packets or flows to the network or to the applications utilizing the stack. In some embodiments, the manner in which the virtual or literal tagging is implemented can be developed into a communication standard specification so that various device or service product developers can independently develop the communication stack and/or service processor hardware and/or software in a manner that is compatible with the service controller specifications and the products of other device or service product developers.

[0330] It will be appreciated that although the implementation/use of any or all of the measurement points illustrated in FIG. 29 is not required to have an effective implementation, such as was similarly shown with respect to various embodiments described herein, such as with respect to FIGS. 19 and 21, various embodiments can benefit from these and/or similar measurement points. It will also be appreciated that the exact measurement points can be moved to different locations in the traffic processing stack, just as the various embodiments described herein can have the agents affecting policy implementation moved to different points in the traffic processing stack while still maintaining effective operation. In some embodiments, one or more measurement points are provided deeper in the modem stack (e.g., such as for embodiments similarly described herein with respect to FIGS. 35 and 36) where, for example, it is more difficult to circumvent and can be more difficult to access for tampering purposes if the modem is designed with the proper software and/or hardware security to protect the integrity of the modem stack and measurement point(s).

[0331] Referring to FIG. 29, describing the device communications stack from the bottom to the top of the stack as shown, the device communications stack provides a communication layer for each of the modems of the device at the bottom of the device communications stack. Example measurement point VI resides within or just above the modem driver layer. For example, the modem driver performs modem bus communications, data protocol translations, modem control and configuration to interface the networking stack traffic to the modem. As shown, measurement point VI is common to all modem drivers and modems,

and it is advantageous for certain embodiments to differentiate the traffic or service activity taking place through one modem from that of one or more of the other modems. In some embodiments, measurement point VI, or another measurement point, is located over, within or below one or more of the individual modem drivers. The respective modem buses for each modem reside between example measurement points V and VI. In the next higher layer, a modem selection & control layer for multimode device based communication is provided. In some embodiments, this layer is controlled by a network decision policy that selects the most desirable network modem for some or all of the data traffic, and when the most desirable network is not available the policy reverts to the next most desirable network until a connection is established provided that one of the networks is available. In some embodiments, certain network traffic, such as verification, control, redundant or secure traffic, is routed to one of the networks even when some or all of the data traffic is routed to another network. This dual routing capability provides for a variety of enhanced security, enhanced reliability or enhanced manageability devices, services or applications. In the next higher layer, a modem firewall is provided. For example, the modem firewall provides for traditional firewall functions, but unlike traditional firewalls, in order to rely on the firewall for verifiable service usage control, such as access control and security protection from unwanted networking traffic or applications, the various service verification techniques and agents described herein are added to the firewall function to verify compliance with service policy and prevent tampering of the service controls. In some embodiments, the modem firewall is implemented farther up the stack, possibly in combination with other layers as indicated in other figures. In some embodiments, a dedicated firewall function or layer is provided that is independent of the other processing layers, such as the policy implementation layer, the packet forwarding layer and/or the application layer. In some embodiments, the modem firewall is implemented farther down the stack, such as within the modem drivers, below the modem drivers, or in the modem itself. Example measurement point IV resides between the modem firewall layer and an IP queuing and routing layer. As shown, an IP queuing and routing layer is separate from the policy implementation layer where the policy implementation agent implements a portion of the traffic control and/or service usage control policies. As described herein, in some embodiments, these functions are separated so that a standard network stack function can be used for IP queuing and routing, and the modifications necessary to implement the policy implementation agent functions can be provided

in a new layer inserted into the standard stack. In some embodiments, the IP queuing and routing layer is combined with the traffic or service usage control layer. Examples of this combined functionality are shown and described with respect to FIGS. 31, 32 and 33. For example, a combined routing and policy implementation layer embodiment can also be used with the other embodiments, such as shown in FIG. 29. Various detailed embodiments describing how the policy implementation layer can control traffic or other service usage activities are described with respect to FIG. 38. Measurement point III resides between the IP queuing and routing layer and a policy implementation agent layer. Measurement point II resides between the policy implementation agent layer and the transport layer, including TCP, UDP, and other IP as shown. The session layer resides above the transport layer, which is shown as a socket assignment and session management (e.g., basic TCP setup, TLS/SSL) layer. The network services API (e.g., HTTP, HTTPS, FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), POP3, DNS) resides above the session layer. Measurement point I resides between the network services API layer and an application layer, shown as application service interface agent in the device communications stack of FIG. 29.

[0332] As shown, the application service interface layer is above the standard networking stack API and, in some embodiments, its function is to monitor and in some cases intercept and process the traffic between the applications and the standard networking stack API. In some embodiments, the application service interface layer identifies application traffic flows before the application traffic flows are more difficult or practically impossible to identify farther down in the stack. In some embodiments, the application service interface layer in this way assists application layer tagging in both the virtual and literal tagging cases. In the case of upstream traffic, the application layer tagging is straight forward, because the traffic originates at the application layer. In some downstream embodiments, where the traffic or service activity classification relies on traffic attributes that are readily obtainable, such as source address or URL, application socket address, IP destination address, time of day or any other readily obtained parameter, the traffic type can be identified and tagged for processing by the firewall agent or another agent as it initially arrives. In other embodiments, as described herein, in the downstream case, the solution is generally more sophisticated when a traffic parameter that is needed to classify the manner in which the traffic flow is to be controlled or throttled is not readily available at the lower levels of the stack, such as association with an aspect of an

application, type of content, something contained within TLS, IPSEC or other secure format, or other information associated with the traffic. Accordingly, in some embodiments the networking stack identifies the traffic flow before it is fully characterized, categorized or associated with a service activity, and then passes the traffic through to the application interface layer where the final classification is completed. In such embodiments, the application interface layer then communicates the traffic flow ID with the proper classification so that after an initial short traffic burst or time period the policy implementation agents can properly control the traffic. In some embodiments, there is also a policy for tagging and setting service control policies for traffic that cannot be fully identified with all sources of tagging including application layer tagging.

[0333] Various applications and/or a user service interface agent communicate via this communications stack, as shown (illustrating such communications with a reference (A)). Also, the billing agent, which is in communication with the agent communication bus 1630, communicates user information and decision query and/or user input to the user service interface agent, as shown. The policy control agent communicates service settings and/or configuration information via this communications bus 1630, as shown (illustrating such communications with a reference (B) via the application layer, policy implementation agent layer, which is lower in the communications stack as shown, and/or the modem firewall layer). The connection manager agent communicates select and control commands and/or modem and access network information via this communications stack, as shown (illustrating such communications with a reference (C) via the modem selection and control layer). Various other communications (e.g., service processor and/or service controller related communications, such as service usage measure information and/or application information) are provided at various levels of this communications stack, as shown (illustrating such communications with references (D) at the application layer, (E) at the policy implementation agent layer, and (F) at the modem firewall layer).

[0334] As shown in FIG. 29, a service monitor agent, which is also in communication with the agent communication bus 1630, communicates with various layers of the device communications stack. For example, the service monitor agent, performs monitoring at each of measurement points I through VI, receiving information including application information, service usage and other service related information, and assignment information. An access

control integrity agent is in communication with the service monitor agent via the agent communications bus 1630, as also shown.

[0335] In some embodiments, one or more of the networking stack modifications described herein in combination one or more of the service verification and tamper prevention techniques described herein is provided. As similarly described with respect to FIG. 29, the various example embodiments for assisting service control verification described herein and as summarized in the example tables provided in FIGS. 26, 27 and 28 can be employed individually or in combination to create increasingly secure cross-functional service control verification embodiments. In FIG. 29, the presence of the access control integrity agent, policy control agent, service monitor agent and the other agents that perform verification and/or tamper prevention functions illustrates verifiable service control aspects in accordance with some embodiments. Furthermore, the presence of the billing agent combined with the service verification and/or tamper prevention agents and techniques described herein provides for a set of verifiable billing embodiments for service billing, service billing offset corrections, bill by account, transaction billing and other billing functions. In addition, the presence of the user service interface agent in combination with the service control agent functions in the modified networking stack provide for embodiments involving a combination of service control with user preferences, which as described herein, provides the user with the capability to optimize service versus service cost in a network neutral manner. In some embodiments, the user control of service control policy is provided along with the service control verification and/or tamper prevention. The presence of the policy control agent that in some embodiments implements a higher than most basic level of policy decision and control with the policy implementation agents in the modified networking stack allows for, for example, the device to possess the capability to implement a higher level of service control for the purpose of obtaining a higher level service usage or service activity objective. In some embodiments, the application layer tagging in combination with other embodiments described herein provides for deep service activity control that is verifiable.

[0336] In some embodiments, verifiable traffic shaping as described herein can be performed using the device communications stack in a variety of embodiments for the combination of service control within the networking stack and service control verification

and/or tamper prevention, with various embodiments depicted in FIGS. 29 through 37. Additional levels of detail regarding how such embodiments can be used to implement verifiable traffic shaping are provided in and described with respect to FIGS. 38 through 40 which depict example functional diagrams of packet processing flows for verifiable traffic shaping or service activity control in a device service processor for both upstream and downstream flows. Along with several other interesting features embodied in FIGS. 38 through 40, application traffic layer tagging is depicted in additional detail in accordance with some embodiments. For example, the application interface agent can determine service data usage at the application layer using measurement point I and a local service usage counter, and can, for example, pass this information to the service monitor agent. If service usage exceeds a threshold, or if using a service usage prediction algorithm results in predicted service usage that will exceed a threshold, then the user can be notified of which applications are causing the service usage overrun or potential service usage overrun, via the user service interface agent. The user can then identify which application service (e.g., traffic associated with a specified high service use or non-critical application, such as for example a high bandwidth consumption social networking website or service, media streaming website or service, or any other high bandwidth website or service transmitting and/or receiving data with the service network) that the user prefers to throttle. As another example, the user could select a service policy that allows for video chat services until those services threaten to cause cost over-runs on the user's service plan, and at that time the service policy could switch the chat service to voice only and not transmit or receive the video. The traffic associated with the user specified application can then be throttled according to user preference input. For example, for downstream traffic, packets (e.g., packets that are virtually or literally tagged and/or otherwise associated with the application traffic to be throttled) from the access network can be buffered, delayed and/or dropped to throttle the identified application traffic. For upstream traffic, packets (e.g., packets that are virtually or literally tagged and/or otherwise associated with the application traffic to be throttled) can be buffered, delayed and/or dropped before being transmitted to the access network to throttle the identified application traffic. As similarly described above, traffic shaping as described herein can be verified, such as by the service monitor agent via the various measurement points and/or using other agents.

[0337] The embodiments depicted in FIG. 30 and other figures generally require enhancements to conventional device networking communication stack processing. For

example, these enhancements can be implemented in whole or in part in the kernel space for the device OS, in whole or in part in the application space for the device, or partially in kernel space and partially in application space. As described herein, the networking stack enhancements and the other elements of the service processor can be packaged into a set of software that is pre-tested or documented to enable device manufacturers to quickly implement and bring to market the service processor functionality in a manner that is compatible with the service controller and the applicable access network(s). For example, the service processor software can also be specified in an interoperability standard so that various manufacturers and software developers can develop service processor implementations or enhancements, or service controller implementations or enhancements that are compatible with one another.

[0338] FIG. 30 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments. In some embodiments, a portion of the service processor is implemented on the modem (e.g., on modem module hardware or modem chipset) and a portion of the service processor is implemented on the device application processor subsystem. It will be apparent to one of ordinary skill in the art that variations of the embodiment depicted in FIG. 30 are possible where more or less of the service processor functionality is moved onto the modem subsystem or onto the device application processor subsystem. For example, such embodiments similar to that depicted in FIG. 30 can be motivated by the advantages of containing some or all of the service processor network communication stack processing and/or some or all of the other service agent functions on the modem subsystem (e.g., and such an approach can be applied to one or more modems). For example, the service processor can be distributed as a standard feature set contained in a modem chipset hardware of software package or modem module hardware or software package, and such a configuration can provide for easier adoption or development by device OEMs, a higher level of differentiation for the chipset or modem module manufacturer, higher levels of performance or service usage control implementation integrity or security, specification or interoperability standardization, and/or other benefits.

[0339] Referring to FIG. 30, describing the device communications stack from the bottom to the top of the stack as shown, the device communications stack provides a

communication layer for modem MAC/PHY layer at the bottom of the device communications stack. Measurement point IV resides above the modem MAC/PHY layer. The modem firewall layer resides between measurement points IV and III. In the next higher layer, the policy implementation agent is provided, in which the policy implementation agent is implemented on the modem (e.g., on modem hardware). Measurement point II resides between the policy implementation agent and the modem driver layer, which is then shown below a modem bus layer. The next higher layer is shown as the IP queuing and routing layer, followed by the transport layer, including TCP, UDP, and other IP as shown. The session layer resides above the transport layer, which is shown as a socket assignment and session management (e.g., basic TCP setup, TLS/SSL) layer. The network services API (e.g., HTTP, HTTPS, FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), POP3, DNS) resides above the session layer. Measurement point I resides between the network services API layer and an application layer, shown as application service interface agent in the device communications stack of FIG. 30.

[0340] Various applications and/or a user service interface agent communicate via this communications stack, as shown (illustrating such communications with a reference (A)). Also, the billing agent, which is in communication with the agent communication bus 1630 communications user information and decision query and/or user input to the user service interface agent, as shown. The policy control agent B communicates service settings and/or configuration information via this communications stack, as shown (illustrating such communications with a reference (B)) via the application layer. The policy control agent A communicates service settings and/or configuration information via this communications stack, as shown (illustrating such communications with a reference (D)) via the policy implementation agent layer and/or the modem firewall layer. The connection manager agent communicates select & control commands and/or modem and access network information via this communications stack, as shown (illustrating such communications with a reference (C)) via the modem driver layer. Various other communications (e.g., service processor and/or service controller related communications, such as service usage measure information, and/or application information) are provided at various levels of this communications stack, as shown (illustrating such communications with references (E)) at the application layer through the modem driver layer with the service monitor agent B as shown (and an access control integrity agent B is also shown), and communications with references (F) at the policy implementation

agent layer and (G) at the modem firewall layer with the service monitor agent A as shown (and an access control integrity agent A is also shown). In some embodiments, the service usage policy verification or tamper prevention embodiments described herein can be applied, in isolation or in combination, in the context of FIG. 31 to provide for embodiments with increasing levels of service usage policy control verification certainty, such as provided with FIGS. 26A-26H, 27A-27P and 28A-28E.

[0341] FIG. 31 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments. In some embodiments, the service processor is a simplified implementation. For example, this approach can be used for applications with less capable device application processors, rapid time to market needs, fewer service usage control needs, and/or other reasons that lead to a need for a lower complexity implementation.

[0342] Referring to FIG. 31, describing the device communications stack from the bottom to the top of the stack as shown, the device communications stack provides a communication layer for the modem layer at the bottom of the device communications stack. The modem driver layer resides above the modem bus layer as shown. In the next higher layer, the policy implementation agent is provided, and the policy implementation agent is also in communication with the agent communication bus 1630 as shown. The next higher layer is shown as the transport layer, including TCP, UDP, and other IP as shown. The session layer resides above the transport layer, which is shown as a socket assignment and session management (e.g., basic TCP setup, TLS/SSL) layer. The network services API (e.g., HTTP, HTTPS, FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), POP3, DNS) resides above the session layer. Applications communicate with the device communications stack via the network services API as shown. Policy settings from the network (e.g., service settings) are communicated with the policy implementation agent as shown. The connection manager communicates select and control as well as modem and access network information via the modem driver as shown. Although FIG. 31 does not depict all of the service usage control verification functions provided by certain embodiments calling for additional service verification or control agents, a high level of service policy implementation verification certainty can be

achieved within the context of the embodiments depicted in FIG. 31 by applying a subset of the service usage policy verification or tamper prevention embodiments described herein. For example, the embodiments depicted in FIG. 31 can be combined with the service controller embodiments that utilize IPDRs to verify service usage is in accordance with the desired service policy. There are also many other service usage control embodiments described herein that can be applied in isolation or in combination to the embodiments depicted in FIG. 31 to provide increasing levels of service usage control verification certainty, as will be apparent to one of ordinary skill in the art in view of FIGS. 26A-26H, 27A-27P and 28A-28E and the various embodiments described herein.

[0343] FIG. 32 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments. In some embodiments, the service processor is a simplified implementation embodiment with device based monitoring and integrity control. For example, FIG. 32 provides for somewhat higher complexity (e.g., relative to the embodiments depicted in FIG. 30) in exchange for the enhanced service monitoring, control or verification that are possible by implement additional agent embodiments, such as the service monitor agent and the access control integrity agent functions.

[0344] Referring to FIG. 32, describing the device communications stack from the bottom to the top of the stack as shown, the device communications stack provides a communication layer for each of the modems of the device at the bottom of the device communications stack. Measurement point II resides above the modem selection & control layer, which resides above the modem buses for each modem. Measurement point I resides between the policy implementation agent (policy based router/firewall) layer and the transport layer, including TCP, UDP, and other IP as shown. The session layer resides above the transport layer, which is shown as a socket assignment and session management (e.g., basic TCP setup, TLS/SSL) layer. The network services API (e.g., HTTP, HTTPS, FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), POP3, DNS) resides above the session layer. Applications communicate with the device communications stack via the network services API as shown. Policy settings from the network (e.g., service settings) are communicated with the policy implementation agent as shown. The connection manager communicates select and

control as well as modem and access network information via the modem selection and control layer as shown. The service monitor agent, which is also in communication with the agent communication bus 1630, communicates with various layers of the device communications stack. For example, the service monitor agent, performs monitoring at each of measurement points I and II, receiving information including application information, service usage and other service related information, and assignment information. An access control integrity agent is in communication with the service monitor agent via the agent communications bus 1630, as also shown. As similarly described with respect to FIGS. 30 and 31, many of the service usage control verification embodiments described herein can be applied in isolation or in combination in the context of FIG. 32.

[0345] FIG. 33 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments. Referring to FIG. 33, describing the device communications stack from the bottom to the top of the stack as shown, the device communications stack provides a communication layer for each of the modems of the device at the bottom of the device communications stack. Measurement point III resides above the modem selection & control layer, which resides above the respective modem buses for each modem. Measurement point II resides between the policy implementation agent (policy based router/firewall) layer and the transport layer, including TCP, UDP, and other IP as shown. The session layer resides above the transport layer, which is shown as a socket assignment and session management (e.g., basic TCP setup, TLS/SSL) layer. The network services API (e.g., HTTP, HTTPS, FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), POP3, DNS) resides above the session layer. Measurement point I resides between the network services API layer and an application layer, shown as application service interface agent in the device communications stack of FIG. 33.

[0346] Various applications and/or a user service interface agent communicate via this communications stack, as shown (illustrating such communications with a reference (A)). Also, the billing agent, which is in communication with the agent communication bus 1630 communications user information and decision query and/or user input to the user service interface agent, as shown. The policy control agent communicates service settings and/or

configuration information via this communications stack, as shown (illustrating such communications with a reference (B)) via the policy implementation agent layer. The connection manager agent communicates select & control commands and/or modem and access network information via this communications stack, as shown (illustrating such communications with a reference (C)) via the modem selection and control layer. Various other communications (e.g., service processor and/or service controller related communications, such as service usage measure information, application information) are provided at various levels of this communications stack, as shown (illustrating such communications with references (D)) at the application layer and (E) at the policy implementation agent layer.

[0347] As shown in FIG. 33, a service monitor agent, which is also in communication with the agent communication bus 1630, communicates with various layers of the device communications stack. For example, the service monitor agent, performs monitoring at each of measurement points I through III, receiving information including application information, service usage and other service related information, and assignment information. An access control integrity agent is in communication with the service monitor agent via the agent communications bus 1630, as also shown. As similarly described with respect to FIGS. 30, 31 and 32, many of the service usage control verification embodiments disclosed herein can be applied in isolation or in combination in the context of FIG. 33.

[0348] FIG. 34 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments. In some embodiments, the data path processing for the service processor is provided in conjunction with a single modem driver as shown. As shown, the service processor communication stack processing is provided below the standard network communication stack and in combination with a modem driver (e.g., and this approach can be extended to more than one modem).

[0349] Referring to FIG. 34, describing the device communications stack from the bottom to the top of the stack as shown, the device communications stack provides a communication layer for each of the modems of the device at the bottom of the device communications stack. Measurement point II resides above the modem driver 1 layer.

Measurement point I resides between the policy implementation agent (policy based router/firewall) layer and the modem selection and control layer, for the modem driver 1 stack in this single modem driver embodiment. The transport layer, including TCP, UDP, and other IP resides above the IP queuing and routing layer, which resides above the modem selection and control layer, as shown. The session layer, which is shown as a socket assignment and session management (e.g., basic TCP setup, TLS/SSL) layer, resides above the transport layer. The network services API (e.g., HTTP, HTTPS, FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), POP3, DNS) resides above the session layer.

[0350] As shown in FIG. 34, applications communicate with the device communications stack via the network services API as shown (illustrating such communications with a reference (A)). Policy settings from the network (e.g., service settings) are communicated with the policy implementation agent as shown (illustrating such communications with a reference (B)). The service monitor agent, which is also in communication with the agent communication bus 1630, communicates with policy implementation agent layer of the device communications stack. Also, the service monitor agent performs monitoring at each of measurement points I and II, receiving information including application information, service usage and other service related information, and assignment information. An access control integrity agent is in communication with the service monitor agent via the agent communications bus 1630, as also shown. Various other communications (e.g., service processor and/or service controller related communications, such as service usage measure information, application information) are provided at various levels of this communications stack, as shown (illustrating such communications with references (C)) at the policy implementation agent layer. Also, the billing agent, which is in communication with the agent communication bus 1630 communications user information and decision query and/or user input to the user service interface agent, as shown. As similarly described with respect to FIGS. 30, 31, 32 and 33, many of the service usage control verification embodiments disclosed herein can be applied in isolation or in combination in the context of FIG. 34.

[0351] FIG. 35 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments. In particular, FIG. 35 illustrates a

single modem hardware embodiment as shown. As shown, the service processor network communication stack processing is provided on the modem hardware (e.g., and this approach can be extended to more than one modem). This approach allows for the service processor to be distributed as a standard feature set contained in a modem chipset hardware of software package or modem module hardware or software package, which, for example, can provide for easier adoption or development by device OEMs, a higher level of differentiation for the chipset or modem module manufacturer, higher levels of performance or service usage control implementation integrity, or other benefits.

[0352] Referring to FIG. 35, describing the device communications stack from the bottom to the top of the stack as shown, the device communications stack provides a communication layer for each of the modems of the device at the bottom of the device communications stack. As shown, measurement points I and II and the policy implementation agent reside on the modem 1 (e.g., implemented as hardware and/or software on modem 1). Measurement point I resides above the policy implementation agent (policy based router/firewall) layer, and measurement point II resides below the policy implementation agent later. The modem selection and control layer resides above the modem drivers layer, as shown. The transport layer, including TCP, UDP, and other IP resides above the IP queuing and routing layer, which resides above the modem selection and control layer, as shown. The session layer, which is shown as a socket assignment and session management (e.g., basic TCP setup, TLS/SSL) layer, resides above the transport layer. The network services API (e.g., HTTP, HTTPS, FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), POP3, DNS) resides above the session layer.

[0353] As shown in FIG. 35, applications communicate with the device communications stack via the network services API as shown. Policy settings from the network (e.g., service settings) are communicated with the policy implementation agent as shown (illustrating such communications with a reference (A)). The service monitor agent, which is also in communication with the agent communication bus 1630, communicates with policy implementation agent layer of the modem 1. Also, the service monitor agent performs monitoring at each of measurement points I and II, receiving information including application information, service usage and other service related information, and assignment information.

An access control integrity agent is in communication with the service monitor agent via the agent communications bus 1630, as also shown. Various other communications (e.g., service processor and/or service controller related communications, such as service usage measure information and/or application information) are provided at various levels of this communications stack, as shown (illustrating such communications with references (B)) at the policy implementation agent layer. As similarly described with respect to FIGS. 30, 31, 32, 33 and 34, many of the service usage control verification embodiments disclosed herein can be applied in isolation or in combination in the context of FIG. 35.

[0354] FIG. 36 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments. In particular, FIG. 36 illustrates a single modem hardware embodiment, in which modem 1 includes a portion of the service processor networking communication stack processing and measurement points II and III and the policy implementation agent, as similarly shown in FIG. 35, and the higher levels of the device communications stack above the modem 1 layer, such as the application service interface layer, are implemented on the device application processor or in the device application processor memory as similarly described above, for example, with respect to FIG. 33, in which a measurement point I is shown between the application service interface agent layer and the network services API layer. For example, this approach allows for the application service interface agent to be provided on the device application processor or memory so that application layer service usage monitoring or control can be implemented. For example, the differences between the embodiments depicted in FIG. 36 and those of FIG. 30 include a simplified implementation and a policy control agent that is entirely implemented on the modem and not partially implemented in the application processor memory.

[0355] Various applications and/or a user service interface agent communicate via this communications stack, as shown (illustrating such communications with a reference (A)). Also, the billing agent, which is in communication with the agent communication bus 1630 communications user information and decision query and/or user input to the user service interface agent, as shown. The policy control agent communicates service settings and/or configuration information via this communications stack, as shown (illustrating such

communications with a reference (B)) via the policy implementation agent layer. Various other communications (e.g., service processor and/or service controller related communications, such as service usage measure information and/or application information) are provided at various levels of this communications stack, as shown (illustrating such communications with reference (C) at the application layer and communications with reference (D) at the policy implementation agent layer). As shown, the service monitor agent B communicates with the application service interface agent and measurement point I, and the service monitor agent A communicates with the policy implementation agent layer and measurement points II and III of the modem 1. As similarly described with respect to FIGS. 30, 31, 32, 33, 34 and 35, many of the service usage control verification embodiments disclosed herein can be applied in isolation or in combination in the context of FIG. 36.

[0356] FIG. 37 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments. In particular, FIG. 37 illustrates a device communications stack as similarly shown in FIG. 36, with the difference being that the service processor subsystem networking communication stack processing is implemented on a hardware function that is separate from the application processor and the modem. For example, this approach provides security advantages with a dedicated hardware system to protect some or all of the service usage control system from tampering. For example, some or all of the service processor can be implemented on a SIM card module. As another example, some or all of the service processor can be encapsulated on a self contained hardware module that can be added to a device without the need to modify the networking communication stack software or hardware.

[0357] FIG. 38 is a functional diagram illustrating a device service processor packet processing flow in accordance with some embodiments. In particular, both an example upstream service processor packet processing flow (device to the network) and an example downstream service processor packet processing flow (network to the device) are shown in FIG. 38. For example, the service processor packet processing flow can be performed by the device communications stack, such as described above with respect to FIG. 29. The various embodiments for packet processing flow depicted in FIGS. 38 through 40 are self explanatory to

one of ordinary skill in the art and not all the processing steps and flow sequences are described herein.

[0358] In some embodiments, the burst size, buffer delay, acknowledgement delay and drop rate used in upstream and downstream traffic shaping are optimized with the goal of reducing access network traffic overhead, and excess capacity usage that can result from mismatches in traffic transmission parameters with the access network MAC and PHY or from excess network level packet delivery protocol re-transmissions. In some embodiments, an application interface agent 1693 is used to literally tag or virtually tag application layer traffic so that the policy implementation agent(s) 1690 has the necessary information to implement selected traffic shaping solutions. As shown in FIG. 16, the application interface agent 1693 is in communication with various applications, including a TCP application 1604, an IP application 1605, and a voice application 1602.

[0359] Referring to FIGS. 38 through 40, in some embodiments, the upstream traffic service policy implementation step corresponds to the traffic shaping step described herein. Referring to FIG. 38, this step is depicted as shown as an alternate exploded view including four upstream sub-steps of apply QoS queue priority, apply traffic shaping rules, network optimized buffer/delay and remove application ID tag. An additional approach shown in FIG. 38 involves two exploded view sub-steps associated with the firewall service policy implementation step and these sub-steps are pass/block packet and pass/redirect packet. For example, the functions performed by these six sub-steps can be depicted in any number of sub-steps, the order of the steps can be appropriately performed in various different orders to provide for upstream traffic shaping within the network communication stack. For example, FIGS. 39 and 40 show the two steps of policy implementation and firewall as one step and the six exploded view sub-steps are included under the same policy implementation step and are performed in a different order than in FIG. 38. It should also be noted that a number of embodiments are possible in which the access control, traffic control or firewall functions are moved to the application service interface layer or another layer.

[0360] Referring now to the downstream portion of FIG. 38, there are two steps again termed traffic service policy implementation and firewall service policy implementation in this

traffic shaping, access control and firewall example. These two packet flow processing steps are depicted as shown in the exploded view as the five sub-steps of tag with flow ID, pass/block packet, apply QoS, apply traffic shaping rules and network optimized buffer, delay, and drop. As with the upstream packet processing flow, the number of sub-steps, the order of sub-steps and the location of the sub-steps in the downstream networking stack processing can be depicted in any number of sub-steps, order and/or location, and various other embodiments will be apparent to one of ordinary skill in the art, including embodiments which locate some or all of the steps in the application service interface layer or other layers as depicted in FIGS. 39 and 40. The details of the packet flow processing design for the downstream can be somewhat more complex in certain embodiments as compared to the upstream processing in two ways. First, as described herein, in some embodiments, the packet tagging that requires application level information can require the initial portion of the packet flow burst to pass through the upstream networking communication stack until the application service interface layer can associate the packet flow with the appropriate information visible at the application level at which time the packet flow tag is communicated to the other service processor agent functions so that they can properly monitor or control the traffic associated with the flow.

[0361] Independently, another complication arises when upper layer reliable communication protocols, such as TCP, are employed in the networking stack in which the downstream transmitting end repeats the packet transmission if the receiving TCP protocol stack does not send a packet receipt acknowledge (ACK) within a certain period of time. If packets are arbitrarily delayed or dropped, then the TCP re-transmission traffic can reduce, completely eliminate or even reverse the network capacity advantage gained by reducing the average traffic speed or other transmission quality measure for one or more service activities. To solve this problem, in some embodiments, the packet traffic control parameters (e.g., downstream delay, drops, burst length, burst frequency and/or burst jitter) are optimized for TCP re-transmission efficiency so that changes in traffic control access bandwidth or speed for one or more service activities are implemented in such a manner that the TCP re-transmission delay at the network transmitting end adapts to be long enough so that wasted packet re-transmission bandwidth is reduced. In addition, and either in combination or in isolation, in some embodiments, the packet traffic control parameters (e.g., downstream delay, drops, burst length, burst frequency and/or

burst jitter) can be adjusted so that the access network downstream MAC and/or PHY efficiencies are optimized.

[0362] Numerous other embodiments for the detailed implementation of packet flow processing in both downstream and upstream will be apparent to one of ordinary skill in the art in view of the various embodiments described herein. In some embodiments, as described herein, the following are provided: (A) traffic shaping is performed in a verifiable manner, (B) traffic shaping is performed in a manner that results in improved network capacity by taking into account to some degree the manner in which the access network PHY layer and/or MAC layer responds to packet parameters (e.g. burst delay, burst drops, burst length, burst frequency and/or burst jitter), (C) traffic shaping is performed in a manner that results in improved network capacity by taking into account how the packet parameters (e.g., burst delay, burst drops, burst length, burst frequency and/or burst jitter) impact layer 3 and higher ACK protocol or other network protocol network capacity efficiencies, (D) packet shaping is performed in a manner that is aware of and optimized for the particular type of communication protocol or packets being sent (e.g., TCP packets can be dropped to slow the application rate of transfer whereas UDP packets are never dropped, because there is no re-transmission), (E) a virtual or literal packet tagging system is used in a verifiable traffic shaping service control system to provide a deeper level of service monitoring and control or to simplify the processing of the packets, and/or (F) starting with these low level packet processing, traffic control or access control building blocks one or more additional layers of higher level policy control can be added on the device or in the network to create service profiles for the service provider network that define complete services, such as ambient services and many other variations of service profile settings that each define a device or user service experience and can be associated with a billing plan. For example, the use of higher layers of service profile control to form more complete service solutions starting with these relatively simple low-level traffic control, access control or firewall processing steps or functions is also described herein.

[0363] FIG. 39 is another functional diagram illustrating the device service processor packet processing flow in accordance with some embodiments. In particular, both an example upstream service processor packet processing flow (device to the network) and an example downstream service processor packet processing flow (network to the device) are shown in FIG.

39 (e.g., of a less feature rich device service processor embodiment, such as one similar to that depicted in FIG. 32).

[0364] FIG. 40 is another functional diagram illustrating the device service processor packet processing flow in accordance with some embodiments. In particular, both an example upstream service processor packet processing flow (device to the network) and an example downstream service processor packet processing flow (network to the device) are shown in FIG. 40 (e.g., of a mid-featured embodiment of a device service processor, such as one similar to that depicted in FIG. 33).

[0365] FIG. 41 provides a table summarizing various privacy levels for service history reporting in accordance with some embodiments. Many of these privacy levels are similarly described above, and the table shown in FIG. 41 is not intended to be an exhaustive summary of these privacy levels, but rather is provided as an aid in understanding these privacy levels in accordance with user privacy related embodiments described herein. For example, there are many other parameters that can be associated with privacy filtering, and as will be apparent to one of ordinary skill in the art in view of the various embodiments described herein, the unique feature of user defined or user influenced privacy filtering for service usage, service activity or CRM reports can be implemented with a variety of embodiments that are variations of those described herein.

[0366] FIGS. 42A through 42J provide tables summarizing various service policy control commands in accordance with some embodiments. Many of these service policy control commands are similarly described above, and the tables shown in FIGS. 42A-J are not intended to be an exhaustive summary of these service policy control commands and do not include summaries of all the embodiments described herein, but rather are provided as a summary aid in understanding these service policy control commands in accordance with various embodiments described herein.

[0367] In some embodiments, QoS is employed for devices with a service processor 115. For example, QoS can be employed in a crowded hot spot where the service processor 115 profile has been changed from WWAN to WLAN, but the WLAN is backed up as too many users are trying to use it. The service processor 115 can have a hierarchical access to the hotspot

at that point; or the service processor 115 that pays less can be throttled while those that pay more are opened up; or the service processor 115 can initiate a policy that slows down transmissions to improve trunking efficiency.

[0368] FIGS. 43A through 43B are flow diagrams illustrating a flow diagram for a service processor authorization sequence as shown in FIG. 43A and a flow diagram for a service controller authorization sequence as shown in FIG. 43B in accordance with some embodiments.

[0369] Referring to FIG. 43A, at 4302, the device is in an offline state. At 4304, the service processor (e.g., service processor 115) of the device collects device service processor credentials and access control integrity information. At 4306, the service processor of the device selects a best network. At 4308, the device connects to an access network. At 4310, the service processor of the device sends an authorization request to the service controller (e.g., service controller 122) and also sends the credentials and access control integrity information. At 4312, the service processor determines whether an integrity error has occurred. If so, then the service processor performs integrity error handling at 4314. Otherwise, the service processor determines whether the device is activated and/or authorized for network access at 4316. If not, then the service processor performs a device activation sequence at 4318. At 4320, the service processor performs the following: updates critical software, initializes service policy and control settings, synchronizes service counters, updates service cost data, applies policy settings, applies CRM rules settings, obtains transaction identity certificate, and sends stored CRM and billing information. At 4322, the device is in an online state.

[0370] Referring to FIG. 43B, at 4332, device control is in an offline state. At 4334, the service controller (e.g., service controller 122) receives a device authorization request, verifies device service plan standing, verifies device access control integrity standing, verifies device access control integrity information, verifies service processor heartbeat, and performs various additional service processor integrity checks (e.g., as similarly described herein). At 4336, the service controller determines whether the device integrity checks have all passed. If not, then the service controller sends an integrity error to the service processor (e.g., service processor 115) at 4338. At 4340, the service controller performs integrity error handling. Otherwise (the device integrity checks have all passed), the service controller determines whether the device is

activated at 4342. If not, then the service controller sends an activation message to the service processor at 4344. At 4346, the service controller performs a service activation sequence. Otherwise (the device is activated), the service controller sends an authorization at 4348. At 4350, the service controller performs the following: updates critical software on the service processor, initializes service policy and control settings, synchronizes service counters, updates service cost data, applies policy settings, applies CRM rules settings, obtains transaction identity certificate, sends stored CRM and billing information. At 4352, the service controller is in a device online state.

[0371] FIGS. 44A through 44B are flow diagrams illustrating a flow diagram for a service processor activation sequence as shown in FIG. 44A and a flow diagram for a service controller activation sequence as shown in FIG. 44B in accordance with some embodiments.

[0372] Referring to FIG. 44A, at 4402, a service processor activation sequence is initiated. At 4404, the service processor (e.g., service processor 115) of the device displays an activation site (e.g., HTTP site, WAP site or portal) to the user for the user's service activation choice. At 4406, the user selects service plan, billing information and CRM information. At 4408, the service processor sends an activation request and user billing and CRM information to, for example, the service controller. At 4410, the service processor determines whether there is an integrity error. If so, then the service processor performs integrity error handling at 4412. Otherwise, the service processor determines whether there has been a selection input error at 4414. If so, the service processor displays the selection input error to the user at 4416 and returns to the activation site/portal at 4404. Otherwise, the service processor identifies the activated service plan at 4418. At 4420, the service processor performs the following: updates critical software, initializes service policy and control settings, synchronizes service counters, updates service cost data, applies policy settings, applies CRM rules settings, obtains transaction identity certificate, and sends stored CRM and billing information. At 4422, the device is in an online and activated state.

[0373] Referring to FIG. 44B, at 4432, a service controller activation sequence is initiated. At 4434, the service controller (e.g., service controller 122) receives an activation request, including user billing and CRM information, and sends such to central billing. At 4436,

the service controller receives a response from central billing. At 4438, the service controller verifies the integrity of the service processor. If an integrity error is detected, then an integrity error is sent at 4440. At 4442, the service controller performs integrity error handling. At 4444, the service controller determines whether the service plan has been activated. If not, then the service controller sends a selection input error to the device at 4446 and returns to 4432. Otherwise (device has been activated), the service controller sends the service plan activation information to the device at 4448. At 4450, the service controller performs the following: updates critical software, initializes service policy and control settings, synchronizes service counters, updates service cost data, applies policy settings, applies CRM rules settings, obtains transaction identity certificate, and sends stored CRM and billing information. At 4452, the service controller is in a device online and activated state.

[0374] FIGS. 45A through 45B are flow diagrams illustrating a flow diagram for a service processor access control sequence as shown in FIG. 45A and a flow diagram for a service controller access control sequence as shown in FIG. 45B in accordance with some embodiments.

[0375] Referring to FIG. 45A, at 4502, the device is in an online state. At 4504, the service processor (e.g., service processor 115) of the device processes any new heartbeat messages received from the service controller (e.g., service controller 122). At 4506, the service processor updates software if necessary, updates service policy and control settings if necessary, synchronizes service counters, updates service cost data if necessary, and updates CRM rules if necessary. At 4508, the service processor performs access control integrity checks. At 4510, the service processor determines whether there are any access control integrity errors. If so, then the service processor performs integrity error handling at 4512. Otherwise, the service processor updates user service UI gauges, provides notification if necessary, and accepts input if available at 4514. At 4516, the service processor sends new service processor heartbeat messages to the heartbeat message queue. At 4518, the service processor processes any pending billing transactions. At 4520, the service processor determines if a heartbeat transmission is due, and if not, returns to 4504 for processing any received heartbeat messages. If so, at 4522, the service processor sends the new service processor heartbeat message to the service controller.

[0376] Referring to FIG. 45B, at 4532, the device is in an online state. At 4534, the service controller (e.g., service controller 122) processes any new heartbeat messages received from the service processor. At 4536, the service controller performs access control integrity checks. At 4538, the service controller determines whether there are any access control integrity errors. If so, then the service controller performs integrity error handling at 4540. At 4542, the service controller updates the billing database, updates the CRM information, synchronizes service counters, updates cost database if needed, and synchronizes CRM rules if necessary. At 4544, the service controller processes any pending billing transactions. At 4546, the service controller sends new service processor heartbeat messages to the heartbeat message queue. At 4548, the service controller determines if a heartbeat transmission is due, and if not, returns to 4534 for processing any received heartbeat messages. If so, at 4550, the service controller sends new service processor heartbeat message to the service processor.

Open Content Distribution and Transaction System

[0377] Referring now to FIGS. 46 and 47A-47B, in another set of embodiments an open, decentralized, device based system for enabling central billing for third party electronic commerce transactions for mobile commerce is provided as shown. For example, in these embodiments, device information can be embedded in HTTP, WAP or other portal browser/network header request information that indicates a central billing option is available to a compatible third party transaction server, as further described below with respect to FIGS. 46 and 47A-47B.

[0378] FIG. 46 is a functional diagram illustrating open, decentralized, device based mobile commerce transactions in accordance with some embodiments. As shown, a service processor 4615 of the device 100 (e.g., any mobile device capable of storing and executing the service processor 4615) includes access control integrity agent 1694, billing agent 1695, agent communication bus 1630, user interface 1697, policy control agent 1692, service monitor agent 1696, application interface agent 1693, policy implementation agent 1690, and modem router and firewall 1655, as similarly described herein with respect to various other service processor embodiments. In some embodiments, an application 4604 (e.g., an HTML/WAP web browser) and a mobile payment agent 4699 are also included in the device, such as part of the service

processor 4615 as shown. In some embodiments, the application 4604 is not integrated as part of the service processor 4615, but is executing and/or stored on the device. In some embodiments, the mobile payment agent 4699 includes billing agent 1695, user interface 1697 and/or application interface agent 1693, and/or various other functional components/agents. As shown, the service processor 4615 is in communication with a carrier access network 4610, which is in network communication with the Internet 120.

[0379] In some embodiments, device information can be embedded in HTTP, WAP or other portal browser/network header request information that indicates a central billing option is available to a compatible third party transaction server, such as the open content transaction partner site(s) 134. For example, the compatible transaction server can then send a signed confirmation request over a pre-assigned control socket channel to the billing agent 1695 with the billing agent 1695 confirming the signed confirmation request by either performing the signature check locally based on a stored and synchronized list of approved transaction servers or by passing the signed request onto a billing server 4630 for confirmation. Optionally, in another example, a triangle confirmation can be set up in which the billing server 4630 can confirm the transaction set up with the transaction server 134 or the transaction server 134 can confirm the transaction set up with the billing server 4630. Once the device confirms the compatible and approved status of the transaction server 134, the device/transaction server pair can then optionally further exchange keys for the remainder of the transaction for enhanced security. In another example, the transaction server 134 can also redirect the user browsing experience to one tailored to one or more of device type, service provider, device manufacturer or user. When the user selects a transaction, the transaction server sends the billing agent 1695 a transaction bill that describes the transaction and the amount. The billing agent 1695 can optionally confirm that the user account has sufficient credit limit to make the purchase by either confirming the stored credit limit on the device or querying the billing server 4630. The billing agent 1695 then invokes the device UI 1697 to display the transaction description and amount and request user approval for the billing to be conducted through the central billing option. User approval can be acquired, for example, by a simple click operation or require a secure password, key and/or biometric response from the user. Upon user approval, the billing agent 1695 generates a billing approval and sends it to the transaction server 134, the transaction server 134 completes the transaction and then sends a bill to the billing agent 1695. The billing agent 1695 optionally

sends a confirmation to the transaction server 134 and sends the bill to the billing server 4630. Again, optionally a triangle confirmation can be formed by the billing server sending a confirmation to the transaction server 134, or the transaction server 134 can send the bill to the billing server 4630. In some embodiments, the billing server 4630 can also communication such billed transactions to a central provider billing system 4623 via the carrier access network 4610. Also, in some embodiments, an alternate location billing server 4632 is in communication via the Internet 120, and an alternate location central provider billing system 4625 is also in communication via the Internet 120.

[0380] FIGS. 47A through 47B are transactional diagrams illustrating open, decentralized, device based mobile commerce transactions in accordance with some embodiments. Referring to FIG. 47A, the device application 4604 browses (e.g., based on the user submitting a browse request using a browser application) to transaction server 134 (e.g., a transaction web server, such as the open content transaction partner site 134). The transaction server 134 provides an offer to the device application 4604. The device application 4604 selects a purchase (e.g., based on the user's selection input). In response, the transaction server 134 seeks an API connection with the device mobile payment agent 4699, which then confirms the API connection. The transaction server 134 requests user purchase confirmation (mediated by the device mobile agent 4699 as shown), and the purchase is confirmed by the device application 4604 (e.g., based on the user's acknowledgement as similarly described above with respect to FIG. 46). The transaction server 134 then transmits a purchase receipt, and the device application 4604 confirms the receipt. The transaction server 134 then transmits the purchase bill to the device mobile payment agent 4699, which then sends the purchase bill to the device billing server (e.g., billing server 4630). The transaction server also optionally sends a confirmation of the purchase bill to the device billing server for a triangle confirmation, as similarly described above with respect to FIG. 46. The device billing server sends a copy of the purchase bill to the central provider billing system (e.g., central provider billing system 4623).

[0381] Referring now to FIG. 47B, the device application 4604 browses (e.g., based on the user submitting a browse request using a browser application) to transaction server 134 (e.g., a transaction web server, such as the open content transaction partner site 134), in which the browse request includes device ID information, such as similarly described above with respect to

FIG. 46. The transaction server 134 establishes API contact with the device mobile agent 4699, which then confirms contact and good standing for transactional purchases from the device. The transaction server 134 provides an offer to the device application 4604. The device application 4604 selects a purchase (e.g., based on the user's selection input). The transaction server 134 notifies the device mobile payment agent 4699 of the purchase description and amount, and the device mobile payment agent 4699 then requests user purchase confirmation. The purchase is confirmed by the device application 4604 (e.g., based on the user's acknowledgement as similarly described above with respect to FIG. 46), and the device mobile payment agent 4699 then transmits a purchase confirmation to the transaction server 134. The transaction server 134 then transmits a purchase receipt, and the device application 4604 confirms the receipt. The transaction server 134 then transmits the purchase bill to the device mobile payment agent 4699, which then sends the purchase bill to the device billing server (e.g., billing server 4630). The transaction server also optionally sends a confirmation of the purchase bill to the device billing server for a triangle confirmation, as similarly described above with respect to FIG. 46. The device billing server sends the purchase bill to the central provider billing system (e.g., central provider billing system 4623). In some embodiments, the communications described above with respect to FIGS. 47A-47B with the billing server and the central provider billing system are with the alternate location billing server 4632 and/or alternate location central provider billing system 4625 via the Internet 120. Similarly, in some embodiments, the transaction servers 134 are connected to the Internet 120.

[0382] Accordingly, these transaction billing embodiments do not require centralized content storage or content and transaction exchange infrastructure. For example, the transactions can be conducted over the Internet, and the user experience and content can be tailored versions of the transaction server/content provider's normal experience and content. This approach provides for a much wider array of content and transaction partners with minimal or no need to accommodate proprietary specialized systems. Moreover, the compatibility between the device billing agent transaction system and the transaction provider server is easily established, for example, by writing specifications for the header information transmitted by the device and for the secure handshake and signed message transactions that take place between the device billing agent, the transaction server and optionally the transaction server and the billing server. Once a transaction partner shows compatibility test results and concludes a business relationship with

the service provider, the service provider can place the transaction partner on the compatible and approved list and exchange security keys and/or certificates. If a common user experience is desired by the service provider across multiple transaction partners, then the experience specifications for the browser redirects can also be specified in the compatibility specification and tested before the transaction partner gains approval.

Design and Testing for Service Control

[0383] FIG. 48 illustrates a network architecture including a service controller device control system and a service controller analysis and management system in accordance with some embodiments. As described herein, the RAN gateway 410 generally represents the functionality of the various specific RAN gateway functional elements shown and/or discussed herein. For example, these RAN gateway 410 functional elements represent the gateways used to aggregate the radio access network traffic, control, charging and roaming functions and/or other functions and are shown and/or discussed herein using other terminology specific to certain industry standards, including SGSN gateway 410 and gateways 508, 512, 608, 612, 708 and 712. Although the same reference numerals are used for SGSN gateway 410 and RAN gateway 410, it will be appreciated that the RAN gateway 410 represents any or all of the RAN gateway functional elements 410, 508, 512, 608, 612, 708, 712 or any other similar industry equipment or functions depending on the embodiment. Similarly, transport gateway 420 represents the next higher level of gateway aggregation for the transport layer that is used in many networks, and this term transport gateway 420 can be interchanged with any or all of the gateways 420, 520, 620, 720 or any other similar industry equipment or functions depending on the embodiment. Those of ordinary skill in the art will appreciate which gateway description applies to a respective embodiment in which the terms RAN gateway 410, gateway 410, transport gateway 420 or gateway 420 are referenced herein.

[0384] While the embodiments described below with respect to FIGS. 48 through 63 are depicted in the context of a conventional multi-tier access network, one of ordinary skill in the art will appreciate that such embodiments can also be generalized to other network topologies including the various flattened network topologies described herein. As shown, the service controller is divided into two main functions (e.g., as compared with the embodiments of service

controller 122 depicted in FIG. 16): (1) a service controller device control system 4825 and (2) a service controller design, policy analysis, definition, test, publishing system 4835. The service controller device control system 4825 performs the device service control channel functions as previously described herein with respect to various embodiments.

[0385] The service controller design, policy analysis, definition, test, publishing system 4835 separates out the service analysis, control policy design and publishing from the device service control channel functions. The service controller design, policy analysis, definition, test, publishing system 4835 performs a variety of functions as described below. In some embodiments, the service controller design, policy analysis, definition, test, publishing system 4835 provides service usage statistical analysis, notification policy or procedure response analysis and/or billing policy or procedure response analysis for single devices, groups of devices, types of devices, groups of users, classes of users, or an entire set of devices and users that subscribe to a given service. In some embodiments, the service controller design, policy analysis, definition, test, publishing system 4835 detects, singles out and reports device service usage, notification responses or billing behavior that is outside of expected limits but may or may not be violating policy. In some embodiments, the service controller design, policy analysis, definition, test, publishing system 4835 provides service cost and profitability analysis for single devices, groups of devices, types of devices, groups of users, classes of users, or an entire set of devices and users that subscribe to a given service. In some embodiments, the service controller design, policy analysis, definition, test, publishing system 4835 provides user service control policy, notification policy or billing policy statistical satisfaction analysis for single devices, groups of devices, types of devices, groups of users, classes of users, or an entire set of devices and users that subscribe to a given service. In some embodiments, the service controller design, policy analysis, definition, test, publishing system 4835 provides statistical take rate analysis for transaction offers and billing offers for single devices, groups of devices, types of devices, groups of users, classes of users, or an entire set of devices and users that subscribe to a given service.

[0386] In some embodiments, the service controller design, policy analysis, definition, test, publishing system 4835 provides service control policy definition work screens and "dry-lab" (pre-beta) testing against usage database for single devices, groups of devices, types of

devices, groups of users, classes of users, or an entire set of devices and users that subscribe to a given service. In some embodiments, the service controller design, policy analysis, definition, test, publishing system 4835 provides service control policy, notification policy and/or billing policy beta testing (e.g., using beta test server 1658) in which the beta test profile is published to a subset of users or devices. In some embodiments, beta devices/users may or may not know that the service policy is being tested with them. In some embodiments, if they do know, then beta test apparatus includes offering system that provides user options to accept beta test and provide feedback in exchange for an offer (e.g., show them an offer page that comes up with their existing subscription service or ambient service – offer a free trial, a discount to something and/or reward zone points (or other incentives/rewards) if they accept the trial). In some embodiments, a beta test workstation (e.g., in communication with the beta test server 1658, such as VSP remote workstation 4920 as shown in FIG. 49) allows the beta test manager to define one or more beta test service policy, notification policy and/or billing policy control profiles. In some embodiments, the beta test workstation publishes each profile to specific individual (single) devices, groups of devices, types of devices, groups of users, classes of users, or an entire set of devices and users that subscribe to a given service. In some embodiments, the beta test workstation allows the beta test manager to analyze usage statistics, notification response statistics and/or billing/transaction offer response statistics for devices, users, groups of devices or groups of users and compare actual real-time usage versus beta test usage goals. In some embodiments, the beta test workstation allows the beta test manager to fine tune service, notification and/or billing/transaction policies and re-publish to observe changes to actual service usage until the service policy and/or notification control policies achieve the desired result. In some embodiments, the beta test workstation also allows the beta test manager to collect direct user feedback to a set of pre-designed user satisfaction or other questions regarding service usage. For example, questions can be presented through a pre-designed beta test portal or through a series of brief pop-ups that come up when the user initiates a particular action or at a particular time. In some embodiments, the beta test workstation also collects details of service and device usage (e.g., CRM data) that the beta test users have approved for collection. In some embodiments, the beta test workstation can decompose this data to determine if the users are using the service in the manner intended by the beta test goals. In some embodiments, the beta test workstation also allows for publishing multiple variants of the service and/or notification

policy control settings and compare the service usage for each group with convenient screens with information displays (e.g., statistical usage versus time of day, usage of particular activities, billing activity, device discovery activity, user response to notification message and options, user satisfaction with a particular notification policy or billing policy or traffic control policy). In some embodiments, the screens can be designed by the beta test manager.

[0387] In some embodiments, once a service is completely tested and approved for production publication, the service download control server 1660 has a workstation screen that allows the service manager to specify which group of devices are to receive the new service policy configuration. In some embodiments, the service download control server 1660 allows the service manager to define specific individual (single) devices, groups of devices, types of devices, groups of users, classes of users, or an entire set of devices and users that subscribe to a given service.

[0388] In some embodiments, a service (e.g., a newly created or new version of an existing service) is tested and/or enhanced using a new service testing model. For example, a new service (or a new version of an existing service) is loaded onto a server for testing, the new service is (optionally) tested against existing device usage statistics, a new service control definition (e.g., implemented as service processor 115 for publishing to devices 100 and a corresponding new service controller 122 for the service provider, such as a central provider or an MVNO partner, and, for example, the new service processor and service controller can be implemented using the below described SDK) for the new service is developed and possibly adjusted based on the testing against existing device usage statistics, the new service control definition is then published to beta devices (e.g., various devices 100 used for beta testing the new service), which then use the new service, service usage statistics and/or user feedback statistics are then collected (e.g., to ensure that the service is functioning properly and so that the service control definition can be tuned to ensure adequate service, user experience and for service pricing/profitability purposes), the service/service control definition is then fine tuned based on the service usage/user feedback statistics. Upon completion of the above testing and refinement of the service/service control definition, the service control definition can be published to specified groups of devices for using the new service. In some embodiments, this service control testing model for groups of devices and service partners is provided by a virtual

MVNO or VSP. For example, this allows for new services to be more efficiently and more effectively developed, tested and proliferated.

[0389] In some embodiments, service history IPDRs come from within a networking component connected to the central provider core network 110 as depicted by (e.g., real-time) service usage 118 (which as discussed elsewhere is a general purpose descriptor for a function located in one or more of the networking equipment boxes). In some embodiments, service history IPDRs are collected/aggregated (in part) from the central billing system 123. In some embodiments, service history IPDRs are collected/aggregated (in part) from the transport gateways 420. In some embodiments, service history IPDRs are collected/aggregated (in part) from the RAN gateways 410. In some embodiments, service history IPDRs are collected/aggregated (in part) from the base station(s) 125 or a networking component co-located with the base station(s) 125, a networking component in the transport network 415, a networking component in the core network 110 or from another source.

Virtual Service Provider for Service Control

[0390] In some embodiments, virtual service provider (VSP) capabilities include making available to a third party service partner one or more of the following: (1) device group definition, control and security, (2) provisioning definition and execution, (3) ATS activation owner, (4) service profile definitions, (5) activation and ambient service definition, (6) billing rules definition, (7) billing process and branding controls, (8) bill by account settings, (9) service usage analysis capabilities by device, sub-group or group, (10) beta test publishing capabilities by device, sub-group or group, and (11) production publishing, fine tuning and re-publishing.

[0391] FIG. 49 illustrates a network architecture for an open developer platform for virtual service provider (VSP) partitioning in accordance with some embodiments. As shown, the service controller design, policy analysis, definition, test, publishing system 4835 is configured so that multiple "service group owners" (e.g., the service provider for certain smart phones) or "device group owners" (e.g., eReader devices for the eReader service provider(s)) or "user group owners" (e.g., IT for Company X for their employees' corporate mobile devices), collectively referred to as the "Virtual Service Provider" (VSP), are serviced with the same service controller infrastructure and the same (or substantially similar) service processor design

from virtual service provider workstation server 4910 and/or virtual service provider remote workstation(s) 4920. As shown, the virtual service provider remote workstation(s) 4920 communicates with the virtual service provider workstation server 4910 via VPN, leased line or secure Internet connections. The dashed lines shown in FIG. 49 are depicted to represent that, in some embodiments, the virtual service provider workstation server 4910 is networked with the service controller device control system 4825 and/or, in some embodiments, the service controller design, policy analysis, definition, test, publishing system 4835. Based on the discussion herein, it will be apparent to one of ordinary skill in the art that the VSP workstation server 4910 can also be networked in various embodiments with billing system 123, AAA server 121, gateways 410 or 420, or other network components to perform, for example, various network provisioning and activation related functions discussed herein for the device group assigned to one or more VSPs, or for other reasons as will be apparent to a given VSP embodiment.

[0392] In some embodiments, the service controller functionality is partitioned for a VSP by setting up one or more secure workstations, secure portals, secure websites, secure remote software terminals and/or other similar techniques to allow the service managers who work for the VSP to analyze, fine tune, control or define the services they decide to publish to one or more groups of devices or groups of users that the VSP "owns," In some embodiments, the VSP "owns" such groups by virtue of a relationship with the central provider in which the VSP is responsible for the service design and profitability. In some embodiments, the central provider receives payment from the VSP for wholesale access services. In some embodiments, the VSP workstations 4910 and 4920 only have access to the service analysis, design, beta testing and publishing functions for the devices or users "owned" by the VSP. In some embodiments, the user or device base serviced by the central provider network is securely partitioned into those owned by the central provider, those owned by the VSP, and those owned by any other VSPs.

[0393] In some embodiments, the VSP manages their devices from the VSP workstations 4910 and 4920 using device based service control techniques as described herein. In some embodiments, the VSP manages their devices from the VSP workstations 4910 and 4920 using device assisted and network based service control techniques as described herein. In some

embodiments, the VSP manages their devices from the VSP workstations 4910 and 4920 using network based service control techniques (e.g., DPI techniques) as described herein.

[0394] For example, this approach is particularly well suited for "open developer programs" offered by the central providers in which the central provider brings in VSPs who offer special value in the devices or service plans, and using this approach, neither the central provider nor the VSP needs to do as much work as would be required to set up a conventional MVNO or MVNE system, which often requires some degree of customization in the network solution, the billing solution or the device solution for each new device application and/or service application that is developed and deployed. In some embodiments, the service customization is simplified by implementing custom policy settings on the service processor and service controller, and the custom device is quickly brought onto the network using the SDK and test/certification process. In some embodiments, the VSP functionality is also offered by an entity other than the central provider. For example, an MVNE entity can develop a wholesale relationship with one or more carriers, use the service controller to create the VSP capabilities, and then offer VSP services for one network or for a group of networks. In some embodiments, the service customization is simplified by implementing custom policy settings through the VSP embodiments on the network equipment, including, in some embodiments, service aware or DPI based network equipment that has a relatively deep level of service activity control capability. For example, using the embodiments described herein, and possibly also including some of the activation and provisioning embodiments, it is possible to efficiently design and implement custom ambient service plans that are different for different types of devices, different OEMs, different VSPs, different distributors, or different user groups all using the same general infrastructure, whether the service control policy implementation is accomplished primarily (or exclusively) with networking equipment (network) based service control, primarily (or exclusively) with device based service control or with a combination of both (e.g., hybrid device and network based service control).

[0395] As discussed herein, various VSP embodiments for performing one or more of analyzing traffic usage and defining, managing service profiles or plans, dry lab testing service profiles or plans, beta testing service profiles or plans, fine tuning service profiles or plans, publishing service profiles or plans, or other policy related settings can involve programming

settings in the network equipment and/or programming settings or software on the device. For example, as discussed herein, the service processor settings are controlled by the service controller, which can be partitioned to allow groups of devices to be controlled. As another example, equipment in the network involved with network based service control, such as DPI based gateways, routers or switches, can similarly be programmed to utilize various VSP embodiments to implement that portion of the service profile (or service activity usage control) that is controlled by network level functions, and it will be appreciated that substantially all or all of the service activity control for certain embodiments can be accomplished with the network functions instead of the device. Continuing this example, just as the device service processor settings control functions of the service processor can have a group of devices that are partitioned off and placed under the control of a VSP, various VSP control embodiments can partition off a group of devices that have service usage activity controlled by the networking equipment, including, in some embodiments, sophisticated service aware DPI based service control equipment, to achieve similar objectives. It will be appreciated that the discussion herein regarding service controller design, policy analysis, test, publishing 4835, and the discussion regarding device group, user group and other VSP related embodiments, should be understood as applicable to various embodiments described in view of device based services control, control assistance and/or monitoring, or network based services control, control assistance and/or monitoring, or a combination of device based services control, control assistance and/or monitoring and network based services control, control assistance and/or monitoring. The various embodiments described herein related to service activation and provisioning also make apparent how the programming of network equipment service control, service control assistance and/or monitoring can be implemented prior to and following activation of the device. It will also be appreciated that the VSP capabilities described herein can also be applied to those devices that have services controlled by, provided by and/or billed by the central provider, so these techniques can be applied to central provider service embodiments, MVNO embodiments and other embodiments.

Open Development System for Access Services – SDK

[0396] In some embodiments, an SDK is provided that allows developers, such as device manufacturers, service providers, MVNO, MVNE and/or VSPs, to develop various service

processors (e.g., different versions of the service processor 115) for various devices (e.g., various types of devices 100) and corresponding service controllers (e.g., different versions of the service controller 122) for various types of services and network environments. For example, a device manufacturer can use the SDK to develop a new service processor for their new device (e.g., mobile phone, PDA, eBook reader, portable music device, computer, laptop, netbook, or any other network accessible device). The device manufacturer can also preload/preinstall their new service processor on their new devices. In this example, users of the new device would then be able to utilize the new device to access network based services using the new service processor, which communicates with the deployed new service controller, as similarly discussed herein in various embodiments. For example, the device can be preinstalled with the new service processor to provide ambient services, as similarly discussed herein in various embodiments. For example, the SDK can allow for substantially similar service processors to be installed on similar and/or different devices thereby minimizing any unnecessary differences between service processor elements for device assisted services. In some embodiments, for ambient services for a group of devices, or devices associated with a certain service provider, a set of numbers (e.g., dummy numbers) can be assigned for use for attempting access via the access network using a new device that is not yet otherwise subscribed for service. In some embodiments, the set of (dummy) numbers used for ambient access by the device can also be used for associate of the device with a service provider or a type of device (e.g., eReader or some other type of network accessible device), and upon activation, the service provider assigns a real number for the activated device (e.g., which can be provided at the time of manufacture of the device, point of sale of the device, or after the point of sale of the device, such as upon activation of the device). For example, ambient access of the device can use the device ID, SIM ID, assigned phone (real or dummy) number, and/or other information associated with the device for assigning appropriate service control and service policy/profile for the device.

[0397] In some embodiments, the service processor 115 is distributed as an SDK to any device that the central provider or the VSP desires to offer services with so that the service processor 115 can be efficiently designed or adapted by the device OEM, ODM or manufacturer for operation on the service network. In some embodiments, the SDK includes either a complete set of service processor 115 agent software designed for and/or tested for the OS (Operating System) and processor set being used on the device, or a mature reference design for the OS and

processor set being used on the device, or a less mature reference design (potentially for the same OS and/or processor set or a different OS and/or processor set being used on the device) that the OEM (Original Equipment Manufacturer) ports to the desired OS or processor set, or a basic set of example software programs that the OEM or ODM (Original Design Manufacturer) can use to develop software compatible with the service, or a set of specifications and descriptions (possibly forming an interoperability standard) of how to design the software to be compatible with the service. In some embodiments, the SDK includes a set of OEM lab test procedures and/or test criteria to ensure that the implementation of the service SDK is compatible with the service and will operate properly. In some embodiments, the SDK includes a set of network certification test procedures and/or test criteria to ensure that the implementation of the service SDK is compatible with the service and will operate properly. In some embodiments, the certification procedures are approved for testing by the OEM, the central provider, the VSP and/or a trusted third party. For example, the central provider is typically in control of the SDK and the test procedures, but others can be in control. In some embodiments, the test procedures are at least in part common across multiple central provider networks. In some embodiments, the SDK concept is extended to include one or more modem modules where one or more of the SDK embodiments described above is combined with a standard reference design or a standard hardware sales package for one or more modems so that the entire package forms a turn-key product that allows a device manufacturer, central provider, VSP or other entity bring new devices or device applications onto the central provider network possibly in combination with other networks in a manner that requires less engineering time and resources and less network certification time and resources than would be required in some designs that do not use this standard SDK plus module approach. For example, the standard SDK plus module product embodiments can be pre-certified and tested with one or more central providers to further reduce development time and expense. The standard SDK plus module embodiments can also use a multi-mode modem (e.g., modems based on a multimode CDMA, EVDO, UMTS, HSPA chipset as in the Gobi global multimode chipset product or modems based on other recently announced LTE plus HSPA chipsets, WiMax plus Wi-Fi chipsets or LTE plus EVDO chipsets) and a multi-mode connection manager agent so that the same SDK plus modem embodiment may satisfy a wide range of applications for many service providers around the world.

[0398] In some embodiments, at the time of manufacture, the device is associated with an MVNO. For example, the MVNO can provide an ambient service that provides a service provider clearing house, in which the device can access a network in ambient access mode (e.g., a wholesale MVNO connection through the access network) for purposes of selecting a service provider (e.g., a VSP, MVNO or carrier). Based on the service provider selection, the device credentials and/or service processor are reprogrammed and/or new software is downloaded/installed to activate the device with the selected service provider, as described herein for provisioning the device and the account on that service provider network (e.g., the ATS can track such activation, for example, for revenue sharing purposes, as an activation incentive fee).

[0399] In some embodiments ATS is implemented entirely in the network as described below. At the time of manufacture or at sometime during device distribution, the device master agent programs a unique credential in the device that cannot be re-programmed or removed (or is difficult to re-program or remove) and that can be recognized and recorded by the network at the time of activation or at some other time. In this manner, even if other, possibly primary, device credentials are reprogrammed or removed, there will still be a credential that is associated with the device master agent. The ATS process can then be implemented by using a database search function to scan through the database of activated devices to form a list of devices that have been activated for the purpose of master agent reconciliation. Example credentials that can suffice are MEID, hardware MAC address, and/or serial number, that are picked up and recorded by the service provider or other service entity at time of activation or before or after activation.

Interface Server Overlay for Billing/IPDR Feed Mediation

[0400] FIG. 50 illustrates a network architecture including a billing to service controller interface for accommodating minimum changes in existing central billing, AAA and/or other network components in accordance with some embodiments. As shown, the central billing system 123 includes a mediation, customer service and billing databases, historical usage, billing systems component 5010 and a billing to service controller interface component 5020. For example, the billing to service controller interface component 5020 allows for the central billing

system 123 to efficiently communicate with the service controller (e.g., service controller device control system 4825).

[0401] In some embodiments, an interface server (e.g., the billing databases, historical usage, billing systems component 5010 and/or the billing to service controller interface component 5020) is provided that reads the IPDRs, service profile and/or service plan information stored in the billing and/or service record database(s). In some embodiments, the interface server performs these functions in a manner that is compatible with communication formats of the billing and/or service record database(s) so that little or no changes are required in the configuration, communication formats or software of the existing central billing, AAA and/or other network components. In some embodiments, the interface server (e.g., including the billing databases, historical usage, billing systems component 5010 and the billing to service controller interface component 5020) is co-located with the central billing system components as shown, or in other embodiments, the interface server is located elsewhere. For example, the interface server can be located close to or within the components that comprise the service controller or anywhere else in the network.

[0402] In some embodiments, the interface server performs certain communication protocol translation or data format translation required to interface the information stored in the billing and/or service record database(s) to the service controller functions so that the central billing system 123 and other existing components in the network do not need to change much (if at all) to enable the service controller and service processor to implement device based/assisted service control. In some embodiments, the central billing system 123 or other network components are not required to be aware of the service control functions being implemented by the service controller or service processor, because the interface server acquires the network based information needed by the service controller and/or service processor while requiring little or no specialized awareness, communication, data formatting, user interfacing, service profile processing or service plan processing on the part of existing billing, database or networking components. In this type of overlay approach, various embodiments described herein can be used to quickly upgrade the capabilities of existing networks for new devices while minimizing the required changes to the existing network that supports legacy devices.

[0403] For example, a new ambient service plan can be implemented within the central billing system 123 that is associated with a zero or low cost billing plan and a usage limit (e.g., ambient service) that may be difficult or impossible to support in a manner that would result in high user satisfaction and a high level of control for service cost and service policy definition. Even if the central billing system 123 is not highly involved in the process, the zero or low cost plan can be implemented in a manner that results in high user satisfaction and a cost controlled service by using the service controller and/or service processor and the interface server to implement the ambient services access control, service usage control, user interface, service usage notification, transaction billing or bill by account functionality. For example, this approach can be implemented by reading the service plan and/or service policy settings for a device in the central billing database using the interface server, looking up the corresponding service policy, user notification policy, transaction billing policy and bill by account policy associated with the particular service profile or service plan, and then implementing the policies with the assistance of the service controller and/or service processor. Similarly, in another definition, multiple tiers of service control and user notification policies can be added to any number of new service profiles or service plans that would not otherwise be supported with the central billing system 123 and other network components, all with minimal or no modifications to the pre-existing network and billing system.

[0404] Another embodiment calls for receiving a standard IPDR feed from central billing 123 or another network component just like an MVNO would. For example, the interface server function can be located in the central billing system, service processor or elsewhere in the network. This provides the IPDR records for service usage policy verification and service usage notification synchronization with little or no need to modify existing billing or network apparatus.

[0405] In some embodiments, duplicate the IPDRs are sent from the network equipment to the billing system and/or network management system that are currently used for generating service billing or are used for device management or network management. In some embodiments, duplicate records are filtered to send only those records for devices controlled by the service controller and/or service processor. For example, this approach can provide for the

same level of reporting, lower level of reporting, and/or higher level of reporting as compared to the reporting required by the central billing system.

[0406] In some embodiments, a bill-by-account billing offset is provided using the interface server. For example, bill-by-account billing offset information is informed to the billing system through an existing data feed and by updating the billing database using the interface server. In some embodiments, transaction billing is provided using the interface server. For example, transaction billing log information is provided to the billing system through an existing data feed and by updating the billing database using the interface server.

[0407] In some embodiments, existing/new service plan choice screens are displayed to the user, a user choice or decision/input is confirmed for a selected service plan, and then the service is implemented upon confirmation of the billing system update for the new service plan. In some embodiments, the service is implemented upon the user selection of a new service plan and then retracted if not confirmed as updated by the billing system within a certain period of time. In some embodiments, the new service plan information is updated in the billing system through an existing data feed or by updating the database using the interface server.

Integrated Service Control

[0408] FIG. 51 illustrates a network architecture for locating service controller device control functions with AAA and network service usage functions in accordance with some embodiments. As shown, an integrated device service control, AAA, device usage monitoring system 5110 is provided that integrates service controller functions (e.g., service controller device control system functions 4825 of FIG. 48) with access network AAA server 121 functions and network (e.g., real-time) service usage 118 functions.

[0409] FIG. 52 illustrates a network architecture for locating service controller device control functions in the access transport network in accordance with some embodiments. As shown, the service controller device control system 4825 is located in the access transport network 415, or in some embodiments, in the 4G/3G/2G RAN gateways 410 (as indicated by the dashed line with the arrow), or alternatively, in the 4G/3G/2G transport gateways 420 (as indicated by the dashed line with the arrow).

[0410] FIG. 53 illustrates a network architecture for locating service controller device control functions in the radio access network in accordance with some embodiments. As shown, the service controller device control system 4825 is located in the radio access network 405, or in some embodiments, in the 4G/3G base station(s) 125 (as indicated by the dashed line with the arrow), or alternatively, in the 3G/2G base stations 125 (as indicated by the dashed line with the arrow).

Ambient Services

[0411] In some embodiments, improved and simplified processes for provisioning a device or user for service on a central provider network, an MVNO network or a virtual service provider (VSP) on the central provider network are provided. In some embodiments, provisioning includes one or more of the following: a process or result of assigning, programming, storing or embedding into the device and/or network a set of credentials, or otherwise providing the credentials to the user; the credentials being at least in part carried on the device or with the user; and/or at least a portion of or a counterpart to the credentials being stored or recognized by the network so that the various network elements responsible for admitting the device access to the appropriate service activities do so once the device or user service is active.

[0412] As an example, as discussed herein, the credentials can include one or more of the following: phone number, device identification number, MEID or similar mobile device identifier, hardware security device ID, security signature or other security credentials, device serial number, device identification and/or credential information via security hardware such as a SIM, one or more IP addresses, one or more MAC addresses, any other network address identifier, embedded device descriptive information block (static or programmable), security key, security signature algorithms, passwords or other secure authorization information, service processor (or similar device client or agent software) identifier or settings or version, device type identifier, browser (e.g., http, https, WAP, other browser client) header information or similar identifier, browser token information or similar identifier, browser cookie information or similar identifier, embedded browser instructions, portal-client (e.g., interface or communication agent that connects to a network portal used at least in part for provisioning or activation for the device or by the user) header information or similar identifier, portal-client token information or similar

identifier, portal-client cookie information or similar identifier, embedded portal-client instructions, service provider, OEM, master agent (service distributor), VSP, device service owner identifier, distributor or master agent, and/or any information the network can use to authorize network admission, provision the device, provision the network, activate service, authorize, associate or enable the device with a provisioning sequence, associate or enable the device with one or more service profiles, associate or assist the device with an activation sequence, associate or enable the device with an ambient profile or service experience, associate or enable the device with one or more service plans or service capabilities, associate the device with a service provider or service owner, associate the device with an OEM or master agent, associate the device with a distributor or master agent, or associate the device with a device group, user group or user.

[0413] In some embodiments, provisioning includes assigning, programming or embedding into the device and/or network the information to define the level of service activity, referred to as a service profile, that the device is authorized to receive. In some embodiments, provisioning also includes establishing the device settings and/or network settings to define an ambient activation experience in which the device user receives a set of services after (e.g., within a short period of time after) purchasing or otherwise obtaining or installing the device whether the device has or has not been registered and activated with the device user or device owner.

[0414] In some embodiments, the ambient experience is the user experience that is available at the time the device is sold in the event the user has not yet signed up for a service plan. For example, the ambient experience is defined by an ambient service profile, an ambient service plan and/or the other service usage activity control policies in effect in the network, on the device, or a combination of both. For example, if the device service processor is used in large part to define the ambient service profile, then the initial provisioning and activation settings in the service processor, and possibly the service controller, can define the user service upgrade offering choices, network destination access control possibilities, traffic control policies, mobile commerce transaction capabilities (e.g., which transaction websites, WAP sites or portals the user can access to purchase information, content, music, games and/or eBooks), possibly free news or weather or other modest bandwidth Internet services that are provided free of charge to

entice the user into using/upgrading the service or using the transactions or viewing advertisements, what advertisements are displayed to the user or what advertisement based websites the user is exposed to, certain applications may have access while others are blocked (e.g., Internet based text services have access but email downloads do not), or other example service capabilities. It will be apparent to one of ordinary skill in the art that allowing all of these services, and blocking other ambient user service attempts (e.g., unpaid large file size Internet downloads or uploads or movie viewing or other access that would consume bandwidth and cause the ambient service to be a potential source of losses for the service provider) is made possible by the service profile control capabilities of the service processor and/or the service controller. The bill by account embodiments, as discussed herein, in which each service activity can, for example, be separately tracked with the service monitor and other agents and server functions to produce a billing offset that allows categorization and mediation of different billing entities (accounts) provides the capability for the service provider to individually account for the costs of each ambient service element. This allows business models wherein the free access to the end user is paid for or partially paid for by one or more service provider partners who are billed for service access using the bill by account capabilities (e.g., the transaction partners pay for user access to their transaction experience and perhaps pay a revenue share for transaction billing, the advertising sponsored website partners pay for their access service share).

[0415] While the service control capabilities of the service processor and the bill by account service cost sharing and transaction revenue sharing in some cases can create a profitable ambient business model, in other cases, the ambient services can be a potential source of losses for the service provider. Accordingly, in some embodiments, the ambient service capabilities can be modified over time to reduce service cost to the service provider or VSP based on a variety of decision factors. For example, the user can have one level of traffic control for a period of time, and if the user has not signed up for service by the end of the period, the ambient service access is reduced by changing the service control policy settings in the service processor, and the service level can be further reduced over time if the user continues to not sign up for service or the user does not create much transaction revenue. As another example, the recursive throttling algorithms discussed herein can be utilized to one or more of the service activities offered in ambient service mode so that the user experiences what full speed service is like, and if the user continues consuming appreciable bandwidth with the service activity, then

the activity is throttled back to reduce costs. In these examples, the service processor or service controller can issue the user a notification explaining that their service is currently free so their usage is being throttled, and if they desire to receive better service, service plan upgrade offers can be delivered to the UI. It will now be apparent to one of ordinary skill in the art that the various ambient service parameters, including the provisioning and activation processes used to create the ambient service activation, can also be managed by the VSP apparatus and processes described herein. For example, this allows the same service controllers and service processor solutions to be used to define a wide range of ambient experiences for various device groups or user groups that are controlled by different VSPs.

[0416] Similarly, rather than controlling the ambient service profile settings using the VSP functions to control the service controller, service processor, provisioning and activation settings, other embodiments call for the ambient service profile settings to be controlled by the network based service activity control equipment as similarly discussed herein. Depending on the level of service control and service monitoring sophistication (e.g., highly advanced DPI or service aware techniques), some, much, most or all of the above described ambient services functionality can be implemented using network based service controls and the VSP management and control embodiments described herein.

[0417] In some embodiments, a device is suspended based on inactivity, or the device is placed in a suspended service state or suspended account state, so that the network does not get bogged down with a significant number of devices and credentials that are inactive. For example, this can also result in a portion of the device credentials being assigned back to an available pool rather than reserved for that particular device (e.g., phone numbers if phone numbers are scarce). The device account and/or activation state can be re-activated when the device comes back online. For example, the suspend state can be a simple suspension of services without changing the account status, in which case the re-activation process can be automatically completed as a subset or entire set of the activation sequence that occurs when the device is initially used as described herein. The suspend state can also involve changing the account status to inactive, in which case the re-activation process can automatically reconfigure the account status back to an active state when the device re-accesses the network. For example, the suspend state can involve de-assigning or possibly re-claiming a portion of the device credentials. If a

portion of the credentials are de-assigned, then when the device re-accesses the network credentials can be automatically re-assigned as described in various embodiments described herein.

Network Based Service Monitoring, Notification and Control

[0418] In some embodiments, as described herein, it is desirable to implement some or all of the deep service usage monitoring, service control or control assistance, or service notification or notification assistance associated with a service profile in network apparatus rather than in the device, or to implement some of the deep service monitoring, control, control assistance, notification or notification assistance in the device and others in the network. This is the case, for example, in a mixed network in which some devices have some, or at least one, or all of the service processor capabilities discussed herein, but other devices do not have as much or any of the service processor capabilities. Another example is for networks or devices that do not have any service processor capabilities or where it is desirable to do all of the service monitoring, control and notification in the network rather than the device. As described below, FIGS. 54 through 63 depict various embodiments for combinations of device based service monitoring, control or control assistance, usage notification or usage notification assistance and/or network based service monitoring, control or control assistance, usage notification or usage notification assistance.

[0419] FIG. 54 illustrates a network architecture for locating service controller device control functions with AAA and network service usage including deep packet inspection functions in accordance with some embodiments. As shown, an integrated device service control, device usage monitoring system 5410 is provided that integrates service controller functions including a deep packet control (DPC) policy implementation function 5402 with access network AAA server 121 functions and network real-time service usage 118 functions. In the following discussion, it is understood that the AAA server 121 function can be re-located to another point in the network or network equipment partitioning with no loss in generality. It is also understood that many of the functional partitions described for the various embodiments within integrated device service control, device usage monitoring system 5410 can be re-drawn with no loss in applicability, function or generality. Finally, it is understood that one or more of

the functional elements described within the integrated device service control, device usage monitoring system 5410 can be removed for simplified embodiments and that not all the functionality described herein is necessary in some embodiments.

[0420] In some embodiments, the integrated device service control, device usage monitoring system 5410 provides for network based service monitoring or control that satisfies various network neutrality and/or privacy requirements based on indication(s) received from the device or user (e.g., user input provided using the device UI using the service processor 115; user input provided through another website, WAP site or portal; or user input provided through the service contract where the user agrees to the monitoring and/or service control levels) and network based service control using a DPI service monitor 5412 and/or the DPC policy implementation 5402.

[0421] In some embodiments, the integrated device service control, device usage monitoring system 5410 provides for network based service monitoring or service control that satisfies various privacy requirements using indication(s) received from the device or user (e.g., user input provided using the device UI using the service processor 115; user input provided through another website, WAP site or portal; or user input provided through the service contract where the user agrees to the monitoring and/or service control levels) and network based DPI service usage monitoring or DPC policy implementation using the DPI service monitor 5412 or DPC policy implementation 5402 as described below. In some embodiments, the DPI service monitor 5412 and/or DPC policy implementation 5402 include a secure database for storing service monitoring and CRM information for each device/device user. In some embodiments, the DPI service monitor 5412 and/or DPC policy implementation 5402 can be integrated with the integrated device service control, device usage monitoring system 5410 (as shown) or provided within a separate router, server, and/or software/hardware implemented function that is in secure communication with the integrated device service control, device usage monitoring system 5410 and/or other network elements based on the network architecture. In some embodiments, a secure data store, such as a secure database, is not integrated with the DPI service monitor 5412 or DPC policy implementation 5402 but is in secure communication with the DPI service monitor 5412 or DPC policy implementation 5402, the integrated device service control, device usage monitoring system 5410 and/or other network elements depending on the architecture

(e.g., a billing server or any other network element). In some embodiments, the user selects limits and/or restrictions on who can access remotely stored service usage history and/or other CRM/privacy related data (e.g., CRM/privacy gatekeeper settings), and, for example, other network elements and/or network administrators access to such data can be limited and/or restricted accordingly. For example, access to such stored service monitoring and CRM information can require certain security credentials and/or using various other well known secure data storage techniques, such as the various secure storage techniques described herein.

[0422] In some embodiments, the secure database possessing user service usage information that is considered sensitive and has not been approved for distribution by the user can be made unavailable to the credentials possessed by network managers or network functions except, for example, for emergency service situations of government mandated monitoring needs where special credentials are brought out of secure storage that are not normally available. In some embodiments, rather than the user selecting limits, a certain set of restrictions are assumed unless the user selects information filtering settings that allow more information to be shared with the network functions, network administrators or service provider partners. In some embodiments, the information is filtered to remove information thought to be sensitive but still transmits service usage information needed for monitoring network services or other important parameters. For example, the website destinations a user is visiting can be classified with generic identifiers that are not decodable or the individual website information can be completely removed. Many other examples will be apparent to one of ordinary skill in the art.

[0423] For example, the stored service monitoring and CRM information can also be organized into groups to define group CRM profiles to store service monitoring information for every user indexed by the user credentials (e.g., such groups can also be used for various VSP related functions, as described herein). The DPI service monitor 5412 or DPC policy implementation 5402 also uses the secure storage to store service monitoring information for each user indexed by the user credentials or another aspect of the device identifier or address assignment (e.g., IP address or MAC address). In some embodiments, a CRM information manager (e.g., a supervisor program executing on the integrated device service control, device usage monitoring system 5410) communicates with the other network functions and provides filtered service usage and CRM information according to CRM filtering rules for each user or for

groups of users. In some embodiments, the filtered CRM data can be made available using secure communications with other networking equipment by the integrated device service control, usage monitoring system 5410. In some embodiments, the filter settings for some users allow more information to be shared from the secure service usage information than others due to the differences in user preference settings and/or service plan agreements.

[0424] In some embodiments, user privacy preference information is used to determine the privacy filter settings, which are securely implemented by the integrated device service control, device usage monitoring system 5410. For example, service CRM filter settings can be received at the time of service contract sign up (e.g., service plan selection) and/or allow the user to log into service preferences web page to change settings (e.g., without involving any interaction with local software on the device). As another example, software on the device (e.g., including the service processor 115) can be used for selecting user CRM/privacy preferences, which are securely communicated to the integrated device service control, device usage monitoring system 5410 (e.g., the device can include credentials that can be verified to allow for selection/modification of CRM/privacy preferences or other user based preferences securely maintained in a network server, such as the integrated device service control, device usage monitoring system 5410 or another network element, such as shown in various other embodiments described herein). In these examples, the filtered CRM data is available from the integrated device service control, device usage monitoring system 5410 for other network components over a secure or open communication link. In another example, user CRM/privacy preferences are input using a web server hosted by the integrated device service control, device usage monitoring system 5410 or the central billing system 123. In another example, software on the device (e.g., including the service processor 115) can be used for securely communicating user preference decisions to an intermediate server that acts as a device manager and intermediate server for devices or device groups and the integrated device service control, device usage monitoring system 5410.

[0425] In some embodiments, the integrated device service control, device usage monitoring system 5410 provides for network based service control as described below. In some embodiments and similar to the above described network based CRM filtering embodiments, the DPI service monitor 5412 or DPC policy implementation 5402 includes secure storage (e.g., a

secure database) for storing service monitoring information (e.g., based on user selections/preferences), and the DPC policy implementation 5402 performs traffic shaping/throttling algorithms for each user based on the stored service monitoring information from DPI service monitor 5412. For example, network based DPI traffic inspection by the DPI service monitor 5412 can use the secure storage to save service monitoring information for each user indexed by the user credentials or other parameters, such as IP address or other network tag. As another example, the DPC policy implementation 5402, for example, which can be supervised by policy management server 1652 as described herein with respect to various other embodiments, can implement service usage history statistical analysis inside the secure storage and maintain a service usage history analysis for each device/user and/or perform various traffic shaping and/or throttling algorithms based on various device, user selected and/or service plan related settings (e.g., for network neutrality purposes) allowing for various higher level service usage goals for one or more users, as similarly described herein with respect to various device based service usage monitoring embodiments (e.g., except for certain encrypted network traffic flows or application related flows for which traffic control generally needs information from the application level and/or content specific traffic control).

[0426] In some embodiments, input is collected on how to implement service control (e.g., from the user of the device). For example, such input can be determined based on one or more of the following: a service plan choice for the device; input provided by a user via a website (e.g., web based portal) for indicating changes to service control policies, as similarly described above; input provided by a user via the device (e.g., including the service processor 115), which securely communicates the input to the DPC policy implementation 5402, for example, which can be supervised by the policy management server 1652; and input provided by a user via the device (e.g., including the service processor 115), which securely communicates the input to an intermediate server for the DPC policy implementation 5402, as similarly described above. In some embodiments, such service control is based on various algorithms as described herein that identify the heaviest usage service activities and recursively control the speed for those activities while leaving certain others unaffected, and in a manner that is specified or selected by the user to ensure network neutrality. In some embodiments, the user is offered a choice for controlling service usage and/or selects an algorithm that controls all activities equally/neutrally (e.g., based on selected user preferences). For example, by

implementing service control algorithms that are network neutral (e.g., throttling all activities equally or throttling the highest usage algorithms without singling out certain activities for throttling unless they satisfy certain network neutral usage history or usage statistics criteria), or that are approved, selected or otherwise specified by the user, network neutral traffic control or service usage control can be maintained.

[0427] In some embodiments, the DPI service monitor 5412, possibly in conjunction with the service usage notification 5420 and/or service history server 1650, provides service usage/service cost (e.g., a real-time service usage counter) related notifications to the device based on user preferences, as similarly described above with respect to various device based service usage/service related notification embodiments. For example, the DPI service monitor 5412, for example, in conjunction with the service usage notification 5420 and/or service history server 1650, can perform service usage/service related notification algorithms based on one or more of the following: service plans, device settings, and/or user selected preferences (e.g., such notification messages can be securely communicated to the device and/or to the device via an intermediate server). For example, the policies that govern how the user is notified of service usage or service cost can be determined by the policy management server 1652 and/or the service usage notification 5420. As another example, user acknowledgements of important notification messages and/or user choices related to important service usage decisions can be requested, as similarly discussed above with respect to device based service usage/control embodiments, which can then be communicated to the central billing system 123 as confirmation for any such important notification messages (e.g., related to service usage overage charges and/or confirmation of service upgrades). In some embodiments, various other service usage algorithms related to service usage and/or service cost forward projections described herein with respect device based service usage forward projection embodiments are performed in the network, such as by the integrated device service control, device usage monitoring system 5410, and such forward projections can then be communicated to each respective device as service usage notification messages (e.g., using a push based approach (initiated in the network) and/or pull based approach (initiated by a request from the device)). For example, these embodiments for projected service usage methods, as described herein, can be helpful for determining when the user is using services in a manner that will cause the user to run over a service limit so that

the user can be notified, or the service can be controlled or throttled if the user has selected a control or throttling option.

[0428] In some embodiments, one or more intermediate servers are provided for workload balancing and/or off-loading the integrated device service control, device usage monitoring system 5410 and perform one or more of the functions described above with respect to various embodiments of the integrated device service control, device usage monitoring system 5410. In some embodiments, service plans, device settings, and/or user selected preferences are used to associate each device/user with a preprogrammed profile to more efficiently associate such devices/users with their selected service plans, device settings, and/or user preferences. For example, the process of setting a service profile for a given device can be determined by assigning the device to a service flow that has the pre-defined service profile and is shared with other devices within the integrated device service control, device usage monitoring system 5410 rather than individually processing the service flow manipulations for each device. In some embodiments, the act of provisioning and activating a service profile for a given devices involves setting up the service flow definition and identifier within the integrated device service control, device usage monitoring system 5410 (if it is not already set up) and then assigning the routing of the device credentials to that service flow identifier. User preferences can, for example, be accounted for by assigning the device service flow to one of several pre-defined profiles based on user preferences that are all supported under the same service plan. For example, one service flow profile can call for service usage notification but no control under the same service plan as another service flow profile that calls for less notification but active service usage control to maintain user costs to a monthly post-pay limit.

[0429] In some embodiments, the bill by account function is implemented in the context of the integrated device service control, device usage monitoring system 5410 or other network based system embodiments described herein. For example, the DPI service monitor 5412, in some cases in conjunction with service history server 1650, can operate in conjunction with bill by account policy settings stored in the billing event server 1662 so that service activities are divided into the account classifications defined by the service profile settings. The bill by account feeds can then be sent to the billing system or to an intermediate billing event aggregation server that collects this type of deep packet inspection generated information from

one or more integrated device service control, device usage monitoring system 5410 units to aggregate and format the information in a manner that may be used by the central billing system 123. In some embodiments, the bill by account information collected in a network box like the integrated device service control, device usage monitoring system 5410 is augmented by bill by account information collected on the device as described herein, and any intermediate server that can be used to aggregate and format these bill by account feeds for the central billing system deals with both types of data, from the network and from the devices.

[0430] As shown in FIG. 54, in some embodiments, integrated device service control, device usage monitoring system 5410 includes the service control server link 1638, which, for example, can be used as described above (e.g., with respect to FIG. 16 and other embodiments described herein) to communicate with device service processors 115. In some embodiments, billing server 1662 within integrated device service control, device usage monitoring system 5410 detects service usage events reported by DPI service monitor 5412, in some cases in conjunction with service history server 1650, generates a billing event that can be recorded or transmitted to the central billing system 123. In some embodiments, billing server 1662 receives information from device billing agent 1695 and/or device service monitor agent 1696 and transmits the device service usage billing events to the central billing system 123. In some embodiments, certain billing events that are advantageously collected in the network (e.g., DPI service monitor 5412 and/or billing event server 1662) are combined with certain billing events that are advantageously collected on the device (e.g., service monitor agent 1696 and/or billing agent 1695), and both sources of billing information are transmitted to the billing system 123. Similarly, in some embodiments, certain service usage information is collected with service usage monitor agent 1696, and that information is combined with service usage information collected from DPI service monitor 5412 and/or service history server 1650 and/or service usage 118. In some embodiments, certain service aspects are controlled using network based DPC policy implementation 5402, in some cases in conjunction with or supervised by network based policy management server 1652, and other service aspects are controlled using device based policy implementation agent 1690, in some cases in conjunction with or supervised by policy control agent 1692. As will now be apparent to one of ordinary skill in the art in view of the numerous embodiments described herein, many hybrid approaches to service usage monitoring, service control, service notification or service billing can be accomplished with some aspects of

the policy, notification, control, monitoring or billing being implemented/performed on the device apparatus described herein and others implemented/performed on the network apparatus described herein. The presence of access control integrity server 1662 and many other service control verification embodiments described herein make it apparent that the integrated device service control, device usage monitoring system 5410 embodiments also provide for affirmative verification of whatever functions are implemented on the device. It will also be apparent that all of the above combinations of device and network functions, and many others, can be accomplished in ways that are network neutral and/or protect user privacy preferences by implementing the service control algorithms in a network neutral manner and/or receiving user preference input on how to implement service control, and by maintaining service usage and CRM information security and filtering on both the device 100 and the network based integrated device service control, device usage monitoring system 5410.

[0431] In some embodiments, the integrated device service control, device usage monitoring system 5410 facilitates or plays a part in automated provisioning and activation of the devices as similarly described above with respect to various device based automated provisioning and activation embodiments. In some embodiments, the activation server 160 is integrated into or partially integrated into device service control, device usage monitoring system 5410.

[0432] In some embodiments, the integrated device service control, device usage monitoring system 5410 facilitates ambient services as similarly described above with respect to various device based ambient services embodiments.

[0433] In some embodiments, the integrated device service control, device usage monitoring system 5410 facilitates VSP and ODI solutions as similarly described above with respect to various device based VSP and ODI embodiments.

[0434] Various other network architectures for network based service control including deep packet inspection functions can similarly be used as will be apparent to one of ordinary skill in the art in view of the various embodiments described herein.

[0435] FIG. 55 illustrates another network architecture for locating service controller device control functions with AAA and network service usage including deep packet inspection functions in accordance with some embodiments. As shown, the service processor 115 is not present on the devices 100, and the integrated device service control, device usage monitoring system 5510 performs all service monitoring, service control, billing, and notification functions.

[0436] FIG. 56 illustrates a 4G/3G/2G DPI/DPC enabled gateway in accordance with some embodiments. As shown, a 4G/3G/2G DPI/DPC enabled gateway 5610 (e.g., implemented in either gateway 420 or gateway 410 or a combination of both) where the conventional service gateway functions 5616 (e.g., routing, switching, protocol translation/tunneling, charging data function (CDF), charging gateway function (GCF), mobility management, and/or suspend/resume) are combined with one or more of the following embodiments and integrated into one or a combination of the service gateways (e.g., RAN and/or transport gateways): DPI service monitor 5412, service history server 1650, device usage 118, DPC policy implementation 5402, policy management server 1652, user notification 5618, billing event server 1662, access control integrity server 1654, service control service link 1638, data plane I/O 5612 (e.g., used to represent the I/O port(s) for the gateway), and/or DPI/DPC gateway control plane link 5622 (e.g., used to represent the control plane network channel connecting the above elements to other network equipment and in communication with gateway control communication 5620). The packet processing architecture shown in this figure calls for a multi-point to multi-point backplane bus scheme, but it will apparent that other data path configurations are possible including serial. As will also be apparent, the above described configuration can also be applied to either the transport gateway 420 and/or the RAN gateway 410. As mentioned above, it is possible to maintain a secure storage on the 4G/3G/2G DPI/DPC gateway 420 or 410 that requires secure credentials to get into so that user privacy is protected and service usage information or CRM information is filtered according to user preferences prior to sending to another network function or network manager, and the same allowances can also be applied for emergency or government monitoring purposes. Network neutrality can also be maintained in this configuration by maintaining network neutrality in the service control algorithm and/or soliciting user input on how to control service usage just as discussed above for other network service control implementations or as discussed in the device based service control descriptions.

[0437] In some embodiments, the bill by account function is implemented in the context of the 4G/3G/2G DPI/DPC gateway 5610 embodiment or other network based system embodiments described herein. For example, the bill by account information can be completely derived from the network box (e.g., 4G/3G/2G DPI/DPC gateway 5610) without assistance from device based service monitoring or billing capabilities, or none may exist on the device. In this example, the DPI service monitor 5412, in some cases in conjunction with service history server 1650, can operate in conjunction with bill by account policy settings stored in the billing event server 1662 so that service activities are divided into the account classifications defined by the service profile settings. The bill by account feeds can then be sent to the billing system or to an intermediate billing event aggregation server that collects this type of deep packet inspection generated information from one or 4G/3G/2G DPI/DPC gateway 5610 units to aggregate and format the information in a manner that can be used by the central billing system 123. In some embodiments, the bill by account information collected in a network box, such as the 4G/3G/2G DPI/DPC gateway 5610, is augmented, refined or otherwise added to by bill by account information collected on the device as described herein and any intermediate server that can be used to aggregate and format these bill by account feeds for the central billing system deals with both types of data, from the network and from the devices.

[0438] FIG. 57 illustrates a network architecture including the VSP workstation server 4910 in communication with the 4G/3G/2G DPI/DPC gateways 410 and 420 in accordance with some embodiments. As shown, the VSP workstation server 4910 is in communication with the 4G/3G/2G DPI/DPC gateways 410 and/or 420, the Service Controller Design, Policy Analysis, Test, Publishing System 4835, and/or other networking elements including possibly the central billing system 123, the mobile wireless center 132 (HLR) and/or the AAA server 121 for the purpose of provisioning and/or controlling settings in the 4G/3G/2G DPI/DPC gateways 410 and/or 420, the mobile wireless center 132 and possibly other equipment for the purpose of implementing a portion of the VSP open partner functionality discussed herein. In FIG. 57, the 4G/3G/2G DPI/DPC gateway 5610 functionality as shown in FIG. 56 is implemented in the 4G/3G/2G DPI/DPC RAN gateway 410 and/or the 4G/3G/2G DPI/DPC transport gateway 420 as similarly described above. For example, the VSP functionality can also be used to set higher level policies associated with the 4G/3G/2G DPI/DPC gateway 420 or 410, such as provisioning or activation profiles or policies, ambient service profiles or policies, and/or bill by account

service profiles or the other higher level service profile or service plan embodiments discussed herein. In some embodiments, the provisioning and/or activation steps described herein involve setting service policies in the 4G/3G/2G DPI/DPC gateway 420 or 410. In some embodiments, ambient services or ambient activation involve setting up service profiles within the 4G/3G/2G DPI/DPC gateway 420 or 410 that allow the desired activities and block the undesired activities. For example, these settings can be included as part of the open service provider partner programming capabilities of the VSP workstation server 4910 embodiments.

[0439] FIG. 58 illustrates another 4G/3G/2G DPI/DPC enabled gateway in accordance with some embodiments. As shown, a 4G/3G/2G DPI/DPC gateway 5810 (e.g., implemented in either gateway 420 and/or gateway 410) is provided in which the service processor connection (e.g., via service control server link 1638 as shown in FIG. 56) is not present so that all service monitoring, control, billing event collection and transmission, and notification are performed by the 4G/3G/2G DPI/DPC gateway 5610 (e.g., gateways 410 and/or 420).

[0440] FIG. 59 illustrates another network architecture including the VSP workstation server 4910 in communication with the 4G/3G/2G DPI/DPC gateways 410 and 420, the AAA 121 and the mobile wireless center 132 in accordance with some embodiments. As shown, FIG. 59 provides a network diagram corresponding to FIG. 58, with similar functionality to the embodiment shown in FIG. 57, in which the service processors 115 are not present on the devices 100. In FIG. 59, the 4G/3G/2G DPI/DPC gateway 5810 functionality as shown in FIG. 58 is implemented in the 4G/3G/2G DPI/DPC RAN gateway 410 and/or the 4G/3G/2G DPI/DPC transport gateway 420 as similarly described above.

[0441] FIG. 60 illustrates a 4G/3G/2G DPI/DPC enabled gateway and service controller device control system in accordance with some embodiments. In some embodiments, enhanced network based service monitoring, control, billing and notification as discussed above is implemented using a 4G/3G/2G DPI/DPC enabled gateway 6010 and service controller device control system 6025 as shown. In some embodiments, the functions shown in the figure to be inside of the service controller device control system 6025 have been moved from the 4G/3G/2G DPI/DPC gateway 5610 of FIG. 56 (e.g., or from gateways 410 and/or 420) so that they reside in a separate server embodiment or other network equipment function separate from the 4G/3G/2G

DPI/DPC gateway 6010. For example, this architecture can be used when the network equipment manufacturer desires to separate these functions or has an existing product that it is desirable to upgrade by adding a separate box. As another example, this architecture can be used when the 4G/3G/2G DPI/DPC gateway 6010 is not capable of keeping up with large numbers of individual user profiles so it is desirable to go to a scalable server configuration in which load balancing can be applied with a potentially more flexible programming environment for implementing service policy management functions, statistical service history analysis algorithms, service usage projection, and/or service control (or throttling) algorithms. In some embodiments, a secure storage is provided on the 4G/3G/2G DPI/DPC gateway 6010 and/or the service controller device control system 6025 that requires secure credentials to get into so that, for example, user privacy can be protected and service usage information or CRM information can be filtered according to user preferences prior to sending to another network function or network manager, and the same allowances can also be applied, for example, for emergency or government monitoring purposes. For example, network neutrality can also be maintained in this configuration by maintaining network neutrality in the service control algorithm construction and/or soliciting user input on how to control service usage just as discussed above for other network service control implementations or as discussed in the device based service control descriptions.

[0442] FIG. 61 illustrates another network architecture including the VSP workstation server 4910 in communication with the 4G/3G/2G DPI/DPC gateways 410 and 420, AAA 121 and mobile wireless center 132 in accordance with some embodiments. In FIG. 61, the 4G/3G/2G DPI/DPC gateway 6010 functionality as shown in FIG. 60 is implemented in the 4G/3G/2G DPI/DPC RAN gateway 410 and/or the 4G/3G/2G DPI/DPC transport gateway 420, as similarly described above, and which are in communication with the service controller device control system 6025 as shown.

[0443] FIG. 62 illustrates another 4G/3G/2G DPI/DPC enabled gateway and service controller device control system in accordance with some embodiments. As shown, the capability to communicate with the service processor 115 has been removed so that all service monitoring, control, billing event collection and transmission, and notification are performed by the 4G/3G/2G DPI/DPC gateways 6210 (e.g., implemented in gateways 410 and/or 420) in

conjunction with the service controller device control system 6225 without assistance from the service processors 115.

[0444] FIG. 63 illustrates another network architecture including the VSP workstation server 4910 in communication with the 4G/3G/2G DPI/DPC gateways 410 and 420, AAA 121 and mobile wireless center 132 in accordance with some embodiments. In FIG. 61, the 4G/3G/2G DPI/DPC gateway 6210 functionality as shown in FIG. 62 is implemented in the 4G/3G/2G DPI/DPC RAN gateway 410 and/or the 4G/3G/2G DPI/DPC transport gateway 420, as similarly described above, and which are in communication with the service controller device control system 6225 as shown.

[0445] As will be apparent to one of ordinary skill in the art, the above described embodiments can be extended to include some or all of the functions depicted in the 4G/3G/2G DPI/DPC service gateways of FIG. 56 in the base station or base station controller 125.

Provisioning and Activation

[0446] In some embodiments, automated provisioning and activation includes automation of one or more of the following functions: (1) programming device credentials or partial credentials and recording them in a database (or providing same when they are programmed into the device), (2) associating these credentials with the proper provisioning and/or activation actions to be taken on the device and in the network, (3) directing the device to the proper activation function (e.g., activation server) sequence when it attempts to connect to the network, (4) completing provisioning of the device, (5) programming the AAA, billing system, gateways, mobile wireless center and other network equipment to the proper initial device service control settings, and (6) establishing a service account for the device.

[0447] In some embodiments, improved processes for activating service for a device or user with a network service provided by a central provider network, an MVNO network or a VSP on the central provider network are provided. In some embodiments, activation includes one or more of the following: a process or result of associating a service account with device or user credentials; with the service account potentially further being associated with a service profile defining the service activities that the device is authorized to access; creating or updating

a service usage or billing record and associating it with the service account to create a service plan; and/or initiating service to the device or user in which the network equipment allows access to the appropriate level of service activities. In some embodiments, VSP embodiments include the provisioning and activation apparatus embodiments of any or all forms.

[0448] In conventional mobile device provisioning systems, the provisioning and activation process required to create a user service account and enable the device to access the desired level of service activities can limit mass market, low cost or user friendly applications of the device or service, because the process can often be cumbersome, time consuming and/or expensive for the service provider, service owner, master agent (service distributor), MVNO, VSP and/or user. Accordingly, the various embodiments for provisioning and activation described herein simplify the provisioning and activation process for mobile devices. In some embodiments, provisioning and activation for the device and/or the network accommodates a wide variety of device types and service profile types, with the capability to perform the provisioning and activation at a number of points in the manufacturing, distribution, sales and usage progression for the device, and the ability to either pre-activate before first device use or very quickly activate during first device use (or during some later use of the device).

[0449] In some embodiments, as described herein, the term provisioning generally refers to those actions/processes associated with programming the device with credentials or other device settings or software installations used to later activate the device, as well as, in some embodiments, creating database entries and other credential associations in the network so that the network and/or device have the information used to recognize the device or credentials and implement the service policies in the service profile and/or service plan once the service profile and/or service plan are activated. In some embodiments, as described herein, the term activation generally refers to the process of creating or selecting the service plan and/or service profile, programming the settings that are used in each (e.g., required) network function and/or each (e.g., required) device function so that the system can properly associate the device credentials with the appropriate service activity policies, and then admitting the device onto the network. The term activation can also refer in some embodiments to the creation of a user or device service account, in some cases, with user or device owner information or billing information. In some embodiments, the process of provisioning amounts to assigning credentials to the device

and programming a portion or all of the credentials on the device, entering a portion or all of the credentials in the various necessary network equipment databases so that the network components are capable of identifying the device and associating it with the network based portion of the admission, traffic processing, service monitoring, billing, service limits and other policies that are eventually defined by the service profile and service plan.

[0450] Further examples of the network based service profile policies include network access level, traffic routing, service monitoring, service limits and actions taken upon reaching service limits. Once the service profile is created and activated during the activation process, the device credentials and the associated service profile are communicated throughout the necessary network elements so that each element can implement its part of the network portion of the service profile policies. This process of propagating the service profile settings to all the required network equipment components is a portion of what is referred to herein as activation in accordance with some embodiments. In some embodiments, the activation process includes associating the credentials with the proper service plan and/or service profile, and possibly completing the process of programming the device functions and/or network functions so that the device can be admitted to the appropriate level of network services. In some embodiments, activation also includes the service processor software settings, configurations or installs for each function or agent in the service processor to implement its part of the service profile, service plan, service billing or transaction billing policies. In some embodiments, activation also includes the creation of entries in the various service account databases and/or billing databases to create a user account or device owner account for the purpose of managing the user choices for service plan and other account information storage and management aspects, such as maintaining status information, maintaining the central service profile configuration, conducting reconciliation and billing exchanges, service usage history, and/or account history.

[0451] In some embodiments, the term credentials generally refers to the set of information parameters that the network and/or device uses (e.g., requires) to admit the device onto the network and associate it with the appropriate service profile and/or service plan. For example, the credentials can include one or more of the following: phone number, device identification number, MEID or similar mobile device identifier, hardware security device ID, security signature or other security credentials, device serial number, device identification and/or

credential information via security hardware such as a SIM, one or more IP addresses, one or more MAC addresses, any other network address identifier, embedded device descriptive information block (static or programmable), security key, security signature algorithms, passwords or other secure authorization information, service processor (or similar device client or agent software) identifier or settings or version, device type identifier, browser (e.g., http, https, WAP, other browser client) header information or similar identifier, browser token information or similar identifier, browser cookie information or similar identifier, embedded browser instructions, portal-client (e.g., interface or communication agent that connects to a network portal used at least in part for provisioning or activation for the device or by the user) header information or similar identifier, portal-client token information or similar identifier, portal-client cookie information or similar identifier, embedded portal-client instructions, service provider, OEM, master agent (service distributor), VSP, device service owner identifier, distributor or master agent, and/or any information the network can use to authorize network admission, provision the device, provision the network, activate service, authorize, associate or enable the device with a provisioning sequence, associate or enable the device with one or more service profiles, associate or assist the device with an activation sequence, associate or enable the device with an ambient profile or service experience, associate or enable the device with one or more service plans or service capabilities, associate the device with a service provider or service owner, associate the device with an OEM or master agent, associate the device with a distributor or master agent, or associate the device with a device group, user group or user. In some embodiments, at least some of the credentials are unique to the device, and, in some embodiments, groups of devices share one or more aspects of the credentials. In some embodiments, the term permanent credentials generally refers to the set of credentials that include at least a subset that are intended to be assigned to a device or user on a permanent basis. In some embodiments, the term temporary credentials generally refers to the set of credentials that include at least a subset that are intended to be assigned to a device or user on a temporary basis. In some embodiments, temporary credentials are eventually replaced by permanent credentials. In some embodiments, at least some elements in the temporary credentials (e.g., phone number and/or access or authorization security credential) are used for more than one device. In some embodiments, the temporary credentials are recycled from one or more devices and used for one or more other devices, for example, when they remain unused for a period of

time or when they are replaced with permanent credentials on one or more devices. It should not be inferred from the term permanent credentials that permanent credentials are never recycled, for example, when the user discontinues service or use of the credentials. Also, the term temporary credentials does not imply that temporary credentials are always temporary. In some embodiments, partial credentials or pre-activation credentials generally refer to a subset of credentials that are to gain access to limited network services for the purpose of provisioning of credentials and/or activation of a service plan or service profile. For example, prior to a phone number being assigned, a device can gain access to a limited set of network server destinations in which embedded information contained in the device (e.g., the partial credentials) is provided to the server, the server associates that information with the proper additional credentials (including the phone number) to assign to the device and/or associates the information with the proper service profile to activate service. In this example, partial credentials can include device type, OEM, service provider, VSP, device identification number, SIM, service processor configuration or some other information used by the server to determine what the credentials should be and the proper service profile.

[0452] In some embodiments, a permanent service account generally refers to the service account that is permanently associated with the user and/or device. For example, this account includes an association with the device or user credentials, user information or billing information, service profile, billing profile, network authorization status and other aspects that define the device or user service policies and billing policies. In some embodiments, the term temporary service account generally refers to a service account that is temporarily set up and associated with the device before some or all of the required permanent account information is available or entered for a device or user. For example, this account can be set up with an association with an actual user, or can be set up with a mock user or unassigned user association so that the network and billing system can recognize the credentials, authenticate the device, admit the device, provide the proper level of service activity control according to the service profile associated with the temporary service account, or collect the service activity usage information for various network and billing system accounting needs before actual user information or billing information has been entered into the network systems. For example, a temporary service account can make it possible or easier to use existing billing systems or other network systems to provide simplified provisioning, simplified activation or ambient services. A

temporary service account can also become a permanent service account by replacing mock user or unassigned user information with actual user information, or a temporary service account may need to be replaced by a permanent service account when actual user information needs to be entered into the network systems, possibly including the billing or service profile databases.

[0453] In some embodiments, temporary or permanent device credentials and other information used/required for provisioning the device are generated with apparatus located at the manufacturer or in the distribution channel as discussed below. In some embodiments, the apparatus includes a local onsite server that typically shares some aspects of the provisioning information (e.g., phone number, phone number range, MEID or MEID range, SIM number or SIM number range, IP address or IP address range, MAC address or MAC address range, other secure device credential elements) with a network provisioning database. In some embodiments, the apparatus includes a server terminal, and the aforementioned portion of the credentials is generated by the network and shared with the local provisioning apparatus. In some embodiments, as will be discussed below, the provisioning credentials are in part generated in the network and shared with the device while it is connected online to an activation server (e.g., activation server 160) that is connected to the access network. Similarly, there can be activation servers connected to apparatus in the manufacturing or distribution channel that service device activation, or over the air or over the network apparatus connected to an activation server, which in turn connects to the device, can be used to accomplish activation programming of the network and device as further discussed below.

[0454] In some embodiments, when a device is provisioned and entered into the network provisioning database, it is associated with the automatic provisioning and/or activation sequence the device is intended to go through once it connects to the network or to the apparatus that will complete the process. In some embodiments, one or more device parameters (e.g., service owner, device type, OEM, plan type, IP address, security credential and/or software version) are used to determine what the appropriate network provisioning steps and/or settings are for completing the provisioning and/or activation process, and this association information is stored in the network provisioning database for propagation of the provisioning profiles or activation profiles to the various network equipment elements. In some embodiments, the network provisioning database is provided (e.g., in the network) that associates the pre-activation

provisioning information (e.g., generated, as described herein, at time of manufacture, sometime during distribution, by the user on a website by a sales associate or other activation assistant, or by the network when a new device enters the automatic activation process). For example, the pre-activation provisioning information informs the network whether or not to let the device onto an activation sequence when the device attempts access, and in some cases, also instructs the network to direct the device to a specific activation sequence including, for example, an activation server (or other activation sequencing apparatus) sequence as described herein. In some embodiments, a central database is queried by other network equipment or the central database is included in one or more of the network elements (e.g., the AAA server and/or billing system, mobile wireless center 132), or the database is copied in part or in whole in various network elements (e.g., the central database, AAA server, mobile wireless center, billing system and/or gateways).

[0455] In some embodiments, propagating the network equipment provisioning information for a given device or group of devices is accomplished with a network provisioning system that has access to the network provisioning database and is capable of programming the appropriate network equipment. In some embodiments, this network equipment is referred to as "network management" equipment or "network provisioning" equipment. In some embodiments, there are several functions that take part individually or in concert, including, for example, the AAA server 121, service controller 122 (either with device based/assisted services through the service processor related embodiments or with network only embodiments as described herein), the mobile wireless center 132 (e.g., including the home location register (HLR) or other similar function referred to by other industry terms), the activation server(s) 160, other network provisioning or management equipment attached to or associated with the billing database system, and/or some other equipment apparatus. In some embodiments, the local database on the device, database in the AAA server and/or database elsewhere in network is provisioned to inform the gateway of the process for handling the pre-provisioned device according to, for example, the credentials. For example, if the device is not recognized or not authenticated onto the access network as an activated device with associated active service profile and/or service plan, the device connection or communication can be directed (or routed) to a generic activation server that provides an activation sequence that is not necessarily determined by one or more of the specific device credential elements, partial credential elements,

device profile or partial device profile that define something specific about the activation sequence for the device. In another example, in which the device is not recognized or authenticated as an activated device with associated service profile and/or service plan, the device can be directed (or routed) to an activation service (or other activation sequencing apparatus) that uses some part of the credentials or range of partial credentials or a portion of a partial or complete device profile to determine a desired pre-determined device specific or device group specific activation sequence that is implemented by a specific activation service sequence or other activation sequence apparatus. In another example, in which the device is not recognized or authenticated as an activated device with associated active service profile and/or service plan, a portion of the device credentials or partial credentials can be used as a look-up index into a database that determines what the specific device activation sequence should be, and the device can be directed (or routed) to a specific activation server sequence or other activation sequencing apparatus.

[0456] In some embodiments, a database in the AAA server or database elsewhere in network is provisioned to inform the gateway what to do with a pre-provisioned device according to the credentials. For example, devices can be authenticated (for activated devices), routed to activation servers (or other activation sequencing apparatus) or denied access. In some embodiments, the AAA server (and/or other network elements) provide the above discussed look-up function for the above gateway description in which a lookup database, locally stored or stored in a central database, is queried to provide secondary routing information to the specific or generic activation servers.

[0457] In some embodiments, the pre-provisioned database is located in the billing system. In some embodiments, the billing system accesses the pre-provisioned database (e.g., stored on the billing system or another network element) for the purpose of setting up temporary accounts or permanent accounts and associating those accounts with pre-activation status, activated free ambient or activated paying customer.

[0458] In some embodiments, for zero activation, all the required pre-provisioning or programming of the above network elements, or others, is coordinated by the network provisioning system at some point after the partial or full device credentials have been associated

with the device or reserved for a particular device type or service type. In some embodiments, the network provisioning system also coordinates the information to or from the device provisioning apparatus that is described elsewhere.

[0459] In view of the various embodiments described herein, it will be appreciated that many of the automated or background provisioning, activation and ambient embodiments described herein can be accomplished with network based approaches, device based approaches, or network/device combination/hybrid based approaches. For example, when the access control for the provisioning process is accomplished in the device (e.g., a device based approach), the activation server can be located anywhere on the Internet, and the device will ensure that the activation process is conducted with the activation server while blocking other traffic from occurring. As another example, some or all of the ambient provisioning programming steps become steps to program the access control, traffic control, application control, bill by account rules, and/or other aspects in the service processor or service controller as described herein.

[0460] In some embodiments, the provisioning apparatus described herein can be a computer located in the user's home or business, and the user or an IT manager has access to a website that provides the provisioning information, in which the computer serves as the provisioning or software programming apparatus. In some embodiments, the network itself, possibly through an activation server 160, website or other interface to the device, becomes the provisioning apparatus, in some cases, with the assistance of software on the device to affect the programming of provisioning information from the network or the communication of device credentials or other information to the network. For example, this software can be a background process that runs without user interaction, a portal/widget program, a web browser based program, a WAP browser based program, and/or any other program that provides a counterpart function to the network functions effecting the provisioning (e.g., activation server). In some embodiments, the activation server either initiates a specific provisioning sequence if device software is present to assist or routes to a website for manual entry if there is no software present.

[0461] FIG. 64 illustrates another network architecture including a system located in the manufacturing or distribution chain for the device that provides the device provisioning or partial

provisioning, and any pre-activation required for the device to later activate on the network in accordance with some embodiments. Device credential, software and settings server 6420 provides a link to the network functions that generate or provide device credentials, and/or associate device credentials with activation profiles or pre-activation profiles in the network equipment (e.g., the billing system 123, service controller device control system 6225, gateways 410, 420, base station 125, credential generation and association server 6410, activation server 160, service download control server 1660 and/or other network apparatus). For example, the link between the device credential, software and settings server 6420 to the central provider core network equipment can be over the Internet 120 (e.g., a secure link over the Internet) as shown or over another connection such as a leased line. The device credential, software and settings server 6420 obtains credentials or partial credentials from the network apparatus that generates them, illustrated by the credential generation & association server 6410. Credential generation & association server 6410 need not be directly connected to the central provider core network 110 as shown, but can be located elsewhere (e.g., in another location connected by a secure Internet link). Credential generation & association server 6410 assigns credentials, or partial credentials, for use by device credential, software and settings server 6420. When these credentials are assigned to a device, they are programmed, loaded or otherwise associated with the device by device credential provisioning apparatus 6430, which is connected to the device wirelessly or via a wire line connection.

[0462] In some embodiments, a device software loading and programming apparatus 6440 provides software loading or device settings functions that form a portion or all of the provisioning or pre-provisioning device configuration, or form a portion or all of the device activation profile configuration, or form the device service owner, master agent or VSP device assignment or signature, and in some embodiments, using an activation tracking service (ATS) system. As discussed herein, the ATS monitors network connections and aspects of traffic that provide insight into which networks the device 100 is gaining access to, in some embodiments, for the purpose of ensuring that an OEM, master agent, device service owner or VSP is being compensated for devices that activate on a service provider network. In some embodiments, the ATS agent connects to a server counterpart that records and, in some embodiments, also analyzes the service or network connection information to make a determination of the type of access service the device is receiving and, in some cases, determine which networks the device is

activated on. In some embodiments, the ATS is installed on the device in a manner that makes it difficult to tamper with or remove so that the entity that is intended to get credit for device service activation does get credit (e.g., the ATS agent can be loaded into secure memory, it can be installed with software that makes it difficult to de-install, it can be installed on the modem possibly in secure memory, it can be installed in the BIOS, it can be installed deep in the OS kernel, it can be installed with one or more additional device agents that monitor the ATS agent and alert a network function or re-install it if tampered with). The SIM inventory 6450 is provided to illustrate that, in some embodiments, hardware elements (e.g., a SIM security module as shown) or hardware configurations are also installed or manipulated in device 100 and these operations and the recording of the resulting associations form a portion of the provisioning or pre-provisioning process.

[0463] In some embodiments, at the time the credentials or partial credentials are loaded, programmed, set, installed, read from the device or otherwise recorded, they are, in some cases, all associated together in a database that allows for later identification of the device and its appropriate provisioning and/or activation process through such associations. For example, this can involve reading device parameters such as MEID, MAC address, device type, or other information that is associated with the information being loaded or configured on the device. As discussed herein, this credential configuration and association information is stored in the network equipment responsible using it to configure the network to activate the device in one of the various embodiments disclosed herein.

[0464] Some embodiments include tying some or all of the activation provisioning steps and information settings together into a database that defines a higher level activation profile for a group of users(/devices), and a server is used to perform device and equipment programming for the devices in the group, including, for example, associating the following device information into the group definition: credentials, service owner or master agent, provisioning information and/or activation profile. Some embodiments further provide for this device group information being distributed to the various network equipment components required to activate the devices as discussed elsewhere. In some embodiments, this programming and device group association is accomplished using the VSP workstation server 4910. For example, a device can be

manufactured and distributed in a manner that provides flexible assignment of the device to a group that is assigned to an activation profile or a service owner.

[0465] In some embodiments, multiple activation servers 160 are provided (as shown), which illustrates that there can be multiple device activation servers 160 each with a different device activation experience and potentially controlled by a different VSP, service owner, service provider, OEM or master agent. As discussed herein, there are several ways that a device 100 can be routed to the proper activation server 160 so that the device provisioning and activation process can be completed. In some embodiments, all devices that are not activated are re-directed (or routed) to an activation server that reads one or more parameters in the device credentials. The device credential information can be determined either through the device identification information associated with the access network connection itself (e.g., MEID, IP address, phone number, security credentials, or other credentials identified for a device that gains access with the network), or with the aid of the device in a pre-arranged query-response sequence. The device can then be re-directed (or routed) to the appropriate activation server for that device, device group, device service owner or VSP. In some embodiments, the same process described above can be accomplished with a single re-direction from a service gateway 420 or 410, or another router enable network element. In some embodiments, the gateway or network element itself decodes the device credential information as described herein and performs the correct re-direct (or route) to the appropriate activation server 160 for that device. In some embodiments, the activation server 160 can be incorporated directly into the gateway 420 or 410, the base station 125 or other network component. In some embodiments, the activation server 160 can be incorporated into the service controller 122 or the service controller device control system 6225.

[0466] In some embodiments, apparatus other than the activation server are used to facilitate provisioning of credentials or partial credentials, or activation, during manufacturing or device distribution, and, for example, these apparatus can augment, supplement, compliment or replace the activation server function. Such apparatus include, for example, device programming equipment (e.g., device credential provisioning apparatus 6430, device software loading and programming apparatus 6440 or SIM inventory 6450), equipment that is networked into a central provider, MVNO or VSP database (e.g., device credential, software and settings server 6420) to

gain access to provisioning information or activation information that is programmed into a device or group of devices, or to place device credential or partial credential information in a network database for later recognition, or to receive or communicate security information such as certificates for devices or SIM modules that will later be used to complete provisioning or complete activation or gain access to a network. For example, these apparatus, or any other apparatus including the activation server, can be networked into a service provider network or device database, an MVNO network or device database or a VSP network or device database. In some embodiments, programming of the device credentials or other information associated with the service processor or device is provided, so that, for example, the device can be recognized by an activation server or similar network function at a later point in time so that provisioning or activation can be completed in an automated manner, potentially with reduced or no user involvement, that provides a provisioning or activation configuration that is in some way unique for the service provider or service provider partner, device type, user group, VSP, MVNO, master agent or other entity. In some embodiments, this programming is provided in a manner that is difficult to change without the proper authorization so that the device is properly associated with the proper "service owner" or master agent (e.g., for the purpose of activation incentive payments). For example, as discussed herein, various approaches can be applied to the device credential or other settings or software provisioning so that the settings or software are secure or protected, or so that if the software is removed, replaced or modified it is reported or replace or restored. In some embodiments, VSP control of the provisioning, partial provisioning or activation of devices is provided during manufacture or at different points in the distribution channel. As discussed herein, some of these embodiments allow the central provider to offer to service partners (e.g., VSPs, MVNOs, master agents, and/or OEMs) similar types of control for device activation experience design or device service assignment control (e.g., sometimes referred to as service provider device locking so that other service providers cannot provide primary access to the device) during the manufacturing or distribution process that are possible with devices manufactured and distributed for the central service provider.

[0467] In some embodiments, the device is provisioned before the user obtains the device with permanent credentials, temporary credentials or partial credentials. In this case, the necessary credential programming of the device occurs during manufacture, at some point in the device distribution, such as at a distribution depot or in a store, or at the point of sale or point of

shipment. In some embodiments, provisioning of network information as discussed above is used, and the network information is provisioned at the same time, before or after the device information is provisioned. In some embodiments, the device provisioning information is programmed with dedicated apparatus that connects to the device either with wires or wirelessly. For example, the dedicated apparatus can be local to the location where the device is being provisioned, or it can be partially or entirely networked into a database or provisioning solution located elsewhere and operated by the central provider, a VSP, OEM or other entity. For example, the apparatus to program the network portions of the provisioning information can also be networked and the operators who set up the required network programming for a device or group of devices may be in the vicinity of the servers that host the provisioning and management tools or they may network into the servers. In some embodiments, provisioning system operators have full or partial control of any device provisioning equipment associated with the entity they work for (e.g., OEM, VSP or master agent) but only have remote access via secure terminal, secure website or other techniques to network into a central provider or VSP server farm in which they control or partially control the network portion of provisioning capabilities for that subset of devices that are assigned to the entity they work for with (e.g. OEM, VSP or master agent).

[0468] In some embodiments, provisioning is accomplished over the air on the mobile access network for mobile devices, or over the wired access network or WLAN connection for wired access networks, either before the user receives the device or after the user receives the device. In some cases, the device can be connected to general purpose equipment, such as a computer to perform the programming required to complete provisioning. In the cases in which the device is provisioned at point of sale or after point of sale, the device provisioning can be triggered by a user initiated sequence, or can be initiated by an automated background sequence at any time after the device is powered on. In such cases, in some embodiments, partial credentials that include information such as device type, OEM or service provider are used to assist in determining how to complete the provisioning, and the information can also include secure information, certificate or signature programmed into the partial credentials that is required for the network to perform the provisioning of the remaining credential information in the device and possibly the network. In some embodiments, any network information

used/required to provision the device or service is generated at the time the partial credentials are determined rather than beforehand.

[0469] In some embodiments, the device is activated for service before the user obtains the device with permanent credentials, temporary credentials or partial credentials, or with a permanent service account or a temporary service account. For example, in this case, the necessary steps of provisioning and activating service for the device can occur during manufacture, at some point in the device distribution, such as at a distribution depot or in a store, or at the point of sale or point of shipment. In some embodiments, the steps for activating service include one or more of the following: provision the device (e.g., with permanent, temporary or partial credentials), provision the necessary network databases and equipment to prepare them to recognize the device and associate it with the service profile and/or service plan, create or select the service account (e.g., permanent or temporary service account), select or create the service profile and/or service plan, program any elements in the device required to activate service (e.g., account ID, device aspects of the service profile and/or service plan), and program the necessary network databases and equipment with the required associations of device credentials and service profile and/or service plan policy settings. In some embodiments, the device oriented programming portions of the service activation steps occur at the same time, before or after the network oriented programming portions of the service activation steps.

[0470] In some embodiments, the device activation information is programmed with dedicated apparatus that connects to the device via a wireless or wire line connection. For example, the dedicated apparatus can be local to the location where the device is being provisioned, or the dedicated apparatus can be partially or entirely networked into a database or service activation solution located elsewhere and operated by the central provider, a VSP, OEM or other entity. For example, the apparatus to program the network portions of the activation information can also be networked and the operators who set up the required network programming for a device or group of devices can be in the vicinity of the servers that host the service activation and management tools or they can network into the servers. In some embodiments, activation server tools operators have full or partial control of any device activation apparatus associated with the entity they work for (e.g., OEM, VSP or master agent) but only have remote and partial access via secure terminal, secure website or other techniques to

network into the network portion of the activation tools that are controlled by the central provider or VSP. The server tools operators can be restricted in some embodiments to providing network activation information or settings only for those devices or device groups that are assigned to the entity they work for with (e.g., OEM, VSP or master agent). For example, the device control group restriction can be accomplished with a secure database that has secure sub-partitions for one or more entities so that they cannot impact the control of one another's network activation settings but can control their own devices. In this way, a centralized set of activation tools resources controlled by a central provider, VSP or other entity can be partitioned so that different entities can have partial or full control of the activation service definition for devices or groups of devices without impact or risk to others who share the network and activation tools resources.

[0471] In some embodiments, activation is accomplished with an over the air interface to a mobile device, or over the wired access network or WLAN connection for wired access networks, either before the user receives the device or after the user receives the device. In some cases, the device can be connected to general purpose equipment such as a computer to perform the programming required to complete activation. In the cases in which the device is activated at point of sale or after point of sale, the final device activation process can be triggered by a user initiated sequence, or can be initiated by an automated background sequence at any time after the device is powered on. In such cases, some embodiments call for a temporary service account that is used to bring the device onto the network before the user has input the information necessary to create a permanent service account. In some embodiments, a temporary or permanent service account can be applied to the device at the time the device reaches the network, and the type of account, service profile and/or service plan can be influenced (e.g., partially determined or informed) or determined by information embedded in the device credentials or partial credentials, such as device type, device ID, SIM, OEM or service provider. For example, the device credentials can also include secure information, certificate or signature that can be required by the network to perform the activation steps for temporary or permanent service account status. In some embodiments, in which the device is activated in this manner before the user information is available, or before the user has selected a pay for service plan, the service profile and service plan are set up for ambient services as described herein.

[0472] In some embodiments, the device is activated during the manufacturing or distribution process, and then the activated device status is suspended. Once the temporary or permanent service account is set up, with appropriate service profile and/or service plan and temporary or permanent credentials, in some networks and billing systems the service can often be more easily resumed once suspended as compared to provisioning and activating the device from scratch. The device is then later resumed (or re-activated) when some event triggers the resume process, such as when it ships to the end user or when the end user attempts to use it. This process prevents the network from needing to manage credentials and accounts for devices that have been activated but are not yet on the network.

[0473] In some embodiments, provisioning is accomplished at least in part with temporary credentials in a manner which is automated and convenient for the user or device owner. In some embodiments, at least some subset of the temporary credential elements replaced at a later point in time by permanent credential elements in a manner that is also automated and convenient for the user or device owner. In some embodiments, the temporary credential set is pre-programmed into the device along with a temporary or permanent service account including service profile during the manufacturing or distribution process so that the device is activated with temporary credentials when it ships. In some embodiments, the aforementioned pre-programming is performed for the network via a secure set of server access equipment that networks into the network databases used to define the service profile and/or the service plan. In some embodiments, a subset of the temporary credentials is recycled once it is replaced, if a temporary service account is not activated or used after some period of time, if a permanent account is not activated or used after some period of time, or if the credentials subset is revoked from the device for some other reason.

[0474] In some embodiments, more than one device is assigned one or more elements of the temporary credentials, such as the phone number, which may be limited in supply. In some embodiments, a network will accept more than one set of temporary credentials, one or more redundant elements, for two or more different devices. In some embodiments, a device that has two or more temporary credential sets, in which at least a subset of the credential elements are different for the sets, so that if one set of credentials has elements that are already being used to

access the network, then one or more reserve sets can be drawn upon to gain access to the network.

[0475] In some embodiments, the temporary credentials are used to log onto the network to conduct an over the air or over the network activation process in which an activation server reads at least a portion the device credentials to determine some aspect of how the device service profile. In some embodiments, the aforementioned over the air activation process is accomplished in the background without user intervention. In some embodiments, the over the air activation process is initiated when the user first attempts to use the device or when the user first attempts to access the network or upon user request or approval. In some embodiments, the over the air activation process is initiated using a temporary service account for the device and/or network to gain access to the network. In some embodiments, the over the air activation process is initiated after the user has entered the information required to create a permanent user account into the device or into the network. In some embodiments, the user is required to enter the aforementioned user information before using the device or using some aspect of the device. In some embodiments, the temporary service account is replaced by a permanent service account some time after the user has entered the necessary information to create a permanent account into the device or network. In some embodiments, the over the air activation process is initiated using a permanent service account assignment for the device and/or network to gain access to the network.

[0476] In some embodiments, the service profile is assigned to the device and/or network during the aforementioned over the air activation to be a pay for service profile with a free trial period. In some embodiments, the service profile assigned to the device and/or network during the aforementioned over the air activation includes pre-pay, post-pay, session based pay or pay as you go options for service. As will be apparent to one of ordinary skill in the art, various embodiments disclosed herein are particularly well suited for control or pre-pay services. In some embodiments, the service profile that is assigned to the device and/or network during the aforementioned over the air activation is an ambient service profile providing service access before all the user information is available to assign a permanent account. In some embodiments, the service profile that is assigned to the device and/or network during the aforementioned activation is an ambient service profile providing a service upgrade selection

option interface to the user. In some embodiments, the service profile that is assigned to the device and/or network during the aforementioned activation is an ambient service profile providing transaction services to the user. In some embodiments, the service profile that is assigned to the device and/or network during the aforementioned activation is an ambient service profile providing bill by account functionality for the network. In some embodiments, the service profile that is assigned to the device and/or network during the aforementioned activation is an ambient service profile providing some amount of free networking or information service to entice the user to use the other ambient services. In some embodiments, the aforementioned ambient service is at least partially implemented with device based service activity control or control assistance. In some embodiments, the aforementioned ambient service is at least partially implemented by gateways, routers or switches in the network that are programmed according to the ambient access profile for the device to implement the ambient policies for network access control, routing control, traffic control or service monitoring and reporting for bill by account.

[0477] In some embodiments, activation is accomplished at least in part with a temporary service account in a manner that is automated and convenient for the user or device owner. In some embodiments, at least some subset of the temporary service account is replaced at a later point in time by permanent service account subset in a manner that is also automated and convenient for the user or device owner. In some embodiments, the temporary service account settings (e.g., including the service profile settings and/or the service plan settings) are pre-programmed into the device along with a temporary or permanent credentials set during the manufacturing or distribution process so that the device is activated with temporary credentials when it ships. In some embodiments, the aforementioned pre-programming for the network is performed via a secure set of server access equipment that networks into the network databases used to define the service profile and/or the service plan. In some embodiments, the device is suspended once it is activated but before the user is using it, and then resumed before or commensurate with the point in time that the user begins to use it. In some embodiments, some subset of the temporary service account is recycled once it is replaced, if the temporary service account is not used after some period of time, if the temporary service account is not upgraded to a permanent service account after some period of time, or if the activation is revoked from the device for some other reason. In some embodiments, more than one device is assigned to the

same temporary service account. In some embodiments, a network accepts more than one device on the same temporary service account. In some embodiments, a device includes or is associated with two or more temporary service accounts, in which at least a subset of the temporary service account elements are different, so that if one account is already being used to access the network then one or more reserve accounts can be drawn upon to gain access to the network. In some embodiments, the temporary service account is associated with a temporary credentials set. In some embodiments, the temporary service account is associated with a permanent credentials set.

[0478] In some embodiments, un-activated devices are detected by the network routing equipment (e.g., service gateways or routers in hierarchical networks or base stations with embedded gateways in flat networks) and the device routing is programmed to re-direct un-activated devices to an activation server network destination. For example, the activation server can first inspect the information associated with the device to determine if the device belongs to the list of devices, device types or device groups that the network is programmed to provide access to. For example, the information used to determine this can include device type, service provider, phone number, device ID, SIM ID or configuration, secure information used to qualify the device, IP address, MAC address, user, user group, VSP, OEM, device distributor, service distributor (master agent), service processor presence or configuration, presence or configuration of other software or hardware. There can also be some activation definition information embedded in the credentials, or associated with some portion of the credentials, or programmed additionally on the device that informs the activation server as to the service profile and/or service plan and/or service account that should be established for the device. If activation information (the service profile, service plan and/or service account information) is found through association with the device credentials (e.g., device ID, phone number, IP address, MAC address, SIM or other security credentials) rather than being read directly from information embedded in the device or device credentials, then the pertinent aspects of the credentials can be used as a cross reference to look up the service plan and/or service profile information stored in a database networked to or within the activation server. The activation information can include information to define a wide variety of service plans and service profiles that when properly implemented on the network functions, and perhaps device if necessary, can provide for a wide range of service activity policies, service billing policies, transaction billing policies and service account types that can be associated with the device over the air or over the network.

[0479] In some embodiments, once the activation server has determined the activation information from the device or from a look up based on some aspect of the device credentials, then the activation server initiates the necessary network settings and billing database entries to be programmed by sending the service profile instructions to the network provisioning and activation apparatus and the service plan instructions to the billing system. In some embodiments, the activation server can then also send the any necessary service profile and/or service plan settings required for the device to a provisioning and activation support software function on the device, such as various embodiments of the service processor, so that the device provisioning and activation can be completed. The provisioning can be with permanent credentials or temporary credentials, and the service account that is set up may be permanent or temporary. In some embodiments, the activation process described above is completed perhaps before the user has entered some or all of the user information necessary to set up a permanent service account, and, in these cases, a temporary service account can be set up. In some cases, the activation process can be completed in the background before the user has completed an attempt to access the network and the service profile can be set up to provide ambient services to a temporary service account. In some embodiments, the user is required to enter the information required to establish a permanent service account prior to gaining full use of the device, either on the device, on a computer or in the store, so that by the time the user begins using the device the above activation embodiments can provide for ambient services activation with permanent account status so that the user can purchase a service upgrade or any transaction without entering any more account information.

[0480] In some embodiments, a device status is changed from a temporary service account to a permanent service account. If the device is activated with a temporary service account, and the user information is available to set up a permanent account, then if the billing system rules and interfaces allow for such, the user information can be changed from the mock information to the actual user information while maintaining the same account identifiers in the billing system. If the billing system will not allow for such, then the user information can be used to establish a new account, the device credentials can be re-associated with the new account, in some cases, after modifying one or more of the device credential parameters, and the network functions can be re-programmed as required, and, in some cases, the device can be re-programmed as required to accommodate the new permanent account.

[0481] In some embodiments, code on the device pulls a temporary or permanent set of credentials. When the credentials are pulled, the network associates the device with an ambient service profile according to one or more of the following: embedded device information identifying device type, service owner (e.g., VSP), user group, or user, or device ID is cross referenced to a database that is populated some time from manufacturing time to post sale where the database provides information identifying device type, service owner (e.g., VSP), user group, or user. The device is then re-directed accordingly (e.g., for device based this is a matter of setting the policies or loading the software for the service processor, for the network based approach this is a matter of populating the routing tables and service profile). For example, credentials can be re-cycled after a period of time, and/or some portion of the credentials can be redundant with other devices. For example, this is essentially a dynamic service for (temporarily) assigning device credentials, and the duration of the temporary credential validity for that device ID can be time limited to give the user time to activate a real account or a free trial, session limited, or a longer duration of time that is perhaps refreshed each time the device logs on. For example, the device could also already have permanent or temporary credentials but not have a service account. The above process can be used to assign a temporary or permanent service account as well. Once the service account is assigned and the appropriate service profile is propagated to the network elements, the device can then be directed to or use the appropriate activation profile service activities or the appropriate ambient service activities.

[0482] In some embodiments, the device is activated in the background in a manner that is virtually transparent to the user. For example, at some point in the distribution channel, the device is programmed to seek the activation server system described above as soon as it is turned on, or as soon as some other event occurs like the user using the device or the user attempting to gain access. When the pre-programmed event is triggered, the device connects to the network and the gateways or routers re-direct the device to an activation server, as discussed above. As also described herein, the activation server either derives information from the device that informs the server what service the device should be activated with, or the server derives that information from a database look up with a portion of the device credentials as the cross reference parameter. Once the activation server has determined the activation information from the device or from a look up based on some aspect of the device credentials, then the activation server causes all the necessary network settings and billing database entries to be

configured/programmed by sending the service profile instructions to the network provisioning and activation apparatus and the service plan instructions to the billing system. In some embodiments, the activation server can then also send the any necessary service profile and/or service plan settings required for the device to a provisioning and activation support software function on the device, such as various embodiments of the service processor, so that the device provisioning and activation can be completed. For example, the provisioning can be with permanent credentials or temporary credentials, and the service account that is set up can be permanent or temporary.

[0483] In some embodiments, background activation is performed using the aforementioned activate/suspend process. At some point in the distribution channel, the device is programmed to seek to resume service as soon as it is turned on, or as soon as some other event occurs like the user using the device or the user attempting to gain access. When the pre-programmed event is triggered, the device attempts to connect to the network and the gateways or routers re-direct the device to an activation server as described herein. As also described herein, the activation server either derives information from the device that informs the server that the device is ready to resume service, or the server derives that information from a database look up with a portion of the device credentials as the cross reference parameter. Once the server is aware of this information, it sends a message to resume service to the billing system, or other network function that controls the suspend/resume function, and the service is resumed.

[0484] In some embodiments, background activation is performed as described below. The service processor and the credentials are pre-programmed during the manufacturing or distribution process to provide the desired service profile support and/or billing profile support for the desired initial ambient service. As described herein, this programming can be accomplished with dedicated apparatus at the manufacturer or distribution depot. Furthermore, the party responsible for defining the service (e.g., typically the central provider, OEM, VSP, distributor or master agent) can network into the service processor programming apparatus to control service processor and/or credential programming for all or a subset or group of the devices or device types locally available. The service processor enabled device is programmed to seek the activation server system described above as soon as it is turned on, or as soon as some other event occurs like the user using the device or the user attempting to gain access. In some

embodiments, the activation server is the access control server previously discussed or the access control server can act in concert with another server that performs the activation function. When the pre-programmed event is triggered, the device connects to the network and the gateways or routers re-direct the device to the activation server. As also described herein, the activation server can communicate with the service processor to verify the service processor security credentials, agents and configuration.

[0485] In some embodiments, if the activation server determines that the pre-programmed settings stored in the service processor need to be modified to provide the latest version of the desired service, or if the service processor agent software needs to be updated, then this can be accomplished prior to completing the activation process. Once the service processor configuration and settings are confirmed, the activation server causes the necessary network settings and billing database entries to be programmed by sending the service profile instructions to the network provisioning and activation apparatus and the service plan instructions to the billing system. Given that the service processor can perform some or much of the service activity control or control assistance, the service control options are generally larger than without the service processor, and there can be less configuration to perform for other networking equipment to complete the provisioning and activation process. The provisioning can be with permanent credentials or temporary credentials, and the service account that is set up can be permanent or temporary.

[0486] In some embodiments, pre-programming and pre-activation of devices with temporary credentials and a temporary service account are used to ship devices that are pre-activated. Given that the credentials are temporary and can be recycled when the permanent credentials are assigned, concerns about using up too many pre-assigned credentials are reduced. In embodiments in which a portion of credentials elements can be used for multiple devices, this concern is further reduced. If there is a concern about too many activated devices being assigned that are not actually active and generating service revenue, then the suspend/resume process discussed herein can be employed. In some embodiments, the temporary credentials and/or temporary account can be replaced with permanent credentials and/or account assignments at any time as follows. When a pre-programmed event in the device is triggered, then the device initiates a program that seeks the aforementioned activation server or another server that has the

capability of fulfilling the device request to exchange the temporary credentials for permanent credentials and/or exchange the temporary account for a permanent account. The event that triggers the credential exchange can be the same or different than the event that triggers the service account exchange. The service account exchange can typically be triggered by the point in time that the user enters account information.

[0487] In some embodiments, the aforementioned ambient service is partly implemented with a combination of the techniques for pre-provisioning during manufacturing or distribution and at least partially implementing the service activity control (e.g., access control, routing policy, traffic control, usage limits, and/or policy for usage limit overage) required for implementing ambient using the service policy provisioning capabilities in the data path gateways, routers or switches in the network. The gateways, router or switches are pre-programmed as discussed herein according to the ambient access profile for the device to implement the ambient policies for network access control, routing control, traffic control or service monitoring and reporting for bill by account. In some embodiments, the provisioning credential elements are not all pre-programmed before the device ships, but a subset of the credential elements are programmed using the activation server technique discussed herein. This over the air automated provisioning is combined with the activation server reading the device credentials to derive the service activity control settings for the gateways, routers or switches that will result in the desired ambient services activity controls.

[0488] In some embodiments, the aforementioned ambient service is implemented with a combination of the techniques for pre-activation during manufacturing or distribution and at least partially implementing the service activity control (e.g., access control, routing policy, traffic control, usage limits, and/or policy for usage limit overage) required for implementing ambient using the service policy control capabilities in the data path gateways, routers or switches in the network. The gateways, router or switches are programmed to recognize the pre-activated device credentials as discussed herein according to the ambient access profile for the device to implement the ambient policies for network access control, routing control, traffic control or service monitoring and reporting for bill by account. In some embodiments, the device activation profile and/or service account are not pre-programmed in the network and/or the device before the device ships but the activation profile and/or service account are programmed

using the activation server technique discussed herein. This over the air automated provisioning is combined with the activation server reading the device credentials to derive the service profile activity control settings for the gateways, routers or switches that results in the desired ambient services activity controls.

[0489] In some embodiment, a VSP capability is enabled by providing a secure network connection to the service policy settings tools that define the device pre-provisioning settings, the device pre-activation service profile settings, the network equipment service activity control policy settings (e.g., access control, routing policy, traffic control, usage limits, and/or policy for usage limit overage), and the network billing system database. By providing server tools that enable all these settings to be controlled (or perhaps only observed in the case of the billing system) by a secure workstation or secure website interface that networks into the equipment that programs the settings, and providing for a secure partitioning of the devices that can be controlled by a given secure workstation or secure website interface, a central provider can provide VSP services to multiple entities who all have different device and service plan combinations that they desire different flavors of ambient services for. These techniques can also be extended beyond ambient to any device/service profile/service plan combo the VSP desires to create. In some embodiments, the networking equipment is implemented to secure device service group domains in which the service policies for a group of devices can be controlled. In some embodiments, the pre-provisioning and pre-activation techniques are substituted with the over the air activation server techniques discussed herein, and a secure device group partition capability is provided in the activation server as well so that the activation server device group partition control capabilities can be added to the secure device group partition control capabilities of the network gateways, routers and/or switches, the device programming tools and the billing system to form a VSP partition solution for over the air activation of various device/service plan combinations. In some embodiments, the device groups are relatively small so that beta trials of arbitrarily large or small size can be designed and implemented by defining a service control group as described above, and after fine tuning and perfecting the beta trial settings the device group can be expanded to publish the automated provisioning and activation service settings to a larger user or device group for production services.

[0490] In some embodiments, device based service activity control assistance (e.g., based on the various service processor embodiments described herein) is combined with simplified provisioning techniques described herein so that service processor enabled devices can be shipped with pre-provisioned credentials (temporary or permanent) or can obtain credentials in an automated manner that is convenient and efficient for the user or device owner. In some embodiments, the service processor embodiments in combination with the manufacturing and supply chain credentials and provisioning apparatus described elsewhere provide various approaches for provisioning pre-provisioned service processor enabled devices. In some embodiments, the service processor embodiments in combination with the activation server variants discussed above provide various approaches for over the air or over the network simplified post-sale provisioning for service processor enabled devices. For example, these embodiments can also be used for ambient services given that as discussed herein the service processor has capability to implement service profile policies for deep control of ambient service activity control.

[0491] In some embodiments, provisioning includes provisioning partial device credentials that include, for example, a secure certificate that is used to authorize full credential provisioning and/or activation by performing a process for a later look-up/validation of the full device credentials. For example, the look-up/validation of the full device credentials can be performed by a gateway, router or similar network device that re-directs to a provisioning server and/or activation server or other network components that either: (1) recognizes the partial credentials that serve as a reference to direct the device communication to a specific provisioning/activation server determined from the partial credentials; or (2) does not recognize the partial credentials, and directs the device communication to a less specific provisioning/activation server that is not necessarily associated with a reference to the partial credentials.

[0492] In some embodiments, if the partial device credentials (e.g., temporary or permanent credentials) are being used for provisioning, then the partial credentials are read (e.g., and/or other credentials can be looked up based on the partial credentials as described above). The device is authorized if the proper credentials and/or secure certificate is present. The device credential provisioning is then completed (e.g., using activation server commands or settings to a

device based software and/or hardware element), and the credentials are, in some cases, also communicated to the various network equipment elements.

[0493] In some embodiments, if the partial device credentials are being used for activation, then partial or full device credential provisioning is performed, such as described above. A service account (e.g., temporary or permanent service account) is created or looked up based on the partial device credentials (e.g., a user account associated with the device through embedded partial or full credentials or a look up process, or based on a dynamically created/assigned temporary account associated with the device through embedded partial or full credentials). An initial service profile and, in some cases, an initial service plan (e.g., service control policy settings including a billing profile) are determined from embedded information and/or using a look up process (e.g., based on the device type and/or partial or full device credentials). The device is then programmed to enable access with the service profile and plan, and, in some cases, the various network components/elements are programmed to enable the service profile and plan, and, in some cases, proper entries in the billing system are made or confirmed, and the device credentials are, thus, activated for service.

[0494] In some embodiments, the above described provisioning and/or activation processes are performed with the provisioning server(s) and/or activation server(s) in the background with reduced, minimal or no user input required, for example, after the device is sold to the user and the user turns on the device so that by the time the user attempts to access the service using the device, the provisioning and/or activation process is already completed.

[0495] In some embodiments, device based service activity control assistance (e.g., based on the service processor embodiments) is combined with simplified activation techniques described herein so that service processor enabled devices can be shipped with pre-activated accounts (temporary or permanent), or can obtain activated account status in an automated manner that is convenient and efficient for the user or device owner. In some embodiments, the service processor embodiments in combination with the manufacturing and supply chain activation and provisioning apparatus described elsewhere provide various approaches for pre-activated service processor enabled devices. In some embodiments, the service processor embodiments in combination with the activation server variants discussed above provide various

approaches for over the air or over the network simplified post-sale account activation for service processor enabled devices. These embodiments can also be used for ambient services given that as discussed herein the service processor has capability to implement service profile policies for deep control of ambient service activity control.

[0496] As discussed herein, in some embodiments for activation, the network AAA (or other network function) either recognizes one or more aspects of a pre-activated device credentials and routes the pre-activated device communication to an activation server that is appropriate for that device (routing information either derived through look up of the credential aspect or by obtaining the required information directly from the credential itself), or the AAA (or other network function) does not recognize the credentials and routes the device communication to an activation server for unrecognized device credentials. In either case, in some embodiments, one or more of the credential aspects can then be used to perform a secondary determination of what provisioning and/or activation sequence to perform in association with the device, or which activation server sequence the device should be directed to. For example, one or more device credential aspects can be read and used as a cross-reference to determine a routing for the device communication (or the information required for routing can be in the device credential information itself) so that the device can be routed to the appropriate activation server sequence.

[0497] In some embodiments, an activation server sequence can be determined at least in part by using a browser server or a portal (e.g., http server, https server, WAP server or another standard or custom protocol server for a browser, embedded or automated browser or a portal client in the device). In some embodiments, the browser server is an http or https server. The pre-activated device communication can be routed to the https server in a manner similar to that described above, and the server can read the information embedded in the https communication to determine the device credential information required to initiate the correct provisioning completion and/or activation sequences. For example, the https header information, tokens, cookies or other secure information communicated over https from a secure embedded client on the device (or user) can either provide the activation server with the information required to perform the cross-reference to an appropriate provisioning and/or activation sequence, or the https embedded information or the embedded client (or user) information can instruct the

activation server on which services the device is to be provisioned and/or activated on and any necessary device or user information (e.g., device owner and/or billing information) can be exchanged, or the device might be provisioned and/or activated first on a free ambient service with temporary or permanent credentials or account.

[0498] In some embodiments, the service processor can be combined with the pre-provisioning and pre-activation techniques described above to create an ambient service solution that will work on roaming networks in which the central provider or VSP has no control or minimal control over the network elements. For example, the device includes a service processor pre-programmed for ambient service activity control as discussed herein, and the device credentials and other settings are pre-provisioned and pre-activated for the central provider network, all of which is described in numerous embodiments disclosed herein. Provided that the service provider has a roaming agreement with other service providers, or provided that the device may gain access to the roaming network, when the device is roaming it will be capable of ambient connectivity with bill by account functionality and all the other features of ambient. Furthermore, as also discussed herein, the ambient service activity control policies can be different for different roaming networks to accommodate the varying network costs and performance. Also, for example, it would be permissible to sign up for initial services or additional upgrade services with the central provider while roaming on the roaming partner network. One of ordinary skill in the art will appreciate that this also allows for creating a VSP or MVNO for the purpose of creating a clearing house for central provider service activations according to geography or user choice. By using a global multi-mode modem module, and maintaining service agreements with a multitude of carriers, the MVNO or VSP can provide consistent ambient services across multiple carriers and multiple geographies while still maintaining a good degree of cost control. Using bill by account capabilities, it is also possible to have an activation agreement where a roaming service provider agrees to refund the cost of ambient roaming. From the ambient service platform, the VSP or MVNO can then provide service purchase options to the user based on the carrier networks available to the device, or the VSP or MVNO can broker the user off to any of the carriers by activating the device onto the carriers main central provider service.

[0499] Accordingly, these embodiments provide flexible capabilities for activating a device or group of devices with a broad range of service profiles and service plans by simply programming the device with the proper credentials at some time during manufacturing or distribution, or simply programming a database associated with the network so that a portion of the device credentials can be used to look up the desired service profile and service plan. For example, various activation embodiments described herein are highly convenient for the end user and need not, in many cases, involve any human intervention.

[0500] The service processor 115, service controller 122, policy implementation and/or profile implementation and various embodiments disclosed herein are applicable to conventional communication products as well as machine to machine applications. For example, if the machine to machine device includes a service processor 115 with an activated account, then the service profile settings can be optimized for machine communications to provide only the limited access required to support the particular machine to machine application. This allows for cost optimized access services and prevents the machine to machine device or access modem from being misappropriated and used for some other service access than that intended. For example, by programming the machine to machine communications device at time of manufacture or during distribution with credentials or partial credentials that provide for automated provisioning and activation as described herein, the device can be automatically provisioned and activated on the service network with a service account when deployed, thus eliminating the need for costly or time consuming human intervention. The various embodiments that make it simpler to design, manufacture, test and deploy devices may also be equally applied to machine to machine devices. These embodiments include the service processor 115 developers kit and the automated provisioning and activation management tools among others. Also, the service analysis and test tools and the virtual service provider embodiments can also be applied to machine to machine applications.

Verifiable Device Assisted Services For Intermediate Networking Devices

[0501] It should be appreciated that the various service monitoring, notification, control and billing embodiments disclosed herein can also be applied to intermediate networking device applications.

[0502] In some embodiments, an intermediate networking device is a communications device in which the service processor 115 is configured at least in part to allow the intermediate networking device to act as a service intermediary or intermediate connection between the network and one or more end point devices (e.g., communications devices). In addition, a service controller 122 or other suitable network functions can be employed to assist with the verifiable service usage monitoring, control and verification as disclosed in numerous embodiments described herein. In some embodiments, an intermediate networking device does this by implementing the service policies required for assisting service usage control of the intermediate networking device and connecting the network to provide services to one or more end point devices that are connected to the intermediate networking device. In some embodiments, the intermediate networking device also monitors the service use activities of the intermediate networking device and/or the end point devices connected to the intermediate networking device. In some embodiments, the intermediate networking device and/or end point device service usage is verified to ensure that the service usage is within the expected ranges for the policies that are implemented. In some embodiments, the intermediate networking device connects with the network using one modem technology and connects with the end point devices using one or more additional technologies. In some embodiments, an intermediate networking device connects the end point devices to the network by passing, bridging, forwarding, routing, traffic shaping or otherwise allowing the end point devices to communicate with the network. Example intermediate networking device embodiments include a Wi-Fi to WWAN (e.g., 2G, 3G, 4G or other wireless wide area networking access technology) bridge or router device, a Wi-Fi to DSL, cable or fiber gateway device, a WWAN to DSL or Cable femto cell device, a WWAN and Wi-Fi to DSL, Cable or fiber back-hauled femto cell device, a WWAN to WWAN router device, a WWAN to WLAN, WPAN or LAN bridge, router or gateway device, or a WWAN back up connection device for an enterprise router.

[0503] An intermediate networking device can also be provided in some embodiments by including a bridging, forwarding or routing function between two modems in a communications enabled device that connects to the network. For example, an intermediate networking device configuration can be a cell phone, smart phone, mobile internet device or any other mobile device that includes a WWAN modem and a Wi-Fi, WLAN, WPAN or LAN connection that can be used to connect to other end point devices. For example, the mobile device WWAN modem

can connect to the network, a service processor 115 can be included on the device processor to assist monitoring, controlling and billing for services between the WWAN network and end point devices connected to a Wi-Fi modem. In addition, a service controller 122 or other suitable network functions can be employed to assist with verifiable service usage monitoring, control and verification as disclosed in numerous embodiments disclosed throughout herein. In some embodiments, the Wi-Fi modem can be configured in access point mode or in ad hoc mode to communicate with other end point devices in the area covered by the mobile device WLAN modem. In this manner, a service processor 115 and a service controller 122 or other suitable network functions can be employed to enable the verifiable service usage monitoring, control and verification as disclosed in numerous embodiments described herein.

[0504] Another example embodiment is a notebook or sub-notebook computer with a WWAN modem and a Wi-Fi, Ethernet, Firewire, Bluetooth, near field or Zigbee modem in which the notebook processor has a service processor 115 running on the notebook processor and the service processor 115 is used to assist monitoring, control and billing for services communicated between the WWAN network and end point devices connected to the notebook or sub-notebook WLAN, LAN or WPAN. Another example embodiment is a Wi-Fi hot spot with a service processor 115 capability. Another example embodiment is a WWAN back up modem in an access network router where the back up modem connection to the WWAN network is used when the main wired network connection goes down, and a router processor or a WWAN back up modem processor runs a service processor 115 to assist monitoring, controlling and billing for services between the WWAN network and the access router (e.g., the service provider may only wish to enable a connection when the main wired network is down to ensure that the WWAN modem is not used for everyday access). In this manner, a service processor 115 and a service controller 122 or other suitable network functions can be employed to enable the verifiable service usage monitoring, control and verification as disclosed in numerous embodiments described herein.

[0505] Another example embodiment is a two-way home gateway configured to perform various functions such as reading power consumption of the home and/or components in the home, providing WLAN, WPAN or LAN connectivity for such components or to the power meters/controllers attached to such components, providing a WWAN or WAN connection to a

network that reads, records, monitors and/or controls the home and/or component power consumption, and possibly to provide other wide area network services for other devices in the home such as computers or entertainment electronics in a similar manner to the WWAN, DSL, cable and fiber gateway embodiments. The WLAN, WPAN connections can be made with one or more of Wi-Fi, Zigbee, Bluetooth, NFC or any other suitable wireless modem technology, and any desired wired LAN connections may be made with one or more of Ethernet, USB, Firewire, data over cable, data over power line or any other suitable wired modem technology. The WWAN connections can be made with one or more of 2G (e.g. CDMA 1xRT, GPRS), 3G (e.g. WCDMA UMTS/HSPA/non-MIMO HSPA+, CDMA EVDOrA/B, 802.16d/e WiMax), 4G (e.g. LTE, MIMO HSPA+, MIMO 802.16m WiMax) or any other suitable modem technologies and the wired WAN connections may be made with one or more of DSL, Cable, fiber or any other wired modem technology. A service processor 115 and a service controller 122 or other suitable network functions can be employed to enable the verifiable service usage monitoring, control and verification as disclosed in numerous embodiments disclosed throughout herein.

[0506] In some embodiments, an intermediate networking device can be used to connect one end point device to a network and assist in implementing service policies, or an intermediate networking device can connect multiple end point devices to one or more networks and assist in implementing service policies. In some embodiments, an intermediate networking device can be associated with one service profile, one service plan or one service account, or an intermediate networking device can be associated with multiple service profiles, multiple service plans or multiple service accounts. In some embodiments, end point devices connected to an intermediate networking device can have service usage policies implemented in aggregate for all end point devices, or service policies can be implemented differentially for different end point devices.

[0507] In some embodiments, an intermediate networking device can have a network connection associated with a single account and manage QOS between end point devices under one umbrella service profile or collection of profiles. In some embodiments, an intermediate networking device can treat all connected end point devices equally from a service sharing or QOS perspective so that, for example, service usage is based on end point device demand and/or contention. In some embodiments, an intermediate networking device differentiates service

QOS between different end point devices based on end point device service demand or service usage patterns, EDP device type or device group, end point device user or user group, end point device service account status or service plan status, or end point device application type, and/or traffic type or service type.

[0508] As discussed herein, the service processor 115 function assisting intermediate networking device implementation can be included on the intermediate networking device, can be included in part on the intermediate networking device and one or more end point devices, or can be implemented mainly or entirely on one or more end point devices.

[0509] In some embodiments, an intermediate networking device can be constructed in which end point devices connect to the intermediate networking device and gain access services to a WWAN network through a WWAN/Wi-Fi enabled intermediate networking device that is supplied with services associated with a single account and service profile. The intermediate networking device service processor 115 can assist in monitoring, control and billing for WWAN service usage for all end point devices in the area covered by the intermediate networking device Wi-Fi link. In some embodiments, end point devices receive service on first come first serve basis with no differentiation. In some embodiments, end point devices receive fair distribution of services so that if one end point device is using more significantly more service than the other end point devices, or is demanding more service than the intermediate networking device service profile settings provide for a single end point device (e.g., "bandwidth hogging"), then the high demand end point device is throttled and the other end point devices are not. In some embodiments, end point devices receive hierarchical distribution of services based on one or more of service type, device type, user type, and/or account status. In some embodiments, an intermediate networking device can provide for a large or unlimited number of end point devices to connect to the network and simply control aggregate service usage parameters for the intermediate networking device WWAN connection. In some embodiments, the intermediate networking device limits the number of end point devices that are allowed to connect to the WWAN network according the end point device count limits programmed in the service processor 115 service profile settings in the intermediate networking device. In some embodiments, end point device traffic can be identified by various end point device credential aspects including, for example, by Wi-Fi ID, MAC ID, IP address, user ID, LAN tag, end point

device agent credentials, and/or browser token or cookie. In some embodiments, the intermediate networking device service account can be billed for overall service usage and/or by number of end point device connections allowed or experienced. In some embodiments, as the intermediate networking device user or owner signs up for a higher end point device connection count, one ore more aspects of the service usage policy implementation and/or profile implementations in the service processor 115 profile settings can be increased.

[0510] The various verification techniques described herein can also be applied to the intermediate networking device and extended to multiple end point devices. For example, network based service usage measures for verification can be applied to the intermediate networking device just as if the intermediate networking device were an end point device. For example, network based service usage measures (e.g., IPDR information) can be used to perform network verification checks to ensure that intermediate networking device service usage is within acceptable ranges based on intermediate networking device policy settings as similarly described with respect to various device embodiments. In some embodiments, in the event intermediate networking device service usage is outside the policy limits set for the intermediate networking device service processor 115, a notification can be sent to the intermediate networking device main account owner. The main intermediate networking device account owner can also be required to acknowledge the notification. The notification can also be sent to one or more other users of the intermediate networking device connection, including possibly all users. Other actions that can be taken if the network based intermediate networking device service usage measure does not match the policy limits set on the service processor 115 include notify the user, notify the user and require acknowledgement, bill the user for service overage, suspend the end point device, quarantine the end point device, SPAN the end point device, and/or alert network manager or alert an automated network troubleshooting function. In some embodiments, a device based usage measure can be verified against a network based service usage measure. It will now be apparent that the various service processor 115 verification embodiments, service controller 122 verification embodiments, network verification embodiments, authentication embodiments, and tamper prevention or detection embodiments, such as those shown in and described with respect to FIGS. 22A, 22B, 23, 26A-26H, 27A-27P and 28A-28E, can be applied to intermediate networking device applications and embodiments.

[0511] In some embodiments, it is desirable to match up individual end point device or user intermediate networking device service usage with other service usage measures. For example, the individual end point device service usage measures logged or reported from the end point devices and/or the intermediate networking device can be aggregated to form a total intermediate networking device usage measure that is compared to an aggregate intermediate networking device usage measure logged or reported in the network. In some embodiments, if these measures do not match, then an error condition results and an action is taken. In some embodiments, the aggregate intermediate networking device service usage measure is compared to the aggregate network based service usage measure and as long as these two measures are within an acceptable tolerance, then the intermediate networking device service usage measures are trusted and can be used for deeper intermediate networking device and end point device usage measures for service control and/or billing than may be possible in the network. In such embodiments, the individual end point device service usage measures gained from the intermediate networking device or end point device can be used to verify end point device service usage versus service policy allowances. In some embodiments, end point device service usage measures are compared with intermediate networking device measures for the same end point devices.

[0512] In some embodiments, the IPDR records for one or more networks can include individual end point device service usage information. This is the case for example when the IPDRs include information broken down by end point device credential, such as IP address or other end point device credential. In such cases, intermediate networking device embodiments can be employed in which the individual end point device service usage information measured in the network can be compared with the service usage policy allowances or limits for the end point device. Also, in some embodiments, the individual end point device service usage measures from an end point device service usage monitor and/or an intermediate networking device service usage monitor can be compared with the network based service usage information to verify an end point device and/or an intermediate networking device service usage monitor is operating properly.

[0513] As similarly described with respect to end point device embodiments with no intermediate networking device between the end point device and the network, in some

intermediate networking device embodiments, service usage and service usage monitor reports can be periodically verified by performing a SPAN function on the traffic for an intermediate networking device. The SPAN traffic can be analyzed in a real-time manner or in a non-real-time manner in the network and the results can be compared with the intermediate networking device or end point device service policies or service usage measures.

[0514] The synchronized device notification and acknowledgement embodiments can also be employed in the case in which one service account is applied to the intermediate networking device. The service usage counters in the intermediate networking device can be synchronized or updated with the network based measures and the differences between the two may be minimized. The service usage notification can be sent to one or more of the end point devices connected to the intermediate networking device. For example, the notification can be sent to the intermediate networking device manager or service owner, all end point devices or the most active end point devices.

[0515] Similarly, user preference feedback can be collected from one or more of the service users connected to the intermediate networking device. In some embodiments, user preferences or user service selections or service settings are collected from one user or a subset of end point devices used by the service subscriber. In some embodiments, more than one service user can provide preference information or service settings even if there is only one user account. In some embodiments, there are multiple service subscribers each providing preferences. In some embodiments, as similarly described with respect to various device embodiments, user preferences can be used set service control policies that provide the user with their selected balance of cost and service capability in a manner that meets network neutrality requirements. Similarly, in some embodiments, the service monitoring and customer resource management information collected on the intermediate networking device or end point devices can be filtered according to user privacy preferences to maintain the level of user privacy selected by the user.

[0516] Adaptive intermediate networking device policy implementation can also be performed in the intermediate networking device service processor 115 embodiments, as similarly described with respect to various device embodiments. In some embodiments, the

service policy implementation for the intermediate networking device can be adapted by the service processor 115 agents (e.g., policy control agent 1692 working to control the settings in policy implementation agent 1690, and/or another service processor agent or function) to achieve a higher level service usage goal. In some embodiments, the usage goals or adaptation can be based on aggregate end point device usage for the intermediate networking device network services, and in some embodiments, the higher level usage goals or adaptation can apply to one or more individual end point devices.

[0517] In some embodiments, even though there is one intermediate networking device account, there can be multiple options for multi-end point device or multi-user operation in which the number of end point devices, number of users or service capabilities for some of the end point devices or users are selectable. These parameters are accommodated by an intermediate networking device service profile that includes the service capabilities that are to be delivered to a multitude of end point devices or users. In some cases, some end point devices or users have a different profile within the intermediate networking device service processor 115 with differentiated capabilities as compared to the intermediate networking device service processor 115 profile for other end point devices or users. This is the case for some of the examples provided herein. These multi-end point device or multi-user service profiles in the intermediate networking device service processor 115 can share services equally or can allow more capable access services to some end point devices or users than others. In some embodiments, a service profile implemented by the intermediate networking device service processor 115 for one end point device or user is different than that in the service profile implemented by the service processor 115 for another end point device or user (e.g., providing differentiated service profile implementations by end point devices and/or users). End point devices can be uniquely identified for purposes involving implementation of different service profiles in the intermediate networking device service processor 115 agents (e.g., depending on the embodiment, service monitor agent 1696, policy implementation agent 1690, policy control agent 1692, application interface agent 1693 and/or other service processor agents or functions) based on a number of parameters, such as IP address, local area network address (e.g., Wi-Fi address), MAC address end point device ID, user ID, and/or end point device application layer tag. This allows for independent service usage monitoring and control for different end point devices or users.

[0518] In some embodiments, an intermediate networking device also bridges services to end point devices or users that have individually managed service profiles, service plans or service accounts. As discussed herein, individual end point device service policy implementation and/or service profile implementation can be accomplished by classifying end point device service usage according to an end point device identifier so that service monitoring, control assistance and reporting may be differentiated between one or more end point devices. These end point device identifiers can then be associated with a different service plan or account in the service processor 115 and/or billing system 123. The end point device or user specific service usage monitoring, reporting, notification and control assistance can be accomplished by running one or more profiles for each end point device or each user.

[0519] It will now be apparent that billing can also be implemented with a single account encompassing service usage for all users or end point devices connected to an intermediate networking device, or for individual users, end point devices, user groups or end point device groups connected to an intermediate networking device. As similarly described with respect to the service profile, this is accomplished by associating service usage events and associated billing events with an end point device identifier, user identifier, end point device group identifier, and/or user group identifier.

[0520] In some embodiments, end point devices or users connect to more than one intermediate networking device with the same service account, service plan or service profile. In some embodiments, the intermediate networking device requires an authentication sequence for the end point device or user before allowing connection to the network through the intermediate networking device. This authentication sequence can involve the end point device communicating an active account or admission credential with the intermediate networking device. The intermediate networking device can compare the credential with a local database or may query a database in the network to admit the end point device to the intermediate networking device network connection. In either case, provided the user credential or network authorization process is passed, the service processor 115 service profile settings for the end point device are applied and service is then established as discussed herein. In these cases, the verification can be accomplished as described herein. In some embodiments, even if the end point device does not have a service processor 115, provided that the intermediate networking

device service policy implementations and/or service profile implementations are verified as described herein, then the intermediate networking device will accurately assist in control and reporting of service usage for the different end point devices or users, and the appropriate service policy controls and/or billing can be maintained.

[0521] In some embodiments, when the end point device attempts connection to the intermediate networking device, if the user or end point device does not already have an active account or logon credential that the intermediate networking device recognizes, then the intermediate networking device can offer the end point device or user a service sign up experience. This experience can be implemented in a number of ways, including a website, WAP site, portal, download of agent software, and other methods. For example, an automated recognition of new devices can redirect unauthorized end point devices to browse into a website, WAP site, or portal site located on the intermediate networking device or in the network. If the site is located on the intermediate networking device, it can be cached and refreshed at a time of day when the network is not overly busy. Once on the site, the user or end point device selects the plan choice they desire, inputs account information and, in some embodiments, downloads device agent software to aid in network service policy implementation and/or profile implementation with the intermediate networking device. Once the user signs up, the information is logged into the network data base, the service account is established and the intermediate networking device service profile for that user or end point device is activated and the user can begin using the service.

[0522] In some embodiments, a website, WAP site, or portal site located in the intermediate networking device can be used to provide the end point device user with a service usage monitor interface and a service purchase interface for cases in which the end point device does not posses any special software to allow it to display a more specialized service usage monitor function for information received from the intermediate networking device or network service usage counters. The service usage monitor for the intermediate networking device can be synchronized, as similarly described with respect to various device embodiments. In some embodiments, the service usage notification system can also display cost data from a usage to cost look-up function. In some embodiments, the service usage notification system can display projected service usage or projected cost, as similarly described with respect to various device

embodiments. The service usage monitor to drive these service notification embodiments can be located on one or more of the end point device, the intermediate networking device or the network.

[0523] In some embodiments, if multiple accounts are serviced by one or more intermediate networking devices, verification can be performed on the service controls for the end point device or user service usage. As will now be apparent, just as with the intermediate networking device, the end point device or user service usage comparison with usage policy settings can be verified in the ways described herein. If the usage is found to be out of policy, then any of the out of policy actions described herein can be performed, including, for example, notify the end user, notify and require acknowledgement, bill for overage, suspend, quarantine, SPAN, and/or flag to network manager or network error handling function. For example, the verification methods shown in and described with respect to FIGS. 22A, 22B, 23, 26A-26H, 27A-27P and 28A-28E can be applied for the embodiments where intermediate networking devices have multiple account, multiple service plan, multiple service profile, multiple end point device, and/or multiple user capabilities.

[0524] It will be apparent that the various embodiments described herein for automated provisioning and activation also can similarly be applied to the intermediate networking device embodiments. It will also be apparent that the various virtual service provider embodiments can similarly be applied to the intermediate networking device embodiments.

[0525] Ambient services can be employed on the intermediate networking device and the ambient services can thus be provided to the end point devices. It will be apparent that the ambient service profile embodiments disclosed herein can similarly be applied to the intermediate networking device, and then the intermediate networking device can supply those ambient services to end point devices connected to the intermediate networking device. It will also be apparent that the intermediate networking device can provide an ambient service profile as described herein to end point devices or users that have not yet signed up for service, while providing other paid for service profiles to end point devices or users that have signed up for service.

[0526] Bill by account embodiments can similarly be applied to the intermediate networking device embodiments. For example, bill by account can be used in embodiments in which all end point devices or users are connected to the intermediate networking device under one account, or to embodiments in which some end point devices or users are accounted for separately with different service accounts, service plans or service profiles. In either case, it will be apparent that using one or more of the end point device or user identification credential aspects discussed herein can be used in a bill by account profile to account for any end point device or service activity. In such embodiments, billing event reports for those activities that include the end point device or user identifiers can also be provided for billing mediation and reconciliation down to the individual end point device or user level. For example, this allows for very deep service monitoring and billing capabilities with intermediate networking devices.

[0527] The intermediate networking device embodiments described above also have uses in machine to machine applications. It will be apparent that if the end point device includes the correct credentials to gain access to an existing account, or to allow an automated provisioning and activation account to be established, then the end point device can be connected to the network through the intermediate networking device without human intervention. Furthermore, the service profile that is established with the end point device for machine to machine communications can be set up to provide the access required to support the machine to machine application allowing for low cost access services and preventing the end point device from being misused for some service other than that intended. For example, the verification techniques and embodiments disclosed herein can similarly be applied to such machine to machine applications.

[0528] It will be apparent that the identifiers discussed above for bill by account mediation with accounting down to the individual end point device or user level can be combined with a billing mediation server in the network that accepts intermediate networking device billing events with end point device identification or user identification indexed billing, performs the necessary bill by account mediation functions, formats the billing events into the format used by the billing system, and transmits the mediated billing information to the billing system 123.

[0529] In some embodiments, the intermediate networking device service processor 115 functionality can be split. The division ranges from some or all of the service processor 115 on the device to some or all of the service processor 115 on the intermediate networking device.

[0530] In some embodiments, all of the service processor 115 is on the intermediate networking device. The end point device does not participate in service processor 115 functions and has no service processor 115 interface software. In some embodiments, the end point device has small subset of service processor 115 capabilities, including, for example, a service notification UI or a logon client with credentials. In some embodiments, service monitoring is implemented on the end point device or on both the end point device and in the intermediate networking device. In some embodiments, the end point device has additional service processor 115 capabilities including, for example, application layer tagging that associates application layer activity with service processor 115 service monitoring or service policy implementation and/or service profile implementation information. This can be accomplished by a range of techniques, for example, transmitting the application tagging information disclosed elsewhere to the intermediate networking device service processor 115 so that the policy implementation may be accomplished with knowledge of the application layer information. Another example involves assigning IP addresses in the intermediate networking device networking stack to the end point devices so that different types of end point device traffic can be routed into service processor 115 traffic shaping queues, each queue having a policy profile implementation engine, and application layer tagging information or similar traffic identifying information is used to determine which policy implementation engine the traffic should be routed to in order to accomplish the desired traffic shaping for the traffic type, application type, service type, and/or content type. In some embodiments, the traffic control policy is implemented on the end point device either with an application layer traffic controller, or by implementing more of the service processor 115 functionality, as similarly described with respect to various device embodiments. In the end point device service functionality example, most or all of the service processor 115 functionality is implemented on the end point device and the intermediate networking device functionality can be reduced to a bridging, forwarding or routing function between the end point devices and the network that performs little or no service control, monitoring and/or billing functions. For example, the service usage monitoring agents can also be provided on the end point device to aid in verification.

[0531] In embodiments in which the end point device requires agent software, the software can be loaded at time of manufacture or during distribution, loaded later, and/or made available for download through the intermediate networking device. In the case in which the end point device agent SW is downloaded through the end point device, there can be locally cached copies of the SW for one or more OS variants stored in a cache on the intermediate networking device, with the cache being updated over the network at convenient or conducive times, or the software can be downloaded live over the network when it is needed by the end point device. Logging the service usage to download this software is another example in which bill by account functionality can be used to track network traffic that may not be desirable to bill to an end point device owner or user, and bill by account functionality can be used to log and mediate such usage out of the user or end point device owner's bill.

[0532] Any end point device agent software required to connect to the intermediate networking device can also be implemented as a service processor 115 developer's kit as described herein and distributed to aid manufacturers, service provider and virtual service providers in bringing new devices onto networks with intermediate networking device capability.

[0533] In the case of a femto cell intermediate networking device, in some embodiments, it is desirable to facilitate handover from the WWAN network to the femto cell. In some embodiments, this provided in the intermediate networking device service processor 115 in a variety of ways. In some embodiments, the voice and data traffic is routed through a VPN tunnel controlled by the service processor 115 and connected to a network element, such as the transport gateway or another specified traffic concentration destination for the femto cell. In some embodiments, the voice traffic, the data traffic or both can be routed in secure or open Internet channels to different destinations, or the data can be routed directly to the Internet destination specified by the packets. In some embodiments, the femto cell intermediate networking device controls the femto cell frequencies or local frequency channel strength surveys over the intermediate networking device control channel. In some embodiments, the service processor 115 has a VPN connection to a network base station hand off controller to assist in handoff to and from the WWAN network and/or has the capability to instruct the end point device and the base station handoff controller. In some embodiment, whenever an end point device authenticated for femto cell access is within range of the femto cell, the service

provider desires to set up a service processor 115 profile to get the end point device to connect to the femto cell even if it has a strong signal with one or more WWAN base stations so that the WWAN traffic may be offloaded. In some embodiments, the service processor 115 can form a secure control plane link with network AAA functions to manage authorization and admission of end point devices the femto cell has not yet admitted, or the network policies can require re-authorization every time a end point device attempts access. Once an end point device is connected to the femto cell intermediate networking device, the verifiable traffic monitoring, control and billing functions described herein can be applied to various application embodiments. For example, the intermediate networking device service policy verification techniques disclosed herein, as similarly described with respect to various device embodiments, can similarly be applied to the femto cell intermediate networking device embodiments.

[0534] In some embodiments, the service provider desires to keep the number of end point devices or users that access an intermediate networking device below a certain count specified in the service processor 115 profile. In some embodiments, this is accomplished by controlling the number of IP addresses allowed onto the intermediate networking device local area side connection. In some embodiments, this is facilitated by observing the end point device identification parameters available in the end point device traffic. In some embodiments, this is facilitated by observing the traffic patterns to determine the likely number of devices connecting to the network. For example, traffic demand patterns can be examined to determine how many users are likely to be demanding access at one time. Although the foregoing embodiments have been described in some detail for purposes of clarity of understanding, the invention is not limited to the details provided. There are many alternative ways of implementing the invention. The disclosed embodiments are illustrative and not restrictive.

WHAT IS CLAIMED IS:

1. A system, comprising:

a processor of a communications device configured to:

store a first set of device credentials for activating the communications device for a first service on a first network; and

send an access request to the first network, the access request including the first set of device credentials; and

a memory of the communications device coupled to the processor and configured to provide the processor with instructions.

ABSTRACT OF THE DISCLOSURE

Various embodiments are disclosed for a services policy communication system and method. In some embodiments, a communications device stores a set of device credentials for activating the communications device for a service on a network; and sends an access request to the network, the access request including the set of device credentials.

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	AUTOMATED DEVICE PROVISIONING AND ACTIVATION

As the below named inventor, I hereby declare that:

This declaration is directed to:

- [■] The attached application, or
- [ ] United States application or PCT international application number _____

filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Gregory G. Raleigh Date (Optional) : _____

Signature: _____

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

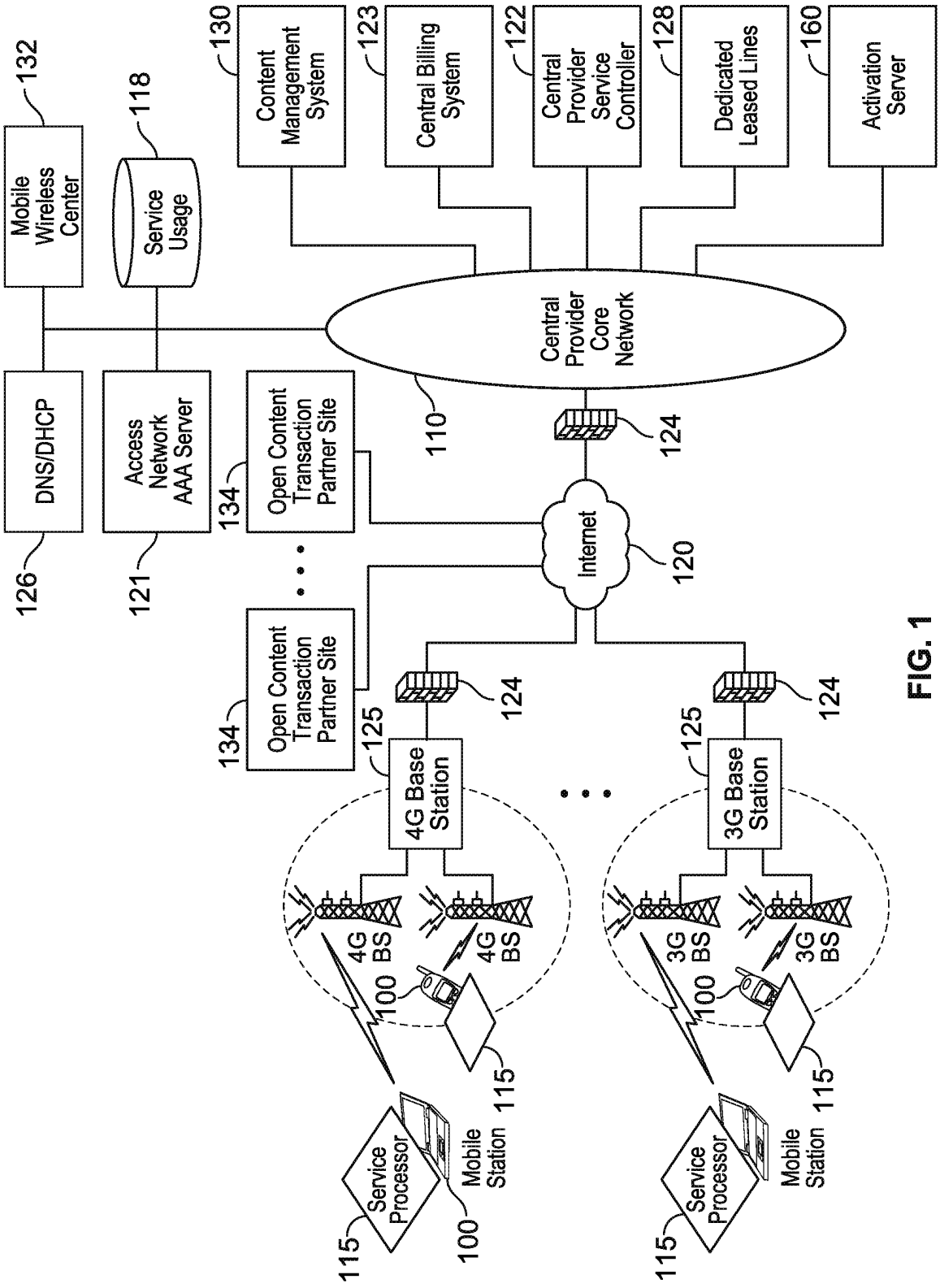

Mobile Wireless Center
132
Service Usage
118
Content Management System
130
Central Billing System
123
Central Provider Service Controller
122
Dedicated Leased Lines
128
Activation Server
160
DNS/DHCP
126
Access Network AAA Server
121
Open Content Transaction Partner Site
134
Central Provider Core Network
110
124
Internet
120
Open Content Transaction Partner Site
134
125
4G Base Station
124
125
3G Base Station
124
4G BS
4G BS
3G BS
3G BS
100
115
Service Processor
Mobile Station
115
100

FIG. 1

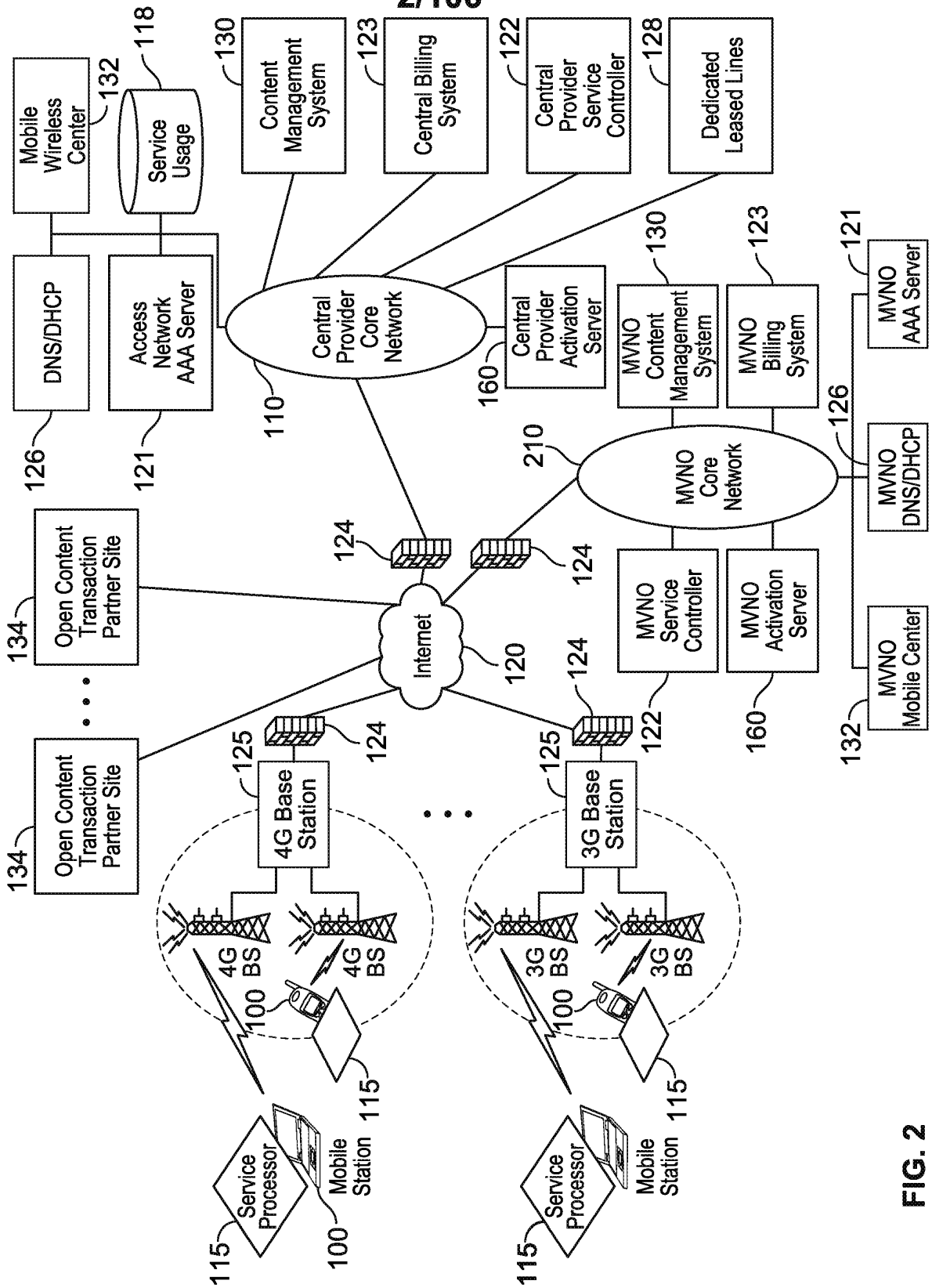

Mobile Wireless Center
132
Service Usage
118
Content Management System
130
Central Billing System
123
Central Provider Service Controller
122
Dedicated Leased Lines
128
DNS/DHCP
126
Access Network AAA Server
121
Central Provider Core Network
110
Central Provider Activation Server
160
MVNO Content Management System
130
MVNO Billing System
123
MVNO AAA Server
121
MVNO Core Network
210
MVNO DNS/DHCP
126
Open Content Transaction Partner Site
134
Internet
120
124
MVNO Service Controller
122
MVNO Activation Server
160
MVNO Mobile Center
132
4G Base Station
125
3G Base Station
125
4G BS
3G BS
100
115
Service Processor
Mobile Station

FIG. 2

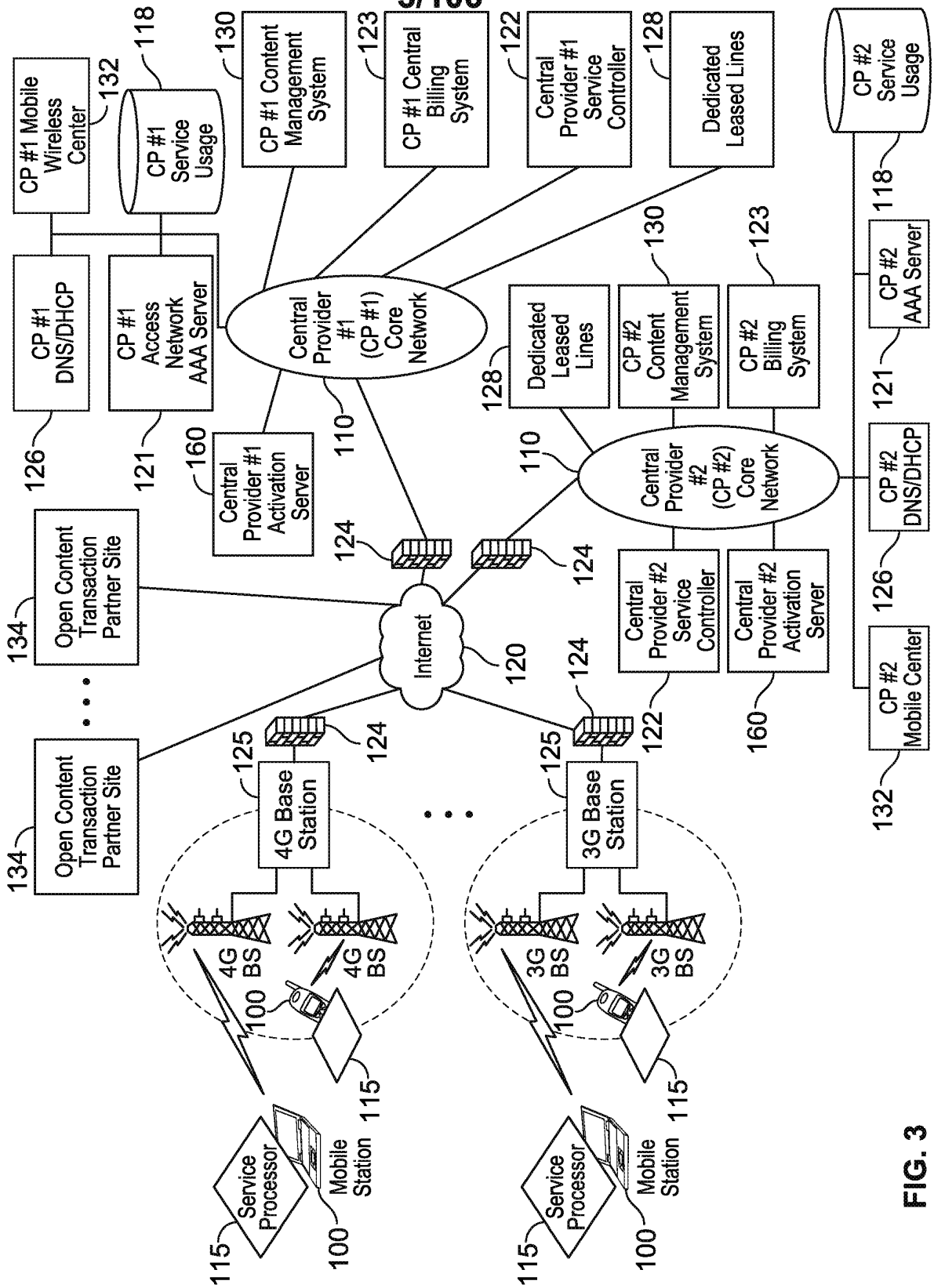

CP #1 Mobile Wireless Center
132
CP #1 Service Usage
118
CP #1 Content Management System
130
CP #1 Central Billing System
123
Central Provider #1 Service Controller
122
Dedicated Leased Lines
128
CP #2 Service Usage
CP #1 DNS/DHCP
126
CP #1 Access Network AAA Server
121
Central Provider #1 Activation Server
160
Central Provider #1 (CP #1) Core Network
110
Dedicated Leased Lines
128
CP #2 Content Management System
130
CP #2 Billing System
123
CP #2 AAA Server
118
121
Central Provider #2 (CP #2) Core Network
110
CP #2 DNS/DHCP
126
Central Provider #2 Service Controller
122
Central Provider #2 Activation Server
160
CP #2 Mobile Center
132
Open Content Transaction Partner Site
134
Internet
120
124
4G Base Station
125
3G Base Station
125
4G BS
3G BS
100
115
Service Processor
Mobile Station

FIG. 3

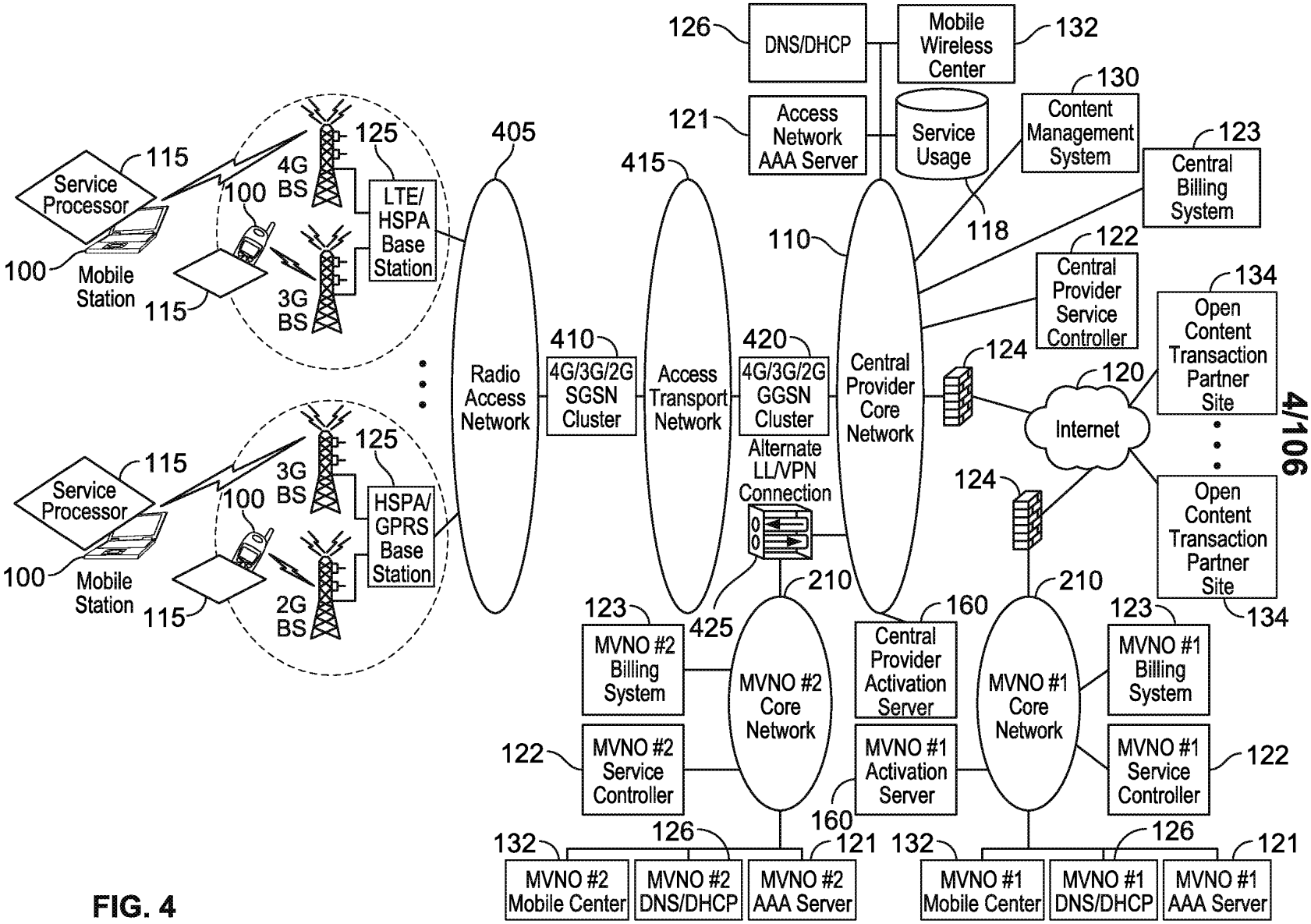

126
DNS/DHCP
Mobile Wireless Center
132
130
Content Management System
121
Access Network AAA Server
Service Usage
118
123
Central Billing System
405
415
110
122
Central Provider Service Controller
134
Open Content Transaction Partner Site
115
Service Processor
100
Mobile Station
100
115
4G BS
125
LTE/ HSPA Base Station
3G BS
Radio Access Network
410
4G/3G/2G SGSN Cluster
Access Transport Network
420
4G/3G/2G GGSN Cluster
Alternate LL/VPN Connection
Central Provider Core Network
124
120
Internet
4/106
Service Processor
100
Mobile Station
115
100
115
3G BS
125
HSPA/ GPRS Base Station
2G BS
425
210
160
123
MVNO #2 Billing System
MVNO #2 Core Network
Central Provider Activation Server
MVNO #1 Core Network
MVNO #1 Billing System
122
MVNO #2 Service Controller
MVNO #1 Activation Server
MVNO #1 Service Controller
132
126
121
MVNO #2 Mobile Center
MVNO #2 DNS/DHCP
MVNO #2 AAA Server
MVNO #1 Mobile Center
MVNO #1 DNS/DHCP
MVNO #1 AAA Server

FIG. 4

949

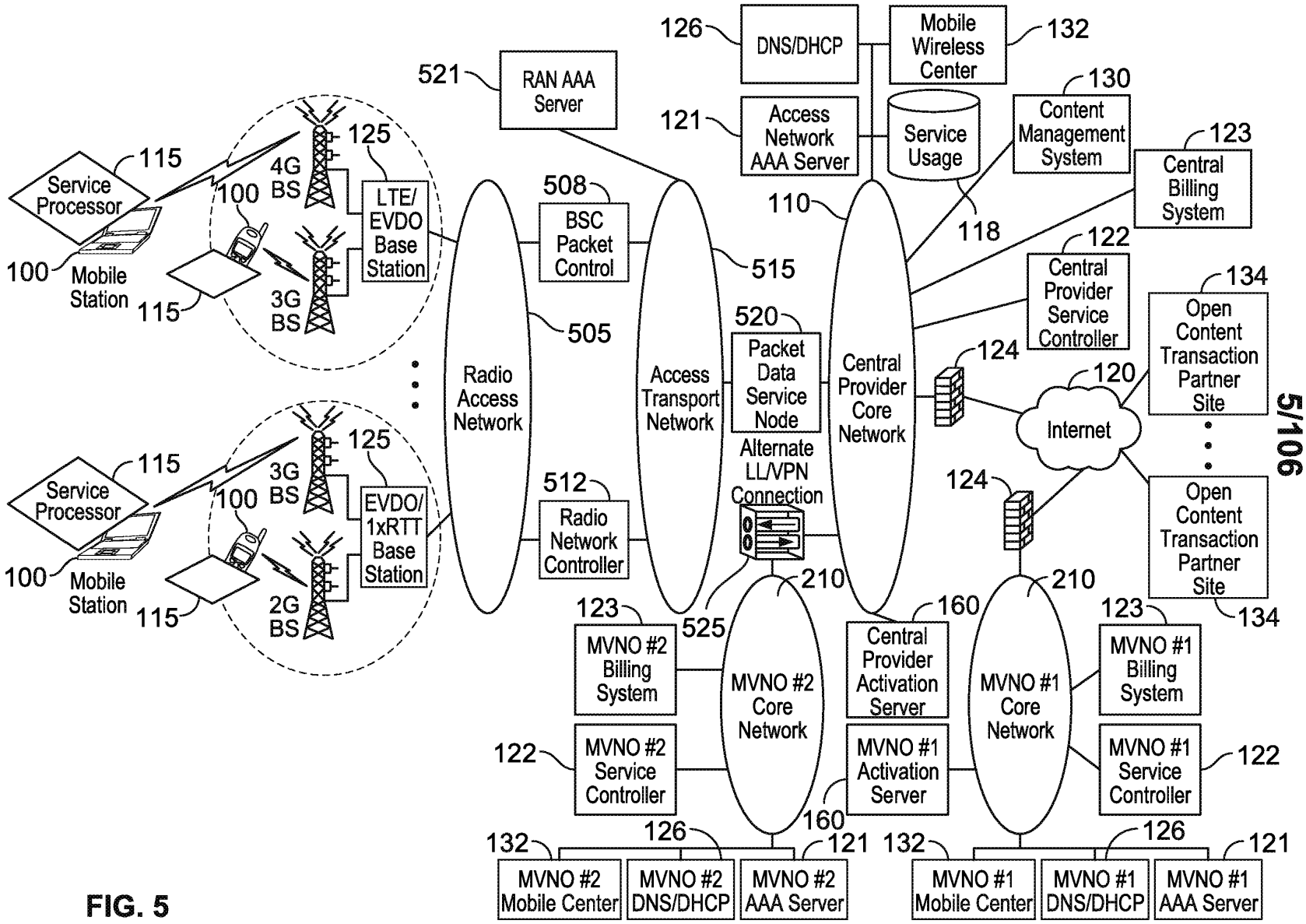

950
Service Processor
100
Mobile Station
115
4G BS
3G BS
125
LTE/ EVDO Base Station
100
115
Service Processor
100
Mobile Station
115
3G BS
2G BS
125
EVDO/ 1xRTT Base Station
Radio Access Network
521
RAN AAA Server
508
BSC Packet Control
505
512
Radio Network Controller
126
DNS/DHCP
121
Access Network AAA Server
Mobile Wireless Center
132
Service Usage
118
130
Content Management System
123
Central Billing System
110
515
Access Transport Network
520
Packet Data Service Node
Alternate LL/VPN Connection
525
122
Central Provider Service Controller
134
Open Content Transaction Partner Site
124
120
Internet
Central Provider Core Network
124
Open Content Transaction Partner Site
134
210
210
123
MVNO #2 Billing System
MVNO #2 Core Network
160
Central Provider Activation Server
MVNO #1 Core Network
123
MVNO #1 Billing System
122
MVNO #2 Service Controller
MVNO #1 Activation Server
160
MVNO #1 Service Controller
122
132
126
121
MVNO #2 Mobile Center
MVNO #2 DNS/DHCP
MVNO #2 AAA Server
132
126
121
MVNO #1 Mobile Center
MVNO #1 DNS/DHCP
MVNO #1 AAA Server
5/106

FIG. 5

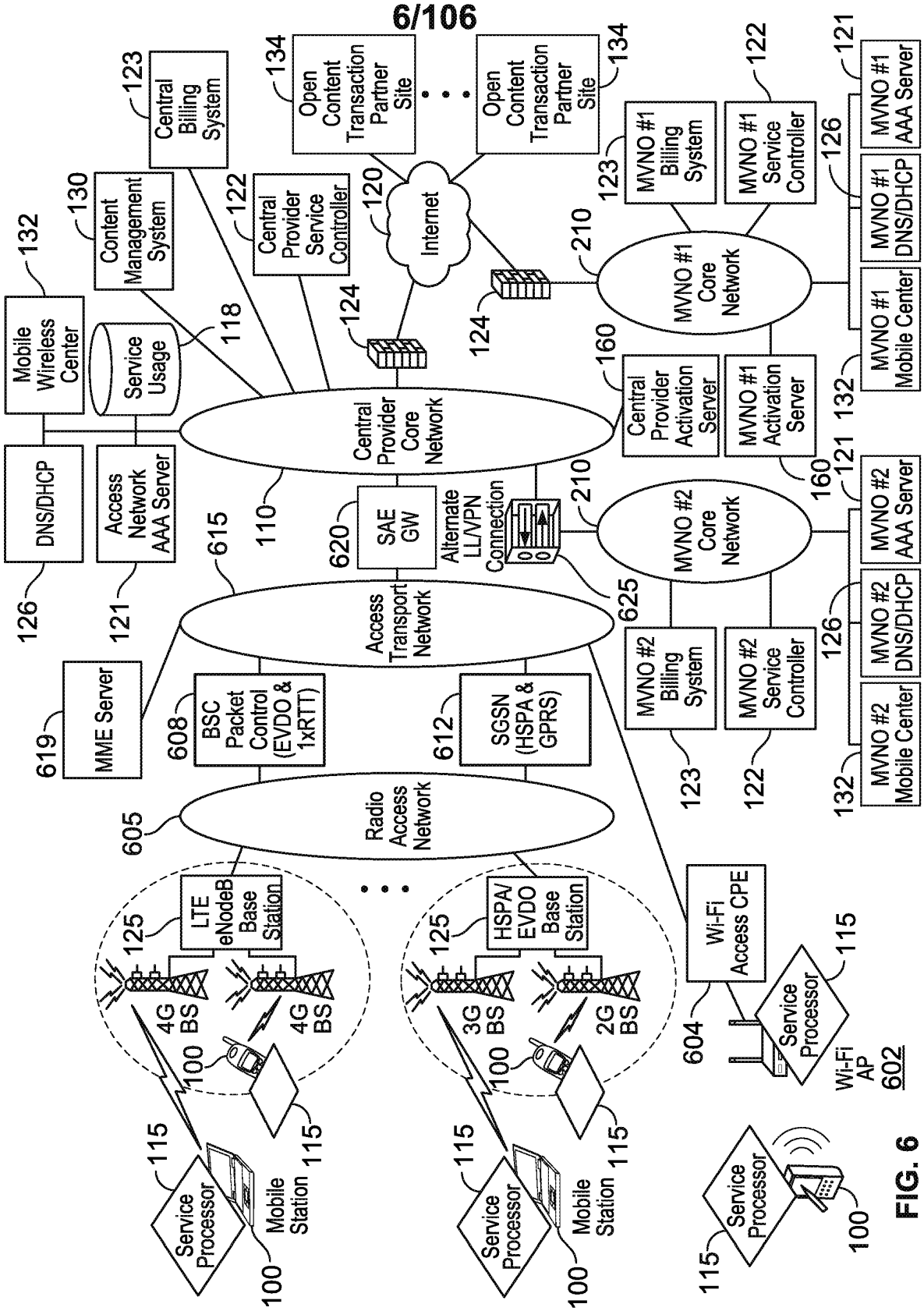

Mobile Wireless Center
132
Content Management System
130
Central Billing System
123
Open Content Transaction Partner Site
134
Open Content Transaction Partner Site
134
Central Provider Service Controller
122
Internet
120
Service Usage
118
DNS/DHCP
126
Access Network AAA Server
121
Central Provider Core Network
110
124
124
MVNO #1 Billing System
123
MVNO #1 Service Controller
122
MVNO #1 Core Network
210
MVNO #1 DNS/DHCP
126
MVNO #1 AAA Server
121
MVNO #1 Mobile Center
132
Central Provider Activation Server
160
MVNO #1 Activation Server
160
615
620
SAE GW
Alternate LL/VPN Connection
210
MVNO #2 Core Network
625
MVNO #2 AAA Server
121
MVNO #2 DNS/DHCP
126
MVNO #2 Mobile Center
132
MVNO #2 Billing System
123
MVNO #2 Service Controller
122
Access Transport Network
619
MME Server
608
BSC Packet Control (EVDO & 1xRTT)
612
SGSN (HSPA & GPRS)
605
Radio Access Network
125
LTE eNodeB Base Station
4G BS
4G BS
100
115
Service Processor
Mobile Station
125
HSPA/ EVDO Base Station
3G BS
2G BS
604
Wi-Fi Access CPE
Service Processor
115
Wi-Fi AP
602

FIG. 6

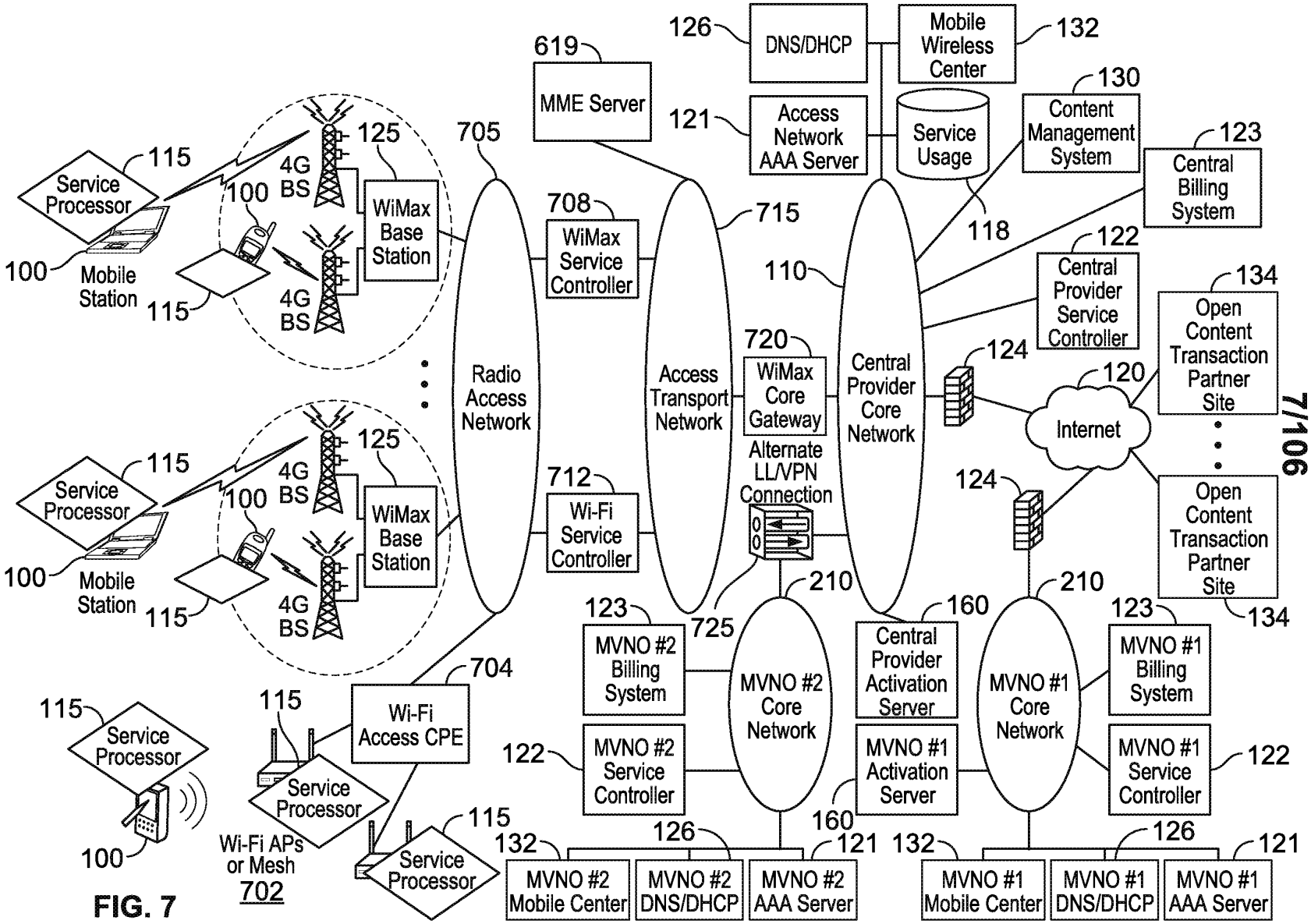


FIG. 7

7/106

952

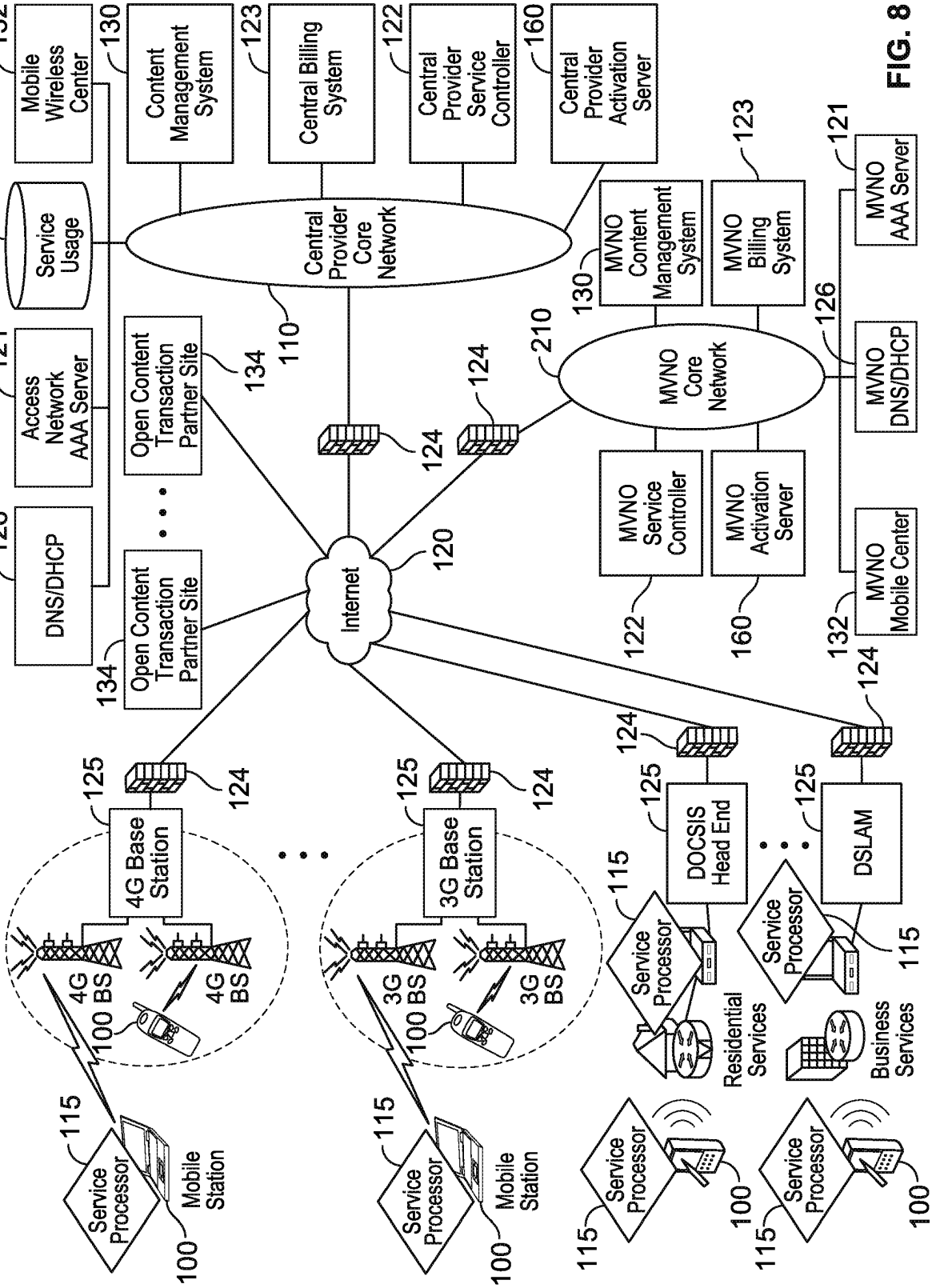

Mobile Wireless Center
132
Content Management System
130
Central Billing System
123
Central Provider Service Controller
122
Central Provider Activation Server
160
Service Usage
118
Central Provider Core Network
110
Access Network AAA Server
121
Open Content Transaction Partner Site
134
DNS/DHCP
126
Internet
120
MVNO Content Management System
130
MVNO Billing System
123
MVNO AAA Server
121
MVNO Core Network
210
MVNO DNS/DHCP
126
MVNO Service Controller
122
MVNO Activation Server
160
MVNO Mobile Center
132
4G Base Station
3G Base Station
DOCSIS Head End
DSLAM
125
124
4G BS
3G BS
100 BS
Service Processor
115
Mobile Station
100
Residential Services
Business Services

FIG. 8

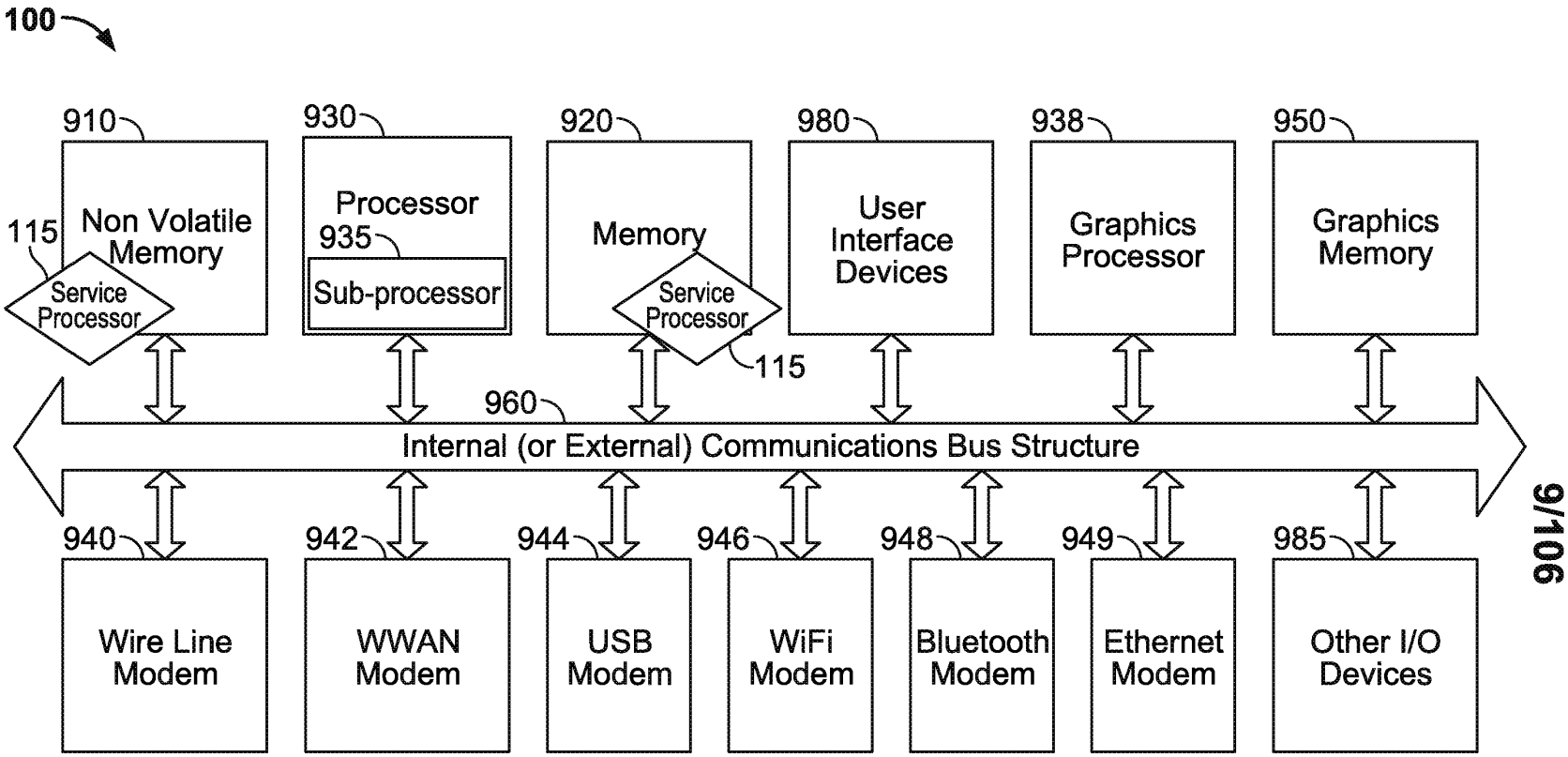

100
910
Non Volatile Memory
115
Service Processor
930
Processor
935
Sub-processor
920
Memory
Service Processor
115
980
User Interface Devices
938
Graphics Processor
950
Graphics Memory
960
Internal (or External) Communications Bus Structure
940
Wire Line Modem
942
WWAN Modem
944
USB Modem
946
WiFi Modem
948
Bluetooth Modem
949
Ethernet Modem
985
Other I/O Devices
954
9/106

FIG. 9

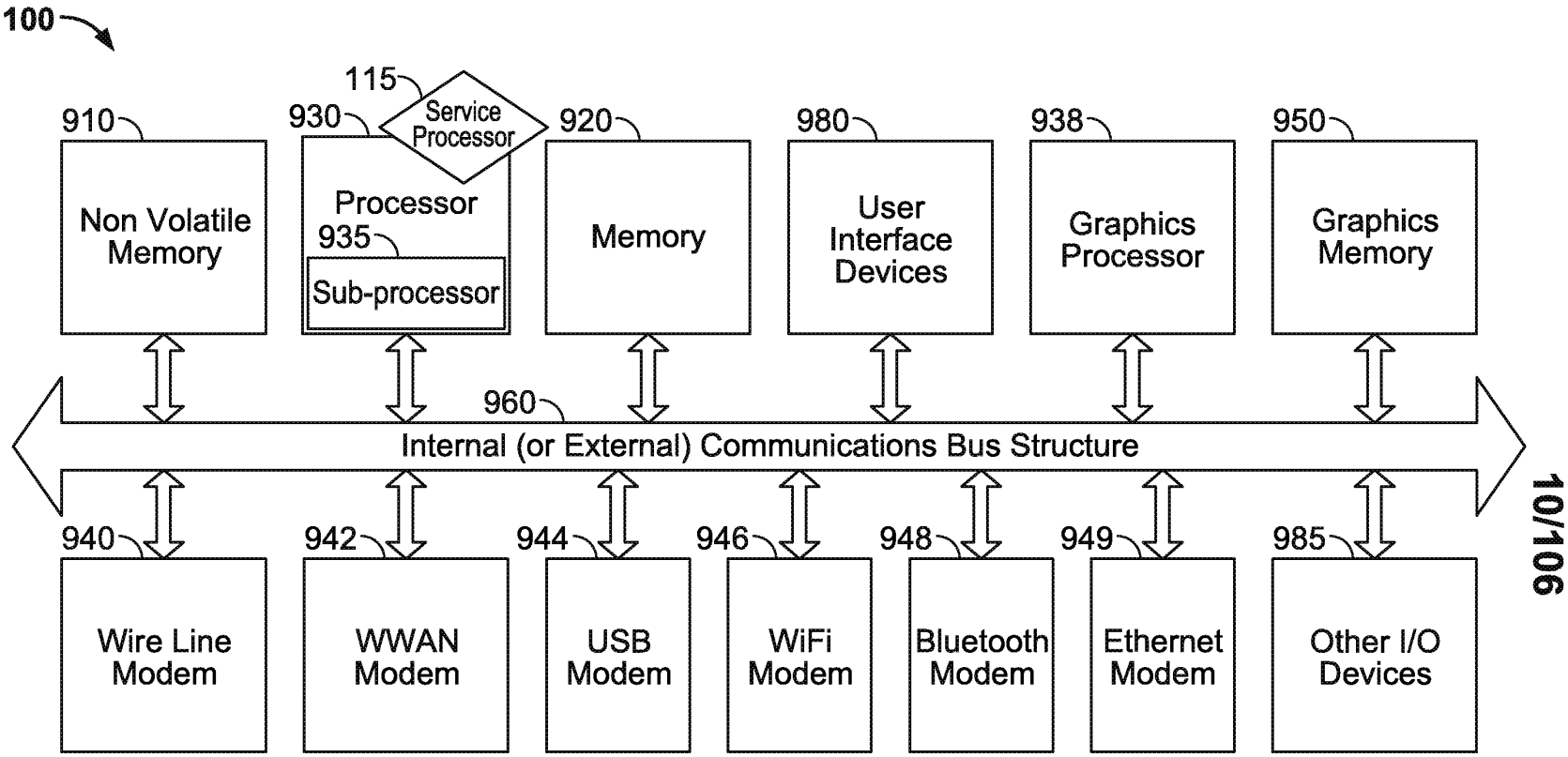

100
115
Service Processor
910
930
920
980
938
950
Non Volatile Memory
Processor
935
Sub-processor
Memory
User Interface Devices
Graphics Processor
Graphics Memory
960
Internal (or External) Communications Bus Structure
940
942
944
946
948
949
985
Wire Line Modem
WWAN Modem
USB Modem
WiFi Modem
Bluetooth Modem
Ethernet Modem
Other I/O Devices
955
10/106

FIG. 10

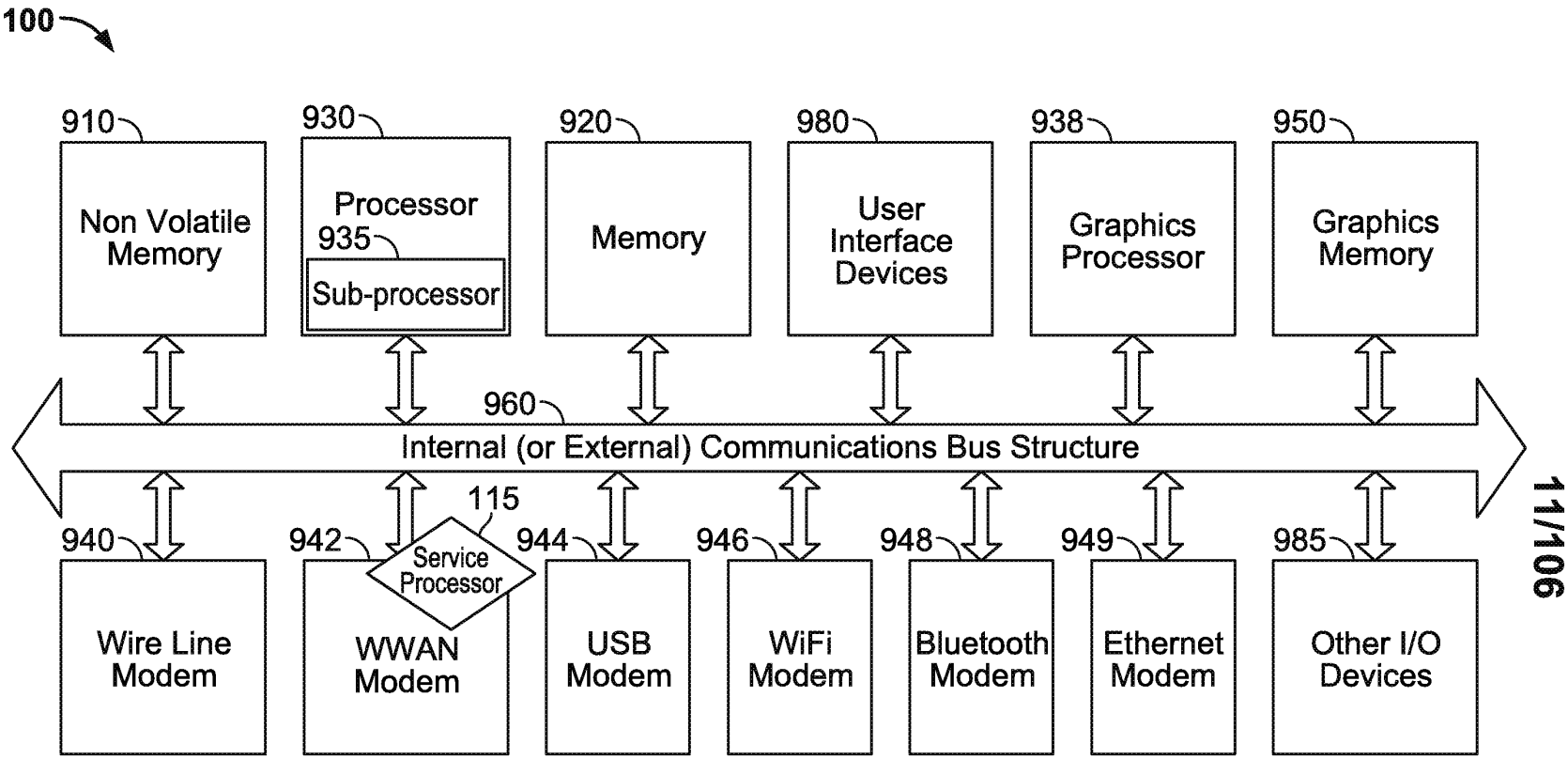

100
910
Non Volatile Memory
930
Processor
935
Sub-processor
920
Memory
980
User Interface Devices
938
Graphics Processor
950
Graphics Memory
960
Internal (or External) Communications Bus Structure
111/106
956
940
Wire Line Modem
942
115
Service Processor
WWAN Modem
944
USB Modem
946
WiFi Modem
948
Bluetooth Modem
949
Ethernet Modem
985
Other I/O Devices

FIG. 11

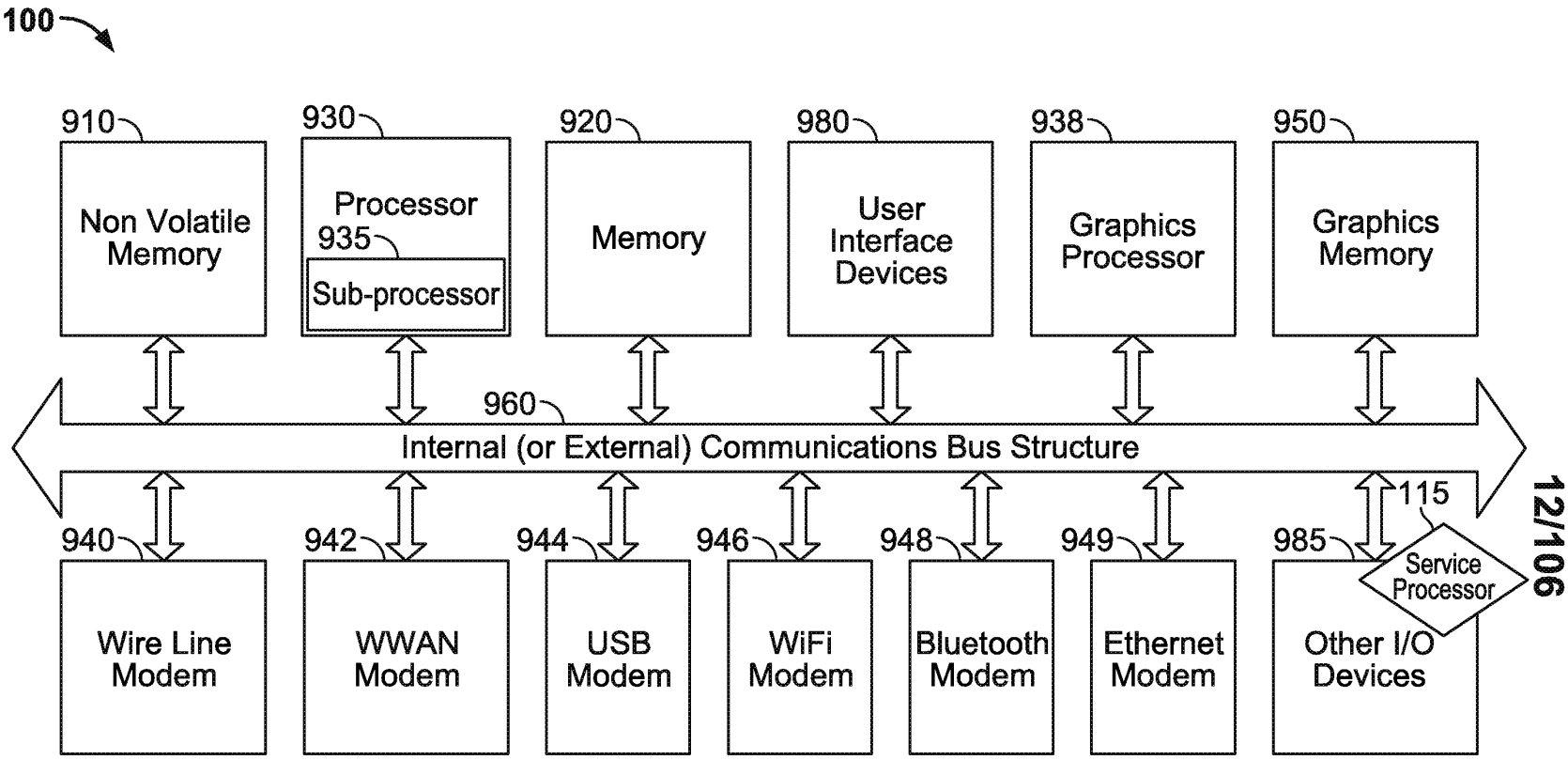

100
910
Non Volatile Memory
930
Processor
935
Sub-processor
920
Memory
980
User Interface Devices
938
Graphics Processor
950
Graphics Memory
960
Internal (or External) Communications Bus Structure
940
Wire Line Modem
942
WWAN Modem
944
USB Modem
946
WiFi Modem
948
Bluetooth Modem
949
Ethernet Modem
985
115
Service Processor
Other I/O Devices
957
12/106

FIG. 12

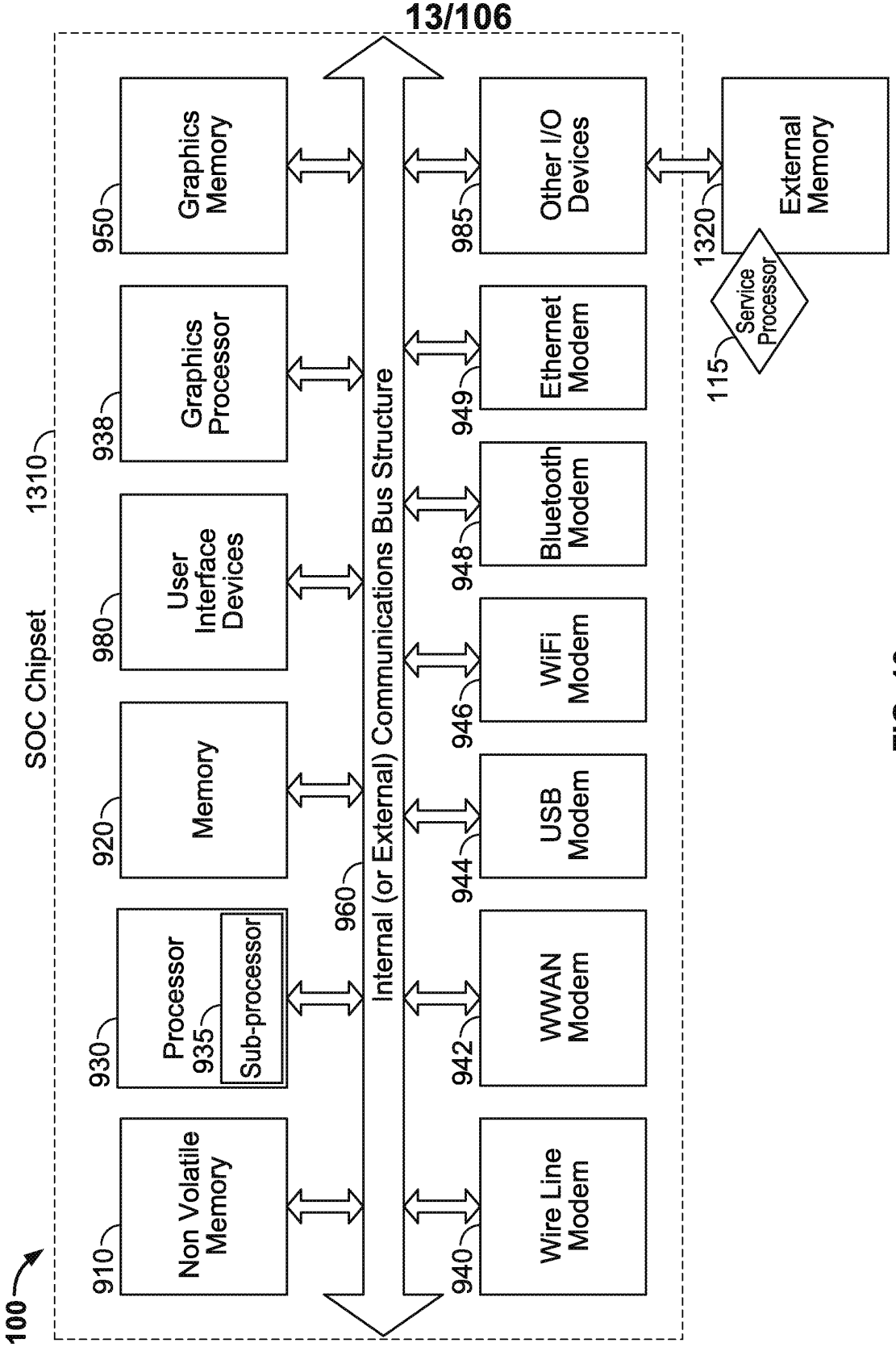

100
SOC Chipset
1310
910
Non Volatile Memory
930
Processor
935
Sub-processor
920
Memory
980
User Interface Devices
938
Graphics Processor
950
Graphics Memory
960
Internal (or External) Communications Bus Structure
940
Wire Line Modem
942
WWAN Modem
944
USB Modem
946
WiFi Modem
948
Bluetooth Modem
949
Ethernet Modem
985
Other I/O Devices
1320
External Memory
115
Service Processor

FIG. 13

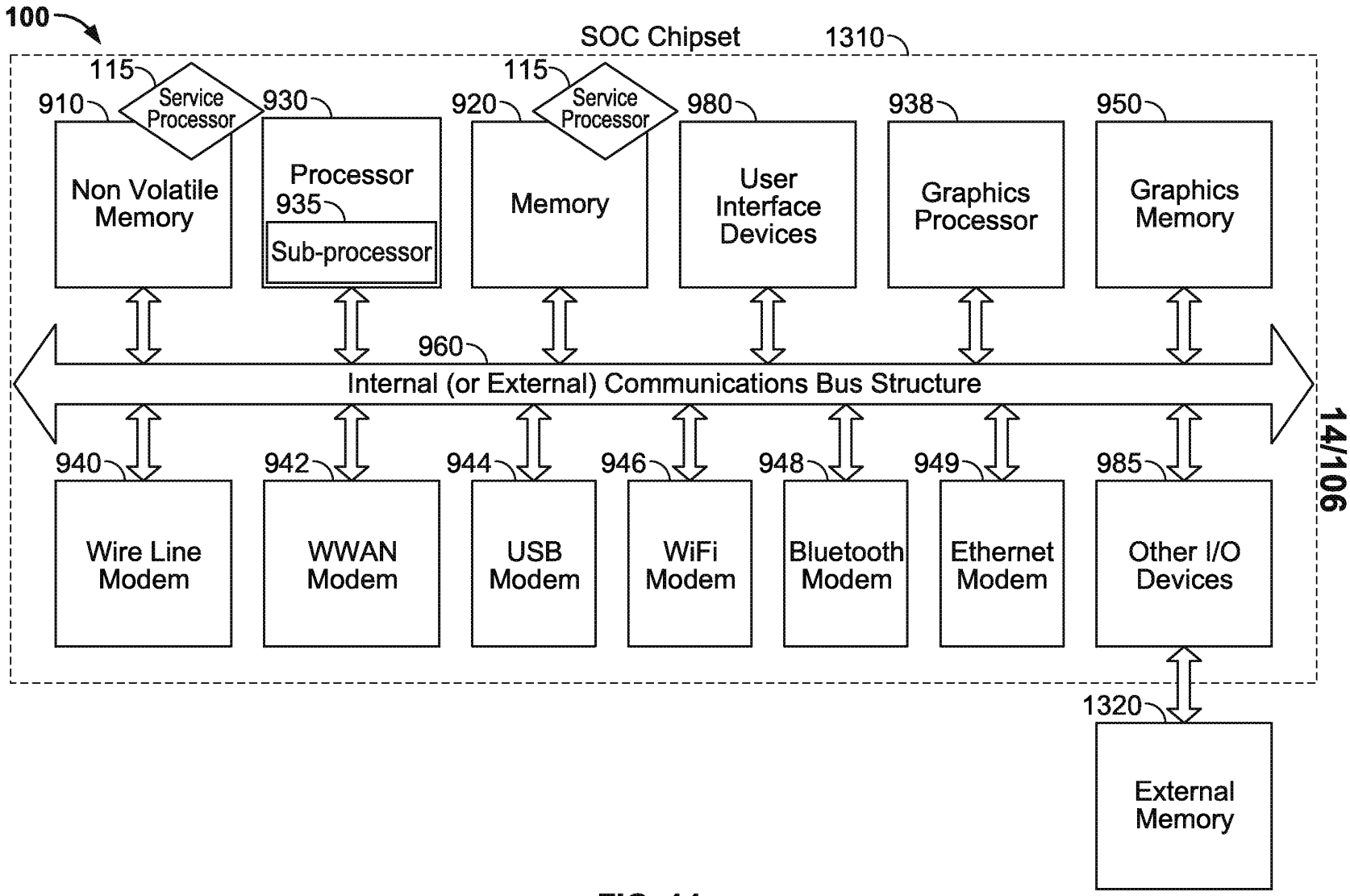

100
SOC Chipset
1310
115
Service Processor
910
Non Volatile Memory
930
Processor
935
Sub-processor
115
Service Processor
920
Memory
980
User Interface Devices
938
Graphics Processor
950
Graphics Memory
960
Internal (or External) Communications Bus Structure
940
Wire Line Modem
942
WWAN Modem
944
USB Modem
946
WiFi Modem
948
Bluetooth Modem
949
Ethernet Modem
985
Other I/O Devices
1320
External Memory
959
14/106

FIG. 14

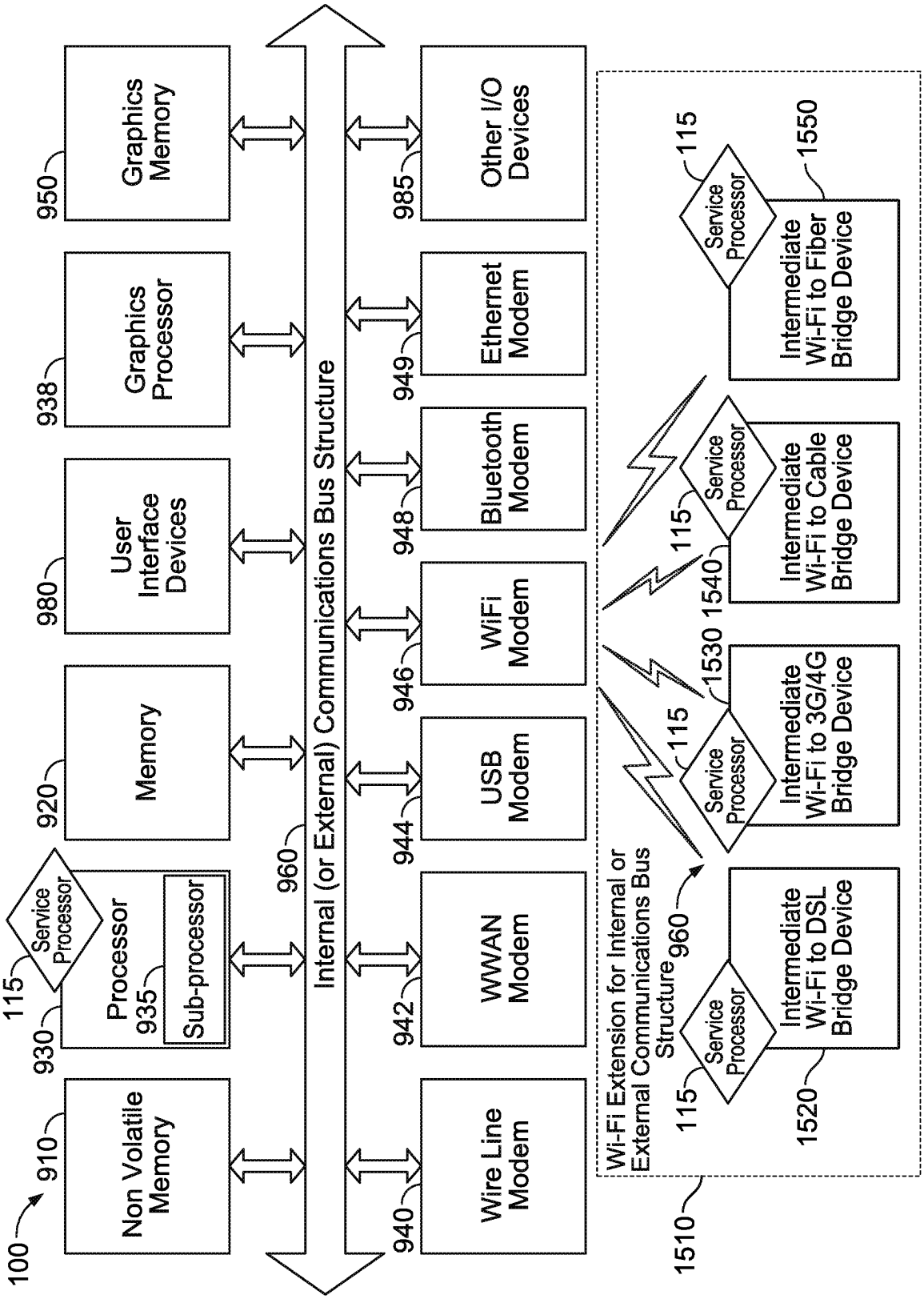

100
910
Non Volatile Memory
930
Processor
935
Sub-processor
115
Service Processor
920
Memory
980
User Interface Devices
938
Graphics Processor
950
Graphics Memory
960
Internal (or External) Communications Bus Structure
940
Wire Line Modem
942
WWAN Modem
944
USB Modem
946
WiFi Modem
948
Bluetooth Modem
949
Ethernet Modem
985
Other I/O Devices
1510
Wi-Fi Extension for Internal or External Communications Bus Structure
1520
Intermediate Wi-Fi to DSL Bridge Device
1530
Intermediate Wi-Fi to 3G/4G Bridge Device
1540
Intermediate Wi-Fi to Cable Bridge Device
1550
Intermediate Wi-Fi to Fiber Bridge Device

FIG. 15A

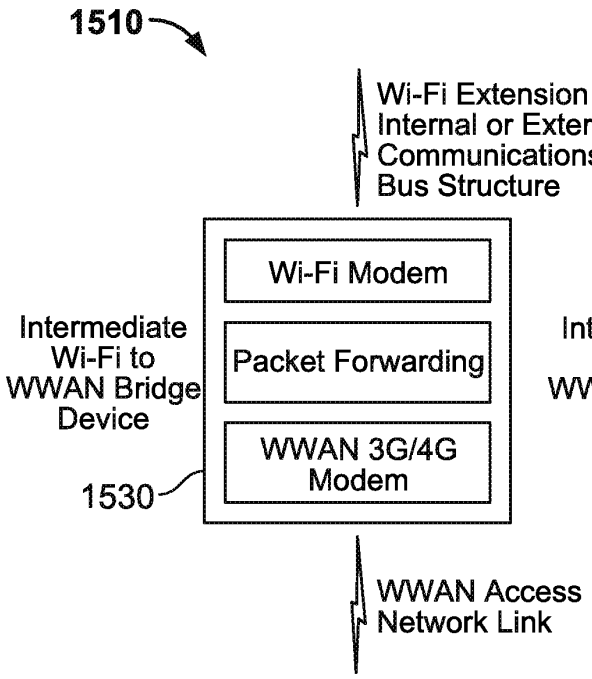


FIG. 15B

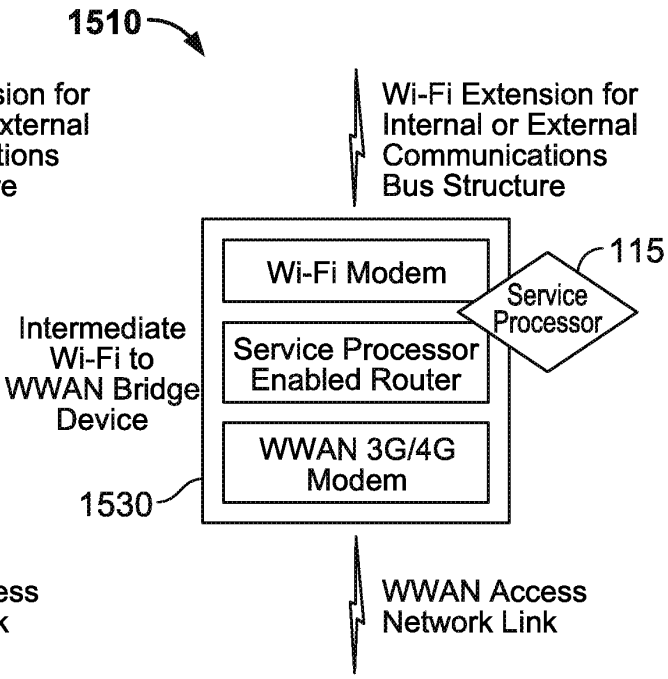


FIG. 15C

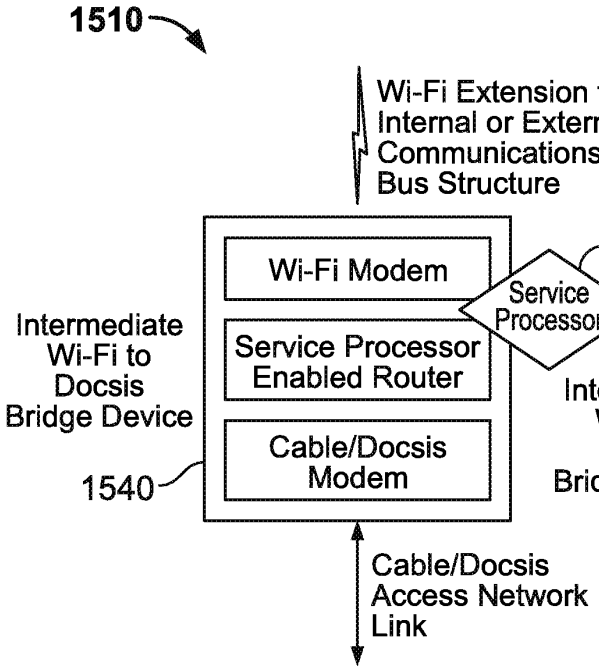


FIG. 15D

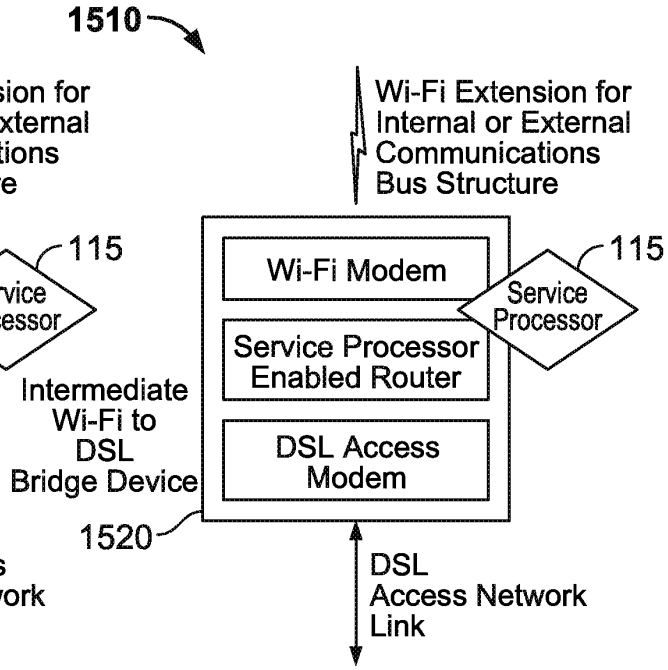


FIG. 15E

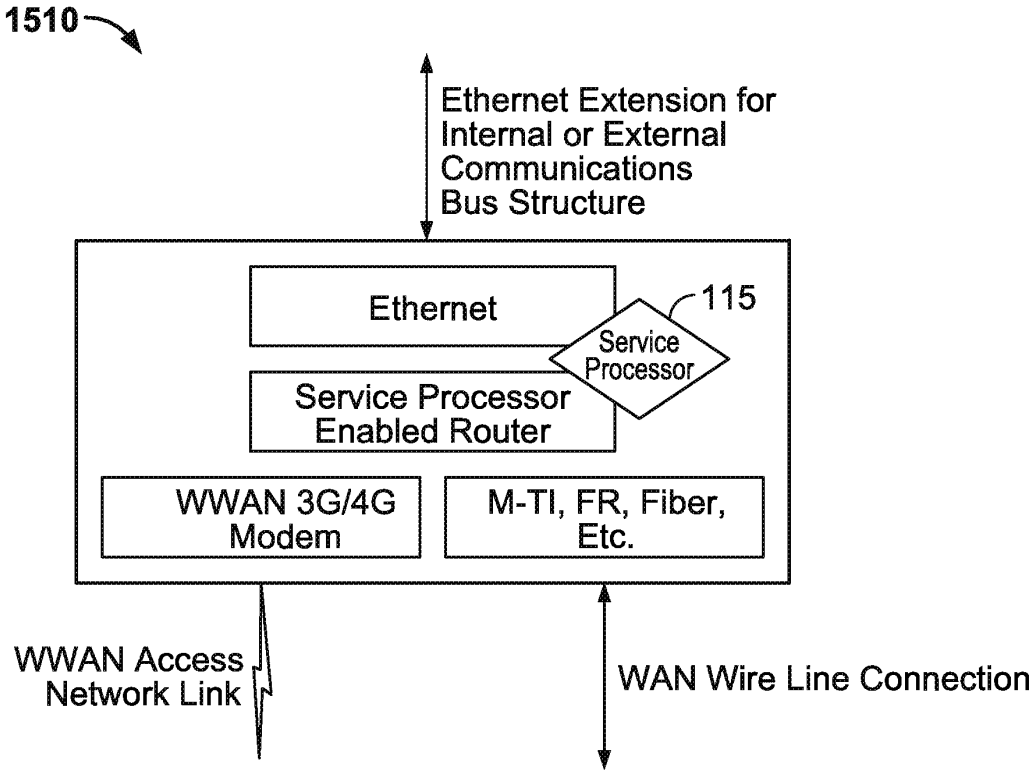

1510
Ethernet Extension for Internal or External Communications Bus Structure
Ethernet
115
Service Processor
Service Processor Enabled Router
WWAN 3G/4G Modem
M-TI, FR, Fiber, Etc.
WWAN Access Network Link
WAN Wire Line Connection

FIG. 15F

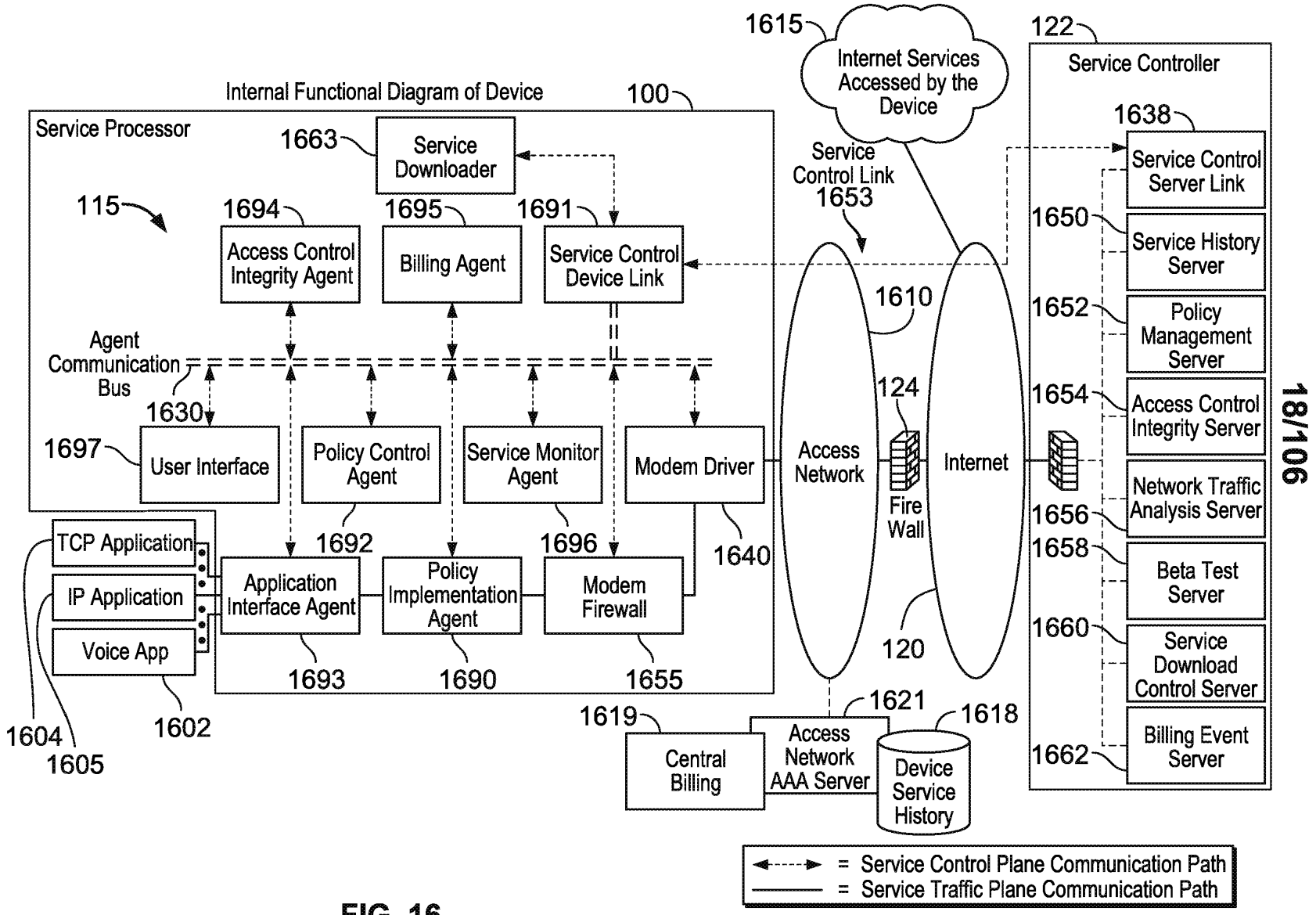

Internal Functional Diagram of Device
100
Service Processor
115
1663
Service Downloader
1694
Access Control Integrity Agent
1695
Billing Agent
1691
Service Control Device Link
Agent Communication Bus
1630
1697
User Interface
Policy Control Agent
1692
Service Monitor Agent
1696
Modem Driver
1640
TCP Application
IP Application
Voice App
1604
1605
1602
Application Interface Agent
1693
Policy Implementation Agent
1690
Modem Firewall
1655
1615
Internet Services Accessed by the Device
Service Control Link
1653
1610
Access Network
124
Fire Wall
Internet
120
122
Service Controller
1638
Service Control Server Link
1650
Service History Server
1652
Policy Management Server
1654
Access Control Integrity Server
Network Traffic Analysis Server
1656
1658
Beta Test Server
1660
Service Download Control Server
Billing Event Server
1662
1619
Central Billing
1621
Access Network AAA Server
1618
Device Service History
= Service Control Plane Communication Path
= Service Traffic Plane Communication Path

FIG. 16

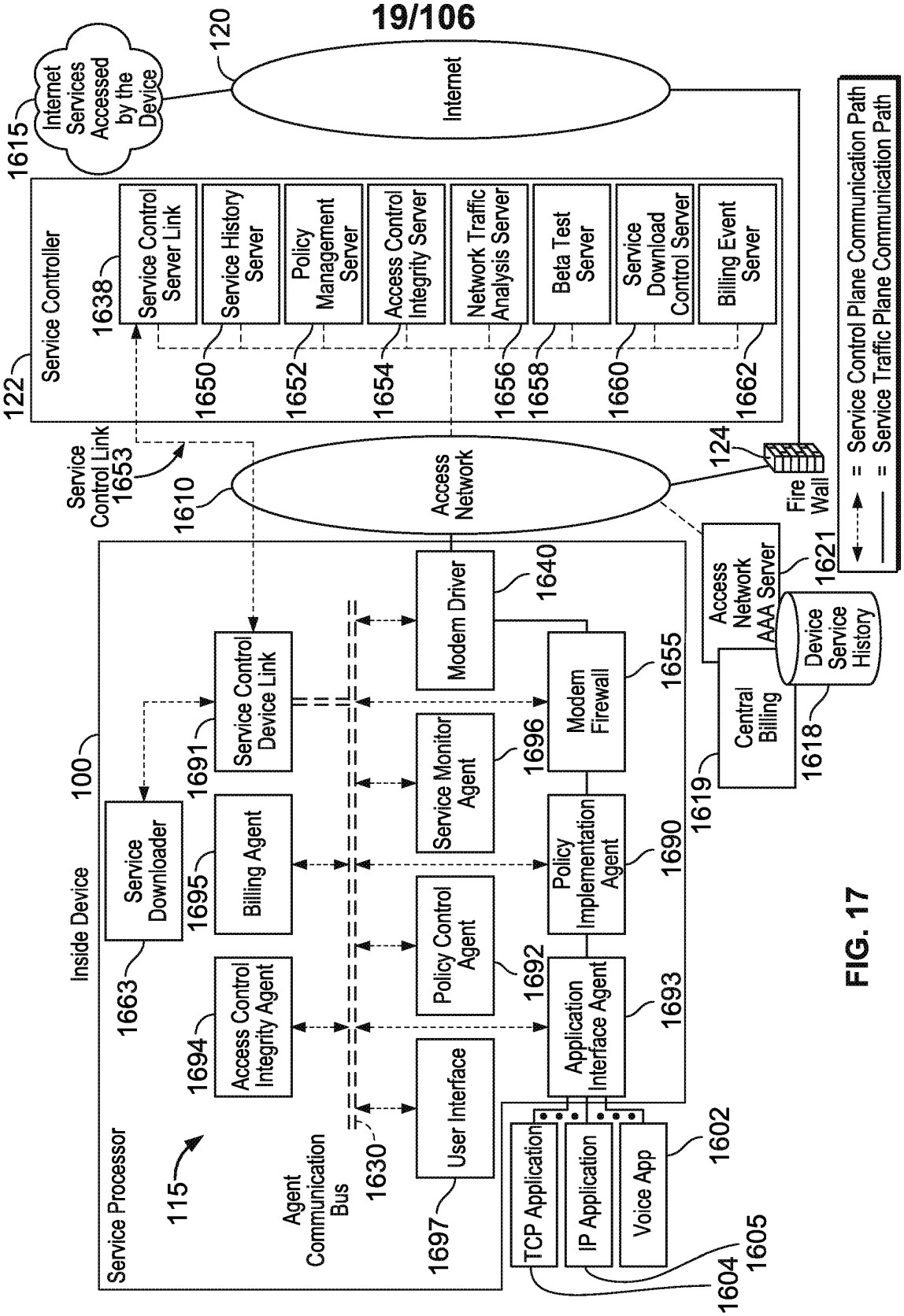

1615
Internet Services Accessed by the Device
120
Internet
122
Service Controller
1638
Service Control Server Link
Service History Server
Policy Management Server
Access Control Integrity Server
Network Traffic Analysis Server
Beta Test Server
Service Download Control Server
Billing Event Server
1650
1652
1654
1656
1658
1660
1662
Service Control Link
1653
1610
Access Network
124
Fire Wall
= Service Control Plane Communication Path
= Service Traffic Plane Communication Path
Inside Device
100
Service Processor
115
Service Downloader
1663
Billing Agent
1695
Access Control Integrity Agent
1694
Service Control Device Link
1691
Policy Control Agent
1692
Service Monitor Agent
1696
User Interface
1697
Agent Communication Bus
1630
Modem Driver
1640
Modem Firewall
1655
Policy Implementation Agent
1690
Application Interface Agent
1693
TCP Application
IP Application
Voice App
1602
1604
1605
1619
Central Billing
1618
Device Service History
Access Network AAA Server
1621

FIG. 17

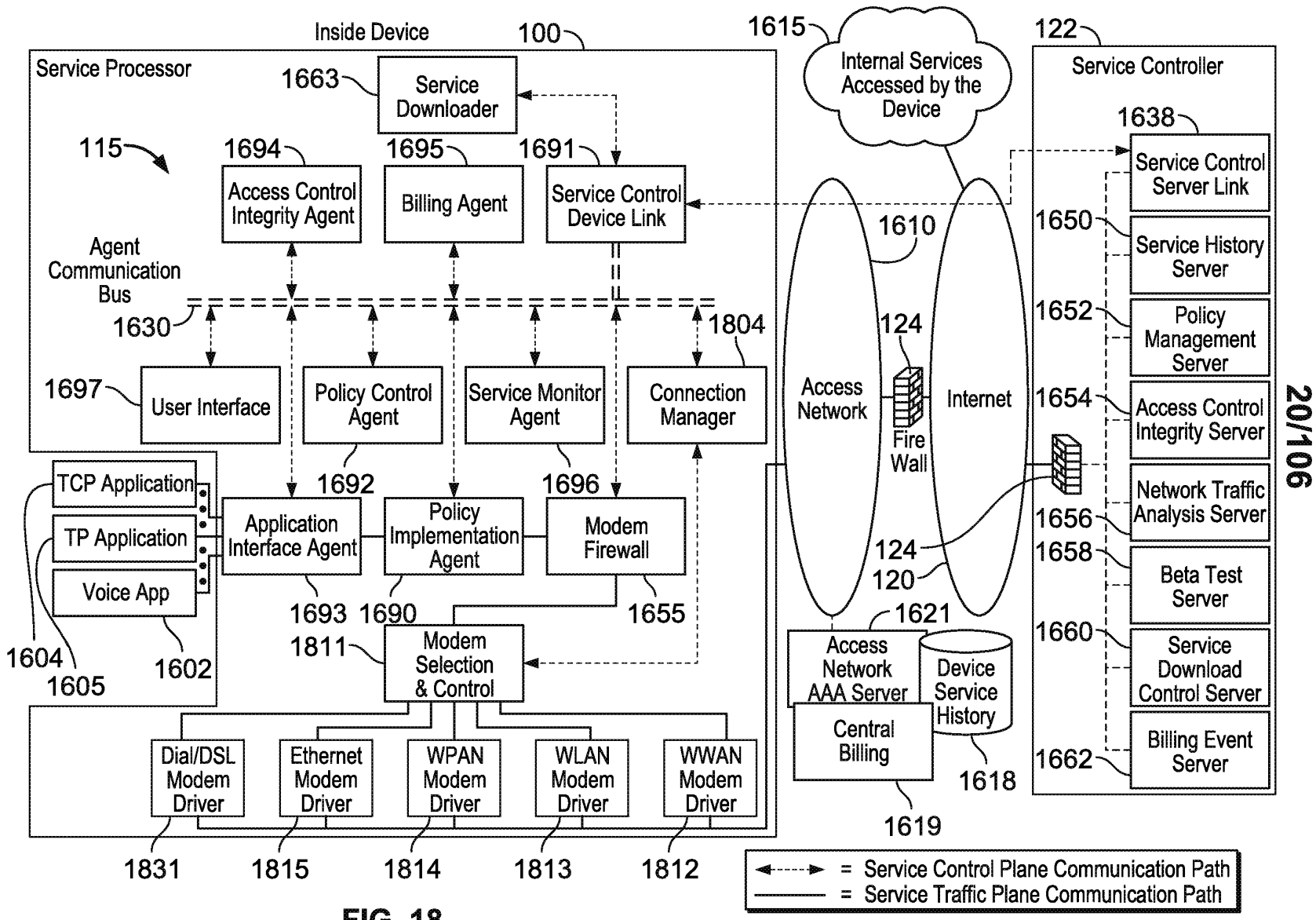

Inside Device
100
Service Processor
1663
Service Downloader
115
1694
Access Control Integrity Agent
1695
Billing Agent
1691
Service Control Device Link
Agent Communication Bus
1630
1804
1697
User Interface
Policy Control Agent
Service Monitor Agent
Connection Manager
TCP Application
TP Application
Voice App
1692
1696
Application Interface Agent
Policy Implementation Agent
Modem Firewall
1693
1690
1655
1604
1605
1602
1811
Modem Selection & Control
Dial/DSL Modem Driver
Ethernet Modem Driver
WPAN Modem Driver
WLAN Modem Driver
WWAN Modem Driver
1831
1815
1814
1813
1812
1615
Internal Services Accessed by the Device
1610
124
Access Network
Fire Wall
Internet
124
120
1621
Access Network AAA Server
Device Service History
Central Billing
1618
1619
122
Service Controller
1638
Service Control Server Link
1650
Service History Server
1652
Policy Management Server
1654
Access Control Integrity Server
Network Traffic Analysis Server
1656
1658
Beta Test Server
1660
Service Download Control Server
Billing Event Server
1662
= Service Control Plane Communication Path
= Service Traffic Plane Communication Path

FIG. 18

965

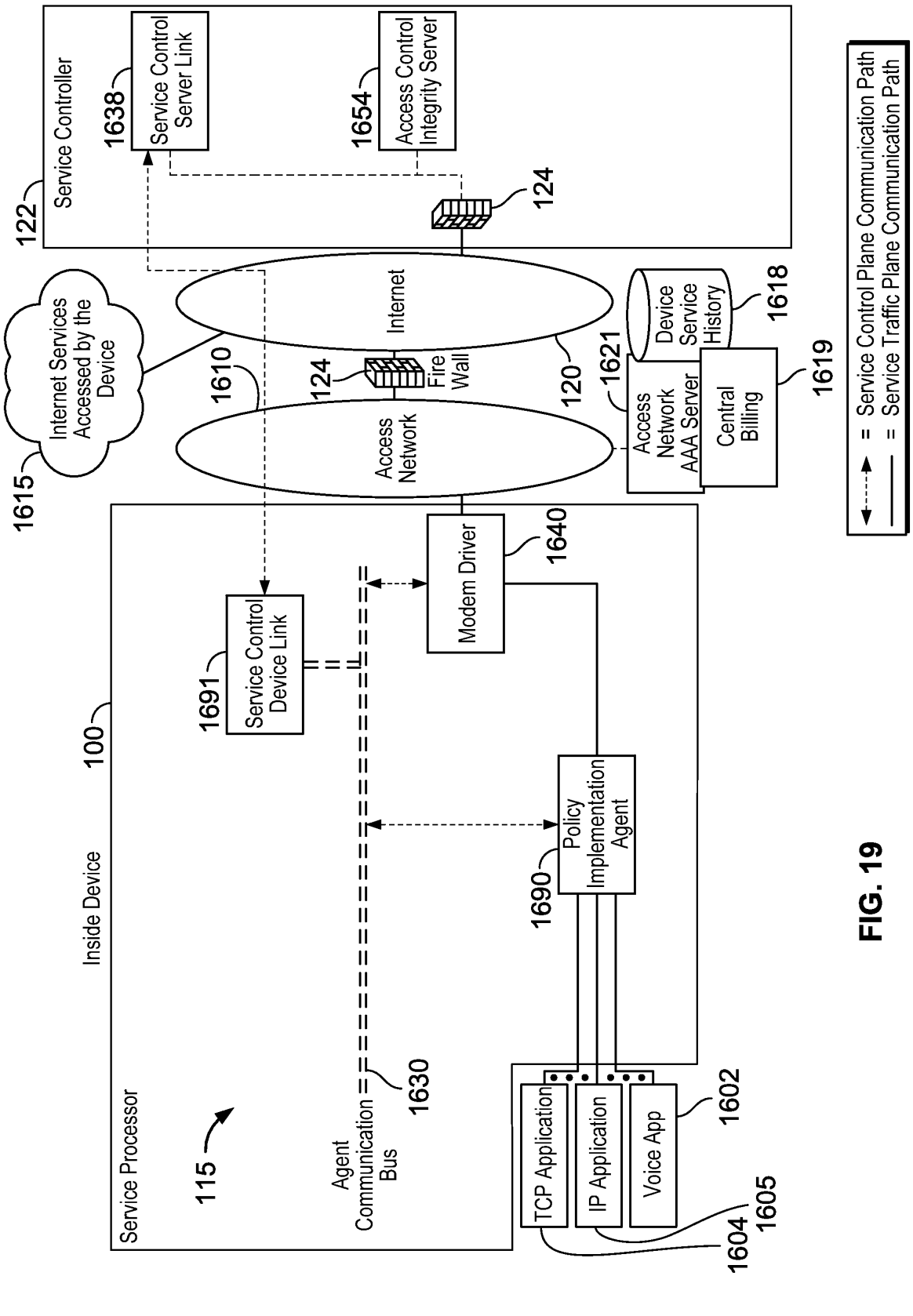

Service Controller
122
Service Control Server Link
1638
Access Control Integrity Server
1654
124
Internet
Internet Services Accessed by the Device
1615
1610
124
Fire Wall
120
1621
Device Service History
1618
Access Network
Access Network AAA Server
Central Billing
1619
Modem Driver
1640
Service Control Device Link
1691
100
Inside Device
Service Processor
115
Agent Communication Bus
1630
Policy Implementation Agent
1690
TCP Application
IP Application
Voice App
1602
1604
1605
= Service Control Plane Communication Path
= Service Traffic Plane Communication Path

FIG. 19

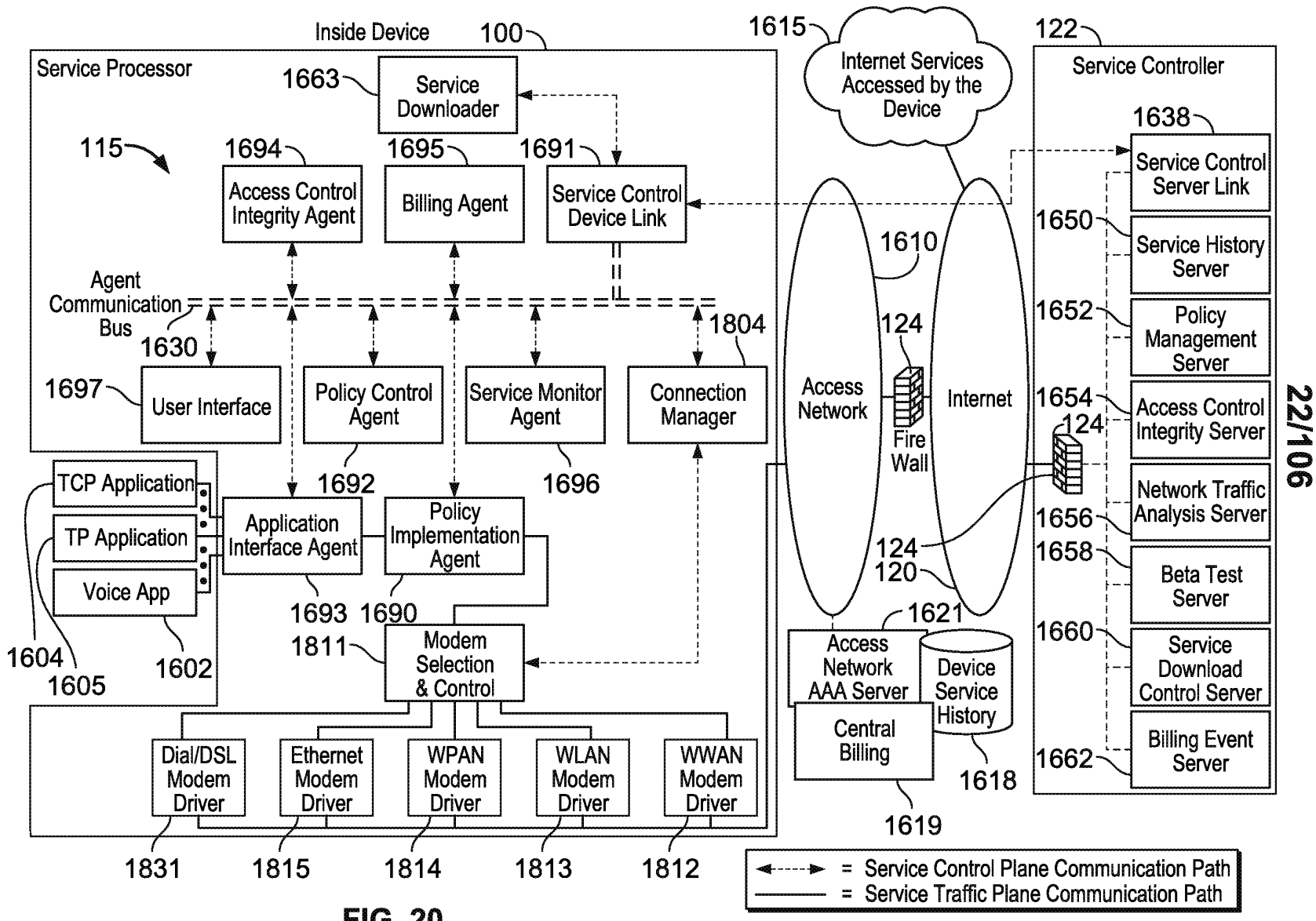

Inside Device
100
Service Processor
1663
Service Downloader
115
1694
Access Control Integrity Agent
1695
Billing Agent
1691
Service Control Device Link
Agent Communication Bus
1630
1804
1697
User Interface
Policy Control Agent
Service Monitor Agent
Connection Manager
1692
1696
TCP Application
TP Application
Voice App
Application Interface Agent
Policy Implementation Agent
1693
1690
1604
1605
1602
1811
Modem Selection & Control
Dial/DSL Modem Driver
Ethernet Modem Driver
WPAN Modem Driver
WLAN Modem Driver
WWAN Modem Driver
1831
1815
1814
1813
1812
1615
Internet Services Accessed by the Device
1610
124
Access Network
Fire Wall
Internet
124
120
1621
Access Network AAA Server
Device Service History
Central Billing
1618
1619
122
Service Controller
1638
Service Control Server Link
1650
Service History Server
1652
Policy Management Server
1654
Access Control Integrity Server
124
Network Traffic Analysis Server
1656
1658
Beta Test Server
1660
Service Download Control Server
Billing Event Server
1662
= Service Control Plane Communication Path
= Service Traffic Plane Communication Path

FIG. 20

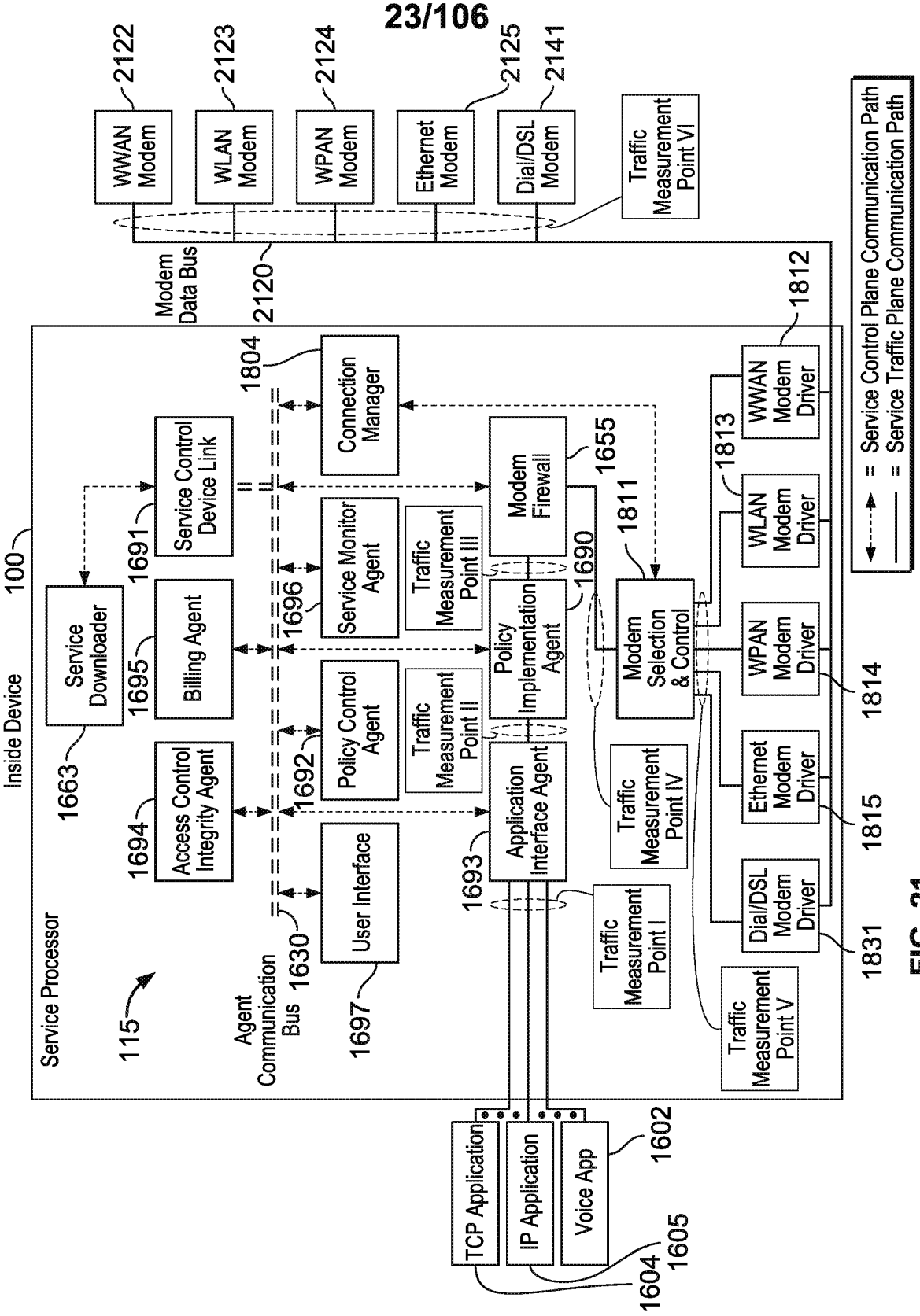

Inside Device
100
Service Processor
115
Agent Communication Bus
1630
Modem Data Bus
2120
WWAN Modem
2122
WLAN Modem
2123
WPAN Modem
2124
Ethernet Modem
2125
Dial/DSL Modem
2141
Traffic Measurement Point VI
Service Downloader
1663
Billing Agent
1695
Service Control Device Link
1691
Connection Manager
1804
Access Control Integrity Agent
1694
Policy Control Agent
1692
Service Monitor Agent
1696
Traffic Measurement Point III
Modem Firewall
1655
Traffic Measurement Point II
Policy Implementation Agent
1690
Application Interface Agent
1693
User Interface
1697
Modem Selection & Control
1811
Traffic Measurement Point IV
Traffic Measurement Point I
Traffic Measurement Point V
WWAN Modem Driver
1812
WLAN Modem Driver
1813
WPAN Modem Driver
1814
Ethernet Modem Driver
1815
Dial/DSL Modem Driver
1831
TCP Application
IP Application
Voice App
1602
1604
1605
= Service Control Plane Communication Path
= Service Traffic Plane Communication Path

FIG. 21

Service Processor 115 Embodiment	Partial Summary of Embodiment Functions
Service Control Device Link 1691	Device side control plane link for connecting Service Processor 115 to Service Controller. In some embodiments, also serves as the link for the agent heartbeat function.
Access Control Integrity Agent 1694	Collects device information on service policy, service usage, agent configuration and agent behavior. Cross checks this information to identify integrity breaches in the service policy implementation and control system. Initiates action when a service policy violation or a system integrity breach is suspected. In some embodiments, verifies configuration of other agents or performs challenge-response sequence testing. In some embodiments, monitors software loading activity, protected memory access or communication with Service Processor agents to detect unauthorized changes to Service Processor software or configuration.
Policy Control Agent 1692	Takes policy instructions from the network and sets instantaneous device service policy. In some embodiments, performs a policy control function to adapt instantaneous service policies to achieve a service usage objective.
Policy Implementation Agent 1690	Implements traffic control and QOS policy rules for device. In some embodiments provides the functions of access control and/or firewall function or perform traffic inspection and characterization. In some embodiments packet inspection is aided by literal or virtual application layer tagging while in other embodiments packet inspection is performed completely in the Policy Implementation Agent 1690.
Service Monitor Agent 1696	Records and reports device service usage. In some embodiments, assists in communicating application tagging of traffic flows through the networking stack policy implementation. In some embodiments, maintains a history and provides reports or summary reports of which networks in addition to the networks controlled by the Service Controller that the device has connected to. In some embodiments, this network activity summary may include a summary of the networks accessed, activity vs. time per connection, traffic vs. time per connection.
Application Interface Agent 1693	Rich feature interface for device application programs. In some embodiments, identifies application level traffic, reports service usage or tags traffic for service QOS control. In some embodiments, interacts with applications or programs applications to arrange application settings such as email file transfer options or browser headers. In some embodiments, intercepts certain application traffic to modify traffic application layer parameters such as email file transfer options or browser headers. In some embodiments implements certain aspects of traffic control or other service policies. In some embodiments, provides the functions of traffic control, access control and/or firewall.
Modem Firewall 1655	Blocks or passes traffic based on service policies and traffic attributes. In some embodiments, assists in traffic flow tagging. In some embodiments provides the functions of traffic control and/or access control.
Billing Agent 1695	Detects and reports billing events. In some embodiments interacts with the User Interface Agent 1697 to provide the user with service plan options, accept service plan selections, provide notification on service usage levels, provide options on service usage control policy, accept choices on service usage policy, provide transaction options or accept transaction choices. In some embodiments, interacts with Transaction Servers 134 to conduct ecommerce transactions with central billing.

696

FIG. 22A

User Interface Agent 1697	Provide service interface to users.
Service Downloader 1663	Provides a download function to install or update service software elements on the device.
Connection Manager 1804	Provides a control and supervision function for one or more modem drivers or modems that connect to an access network.
Modem Selection and Control 1811	Selects the access network connection.
Modem Drivers 1831, 1815, 1814, 1813, 1812	Converts data traffic into modem bus traffic for one or more modems.
Modems 2141, 2125, 2124, 2123, 2122	Connects the device to one or more networks.

970

FIG. 22B

Service Controller 122 Element	Partial Summary of Embodiment Functions
Service Control Server Link 1638	Network side control plane link for connecting Service Controller 122 Service Processor 115 device agents. In some embodiments, also serves as the link for the agent heartbeat function.
Access Control Integrity Server 1654	Collects device information on service policy, service usage, agent configuration and agent behavior. Cross checks this information to identify integrity breaches in the service policy implementation and control system. Initiates action when a service policy violation or a system integrity breach is suspected.
Policy Management Server 1652	Transmits policies to the Service Processor 115.
Access Network AAA Server 1621	Provides access control and authorization functions for the device access layer. Records and reports device network service usage.
Service History Server 1650	Collects and records service usage reports from the Access Network AAA Server 121 and the Service Monitor Agent 1696. In some embodiments, maintains a history of which networks in addition to the networks controlled by the Service Controller that the device has connected to. In some embodiments, this network activity summary may include a summary of the networks accessed, activity vs. time per connection, traffic vs. time per connection. In some embodiments, this activity summary is further analyzed or reported to estimate the type of service plan associated with the traffic activity for the purpose of bill sharing reconciliation.
Central Provider Billing System 1619	Provides mediation function for central provider billing events. Accepts service plan changes. In some embodiments, provides updates on device service usage, service plan limits or service policies.
Billing Event Server 1662	In some embodiments, collects billing events, provides service plan information to the Service Processor 115, provides service usage updates to the Service Processor 115, serves as interface between device and central Provider Billing System 123, or provides trusted third party function for certain ecommerce billing transactions.
Network Traffic Analysis Server 1656	Collects service usage history for devices or groups of devices and analyses the service usage. In some embodiments, presents service usage statistics in various formats to identify improvements in network service quality or service profitability. In other embodiments, estimates the service quality or service usage for the network under variable settings on potential service policy. In other embodiments, identifies actual or potential service behaviors by one or more devices that are causing problems for overall network service quality or service cost.
Beta Test Server 1658	Publishes candidate service plan policy setting to one or more devices. In some embodiments, provides summary reports of network service usage or user feedback information for one or more candidate service plan policy setting. In some embodiments, provides a means to compare the beta test results for different candidate service plan policy settings or select the optimum candidates for further setting optimization.
Service Download Control Server 1660	Provides a download function to install or update service software elements on the device.
Transaction Server 134	Provides an electronic commerce offering and transaction platform to the device.

FIG. 23

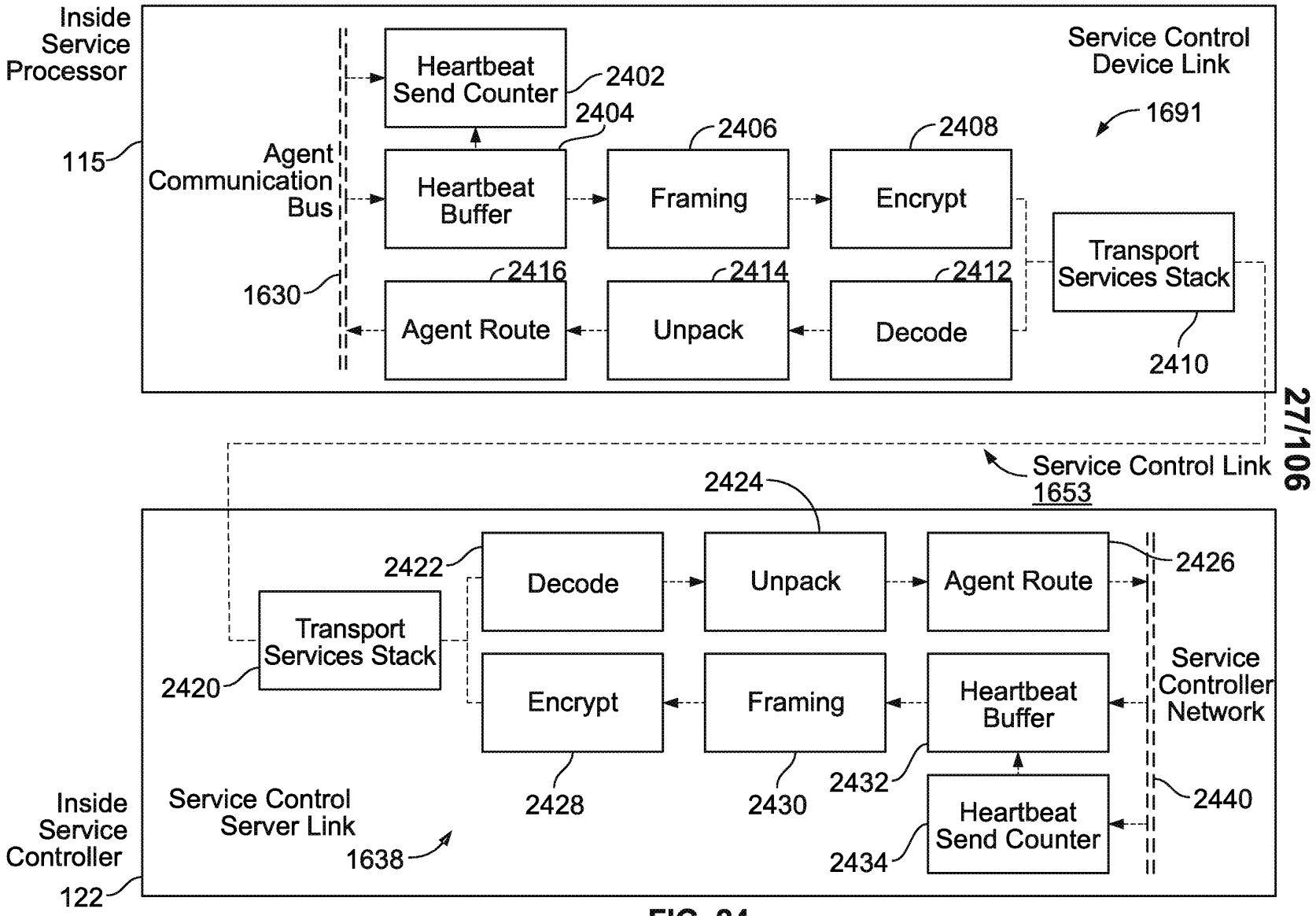

Inside Service Processor
115
Agent Communication Bus
1630
Heartbeat Send Counter
2402
2404
Heartbeat Buffer
2406
Framing
2408
Encrypt
Service Control Device Link
1691
Transport Services Stack
2410
2416
Agent Route
2414
Unpack
2412
Decode
27/106
Service Control Link
1653
2424
2422
Decode
Unpack
Agent Route
2426
Transport Services Stack
2420
Encrypt
Framing
Heartbeat Buffer
Service Controller Network
2428
2430
2432
2440
Heartbeat Send Counter
2434
Service Control Server Link
1638
Inside Service Controller
122

FIG. 24

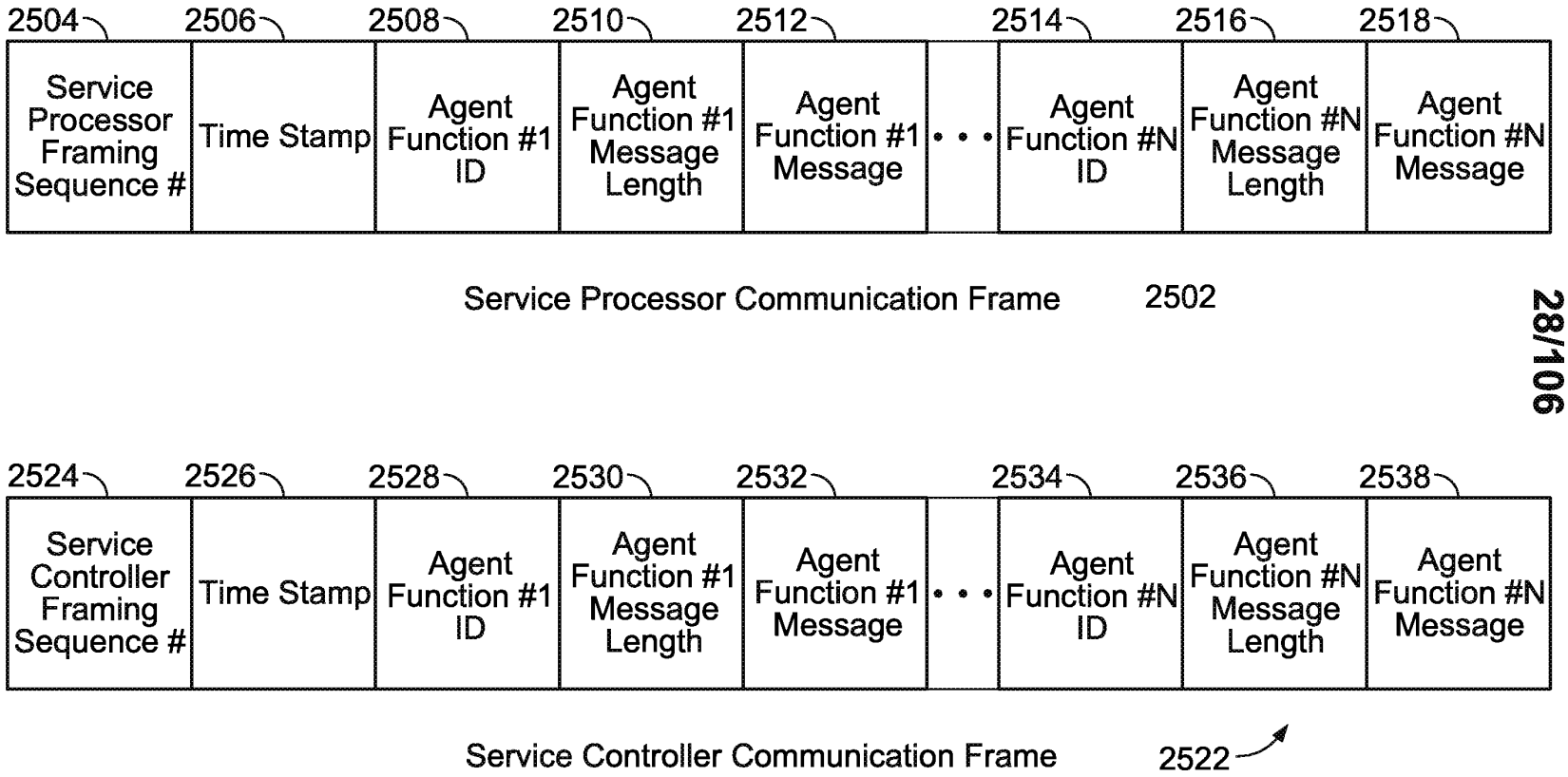

2504
2506
2508
2510
2512
2514
2516
2518
Service Processor Framing Sequence #
Time Stamp
Agent Function #1 ID
Agent Function #1 Message Length
Agent Function #1 Message
• • •
Agent Function #N ID
Agent Function #N Message Length
Agent Function #N Message
Service Processor Communication Frame
2502
2524
2526
2528
2530
2532
2534
2536
2538
Service Controller Framing Sequence #
Time Stamp
Agent Function #1 ID
Agent Function #1 Message Length
Agent Function #1 Message
• • •
Agent Function #N ID
Agent Function #N Message Length
Agent Function #N Message
Service Controller Communication Frame
2522

FIG. 25

Example Service Processor Heartbeat Parameter Embodiments	Description	Frequency
Access control integrity report	Contains the latest results of the Access Control Integrity agents Service Processor system checks and reports any error events.	Not necessary to report in every heartbeat if there are no errors. Can report only on error, set a minimum frequency or respond to Service Controller polling.
Service monitor report	Reports filtered summary of Service Monitor Agent measurements. Summary reduces control traffic and filters out unauthorized private information.	Every heartbeat. Some embodiments link this to amount of data usage in the data path to keep overhead low. Report immediately upon polling from Service Controller.
Billing event report	Reports any billing activity since the last heartbeat. Billing events may include service usage events, transaction events, bill by account records, bill by account offset reports or any other event that results in a billing event report.	Send upon billing event. Report immediately upon polling from Service Controller.
Service Processor settings report	Reports service policy settings for all Service Processor agents.	Not necessary to send every heartbeat. Some embodiments link this to amount of data usage to reduce overhead. Can report every N heartbeats. Report immediately upon polling from Service Controller.
Customer resource management report	Reports filtered summary of Service Monitor Agent measurements or filtered summary of other device or user activity such as service preferences, advertisement behavior and location. Summary reduces control traffic and filters out unauthorized private information.	Not necessary to send every heartbeat. Some embodiments link this to amount of data usage to reduce overhead. Can report every N heartbeats. Report immediately upon polling from Service Controller.
Responses to Service Processor agent queries	Sends agent responses to challenge-response queries from the Service Controller.	Report immediately upon polling from Service Controller.

974

FIG. 26A

Location tracking service update	Reports filtered summary of location tracking information. Summary reduces control traffic and filters out unauthorized private information.	Not necessary to send every heartbeat. Some embodiments call for a minimum time based transmission frequency.
Service usage based transmission frequency	Lowers overhead by buffering and reserving heartbeat communications from agents and servers until a certain amount of data has been transmitted or received in the network, or a certain amount of service has been consumed. When the parameters are chosen properly, this can result in the network control plane traffic overhead being a small percentage of data path traffic or result in the control plane traffic cost being a small percentage of the service usage cost.	Ranges depending on settings. For example, if there are 5 agents messages that typically need to be communicated, and each message is less than 100 bytes, and Service Processor heartbeat framing plus network overhead would result in a packet size of less than 1,000 bytes, and the heartbeat packet is transmitted when 10,000,000 bytes have been communicated over the data path, then the overhead loss due to one heartbeat packet in each direction is less than 0.02%.
Constant frequency transmissions	Since the device may be off line for long periods of time where the Service Control Processor needs to verify service control integrity, in some embodiments it can be advantageous to transmit heartbeat packets at a minimum rate regardless of data traffic activity. This is accomplished by setting a timer that sends queued heartbeat packets on a regular schedule.	Ranges depending on settings and applications.
Service Controller polled transmissions	In some embodiments, the Service Controller may poll the Service Processor for a heartbeat transmission at which time the Service Processor will frame and transmit all queued heartbeat messages.	Ranges depending on applications. In some embodiments this is used as an on demand function while in others it is used as a way to set heartbeat transmission timing functions in the Service Controller.
Service Processor polled transmissions	In some embodiments, the Service Processor polls the Service Controller for a heartbeat transmission at which time the Service Controller will frame and transmit all queued heartbeat messages.	Ranges depending on applications. In some embodiments this is used as an on demand function while in others it is used as a way to set heartbeat transmission timing functions in the Service Processor.

975

FIG. 26B

Agent self-check reports	Agent reports results of various agent self-diagnosis procedures to ensure that the agent is properly configured, operating properly, properly implementing service control policy or has not been tampered with. [provide examples which are extensions of typical software security self diagnosis reporting]	In some embodiments an report is made during every heartbeat transmission. In other embodiments the report is generated by a request from the Service Controller. In other embodiments the report is generated by timing determined by the device. In some embodiments the report is generated when there is a verification error of some kind that is identified.
Environment reports	One or more agents scan the storage or execution environment for one or more of the agents to identify potential threats to the integrity of the service implementation or agent integrity and makes a report. In one example embodiment, a scan is done to determine if unauthorized software or hardware is executing in a secure agent environment. In another embodiment, a scan is done to determine the software that has been loaded into a portion of the device operating environment, memory or storage, and the software list is referenced against a known threat list. In another example embodiment, the list of entities that accessed one or more agents is scanned to determine if an unauthorized access to an agent has occurred. In another embodiment a scan is performed to determine if unauthorized access to secure execution environment, memory or storage has occurred. In another example embodiment, the network access pattern for the device is logged and analyzed to determine if there is an access pattern that is known to be associated with a threat to service or agent control integrity. In another example embodiment, the internal device software, memory or peripheral access pattern is logged and analyzed to determine if there is an access pattern that is known to be associated with a threat to service or agent control integrity.	In some embodiments an report is made during every heartbeat transmission. In other embodiments the report is generated by a request from the Service Controller. In other embodiments the report is generated by timing determined by the device. In some embodiments the report is generated when there is a verification error of some kind that is identified.

976

FIG. 26C

User notification response reports	Billing agent, UI agent or another agent logs user notification events and the response of the user to the notification event. In some embodiments these events may be cross-referenced to the notification policy that should be in force on the device and the device service usage to ensure that the proper notification sequences are being adhered to. In other embodiments, the user notification responses are logged and used to document user choices to notification events, billing event decisions, service control decisions or service cost control decisions. In some embodiments, the user may be asked to provide a password, biometric signature, hardware key or other mechanism to positively identify that the user is in possession of the device or to verify that the service is operating properly or is implemented properly. In some embodiments, the user may be asked to acknowledge a service overage notification and/or to also provide a password, biometric signature, hardware key or other mechanism to verify the service overage acknowledgement.	In some embodiments a report is made during every heartbeat transmission. In other embodiments the report is generated by a request from the Service Controller. In other embodiments the report is generated by timing determined by the device, for example when there has been a user notification sequence action with the user. In some embodiments, the report is generated when there is a verification error of some kind that is identified.
User warning response reports	Billing agent, UI agent or another agent logs user warning events and the response of the user to warning event. In some embodiments the user response is used to determine if the user is in positive control of the device. In some embodiments the response is used to confirm that the user acknowledges a billing overage or other service cost event. In some embodiments, the user may be asked to provide a password, biometric signature, hardware key or other mechanism to positively identify that the user is in possession of the device or to verify that the service is operating properly or is implemented properly.	In some embodiments a report is made during every heartbeat transmission. In other embodiments the report is generated by a request from the Service Controller. In other embodiments the report is generated by timing determined by the device, for example when there has been a warning sequence action with the user. In some embodiments the report is generated when there is a verification error of some kind that is identified.

FIG. 26D

Agent communication log reports	Reports entities that established or attempted to establish communication with the agents. In one embodiment, reports a list of entities and the number of times the entity communicated or attempted to communicate with the agent. In another embodiments, reports an error flag when unauthorized entities attempt to establish communication with an agent.	In some embodiments a report is made during every heartbeat transmission. In other embodiments the report is generated by a request from the Service Controller. In other embodiments the report is generated by timing determined by the device. In some embodiments the report is generated when there is a verification error of some kind that is identified.
Service usage synchronization data	IPDR or other data that is used to synchronize the device service usage counters. In some embodiments the data is time stamped so that the service usage at a point in time may be reconciled between the local device usage count and the network based usage count, and then the local device usage count since the point in time may be used to estimate the present real-time usage count. In some embodiments, the service usage data from the device is used by the network as the actual service usage or billing data base for the device. In other embodiments, a bill by account function is included in the service usage synchronization data so that the service usage may be billed to different accounts other than a single or main user account.	Service usage synchronization is continuous with each heartbeat in some embodiments. In other embodiments service usage synchronization is based on a push from the Service Controller or other network function that sends the IPDR information to the device. In other embodiments, the device requests a synchronization data transmission.
Service cost synchronization data	Information to reconcile a service cost estimate on the local device with a service cost count from a network based function. Similar to the service usage count, in some embodiments the service cost information is time stamped so that service cost at a point in time may be reconciled between the device and the network based function, and then a local measure of service cost may be used to estimate the present real-time service cost. In some embodiments the local service cost is determined by taking recorded billing events and looking up the cumulative cost of one or more billing	Service cost synchronization is continuous with each heartbeat in some embodiments. In other embodiments service cost synchronization is based on a push from the Service Controller or other network function that sends the IPDR information to the device. In other embodiments, the device requests a synchronization data transmission.

978

FIG. 26E

	events using a service usage to cost look up data base stored locally on the device or available from a network function. In some embodiments, service cost estimation is done entirely in the network and the result is pushed out to the device UI. In other embodiments service cost estimation is done in the device based on local usage estimates and a local usage to cost lookup table.	
Available network information and roaming information	Device receives available network or available roaming service provider information from a network function. The available network or roaming service information may include the potential network service or roaming service a device or user may choose to select, or the network service or roaming service the user has already selected. In some embodiments this information includes service cost information to aid the device or the user in determining the potential or actual costs of service usage while using the available network or roaming network. In some embodiments the service cost information is used to help the user in selecting the available network provider or roaming service provider. In some embodiments the available network cost information or roaming cost information is combined with a measure of expected or possible service usage to estimate how much a typical usage scenario may cost. In some embodiments, the available network information or roaming information is used to help the user estimate the present available network or roaming service charges for services used to date. In some embodiments service usage is recorded and sent to a network function that estimates the current service cost. In other embodiments the service cost is estimated locally on the device based on a service usage estimate and a service usage to cost look up function. In other	In some embodiments available network information or roaming information is requested by the device. In other embodiments, the information is periodically updated by the Service Controller or other network function that contains the information.

FIG. 26F

	embodiments, the service cost is derived by querying the available network or roaming network billing system.	
System messages and responses	In some embodiments the heartbeat function may be used as a secure control channel to display a system messages or screen that is generated by a network function or server to the end user and possibly report user inputs to the UI message or screen. Examples include, ….. etc.	System messages are generated by the Service Controller and transmitted as needed in some embodiments. In other embodiments, some system messages are generated in response to user input or requests. In other embodiments, system messages are generated on a regular time table or in accordance with a certain amount of service usage.
UI screen messages and responses	In some embodiments the heartbeat function may be used as a secure control channel to display user interface message or screen that is generated by a network function or serve to the end user and possibly report user inputs to the UI message or screen. Examples include service usage UI, service choice UI, upgrade UI, transaction UI, marketing UI, billing UI, user identify confirmation UI, user service warning UI, user potential service tamper response request UI, etc.	UI screen messages are generated by the Service Controller and transmitted as needed in some embodiments. In other embodiments some user UI messages are generated in response to user input or requests. In other embodiments, UI messages are generated on a regular time table or in accordance with a certain amount of service usage.
Local agent check-in history	Logs and reports agent check-ins or self-reports that are made to a local agent integrity verification function.	In some embodiments a report is made during every heartbeat transmission. In other embodiments the report is generated by a request from the Service Controller. In other embodiments the report is generated by timing determined by the device. In some embodiments the report is generated when there is a verification error of some kind that is identified.
Software install report	Logs and reports one or more aspects of software installs that have occurred on the device.	In some embodiments a report is made during every heartbeat transmission. In other embodiments the report is generated by a request from the Service Controller. In other embodiments the report is generated by timing determined by the device. In some embodiments the report is generated when there is a verification error of some kind that is identified. In some

FIG. 26G

		embodiments, the report is generated when new SW is installed.
Test billing event	In some embodiments the Service Controller or other network function may send or cause a test billing event wherein the device triggers a local billing sequence for the purpose of verifying that the billing sequence is properly logged, conducted and reported. The billing sequence can be related to a service usage event or sequence, a transaction event or sequence, or any other event or sequence that should result in a billing event.	In some embodiments, the test billing event timing is determined by the Service Controller or other network function. In others it is generated by the device or on a regular schedule.
Test service event	In some embodiments the service Controller or other network function may send or cause a service usage event wherein the device triggers a local service usage event or sequence for the purpose of verifying that the service usage event or sequence is properly logged and reported.	In some embodiments, the test service usage event timing is determined by the Service Controller or other network function. In others it is generated by the device or on a regular schedule.

FIG. 26H

Service Policy Implementation Verification Technique Embodiments	Example Error Trigger Criteria Embodiments	Example Error Response Embodiments
Verify service usage measure in network is consistent with expected service behavior	Network service usage measure is in conflict with expected service usage. Examples: traffic usage outside limits, address access outside limits, data rate outside limits, traffic shaping rules not being followed.	In some embodiments the severity of the error and/or the persistence of the error and/or the existence of the other errors are used to determine the appropriate response or action. In some embodiments, reset service policies and see if errors persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/ response to determine agent integrity. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service inspection process, or usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.

FIG. 27A

Verify service usage measure at device is consistent with expected service behavior	Device service usage measure is in conflict with expected service usage. Examples: traffic usage too high, address access outside limits, email accessed against policy.	Same as above.
Verify service usage measure in network is consistent with service usage measure at device	Device service usage measure varies significantly from network service usage measure	Same as above.
Verify service usage measure at one point in device is consistent with service usage measure at a second point in device	Service usage measure at one point in device stack that is inconsistent with another point indicates error or potential parasitic usage	Same as above. In some embodiments, the differences in service measures on the device may be used to evaluate the nature of the service usage policy implementation problem.
Verify that service policies in effect are as intended	Service policy setting queries result in settings that are different than intended	In some embodiments, reset service policies and see if error persist. If this does not clear the error, or if this is not the error correction method employed, then perform one or more of the following actions: In some embodiments, perform agent query/response to determine agent integrity.In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition

FIG. 27B

		to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.
Verify presence of Service Processor agents	Agent does not respond to agent communication or query-response	In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. If this does not clear the error, or if this is not the error correction method employed, then perform one or more of the following actions: In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.
Verify configuration of Service Processor agents	Agent configuration audit or configuration self check fails.	In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. If this does not clear the error, or if this is not the error correction method employed, then perform one or more of the following actions: In some embodiments the severity of the error and/or the persistence of the

FIG. 27C

		error and/or the existence of other errors are used to determine the appropriate response or action. In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.
Verify billing events are reported or are reported properly	Billing Agent query reveals logged billing events that have not been reported.	In some embodiments, perform a billing event test to determine if the billing event reporting sequence is operating properly. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. If this does not clear the error, or if these are not the error correction methods employed, then perform one or more of the following actions: In some embodiments the severity of the error and/or the persistence of the error and/or the existence of other errors are used to determine the appropriate response or action. In some embodiments, reset service

985

FIG. 27D

		policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a service usage test to determine if the device is properly reporting service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.
Verify network reported service usage measure are consistent with reported device billing data.	Billing agent is not properly reporting billing events for service usage, transactions, bill by account, or other billing event functions.	In some embodiments, perform a service usage test to determine if the service usage reporting sequence is operating properly. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. If this does not clear the error, or if these are not the error correction methods employed, then perform one or more of the following actions: In some embodiments the severity of the error and/or the persistence of the error and/or the existence of other errors are used to determine the appropriate response or action. In some embodiments, reset service

FIG. 27E

		policies and see if error persists.In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.
Verify device reported service usage measure are consistent with reported device billing data.	Billing agent reports are inconsistent with service usage reports.	In some embodiments, perform a billing event test to determine if the billing event reporting sequence is operating properly. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. In some embodiments, perform a service usage test to determine if the service usage reporting sequence is operating properly. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. If this does not clear the error, or if these are not the error correction methods employed, then perform one or more of the following actions: In some embodiments the severity of the error and/or the persistence of the error and/or the existence of other errors are used to determine the

FIG. 27F

		appropriate response or action. In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.
Send test billing event through device and verify it is reported.	Test billing event is not properly reported by the device.	In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. If this does not clear the error, or if these are not the error correction methods employed, then perform one or more of the following actions: In some embodiments the severity of the error and/or the persistence of the error and/or the existence of other errors are used to determine the appropriate response or action. In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine

988

FIG. 27G

		agent integrity. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a service usage test to determine if the device is properly reporting service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis
Verify device reports billing events reported from transaction servers.	Transaction server receipts do not correspond with billing events from device.	In some embodiments, perform checks to determine if transaction server receipts are valid. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. If this does not clear the error, or if these are not the error correction methods employed, then perform one or more of the following actions: In some embodiments the severity of the error and/or the persistence of the error and/or the existence of other errors are used to determine the appropriate response or action. In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, a user query or warning is sent to

FIG. 27H

		the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.
Verify activation tracking system presence, configuration or operation	Activation tracking service is not present, is not providing scheduled network activity reporting, or is exhibiting erroneous reports.	In some embodiments the response is to place the device ID. on a list of devices suspected of having activation tracking functions that have been tampered with for the purpose of central provider billing reconciliation. In some embodiments, install a new copy of the activation tracking service agent software either from a locally stored device copy or a network download. In some embodiments where authorization exists to manage device software and some aspects of service tracking, run further checks on device service integrity such as agent query-response. In some embodiments where authorization exists to manage a device access service connection, send error message to device UI, suspend device or place device on quarantine route. In some embodiments send error message to human interface for troubleshooting.
Verify device standing or service plan standing	No service plan on record or device not authorized	In some embodiments, if device is not yet activated with a service plan, provide UI with activation sequence. In some embodiments, if device is not authorized for service on one of the networks controlled by the Service

FIG. 27I

		Controller, send the UI an error message instructing the user how to proceed. In some embodiments, configure the Service Processor for the ambient service intended for that device. In some embodiments, download the appropriate Service Processor agent software that is appropriate for that device.
Verify proper operation of Service Processor agents	Check input to output relationship on Policy Implementation agent, Firewall agent. Check billing event reports to verify events are being recorded. Check application and traffic inspection tagging system correctly tagging traffic. Verify Service Processor heartbeat reports proper agent integrity self-checks, cross-checks and query/response sequences with Service Controller.	In some embodiments the severity of the error and/or the persistence of the error and/or the existence of other errors are used to determine the appropriate response or action. In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.

FIG. 27J

991

Service Processor heartbeat response reports	One or more of the heartbeat reports indicate an error in operation, configuration, or tamper and error prevention system. Heartbeat function not functioning properly but device is still indicating service usage on the network.	In some embodiments the severity of the error and/or the persistence of the error and/or the existence of other errors are used to determine the appropriate response or action. In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.
Test service event	Service usage reporting system does not properly report test service usage event	In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. If this does not clear the error, or if this is not the error correction method employed, then perform one or more of the

FIG. 27K

992

		following actions: In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing test event to determine if the device is properly reporting billing events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.
Load a fresh version of Service Processor software and perform integrity reports	After fresh load of Access Control Integrity Agent, agent discovers one or more of the other agents are corrupted.	Run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh other agents and see if problem persists. If this does not clear the error, or if this is not the error correction method employed, then perform one or more of the following actions: In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, a

FIG. 27L

		user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.
Verify Service Processor code configuration with agent self diagnosis checks	One or more of the agents indicates an error after running a self-check.	Run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh other agents and see if problem persists. If this does not clear the error, or if this is not the error correction method employed, then perform one or more of the following actions: In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the

FIG. 27M

		device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.
Verify that device uses service only after being authorized	Device gains access to the network and does not check in with the Access Control Integrity Server and service measures indicate device is on the network.	In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on

995

FIG. 27N

		quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.
Verify user standing	User does not respond with proper response to UI query such as request for ID., password or biometric input. This process may be part of handling a suspected error.	In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis. In some embodiments, the user may be asked to acknowledge a service overage notification and/or to also provide a password, biometric signature, hardware key or other mechanism to verify the service overage acknowledgment.
Agent communications log	Unauthorized communications with one or more agents is detected	In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control.

FIG. 27O

		In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.

997

52/106

FIG. 27P

Service Policy Implementation Tamper or Error Protection Techniques	Example Error Trigger Criteria	Example Error Responses
Detect or block device networking activity that is potentially harmful for the operation of Service Processor.	Network activity is observed in service monitor reports that fit known patterns that indicated harmful software may be present on device.	Initiate or install and initiate eradication software. Block traffic from the suspect entity. In some embodiments if software can not be eradicated or blocked, then send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.
Detect or block unauthorized Service Processor software from being loaded.	Access Control Integrity Agent discovers software that is on a known malicious list.	Same as above.
Detect or block unauthorized access of protected Service Processor software or hardware memory.	Unauthorized access is detected, memory contents are corrupted or unresponsive.	Identify the entity that has gained access to the Service Processor if possible and eradicate. In some embodiments repair any compromised agents with dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code . In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.
Detect or block unauthorized communication with Service Processor software or hardware.	Unauthorized communication is detected.	Identify the entity that has gained access to the Service Processor if possible and eradicate. In some embodiments repair any compromised agents with dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code . In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.

866

FIG. 28A

Secure loader with signed SW installed into protected memory	Unauthorized access is detected, memory contents are corrupted or unresponsive.	Identify the entity that has gained access to the Service Processor if possible and eradicate. In some embodiments repair any compromised agents with dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code . In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.
Secure encrypted communication between Service Processor agents.	Secure communication link is in error or unauthorized access is detected.	Identify the entity that has gained access to the Service Processor if possible and eradicate. In some embodiments repair any compromised agents with dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code . In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh agents with communication links that are in error or entire Service Processor. In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.
Secure encrypted communication between Service Processor and Service Controller.	Service Processor communication is lost.	Send error message to device UI (if possible), suspend device, place on SPAN, place on watch list, place on further action list or place device on quarantine route. In some embodiments send error message to human interface for troubleshooting.
Execution of Service Processor software within secure memory.	Unauthorized access is detected, memory contents are corrupted or unresponsive.	Identify the entity that has gained access to the Service Processor if possible and eradicate. In some embodiments repair any compromised agents with dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code . In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.

666

FIG. 28B

Storage of service processor software in secure memory	Secure memory violation or Service Processor stored in non-secure memory	Identify the entity that has gained access to the Service Processor if possible and eradicate. In some embodiments repair any compromised agents with dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code . In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.
Detection or removal of software thought to be harmful to Service Processor operation.	Unauthorized software is detected.	Initiate or install and initiate eradication software. Block traffic from the suspect entity. In some embodiments if software can not be eradicated or blocked, then send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.
Recording and reporting of software loading signatures, software activity signatures or network activity signatures for later identification of threat sequences.	Unauthorized software or malicious network activity is detected	Same as above.
Implement critical Service Processor software as a self-refreshing program that resists corruption by running self-audit and reinstall processes such as placing audit function in inaccessible memory or OS functions or bios.	Re-installation function alerts that Re-installation has been required. Continued re-installations or failure to re-install alert increases severity of warnings.	Identify the entity that has gained access to the Service Processor if possible and eradicate. In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.
Encrypted agent code	Code check, agent query-response, agent self check or other agent configuration check discovers error in code encryption	In some embodiments repair any compromised agents with dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code . In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send

FIG. 28C

		error message to human interface for troubleshooting. Identify the entity that may have gained access to the Service Processor if possible and eradicate.
Obfuscated agent code	Code check, agent query-response, agent self check or other agent configuration check discovers error in code obfuscation	Same as above.
Unique agent identification numbers and signatures	Agent is discovered to have an incorrect ID. or fails signature	Same as above.
Secure agent communication bus	Agent communication bus monitoring discovers unauthorized communication or other unauthorized access to one or more agents is discovered	Same as above.
Agent level message encryption	Agent is found to be communicating without the required level of agent communication encryption	Same as above.
Service control link message level encryption	Unauthorized communication traffic is discovered on service control link	In some embodiments repair any compromised agents with dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code. In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting. Identify the entity that may have gained access to the Service Processor if possible and eradicate.
Service control link transport layer encryption	Unauthorized communication traffic is discovered on service control link	Same as above.
Agent communication access permissions	Unauthorized communication is discovered with one or more agents	Same as above.

FIG. 28D

Agent communication log	Unauthorized communication is discovered with one or more agents	Same as above.
Encrypted agent code for downloads	Agent download is found to have incorrect or absent encryption or signature	Same as above.
Secure downloader memory	Unauthorized access to or storage in secure downloader memory is discovered	Same as above.

1002

FIG. 28E

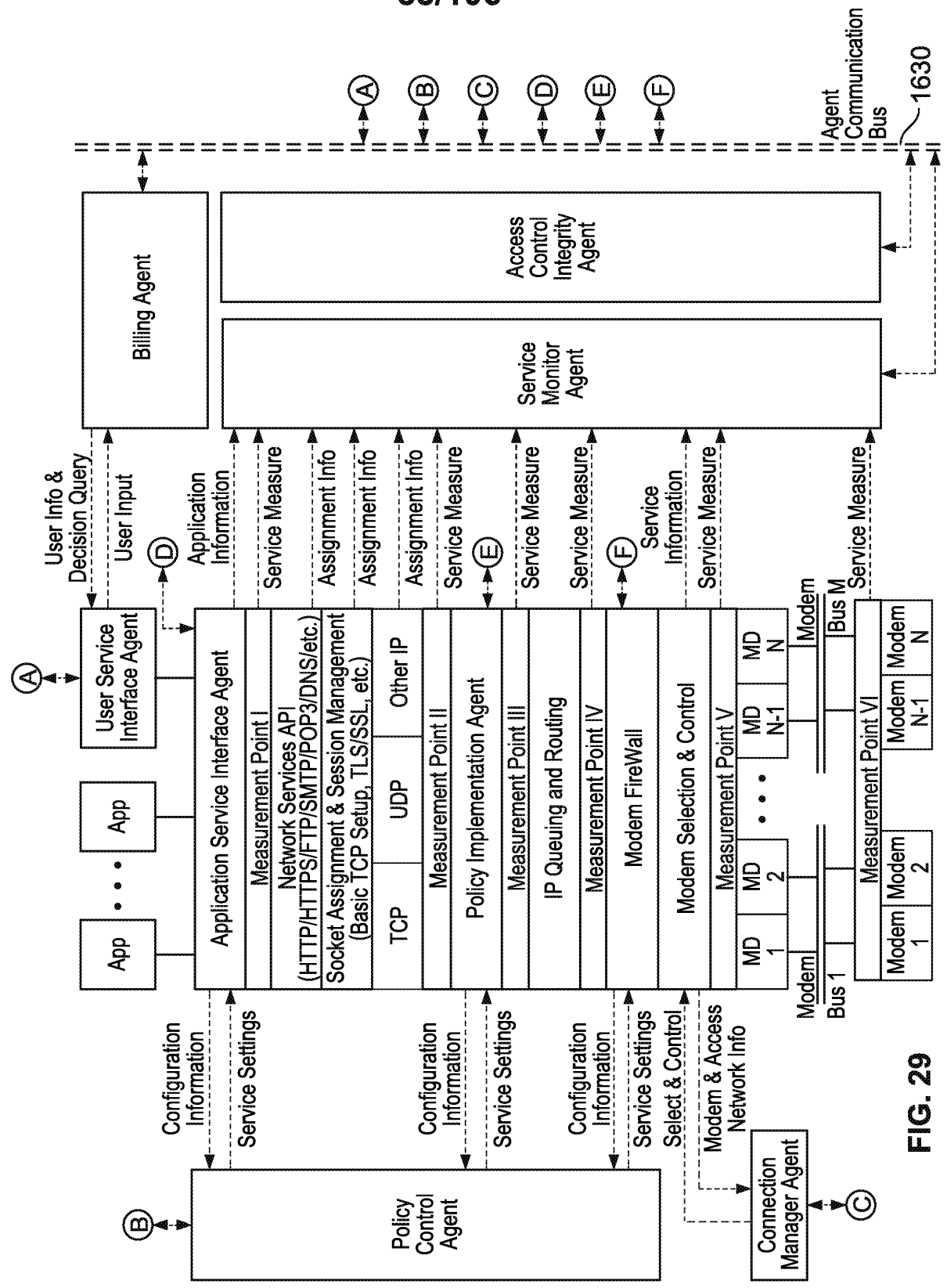

Billing Agent
Access Control Integrity Agent
Service Monitor Agent
Agent Communication Bus
1630
A
B
C
D
E
F
User Info & Decision Query
User Input
Application Information
Service Measure
Assignment Info
Service Information
User Service Interface Agent
App
App
Application Service Interface Agent
Measurement Point I
Network Services API (HTTP/HTTPS/FTP/SMTP/POP3/DNS/etc.)
Socket Assignment & Session Management (Basic TCP Setup, TLS/SSL, etc.)
TCP
UDP
Other IP
Measurement Point II
Policy Implementation Agent
Measurement Point III
IP Queuing and Routing
Measurement Point IV
Modem FireWall
Modem Selection & Control
Measurement Point V
MD 1
MD 2
MD N-1
MD N
Modem
Bus 1
Bus M
Measurement Point VI
Modem 1
Modem 2
Modem N-1
Modem N
Configuration Information
Service Settings
Select & Control
Modem & Access Network Info
Policy Control Agent
Connection Manager Agent

FIG. 29

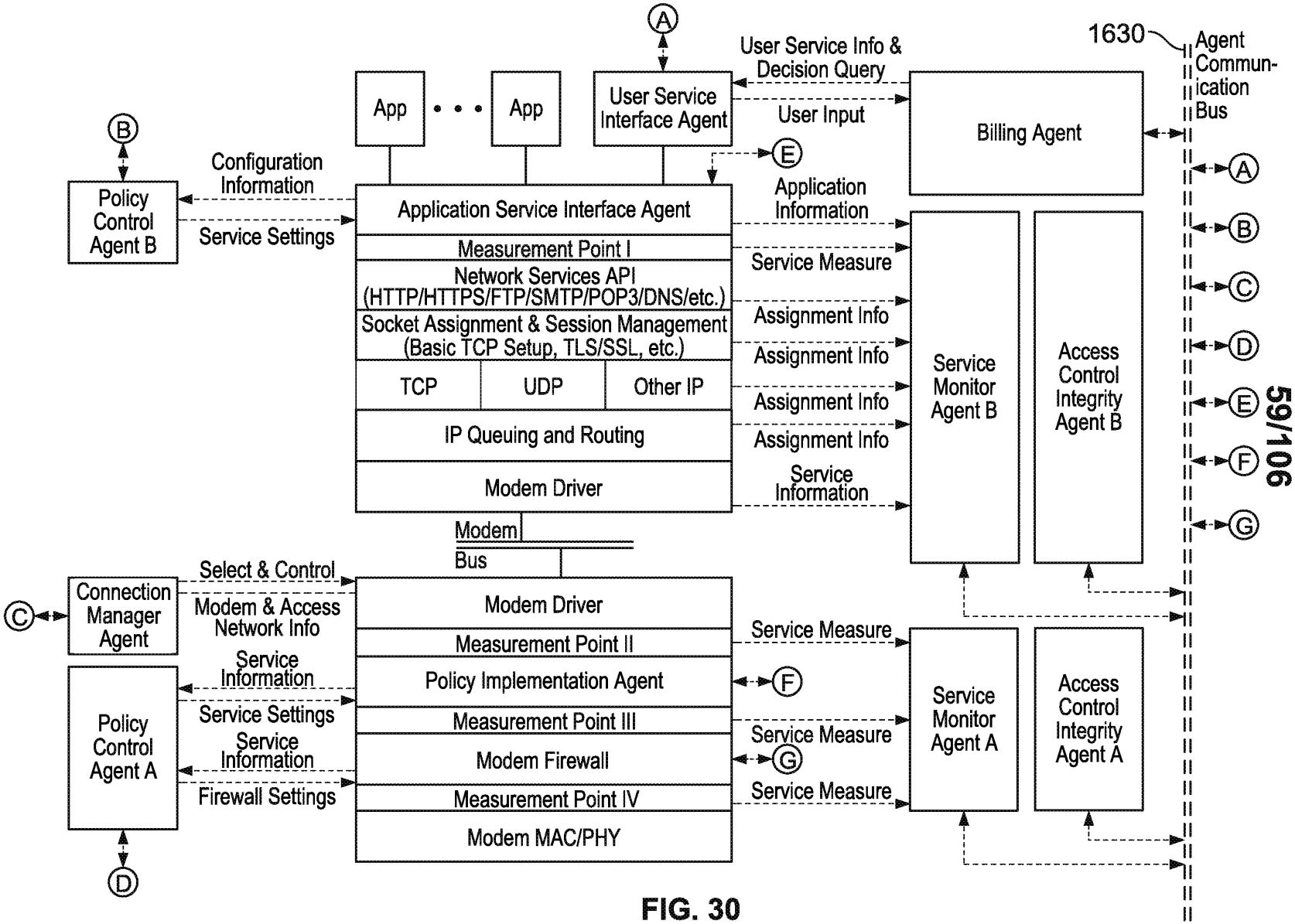

1004
A
B
C
D
E
F
G
1630
Agent Communication Bus
App
App
User Service Interface Agent
User Service Info & Decision Query
User Input
Billing Agent
Policy Control Agent B
Configuration Information
Service Settings
Application Service Interface Agent
Application Information
Measurement Point I
Service Measure
Network Services API (HTTP/HTTPS/FTP/SMTP/POP3/DNS/etc.)
Assignment Info
Socket Assignment & Session Management (Basic TCP Setup, TLS/SSL, etc.)
Assignment Info
TCP
UDP
Other IP
Assignment Info
IP Queuing and Routing
Assignment Info
Modem Driver
Service Information
Service Monitor Agent B
Access Control Integrity Agent B
Modem Bus
Select & Control
Modem & Access Network Info
Connection Manager Agent
Modem Driver
Measurement Point II
Service Measure
Service Information
Service Settings
Policy Implementation Agent
Measurement Point III
Service Measure
Service Information
Firewall Settings
Policy Control Agent A
Modem Firewall
Measurement Point IV
Service Measure
Modem MAC/PHY
Service Monitor Agent A
Access Control Integrity Agent A
59/106

FIG. 30

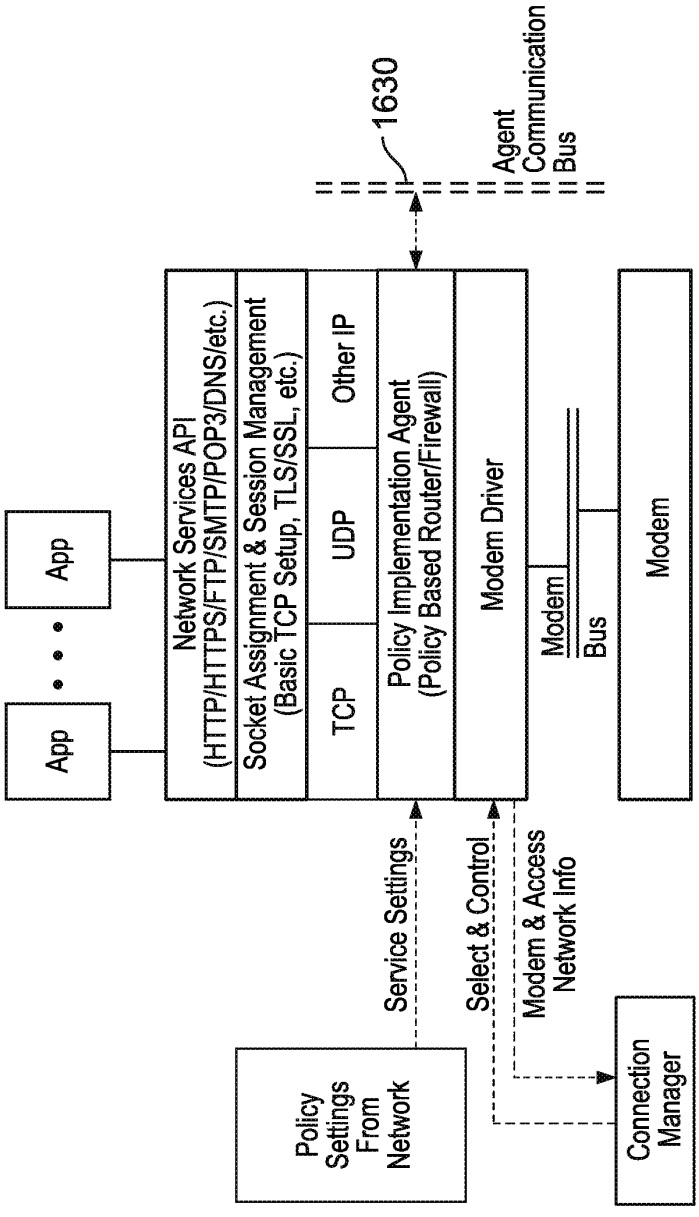

App
App
Network Services API
(HTTP/HTTPS/FTP/SMTP/POP3/DNS/etc.)
Socket Assignment & Session Management
(Basic TCP Setup, TLS/SSL, etc.)
TCP
UDP
Other IP
Policy Implementation Agent
(Policy Based Router/Firewall)
Modem Driver
1630
Agent
Communication
Bus
Modem
Bus
Modem
Service Settings
Select & Control
Modem & Access
Network Info
Policy
Settings
From
Network
Connection
Manager

FIG. 31

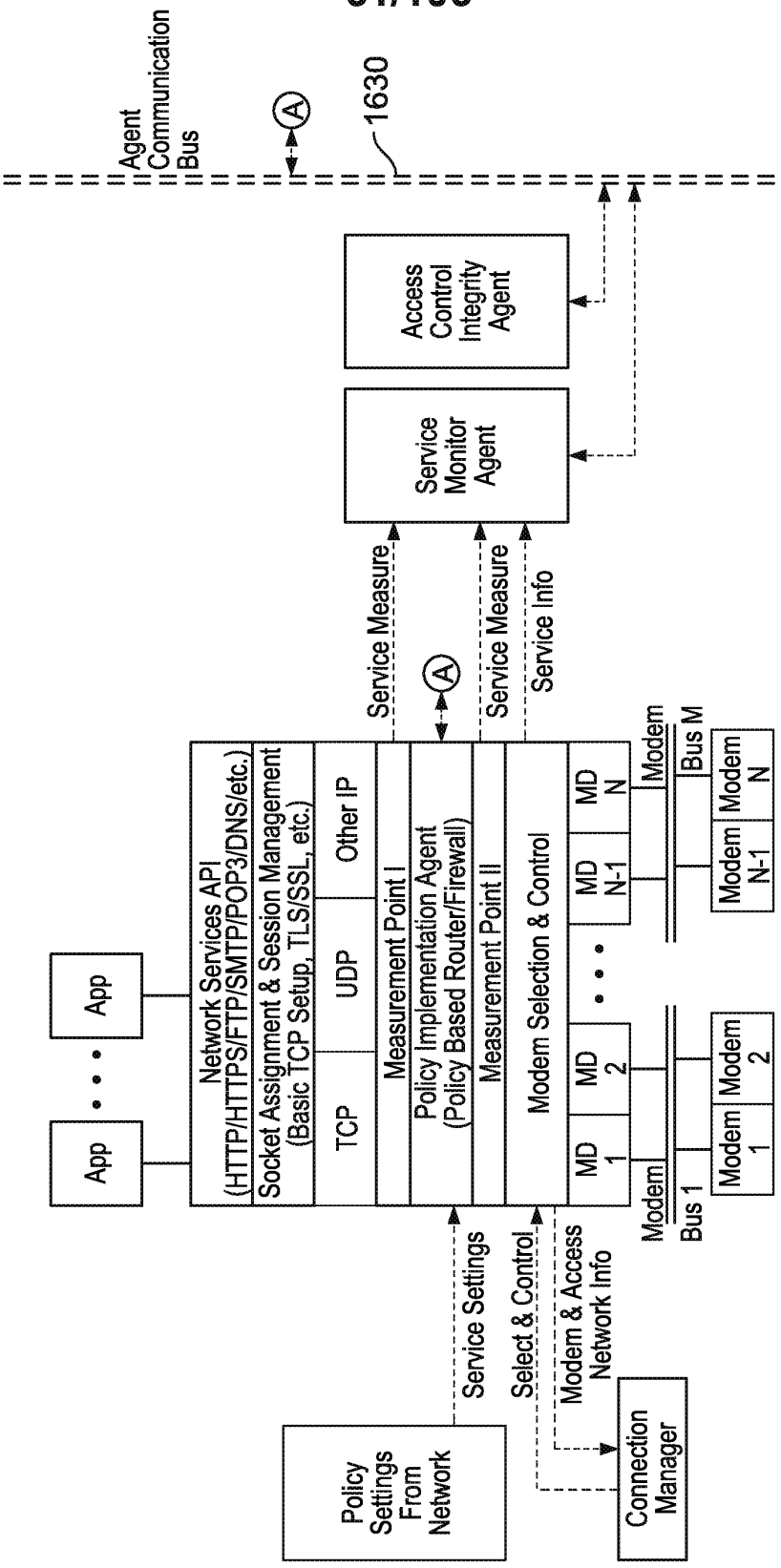

Agent Communication Bus
A
1630
Access Control Integrity Agent
Service Monitor Agent
Service Measure
Service Measure
Service Info
A
App
App
Network Services API (HTTP/HTTPS/FTP/SMTP/POP3/DNS/etc.)
Socket Assignment & Session Management (Basic TCP Setup, TLS/SSL, etc.)
TCP
UDP
Other IP
Measurement Point I
Policy Implementation Agent (Policy Based Router/Firewall)
Measurement Point II
Modem Selection & Control
MD 1
MD 2
MD N-1
MD N
Modem
Bus 1
Modem 1
Modem 2
Modem
Bus M
Modem N-1
Modem N
Service Settings
Select & Control
Modem & Access Network Info
Policy Settings From Network
Connection Manager

FIG. 32

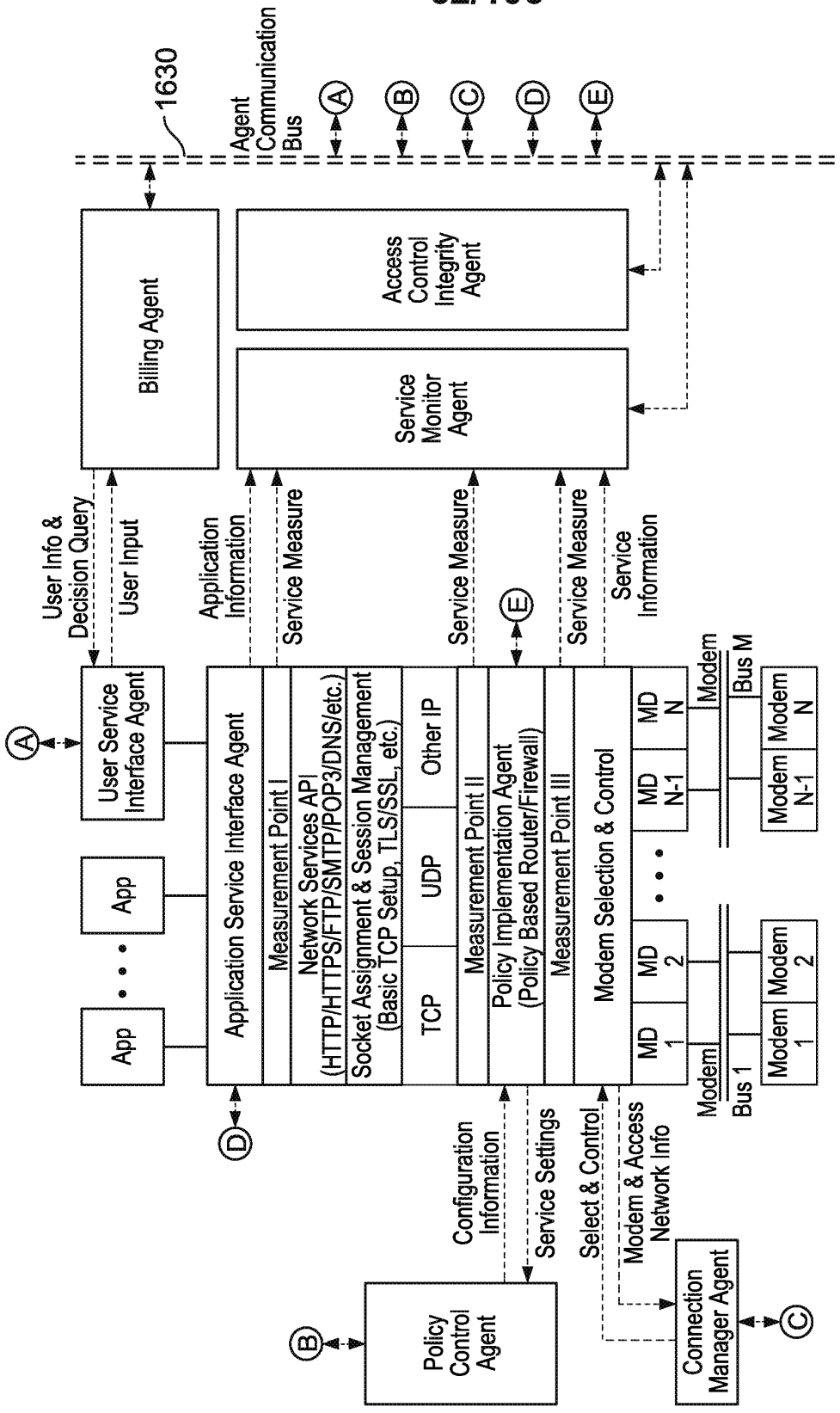

1630
Agent Communication Bus
A
B
C
D
E
Billing Agent
Access Control Integrity Agent
Service Monitor Agent
User Info & Decision Query
User Input
Application Information
Service Measure
Service Measure
Service Measure
Service Information
User Service Interface Agent
App
App
Application Service Interface Agent
Measurement Point I
Network Services API (HTTP/HTTPS/FTP/SMTP/POP3/DNS/etc.)
Socket Assignment & Session Management (Basic TCP Setup, TLS/SSL, etc.)
TCP
UDP
Other IP
Measurement Point II
Policy Implementation Agent (Policy Based Router/Firewall)
Measurement Point III
Modem Selection & Control
MD 1
MD 2
MD N-1
MD N
Modem
Bus 1
Bus M
Modem 1
Modem 2
Modem N-1
Modem N
Configuration Information
Service Settings
Select & Control
Modem & Access Network Info
Policy Control Agent
Connection Manager Agent

FIG. 33

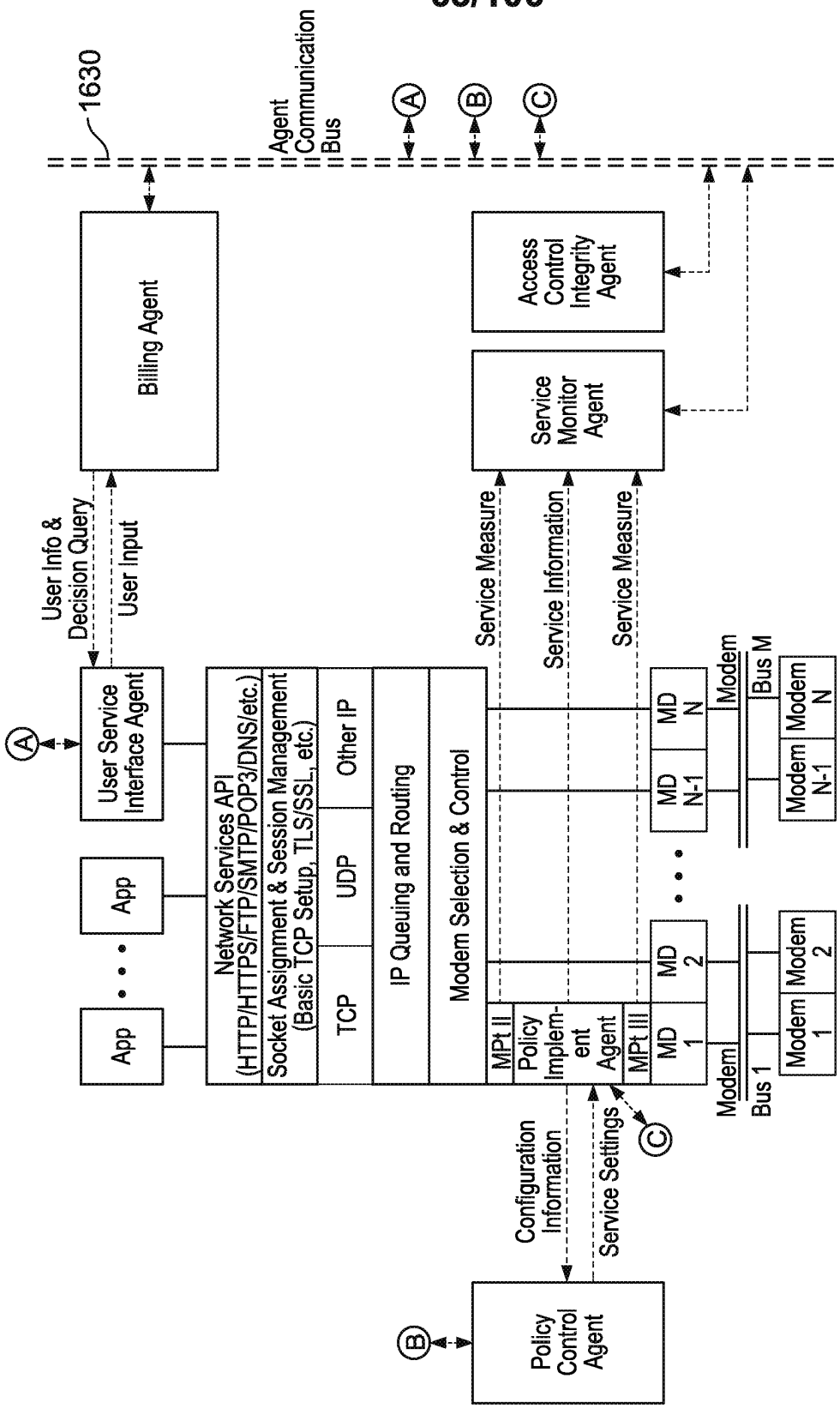

1630
Agent Communication Bus
A
B
C
Billing Agent
Access Control Integrity Agent
Service Monitor Agent
User Info & Decision Query
User Input
Service Measure
Service Information
Service Measure
User Service Interface Agent
App
App
Network Services API (HTTP/HTTPS/FTP/SMTP/POP3/DNS/etc.)
Socket Assignment & Session Management (Basic TCP Setup, TLS/SSL, etc.)
TCP
UDP
Other IP
IP Queuing and Routing
Modem Selection & Control
MPt II
Policy Implem-ent Agent
MPt III
MD 1
MD 2
MD N-1
MD N
Modem
Bus 1
Bus M
Modem 1
Modem 2
Modem N-1
Modem N
Configuration Information
Service Settings
Policy Control Agent

FIG. 34

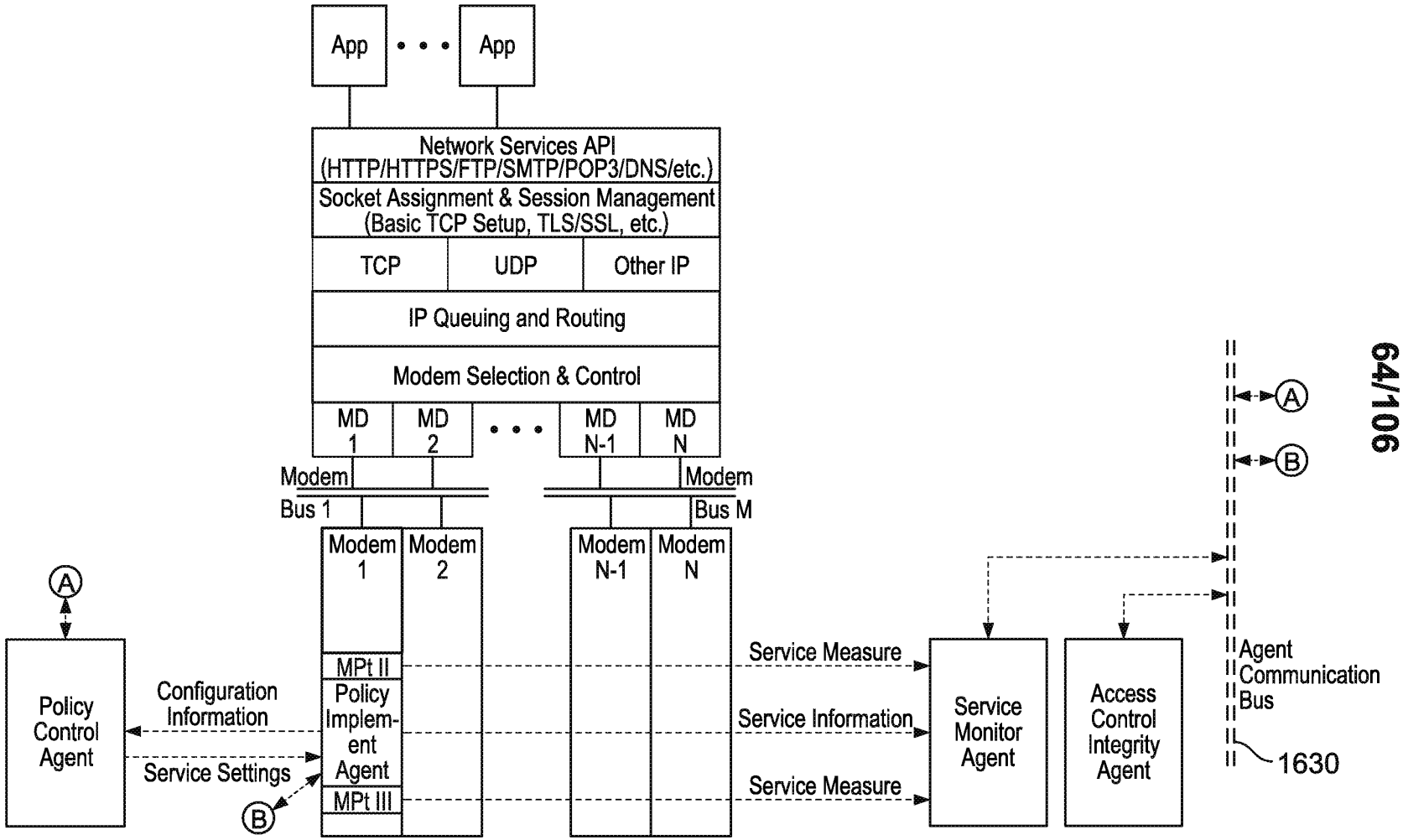

App
App
Network Services API
(HTTP/HTTPS/FTP/SMTP/POP3/DNS/etc.)
Socket Assignment & Session Management
(Basic TCP Setup, TLS/SSL, etc.)
TCP
UDP
Other IP
IP Queuing and Routing
Modem Selection & Control
MD 1
MD 2
MD N-1
MD N
Modem
Bus 1
Modem
Bus M
Modem 1
Modem 2
Modem N-1
Modem N
A
B
Policy Control Agent
Configuration Information
Service Settings
MPt II
Policy Implem-ent Agent
MPt III
Service Measure
Service Information
Service Measure
Service Monitor Agent
Access Control Integrity Agent
Agent Communication Bus
1630
1009

FIG. 35

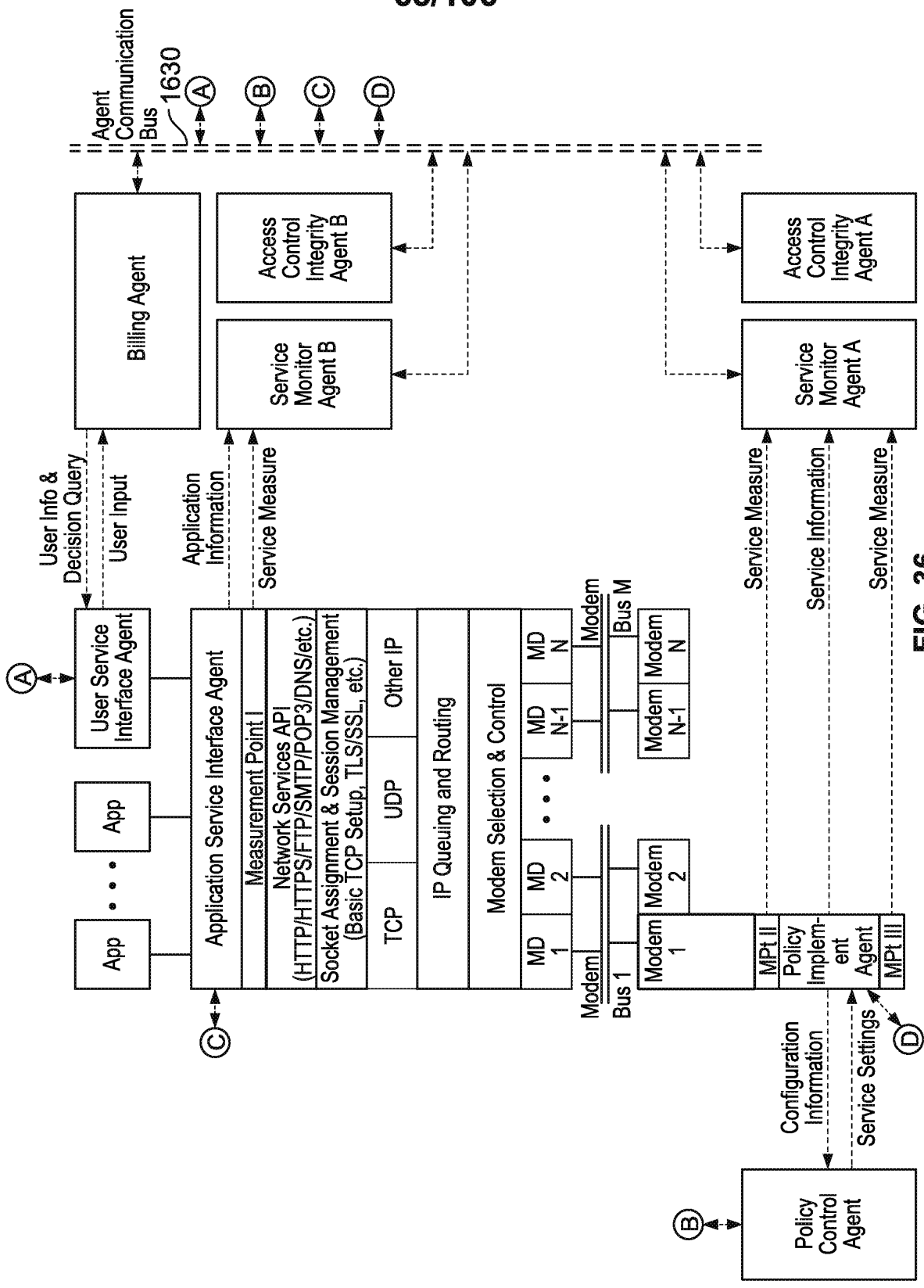

Agent Communication Bus 1630
A
B
C
D
Billing Agent
Access Control Integrity Agent B
Service Monitor Agent B
Access Control Integrity Agent A
Service Monitor Agent A
User Info & Decision Query
User Input
Application Information
Service Measure
Service Measure
Service Information
Service Measure
User Service Interface Agent
App
App
Application Service Interface Agent
Measurement Point I
Network Services API (HTTP/HTTPS/FTP/SMTP/POP3/DNS/etc.)
Socket Assignment & Session Management (Basic TCP Setup, TLS/SSL, etc.)
TCP
UDP
Other IP
IP Queuing and Routing
Modem Selection & Control
MD 1
MD 2
MD N-1
MD N
Modem Bus 1
Modem Bus M
Modem 1
Modem 2
Modem N-1
Modem N
MPt II
Policy Implem-ent Agent
MPt III
Configuration Information
Service Settings
Policy Control Agent

FIG. 36

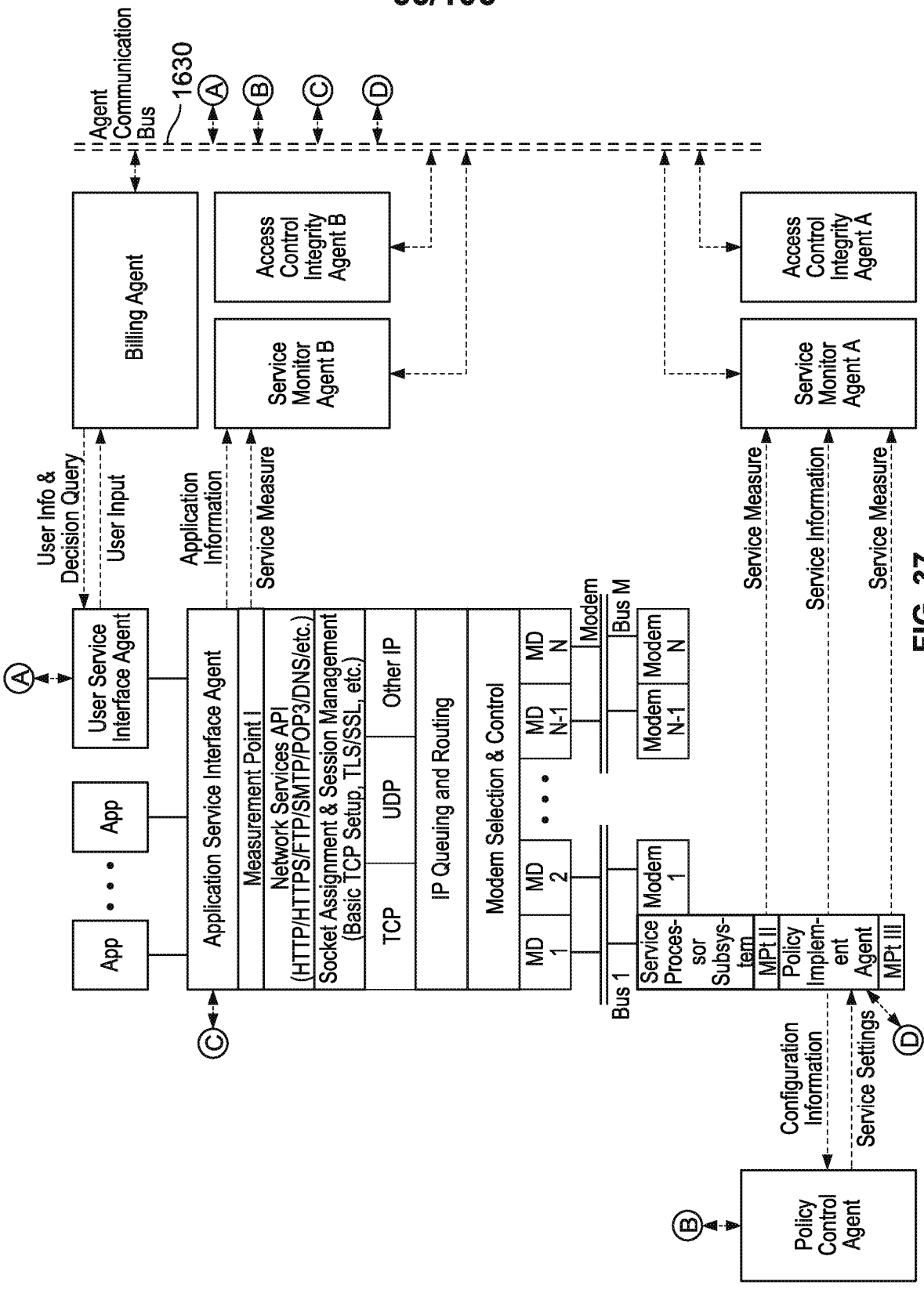

Agent Communication Bus
1630
A
B
C
D
Billing Agent
Access Control Integrity Agent B
Service Monitor Agent B
Access Control Integrity Agent A
Service Monitor Agent A
User Info & Decision Query
User Input
Application Information
Service Measure
Service Measure
Service Information
Service Measure
User Service Interface Agent
App
App
Application Service Interface Agent
Measurement Point I
Network Services API (HTTP/HTTPS/FTP/SMTP/POP3/DNS/etc.)
Socket Assignment & Session Management (Basic TCP Setup, TLS/SSL, etc.)
TCP
UDP
Other IP
IP Queuing and Routing
Modem Selection & Control
MD 1
MD 2
MD N-1
MD N
Modem
Bus 1
Bus M
Service Processor Subsystem
Modem 1
Modem N-1
Modem N
MPt II
Policy Implement Agent
MPt III
Configuration Information
Service Settings
Policy Control Agent

FIG. 37

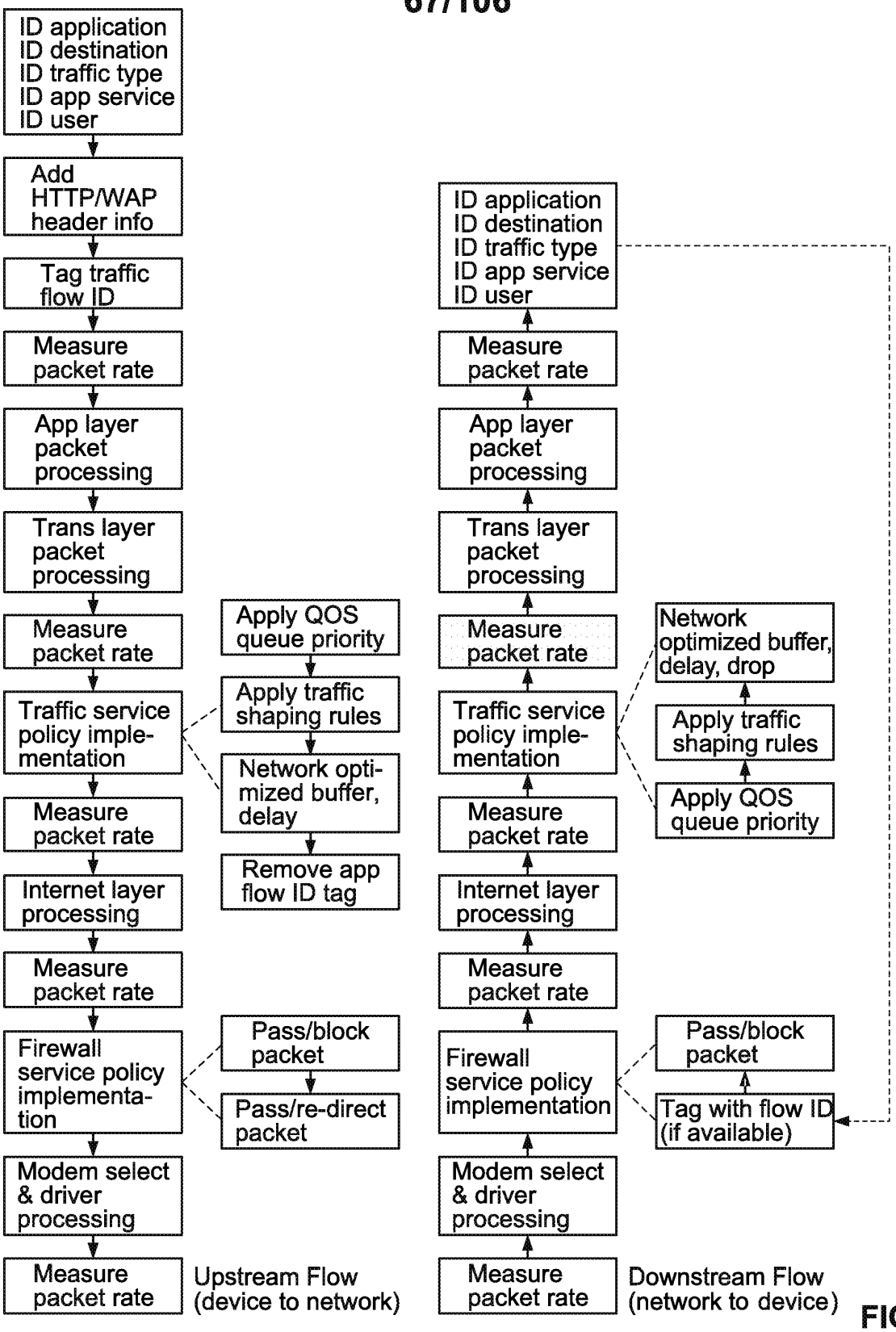

ID application
ID destination
ID traffic type
ID app service
ID user
Add HTTP/WAP header info
Tag traffic flow ID
Measure packet rate
App layer packet processing
Trans layer packet processing
Measure packet rate
Traffic service policy imple-mentation
Apply QOS queue priority
Apply traffic shaping rules
Network opti-mized buffer, delay
Remove app flow ID tag
Measure packet rate
Internet layer processing
Measure packet rate
Firewall service policy implementa-tion
Pass/block packet
Pass/re-direct packet
Modem select & driver processing
Measure packet rate
Upstream Flow (device to network)
ID application
ID destination
ID traffic type
ID app service
ID user
Measure packet rate
App layer packet processing
Trans layer packet processing
Measure packet rate
Traffic service policy imple-mentation
Network optimized buffer, delay, drop
Apply traffic shaping rules
Apply QOS queue priority
Measure packet rate
Internet layer processing
Measure packet rate
Firewall service policy implementation
Pass/block packet
Tag with flow ID (if available)
Modem select & driver processing
Measure packet rate
Downstream Flow (network to device)

FIG. 38

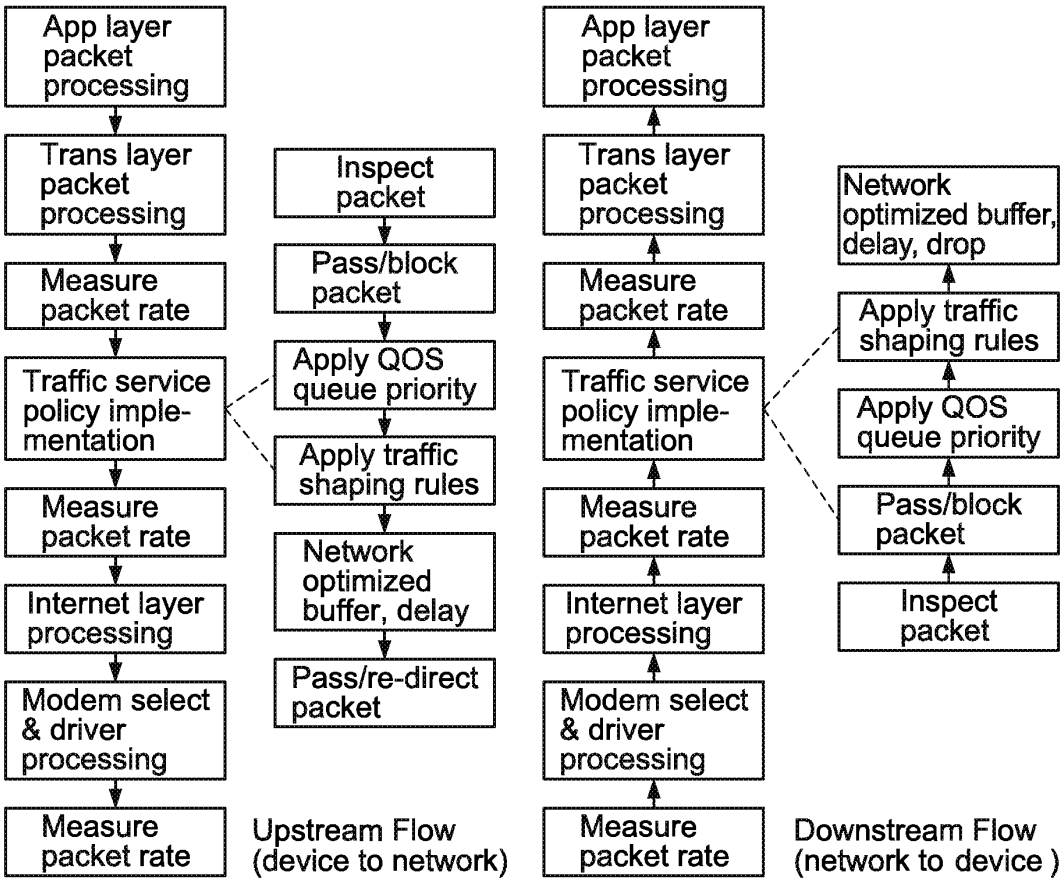

App layer packet processing
Trans layer packet processing
Measure packet rate
Traffic service policy imple-mentation
Measure packet rate
Internet layer processing
Modem select & driver processing
Measure packet rate
Inspect packet
Pass/block packet
Apply QOS queue priority
Apply traffic shaping rules
Network optimized buffer, delay
Pass/re-direct packet
Upstream Flow (device to network)
App layer packet processing
Trans layer packet processing
Measure packet rate
Traffic service policy imple-mentation
Measure packet rate
Internet layer processing
Modem select & driver processing
Measure packet rate
Network optimized buffer, delay, drop
Apply traffic shaping rules
Apply QOS queue priority
Pass/block packet
Inspect packet
Downstream Flow (network to device)

FIG. 39

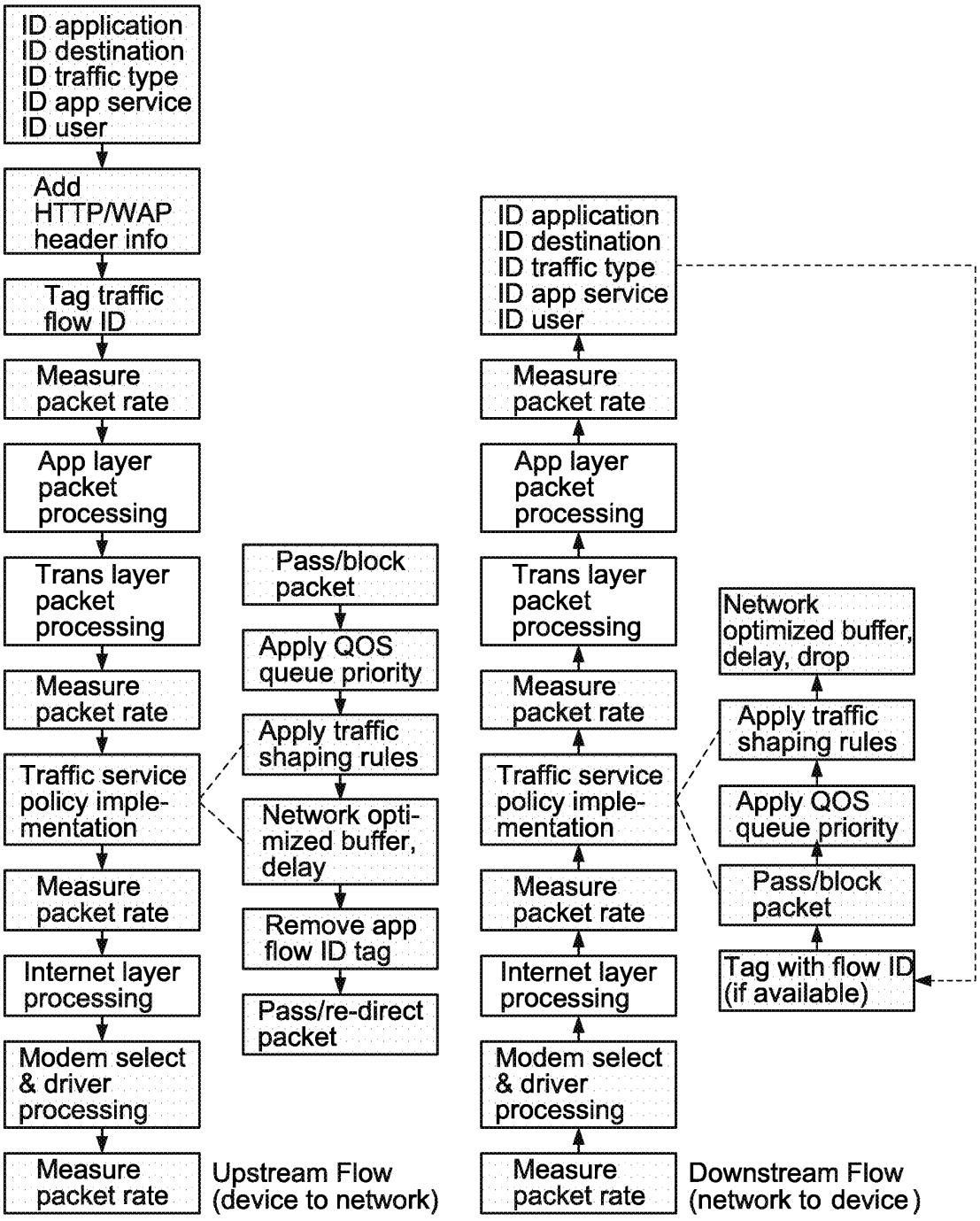

ID application
ID destination
ID traffic type
ID app service
ID user
Add HTTP/WAP header info
Tag traffic flow ID
Measure packet rate
App layer packet processing
Trans layer packet processing
Measure packet rate
Traffic service policy imple-mentation
Measure packet rate
Internet layer processing
Modem select & driver processing
Measure packet rate
Upstream Flow (device to network)
Pass/block packet
Apply QOS queue priority
Apply traffic shaping rules
Network opti-mized buffer, delay
Remove app flow ID tag
Pass/re-direct packet
ID application
ID destination
ID traffic type
ID app service
ID user
Measure packet rate
App layer packet processing
Trans layer packet processing
Measure packet rate
Traffic service policy imple-mentation
Measure packet rate
Internet layer processing
Modem select & driver processing
Measure packet rate
Downstream Flow (network to device)
Network optimized buffer, delay, drop
Apply traffic shaping rules
Apply QOS queue priority
Pass/block packet
Tag with flow ID (if available)

FIG. 40

Example Device CRM Data Collection and Reporting Classification	Partial Description	Example Sensitivity Level Classification	Example Authorization Level to Include in Report
Basic non-specific service usage parameters	User sensitive information is filtered from this report which is used for purposes such as service control, service control integrity monitoring or network traffic analysis.	Low	None
Service billing events or service plan selection events	Documents user selection process from service plan selection or billing options.	Low	Customer authorization with basic service agreement or enterprise agreement
Transaction billing events	Documents user selection process from service plan selection or billing options.	Low	Customer authorization with central billing agreement or enterprise agreement
Device location – customer location based service assist	Reports customer location for the purpose of assisting with location based services such as directions, yellow pages, shopping and social networking.	High	Customer authorization with basic service agreement or enterprise agreement
Device location – device or people tracking	Reports customer location for the purpose of providing tracking services for the device or the user.	High	Customer authorization with separate device tracking service agreement or enterprise agreement
Transaction associated information	Reports customer information such as networking activity, location, advertising usage, shopping behavior that is associated with a commerce transaction or happens around the same time as the transaction.	High	Customer authorization – potential service discount or upgrade or enterprise agreement
URL history	Reports customer web surfing history.	High	Customer authorization – potential service discount or upgrade or enterprise agreement
Served and visited advertisement history	Reports the advertisements served to the user or which advertisements the user responded to. This information may be used to determine customer preferences or for a revenue sharing relationship with the advertisers.	Medium	Customer authorization – potential service discount, perk or upgrade or enterprise agreement
911 Service usage and location trace log	This log contains all information pertinent to emergency service personnel responding to a 911 call or other emergency situation. In some embodiments this information is password protected and generally not available to the service provider unless it happens to also be contained in reports authorized by the consumer as in the examples above.	Very High	Available only for 911 support or enterprise agreement

FIG. 41

1015

Partial List of Example Service Policy Functionality Embodiments	Partial Description of Functionality Example	Example Authorization Level Required to Implement Embodiment
Block Downstream or upstream traffic	Various embodiments block traffic associated with one or more of user, network address identifier, application, content or data type, type of network, central provider, transaction provider, or transaction type. Typical but non-exhaustive examples of command usage are access control prior to authorization, access control policy limits as defined by service plan or special device type, access control for ambient activation services, access control for error handling or access control for tamper prevention. This command may be implemented in instantaneous policy implementation mode or adaptive policy control mode.	Basic authority to pass or block traffic for access control, authorization, ambient services, or plan specific services typically may be provided by the user when they acknowledge the service plan agreement. Authorization to block traffic access as part of controlling user service costs typically may be provided by the service plan agreement options the user chooses to manage cost or may be provided when the user acknowledges the limitations in the UI notifications.
Pass downstream or upstream traffic	Various embodiments allow traffic associated with one or more of user, network address identifier, application, content or data type, type of network, central provider, transaction provider, or transaction type. Typical but non-exhaustive examples of command usage are access control prior to authorization, access control policy limits as defined by service plan or special device type, access control for ambient activation services, access control for error handling or access control for tamper prevention. This command may be implemented in instantaneous policy implementation mode or adaptive policy control mode.	Same as above.
Limit maximum data rate	Various embodiments limit maximum data rate for traffic associated with one or more of user, network address identifier, application, content or data type, type of network, central provider, transaction provider, or transaction type. Typical but non-exhaustive examples of how this command can be implemented include limiting data rate to the device according to service plan; limiting data rate by network address identifier, application or content type for the purpose of implementing a tiered garden; limiting data rate in to different levels according to the type of access technology used by the present network connection; limiting data rate to different levels according to the service provider for the present network; or limiting data rate according to an agreement or lack of agreement with a transaction provider. This command may be implemented in instantaneous policy implementation mode or adaptive policy control mode.	Authorization to limit data rate for all traffic or a subset of traffic typically may be provided in the options the user specifies for how to limit potential or actual service plan usage or cost overages. For example, one user may choose to have no limits and be notified when service usage is over or about to go over, while another user may choose to allow traffic control sufficient to keep service usage under the service plan limit without any notification.

1016

FIG. 42A

Analyze traffic	Provides capability resident on the device to analyze device or user traffic statistics to determine how to implement adaptive policy control or how best to assist the user with notification messages. In some embodiments it is important to perform traffic analysis locally on the device to reduce network chatter with the Control Processor or to maintain user CRM privacy levels by not sharing sensitive raw traffic usage history needed to determine implementation of less sensitive service control policies. Typical but non-exhaustive examples of command usage are analyzing traffic usage statistics or patterns to determine compliance with service plan limits; analyzing traffic usage statistics or patterns to determine likely future compliance with service plan limits; analyzing traffic statistics or patterns to categorize usage according to network address identifiers, applications, content types, network types or central providers; analyzing traffic demand vs. usage statistics or patterns to determine if user may be better served with another service plan; analyzing traffic statistics or patterns to identify potential tamper threats. This command may be implemented in instantaneous policy implementation mode or adaptive policy control mode, but adaptive application of the analysis results is typically associated with adaptive policy control mode.	Authorization to analyze traffic for local device service policy control purposes or 911 service typically may be provided for in the basic service contract. Authorization to transmit a complete or filtered version of the traffic analysis to the Service Controller typically may be provided under user selected options in the service plan contract.
Successive limitation	Provides capability to begin with one limit on access or data rate according to a set of defined service usage trigger criteria, to further limit access or data rate according to said criteria, and then to successively remove limits according to said criteria. In some embodiments this function provides for service usage that starts at a given level for one or more service aspects, but as said service aspect exhibits usage that potentially threatens an overage on service plan limits then the level of service for said service aspect is reduced successively until the threat of service plan overage is reduced or eliminated. In some embodiments, the limits on service level for said service aspect are eventually removed either all at once or successively over a specified time period or set of time periods so that the limits on service level for said service aspect are eventually removed if the service aspect is used less vigorously for a period of time. In this type of embodiment the projection for future service usage by a given service aspect is assisted by the analyze traffic statistics function. As a more specific example, the service aspect may be a URL address that is popular with the user and demands a high service consumption, and the data rate allowed to that URL may start at a relatively high level when the user first begins to surf and as long as the surfing session is finished quickly there is never a reduction in service level, but if the user surfs for a longer time so that service usage begins to threaten plan limit overage, the data rate allowed to that URL is successively reduced the longer the surfing session occurs. Continuing this	Authorization to limit data rate for all traffic or a subset of traffic typically may be provided in the options the user specifies for how to limit potential or actual service plan usage or cost overages. For example, one user may choose to have no limits and be notified when service usage is over or about to go over, while another user may choose to allow traffic control sufficient to keep service usage under the service plan limit without any notification.

FIG. 42B

	example embodiment, if the URL is not visited for a defined period of time then the data rate limitation may be removed in steps over multiple pre-defined time periods, or may be removed all at once back to the initial data rate established in the service policy for that URL. Other specific embodiment examples include email download or upload data rate; download or upload rates for certain types of file transfers; or download or upload rates for a given network access technology or central provider. This command is associated with adaptive policy control mode for the Service Processor. In more advanced adaptive embodiments, the policy control system first identifies those service aspects that are consuming a large percentage of the service usage and then begins to successively limit service level only for these highest usage service aspects so that all other service aspects that are not responsible for potential service plan limit overage continue to receive relatively high service levels. In another embodiment, some high usage service aspects may be exempt or partially exempt from limitations in service level, as for example a service aspect that is associated with a secondary source of service or transaction payment or that may be separately accounted for in the service plan usage reporting.	
Limit email file transfers	Sets and enforces limits on email downloads. In some embodiments this can include use of the successively limit functionality. In some embodiments, this is accomplished by identifying specific email downloads or uploads and controlling traffic for those traffic flows. In other embodiments, this includes interacting with the email application to set download or upload file settings. This functionality may be implemented in instantaneous policy implementation mode or adaptive policy control mode, with the more advanced functionality such as successive limitation on email file transfers being implemented in the adaptive policy control mode.	Authorization to limit data rate for all traffic or a subset of traffic typically may be provided in the options the user specifies for how to limit potential or actual service plan usage or cost overages. For example, one user may choose to have no limits and be notified when service usage is over or about to go over, while another user may choose to allow traffic control sufficient to keep service usage under the service plan limit without any notification.
Seek to manage below service limit	Implements adaptive policy control in an attempt to manage service usage to reduce service plan limit overages. In some embodiments there are successive limits on service level for overall traffic, or for the highest usage service aspects, with the successive limits being lowered until average service usage is projected to be below service plan limits. The algorithms that may be applied to achieve this adaptive service level limitation are quite varied and only a few are given here. In one embodiment, the service usage for the service plan period is projected using the analyze traffic functionality, and overall device data rate is successively limited until service usage is projected to be below the service plan limit. In another	Same as above.

FIG. 42C

	embodiment, the analyze traffic functionality is used to identify those service aspects that are causing the majority of the service plan usage, and then each of those service plan aspects are limited using the successive limitation functionality, with the service level limitations being based on the traffic usage patterns and specific application scenarios for each service aspect. For example, in some embodiments the service aspects that are creating the most service usage are subjected to more service level limitation than service aspects that are creating less service usage. Service usage may be defined as usage of a raw service measurement such as total data consumption, files downloaded or time spent on network, or it may be translated into an economic measure using the lookup service cost functionality. In some embodiments, the period of time elapsed in the service accounting period is taken into account in determining…	
Synchronize service usage counters	Synchronizes service usage counters on device from time to time to minimize service accounting errors between the device data base and the central billing data base. In some embodiments this is a part of the Service Processor heartbeat communication system that need not happen every heartbeat. In some embodiments this occurs with a request for update by the device to the central billing system or to a server function in the Service Processor	Provided for in the basic service agreement.
Lookup service cost	Provides a data base of service usage vs. cost for each type of service offered on the device. Provides for a lookup function of service cost.	Same as above.
Convert service usage to service cost	Uses the service cost vs. usage lookup function to transform one or more service usage aspects to one or more service cost aspect. One example embodiment provides a service cost measure for one specific aspect of service usage, for example total data consumed over a period of time. Another example embodiment provides a total service cost measure for all service usage over a period of time.	Same as above.
Notify user of service overage	Sends a notification message or screen to the UI to inform the user that the one or more aspects of service usage has exceeded the specified limits of one or more service plans. In some embodiments, the user notice is a pop-up window and in some embodiments there is a continuous display on a small gauge in main screen.	Same as above.
Project service usage	Uses the analyze traffic functionality and projects an estimate of what the traffic usage will be at the end of a service plan measurement interval if the service usage does not change. In some embodiments the projected service usage is made based on assuming the average service usage per unit time in the present service plan measurement interval does not change for the remainder of the service plan measurement interval.	Same as above

FIG. 42D

Notify user of service cost overage	Performs a service cost estimate based on one or more aspects of service usage and informs the user that the one or more aspects of service cost has exceeded the specified limits of a service plan. In some embodiments, the user notice is a pop-up window and in some embodiments there is a continuous display on a small gauge in main screen.	Provided for in the basic service agreement.
Notify user of usage behavior likely to run over service usage limit	Uses the project service usage functionality to determine if the service usage is projected to go beyond the service plan limit, notifies the user if the projected usage is over the service plan limit for the service plan measurement interval. In some embodiments, the user notice is a pop-up window and in some embodiments there is a continuous display on a small gauge in main screen. In some embodiments the projected service usage is made based on assuming the average service usage per unit time in the present service plan measurement interval does not change for the remainder of the service plan measurement interval.	Same as above.
Notify user of usage behavior likely to run over cost limit	Uses the project service usage functionality to determine if the service usage is projected to go beyond the service plan limit, uses convert service measure to service cost functionality to estimate the service cost of the projected service overage, notifies the user if the projected cost is over the service plan cost associated with the service plan service limit for the service plan measurement interval. In some embodiments, the user notice is a pop-up window and in some embodiments there is a continuous display on a small gauge in main screen. In some embodiments the projected cost is made based on assuming the average service usage per unit time in the present service plan measurement interval does not change for the remainder of the service plan measurement interval.	Same as above.
Project user service cost if usage behavior continues	Uses the project service usage functionality to determine if the service usage is projected to go beyond the service plan limit, uses convert service measure to service cost functionality to estimate the service cost of the projected service overage, notifies the user of what the projected cost will be if the service usage behavior remains the same. In some embodiments, the user notice is a pop-up window and in some embodiments there is a continuous display on a small gauge in main screen. In some embodiments the projected cost is made based on assuming the average service usage per unit time in the present service plan measurement interval does not change for the remainder of the service plan measurement interval.	Same as above.

1020

FIG. 42E

Limit access likely to cause overage and notify	Uses the project service usage functionality to determine if the service usage is projected to go beyond the service plan limit, if the service usage is projected to go over the service limit, notifies the user that limits are being applied to keep service usage or cost under the service limit, applies limits to various aspects of service usage to bring down usage so that projections are within service limits. In one embodiment, the seek to manage below service limit functionality is used.	Authorization to limit data rate for all traffic or a subset of traffic typically may be provided in the options the user specifies for how to limit potential or actual service plan usage or cost overages. For example, one user may choose to have no limits and be notified when service usage is over or about to go over, while another user may choose to allow traffic control sufficient to keep service usage under the service plan limit without any notification.
Require acknowledgm-ent of notification	Requires the user to acknowledge a notification of potential service or cost overage or a notification of an option to limit the service overage or cost of service overage.	Provided for in the basic service agreement.
Log or report acknowledgm-ent of notification	In some embodiments, the user acknowledgment of notification is stored, or sent to the Service Controller, or stored and later sent to the service Controller.	Same as above.
Notify user of service plan options prior to running over service usage limit	Notifies the user of options to extend the service plan limit before reaching the service plan limit. In some embodiments, accepts user input on which service plan extension option if any the user wishes to accept. In some embodiments, notifies the billing system when the user has accepted a service plan extension option.	Same as above.
Notify user of service plan options after running over service usage limit	Notifies the user of options to extend the service plan limit after reaching the service plan limit. In some embodiments, accepts user input on which service plan extension option if any the user wishes to accept. In some embodiments, notifies the billing system when the user has accepted a service plan extension option.	Same as above.
Time of day variations	Each of the functionalities for traffic control, service cost, service limits may be modified with a time of day variation so that the values used are different for different times of day.	Same as above.

FIG. 42F

Access control enable list	List of service usage activities that are enabled.	Authorization restricted to service controller, VSP or other network function with proper credentials to access the control data base.
Access control block list	List of service usage activities that are blocked.	Same as above.
User service control option UI	Provides the user with a list of options for how they would like to control service usage or service cost.	In some embodiments UI screens and scripts are defined by the UI agent software version and access to modifying this software is restricted to service controller, VSP or other network function with proper credentials to access the UI data base. Some embodiments call for the UI screens or UI screen content to be generated by the service controller, VSP or another network function (e.g. service usage notification gateway or billing system) and in this case access is restricted to service controller, VSP or other network function with proper credentials to access the UI pass through screens.
User service notification option preference	Provides the user with a list of options for how they would like service notification information to be displayed. In some embodiments provides the user with the option to turn off one or more aspects of service notification. In some embodiments the user is not allowed to turn off notification for service usage events that require user decision or acknowledgement.	In some embodiments UI screens and scripts are defined by the UI agent software version and access to modifying this software is restricted to service controller, VSP or other network function with proper credentials to access the UI data base. Some embodiments call for the UI screens or UI screen content to be generated by the service controller, VSP or another network function (e.g. service usage notification gateway or billing system) and in this case access is restricted to service controller, VSP or other network function with proper credentials to access the UI pass through screens.

1022

FIG. 42G

User CRM or service usage monitoring filtering option preference	Filters the device and/or user information that is being collected before it is reported to the network to maintain the desired level of user privacy. In some embodiments the user defines preferences on user privacy that are used to define the filter settings.	In some embodiments this is not accessible by the network and only may be modified by the user. In other embodiments it may be read but not written by the network and in this case authorization is restricted to service controller, VSP or other network function with proper credentials to access the filter settings data base. In some embodiments the network is allowed to change the CRM filter settings and in this case Authorization restricted to service controller, VSP or other network function with proper credentials to access the CRM filter settings data base.
Service usage billing event record	A record of service usage billing events. In some embodiments this record is transmitted to the billing server or another network function to aid service billing or billing reconciliation.	In some embodiments authorization restricted to service controller, VSP or other network function with proper credentials to access the billing data base. In some embodiments the user is allowed to read but not write the data base.
Bill by account	The bill by account embodiments provide for service billing to accounts different than the main user account, for example tracking network device chatter that is not desired to be billed to the user, transaction partner access costs that are shared with or billed to the transaction partner, ambient service cost tracking, tracking temporary account costs, etc.	In some embodiments authorization restricted to service controller, VSP or other network function with proper credentials to access the billing data base. In some embodiments the user is allowed to read but not write the data base.
Central billing transaction and event recording	Billing event tracking and reporting associated with the central provider open billing embodiments. Some embodiments include generation of billing certificates or receipts. In some embodiments the device may serve as a billing feed.	In some embodiments authorization restricted to service controller, VSP or other network function with proper credentials to access the billing data base. In some embodiments the user is allowed to read but not write the data base.
Service owner registration or re-registration	Function that allows a portion of the device credentials to be programmed to indicated the VSP.	In some embodiments authorization to write the device is restricted with security signatures or other security methods to the VSP and possibly the central provider. Some embodiments involve provisions to report to a network function when the VSP settings are changed or the software is uninstalled. Other embodiments involve restoring VSP settings or software if removed.

FIG. 42H

Credentials swap	Function that provides for swapping of credentials, for example temporary credentials to permanent credentials.	Authorization restricted to service controller, VSP or other network function with proper credentials to access the credentials data base.
Account information swap	Function that provides for swapping the account information, for example temporary account to permanent account.	Authorization restricted to service controller, VSP or other network function with proper credentials to access the activation service profile data base.
Configure or re-configure service processor for new device service	Function that provides for service processor programming for all the information that defines the service profile, device credentials, VSP and other necessary parameters.	Authorization restricted to service controller, VSP or other network function with proper credentials to access the service profile data base.
Ambient service profile definition	Function that provides for service processor programming for all the information that defines the ambient service profile, device credentials, VSP and other necessary parameters.	Authorization restricted to service controller, VSP or other network function with proper credentials to access the ambient service profile data base.
Analyze service usage statistics	VSP function to analyzer service usage statistics for a device, defined group of devices, defined group of service plans or service profiles, defined group of users or other groupings.	Authorization typically restricted to service controller, VSP or other network entity with the credentials to access the service usage history data bases.
Dry lab test new service policy	Allows simulated testing of draft service profiles and/or service plans against device usage statistics for a defined group of devices or users or service profiles, or against simulated device service usage behavior. Some embodiments show the estimated profitability of proposed service profile and service plan. Some embodiments allow decomposition of the service usage statistics to identify the user group service usage activities that may be modified by changing the service usage control policies or made more profitable by changing the service plan billing policies.	Authorization typically restricted to service controller, VSP or other network entity with the credentials to access the service usage history data bases.
Beta test publishing system	Function that provides for service processor programming for all the information that defines the service profile device credentials, VSP and other necessary parameters for a beta test device group.	Authorization restricted to service controller, VSP or other network function with proper credentials to access the service profile data base.
Publish new service	Function that provides for service processor programming for all the information that defines the service profile, device credentials, VSP and other necessary parameters for a production device group.	Authorization restricted to service controller, VSP or other network function with proper credentials to access the service profile data base.

1024

FIG. 42I

Roaming selection service	Function that surveys available roaming service partners, looks up the billing rates for the partners, and displays to the user the set of choices and billing rates. In some embodiments the roaming partner billing rates for one or more roaming partners are applied to a typical user service usage scenario for the purpose of estimating possible projected roaming costs and displaying those costs to the user. In some embodiments the roaming data is stored locally on the device and periodically updated with network refreshes, while in other embodiments the data base is looked up at the time of service. In some embodiments, the user is asked if they would like to modify their service usage notification or control profiles to save roaming costs and if the user responds yes they are provided with a set of options for changing service usage notification or service usage control policies.	Authorization to modify the policies typically restricted to the VSP or other entity responsible for managing the roaming service.
Roaming usage count	Provides a service usage estimate to the user while roaming.	Same as above.
Roaming cost service	Provides a service cost estimate to the user while roaming.	Same as above.
Roaming policy control service	Provides the user or VSP with the capability to switch service usage notification or service usage control policies while roaming. Some embodiments provide for restrictions to roaming carrier options. Some embodiments provide policies based on carrier chosen. Some embodiments provide policies based on the service cost for carrier chosen. Some embodiments specify preferred roaming lists that may be different than the central provider roaming list.	Same as above.
Switch policies for new network	Provides the user or VSP with the capability to switch service usage notification or service usage control policies depending on which network the device is connected to. Some embodiments provide for restrictions to certain network options. Some embodiments provide policies based on network chosen. Some embodiments provide policies based on the service cost for network chosen. Some embodiments provide for a network connection preference list.	Authorization to modify the policies typically restricted to the VSP or other entity responsible for managing the network selection policies.

1025

FIG. 42J

Service Processor Authorization

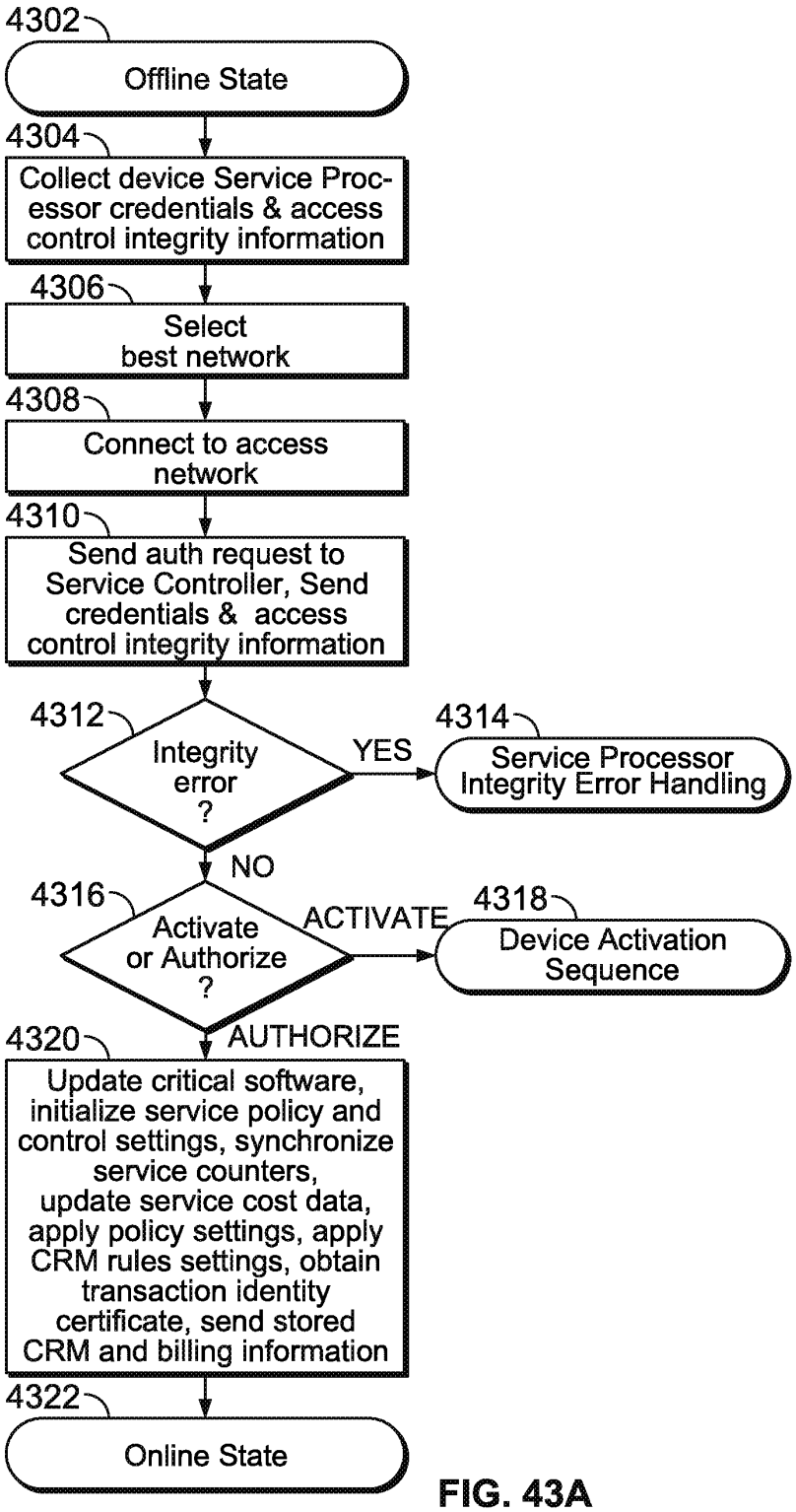


FIG. 43A

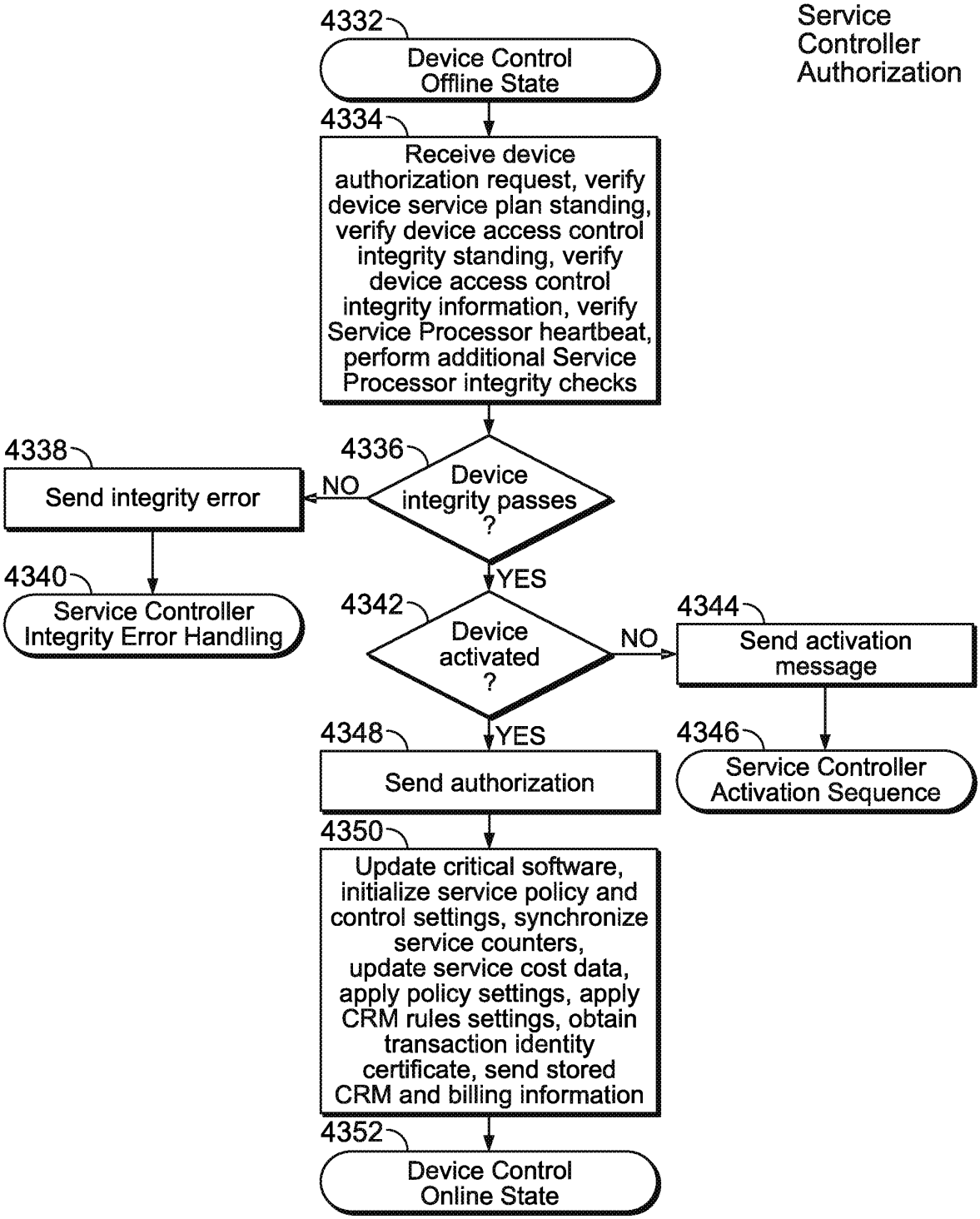

Service Controller Authorization
4332
Device Control Offline State
4334
Receive device authorization request, verify device service plan standing, verify device access control integrity standing, verify device access control integrity information, verify Service Processor heartbeat, perform additional Service Processor integrity checks
4336
Device integrity passes ?
NO
4338
Send integrity error
4340
Service Controller Integrity Error Handling
YES
4342
Device activated ?
NO
4344
Send activation message
4346
Service Controller Activation Sequence
YES
4348
Send authorization
4350
Update critical software, initialize service policy and control settings, synchronize service counters, update service cost data, apply policy settings, apply CRM rules settings, obtain transaction identity certificate, send stored CRM and billing information
4352
Device Control Online State

FIG. 43B

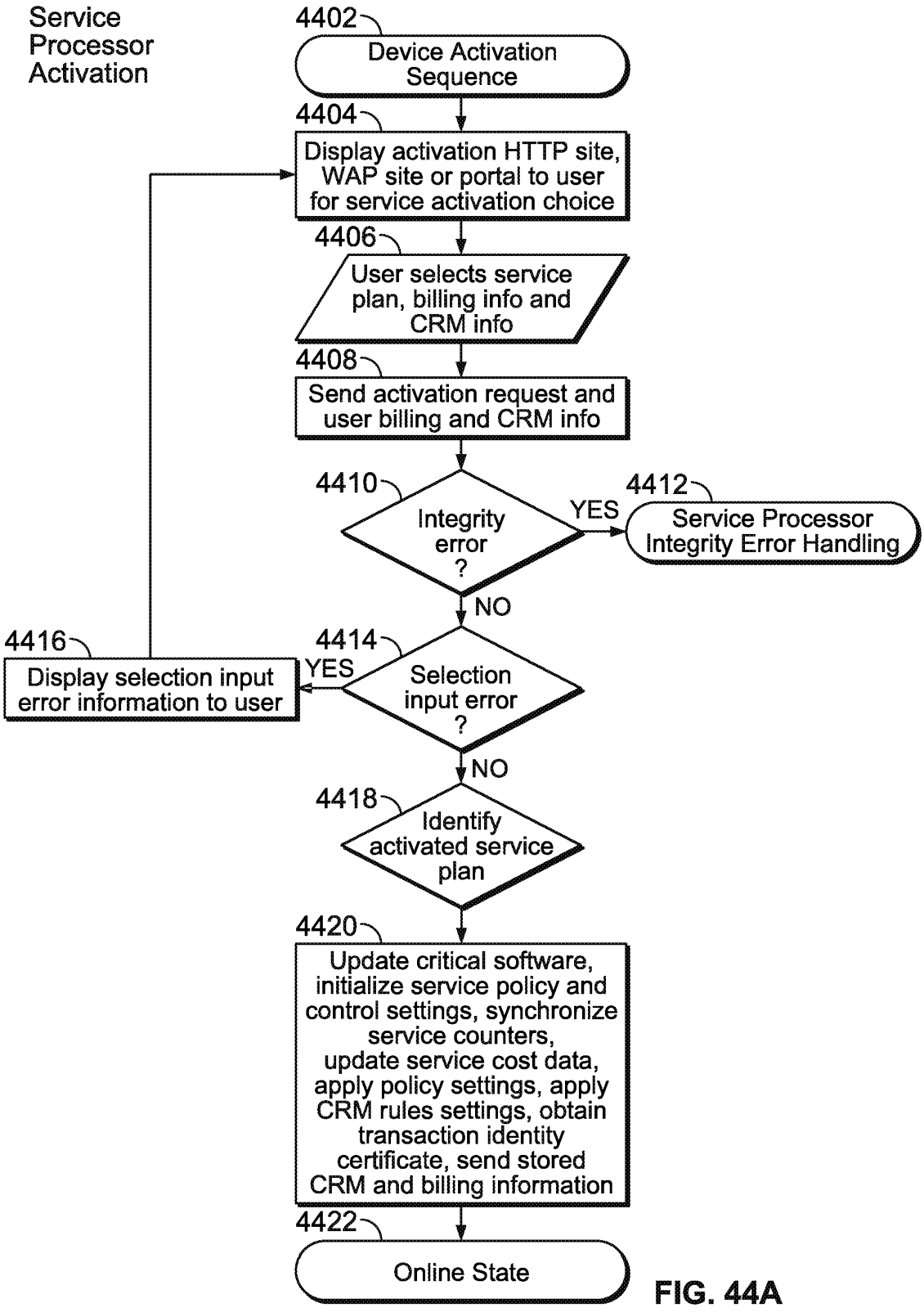

Service Processor Activation
4402
Device Activation Sequence
4404
Display activation HTTP site, WAP site or portal to user for service activation choice
4406
User selects service plan, billing info and CRM info
4408
Send activation request and user billing and CRM info
4410
Integrity error ?
YES
4412
Service Processor Integrity Error Handling
NO
4414
Selection input error ?
YES
4416
Display selection input error information to user
NO
4418
Identify activated service plan
4420
Update critical software, initialize service policy and control settings, synchronize service counters, update service cost data, apply policy settings, apply CRM rules settings, obtain transaction identity certificate, send stored CRM and billing information
4422
Online State

FIG. 44A

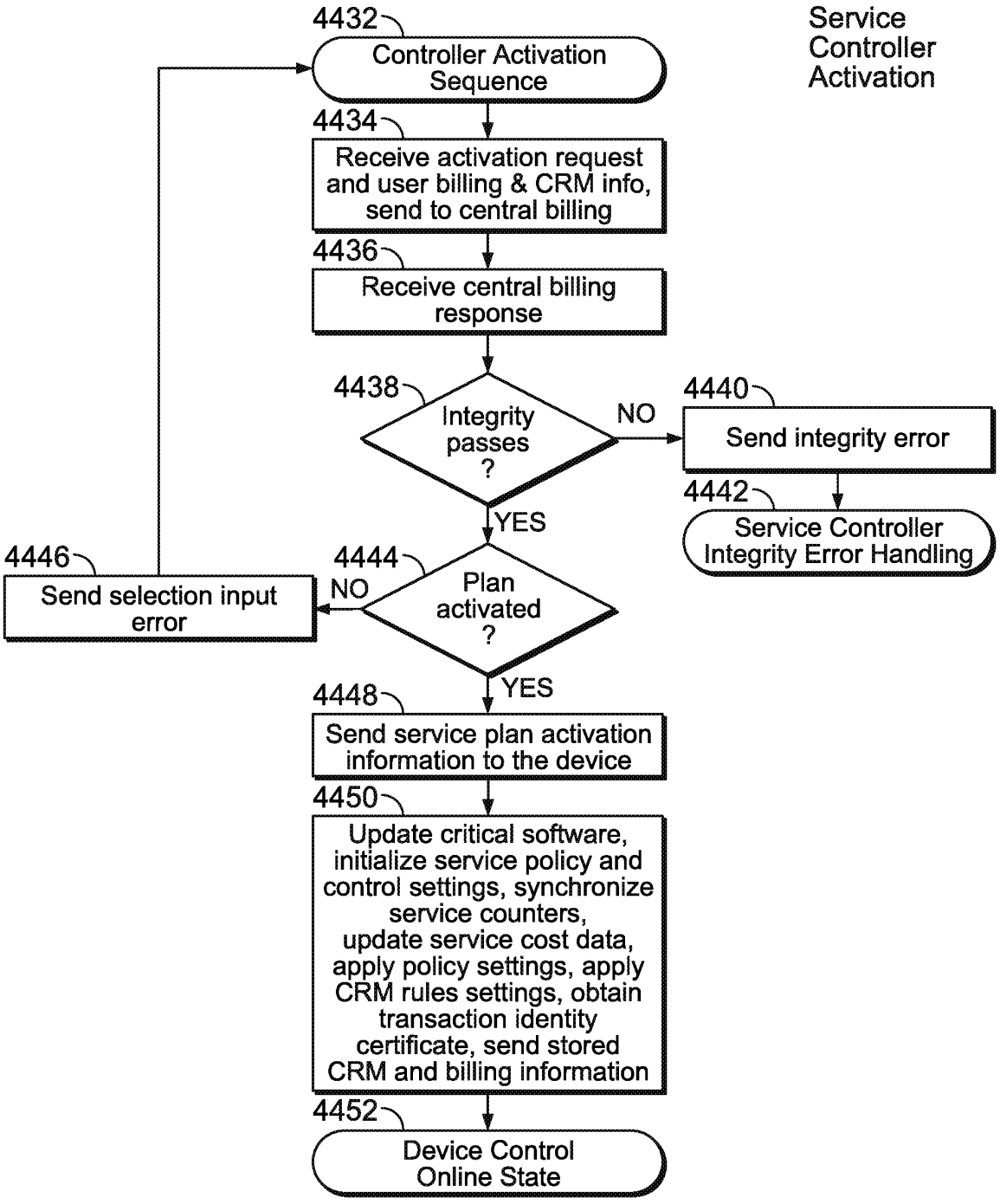

Service Controller Activation
4432
Controller Activation Sequence
4434
Receive activation request and user billing & CRM info, send to central billing
4436
Receive central billing response
4438
Integrity passes ?
NO
4440
Send integrity error
4442
Service Controller Integrity Error Handling
YES
4444
Plan activated ?
NO
4446
Send selection input error
YES
4448
Send service plan activation information to the device
4450
Update critical software, initialize service policy and control settings, synchronize service counters, update service cost data, apply policy settings, apply CRM rules settings, obtain transaction identity certificate, send stored CRM and billing information
4452
Device Control Online State

FIG. 44B

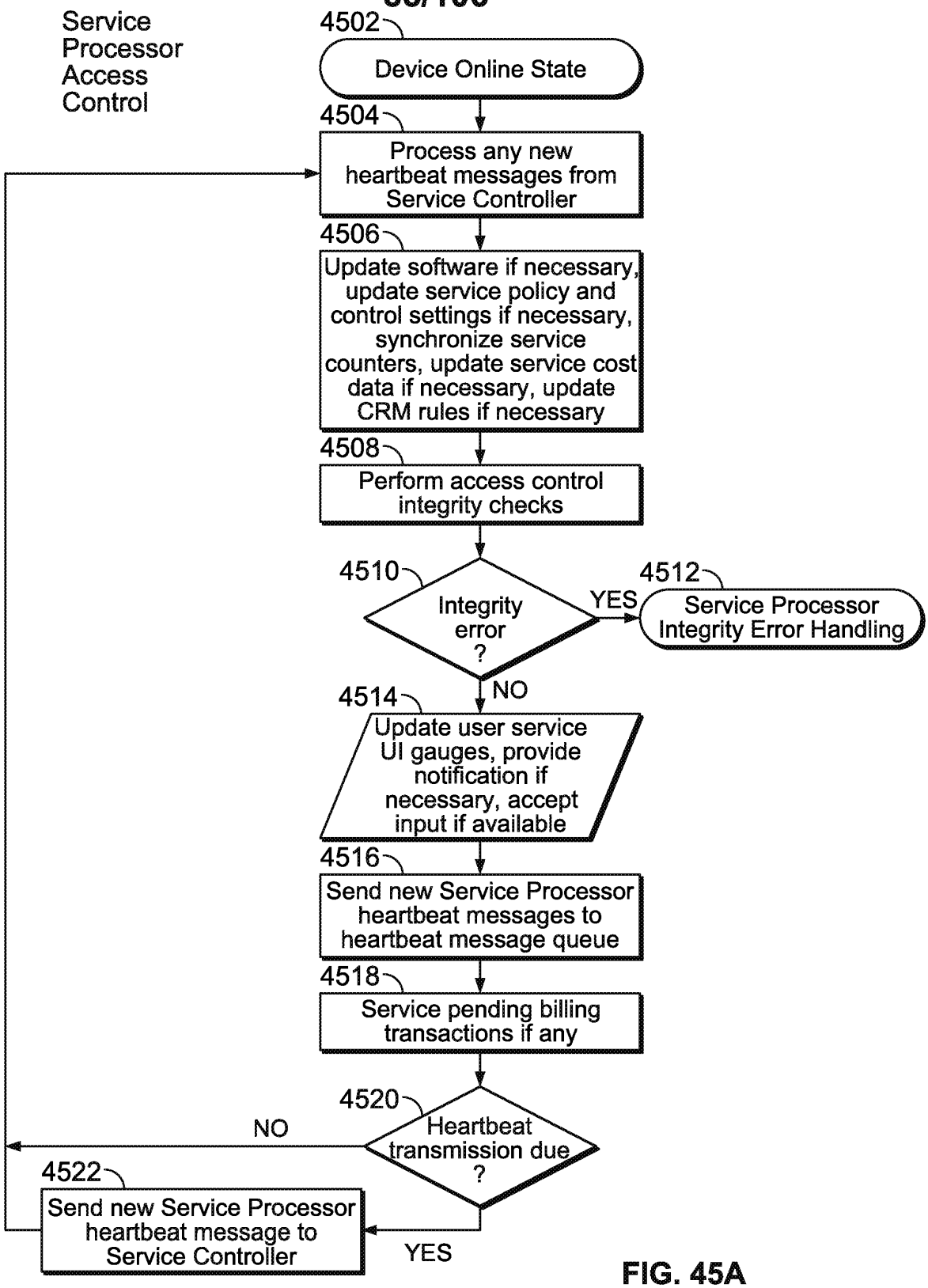

Service Processor Access Control
4502
Device Online State
4504
Process any new heartbeat messages from Service Controller
4506
Update software if necessary, update service policy and control settings if necessary, synchronize service counters, update service cost data if necessary, update CRM rules if necessary
4508
Perform access control integrity checks
4510
Integrity error ?
YES
4512
Service Processor Integrity Error Handling
NO
4514
Update user service UI gauges, provide notification if necessary, accept input if available
4516
Send new Service Processor heartbeat messages to heartbeat message queue
4518
Service pending billing transactions if any
4520
Heartbeat transmission due ?
NO
YES
4522
Send new Service Processor heartbeat message to Service Controller

FIG. 45A

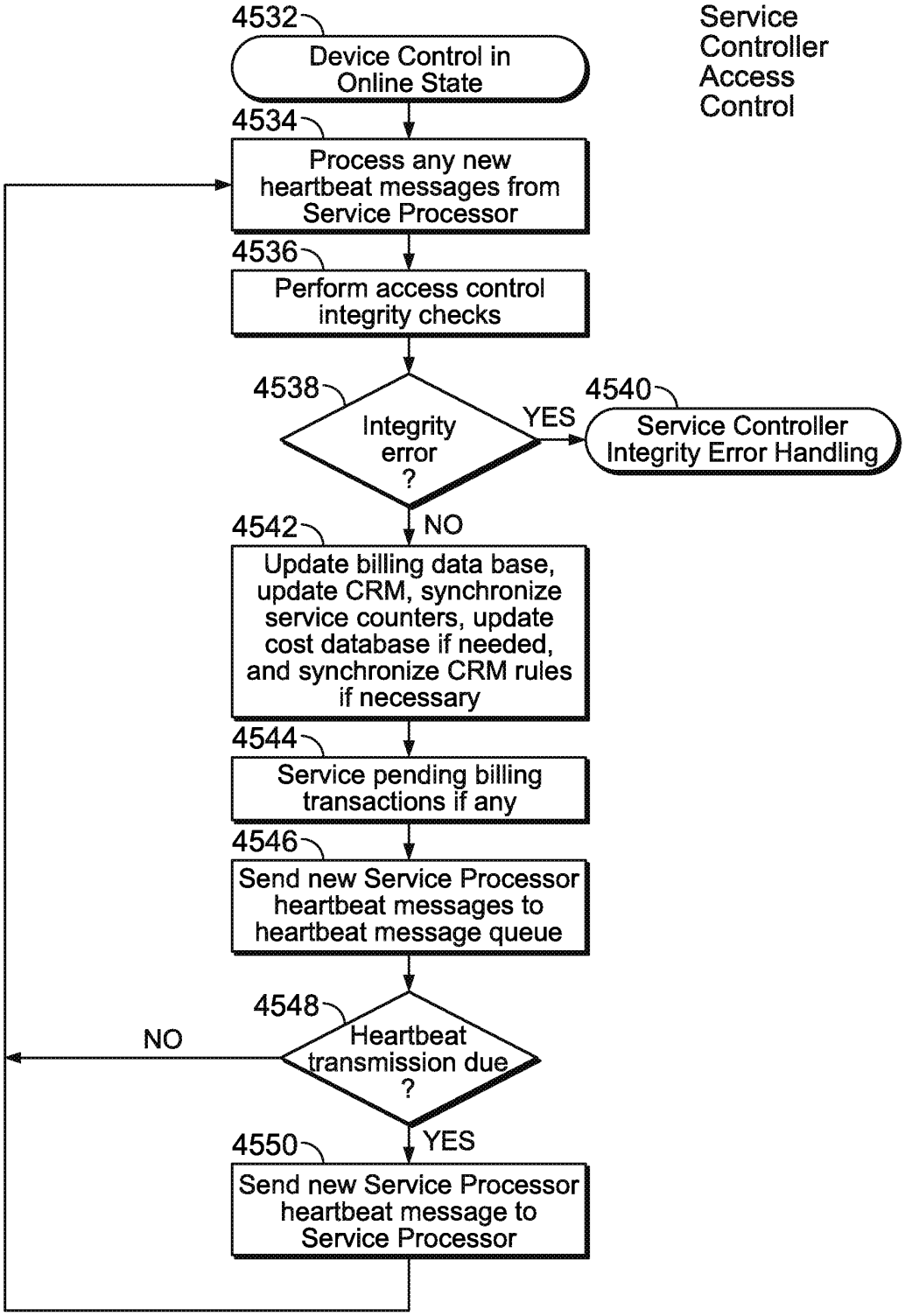

Service Controller Access Control
4532
Device Control in Online State
4534
Process any new heartbeat messages from Service Processor
4536
Perform access control integrity checks
4538
Integrity error ?
YES
4540
Service Controller Integrity Error Handling
NO
4542
Update billing data base, update CRM, synchronize service counters, update cost database if needed, and synchronize CRM rules if necessary
4544
Service pending billing transactions if any
4546
Send new Service Processor heartbeat messages to heartbeat message queue
4548
Heartbeat transmission due ?
NO
YES
4550
Send new Service Processor heartbeat message to Service Processor

FIG. 45B

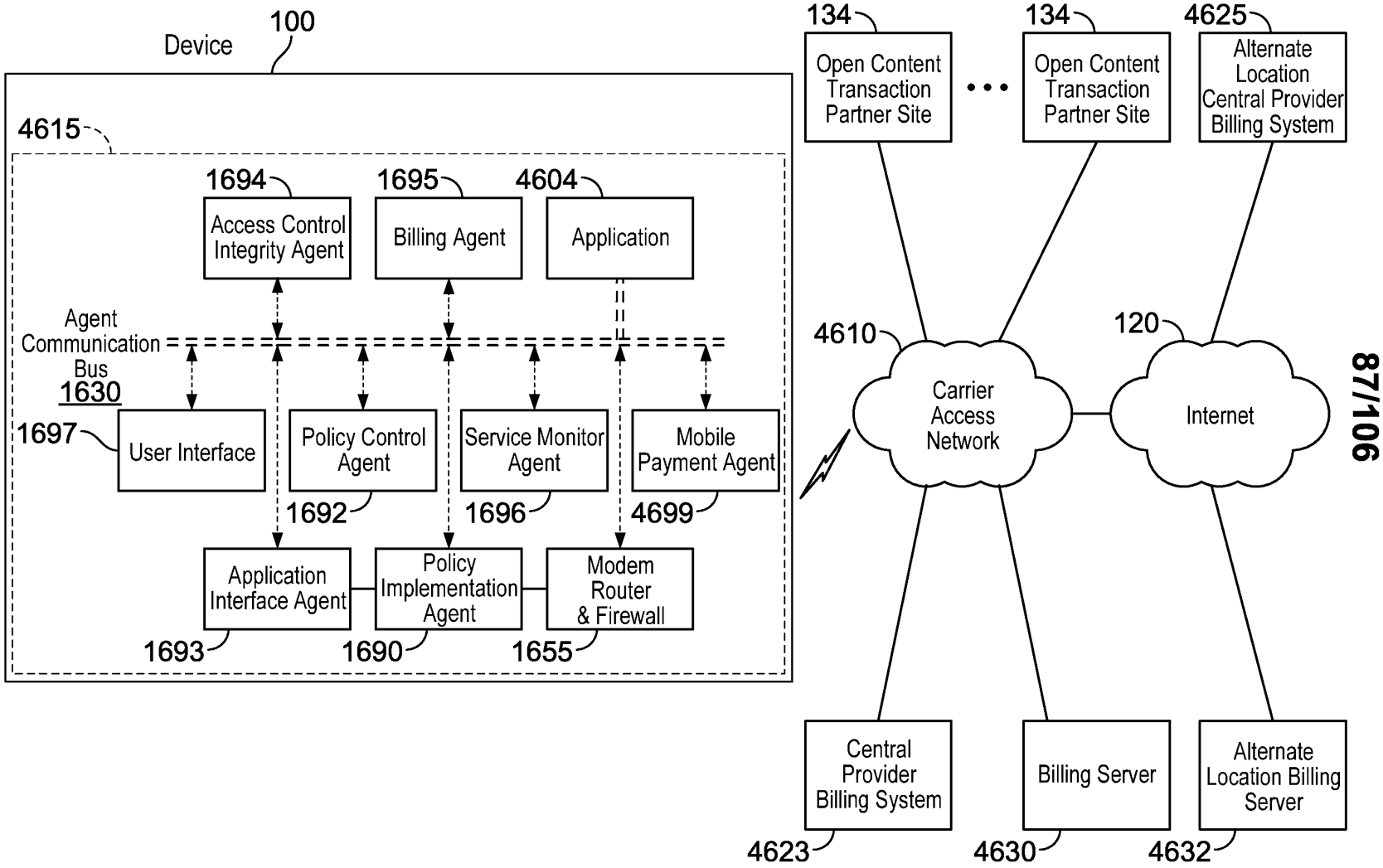

Device
100
4615
1694
Access Control Integrity Agent
1695
Billing Agent
4604
Application
Agent Communication Bus
1630
1697
User Interface
Policy Control Agent
1692
Service Monitor Agent
1696
Mobile Payment Agent
4699
Application Interface Agent
1693
Policy Implementation Agent
1690
Modem Router & Firewall
1655
134
Open Content Transaction Partner Site
134
Open Content Transaction Partner Site
4625
Alternate Location Central Provider Billing System
4610
Carrier Access Network
120
Internet
Central Provider Billing System
4623
Billing Server
4630
Alternate Location Billing Server
4632

FIG. 46

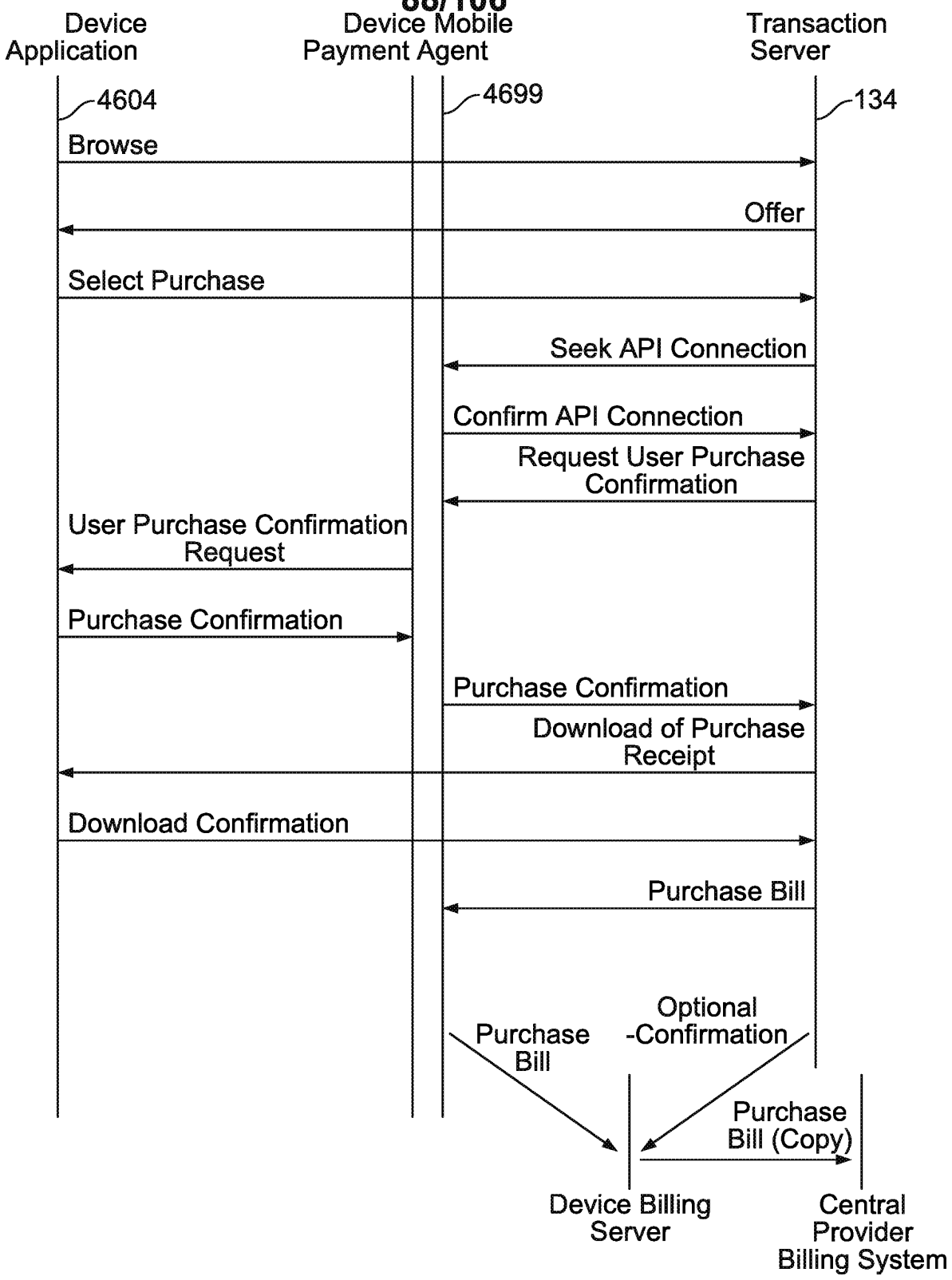

Device Application
Device Mobile Payment Agent
Transaction Server
4604
4699
134
Browse
Offer
Select Purchase
Seek API Connection
Confirm API Connection
Request User Purchase Confirmation
User Purchase Confirmation Request
Purchase Confirmation
Purchase Confirmation
Download of Purchase Receipt
Download Confirmation
Purchase Bill
Optional -Confirmation
Purchase Bill
Purchase Bill (Copy)
Device Billing Server
Central Provider Billing System

FIG. 47A

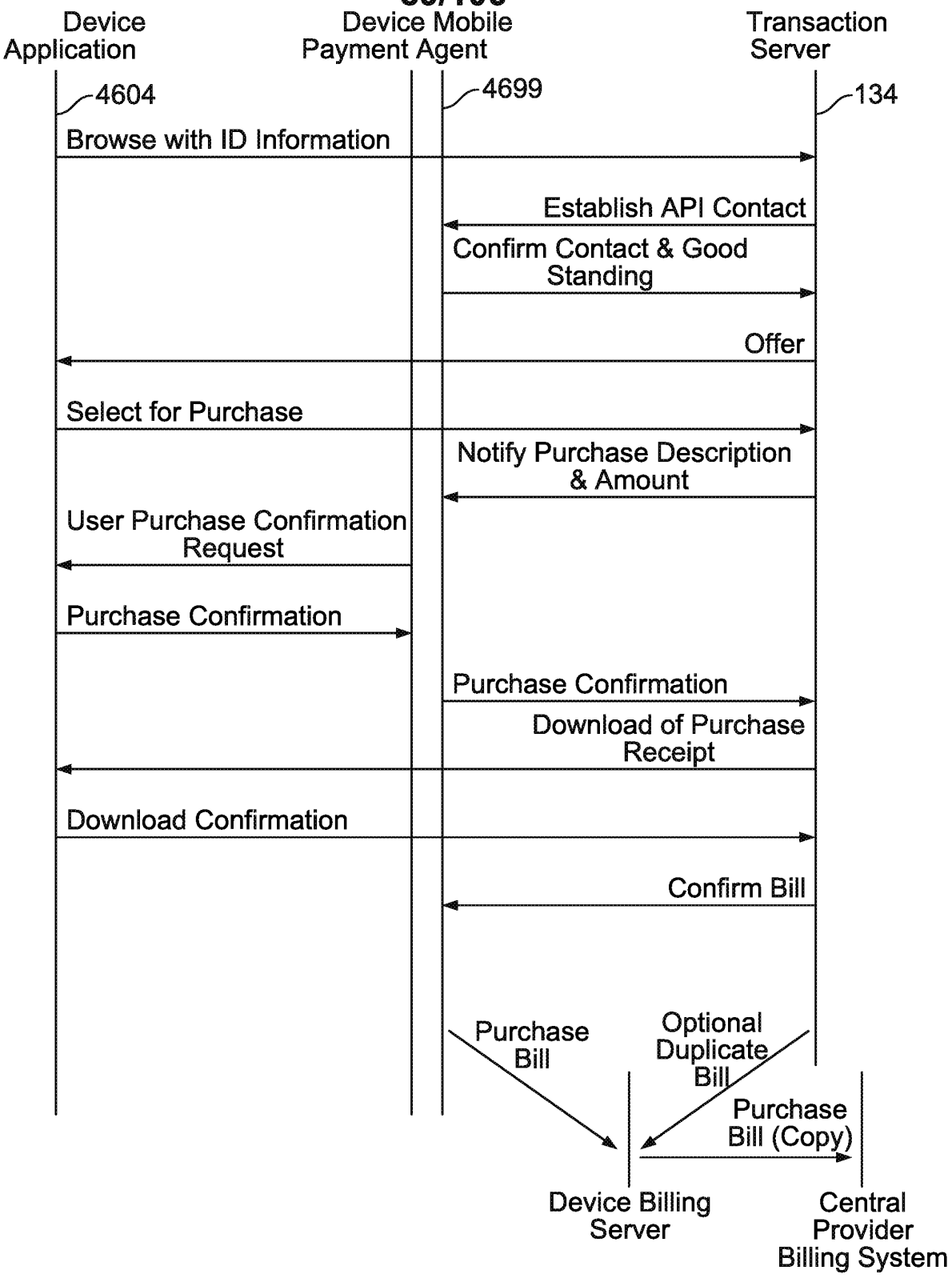

Device Application
Device Mobile Payment Agent
Transaction Server
4604
4699
134
Browse with ID Information
Establish API Contact
Confirm Contact & Good Standing
Offer
Select for Purchase
Notify Purchase Description & Amount
User Purchase Confirmation Request
Purchase Confirmation
Purchase Confirmation
Download of Purchase Receipt
Download Confirmation
Confirm Bill
Purchase Bill
Optional Duplicate Bill
Purchase Bill (Copy)
Device Billing Server
Central Provider Billing System

FIG. 47B

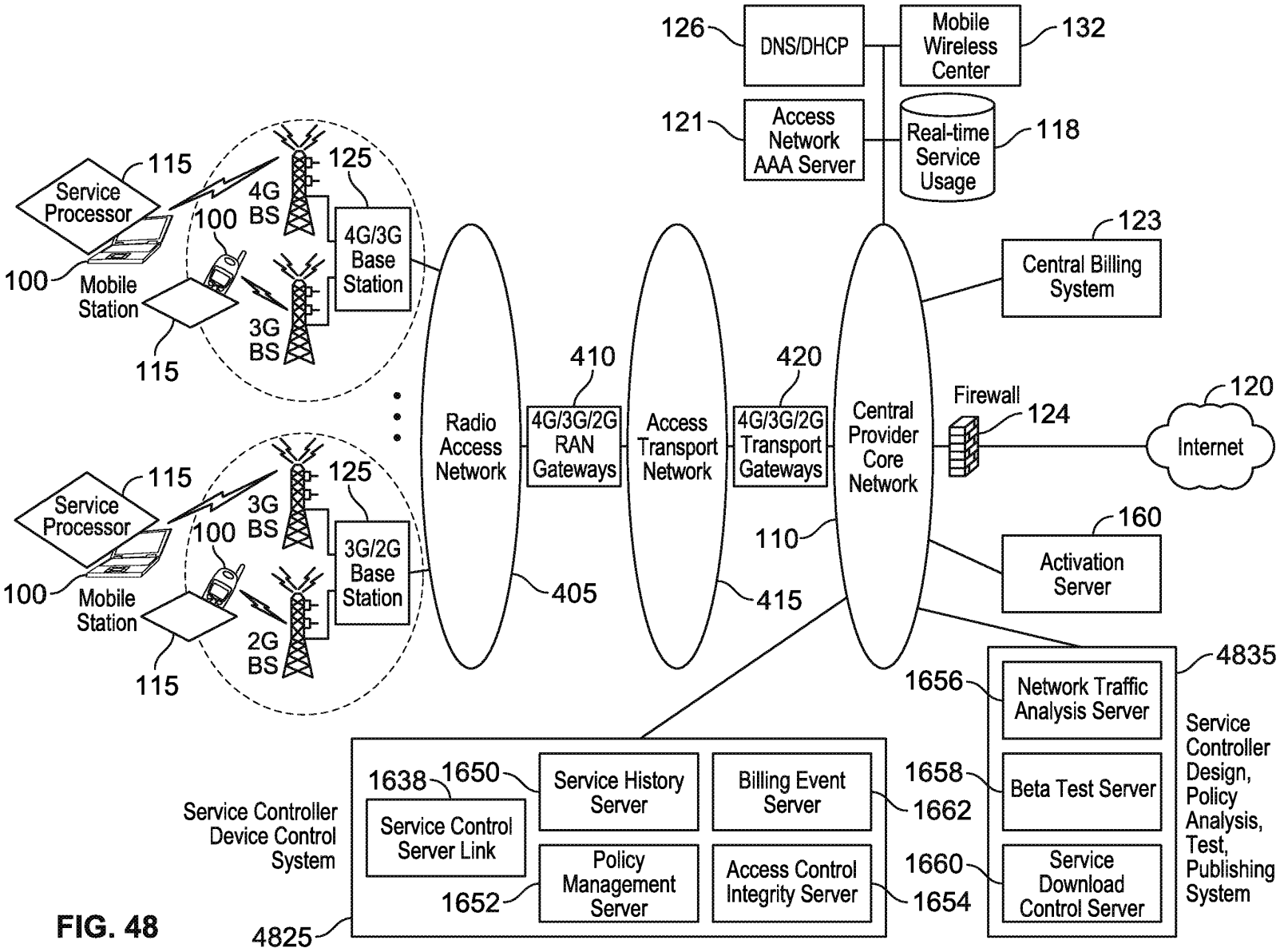


FIG. 48

1035

90/106

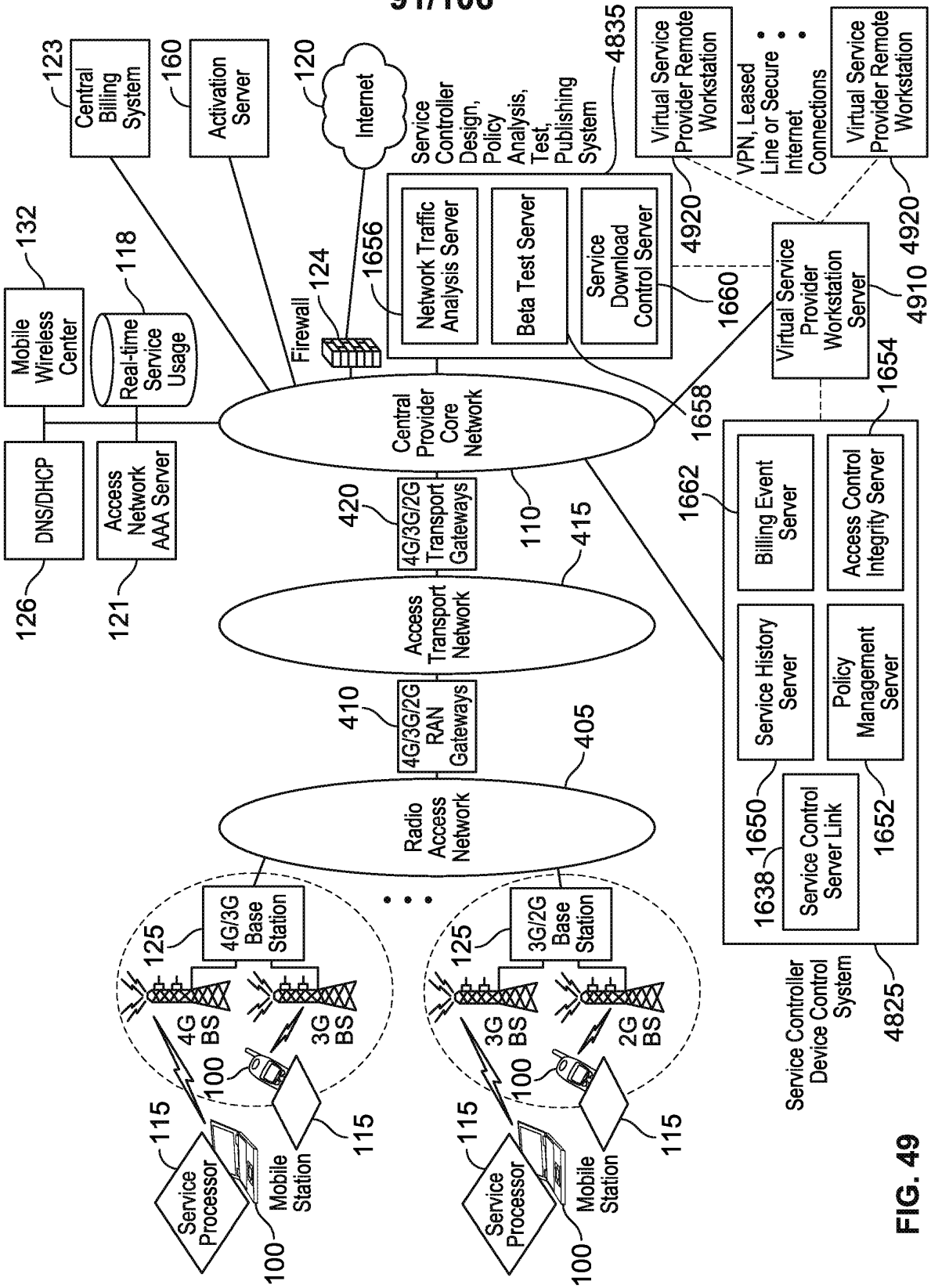

Central Billing System
123
Activation Server
160
Internet
120
Service Controller Design, Policy Analysis, Test, Publishing System
4835
Virtual Service Provider Remote Workstation
VPN, Leased Line or Secure Internet Connections
Virtual Service Provider Remote Workstation
Mobile Wireless Center
132
Real-time Service Usage
118
Firewall
124
1656
Network Traffic Analysis Server
Beta Test Server
Service Download Control Server
4920
1660
Virtual Service Provider Workstation Server
4910
4920
Central Provider Core Network
1658
1654
DNS/DHCP
126
Access Network AAA Server
121
420
4G/3G/2G Transport Gateways
110
415
Billing Event Server
1662
Access Control Integrity Server
Access Transport Network
Service History Server
Policy Management Server
410
4G/3G/2G RAN Gateways
405
Radio Access Network
1650
1638
Service Control Server Link
1652
Service Controller Device Control System
4825
125
4G/3G Base Station
125
3G/2G Base Station
4G BS
3G BS
3G BS
2G BS
100
115
Service Processor
Mobile Station

FIG. 49

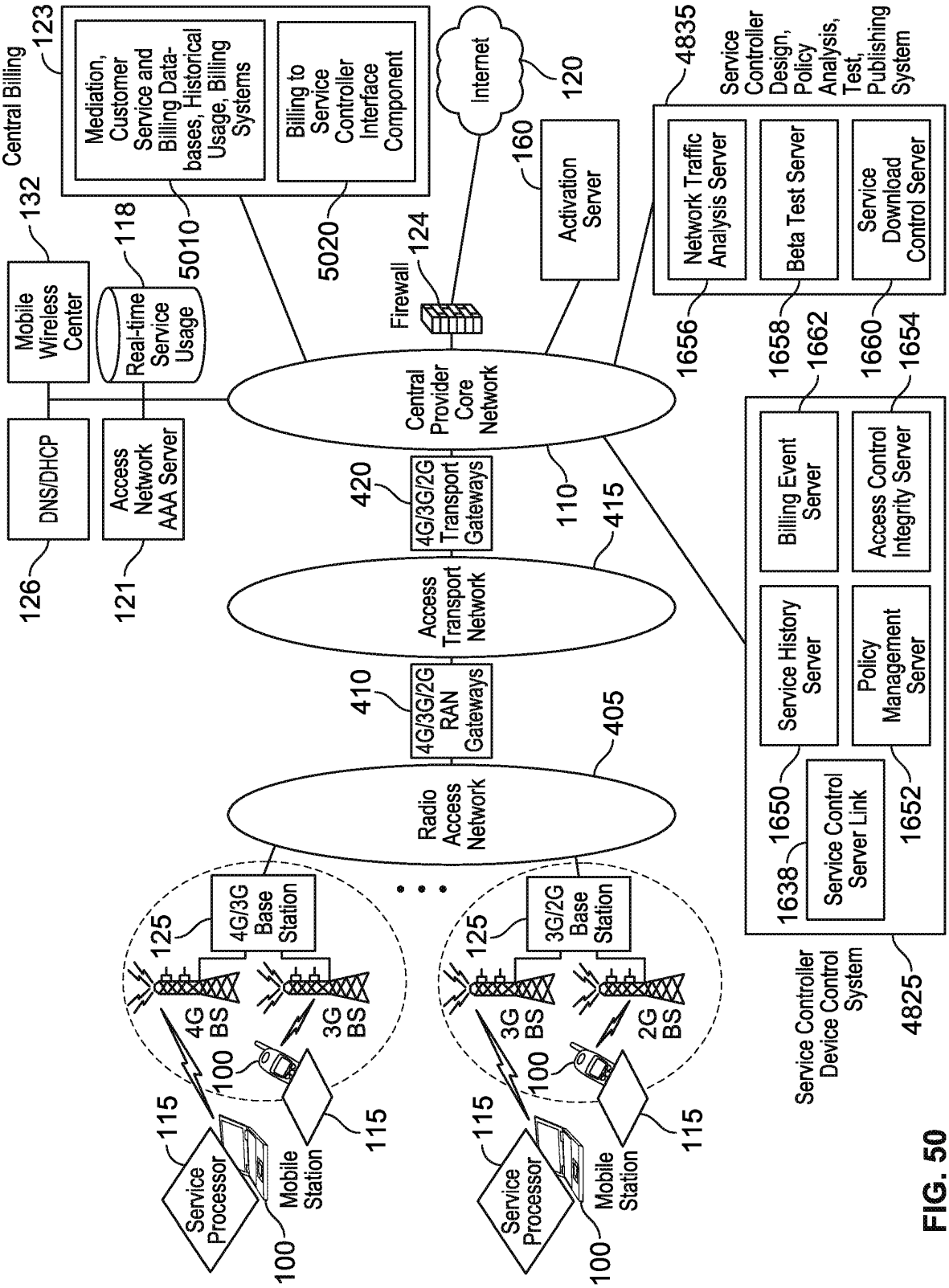

Central Billing
123
Mediation, Customer Service and Billing Data-bases, Historical Usage, Billing Systems
Billing to Service Controller Interface Component
5010
5020
Internet
120
4835
Service Controller Design, Policy Analysis, Test, Publishing System
Mobile Wireless Center
132
Real-time Service Usage
118
Firewall
124
Activation Server
160
Network Traffic Analysis Server
Beta Test Server
Service Download Control Server
1656
1658
1662
1660
1654
DNS/DHCP
126
Access Network AAA Server
121
Central Provider Core Network
110
420
4G/3G/2G Transport Gateways
415
Access Transport Network
410
4G/3G/2G RAN Gateways
405
Radio Access Network
Billing Event Server
Access Control Integrity Server
Service History Server
Policy Management Server
Service Control Server Link
1650
1638
1652
Service Controller Device Control System
4825
4G/3G Base Station
3G/2G Base Station
125
4G BS
3G BS
3G BS
2G BS
100
115
Service Processor
Mobile Station

FIG. 50

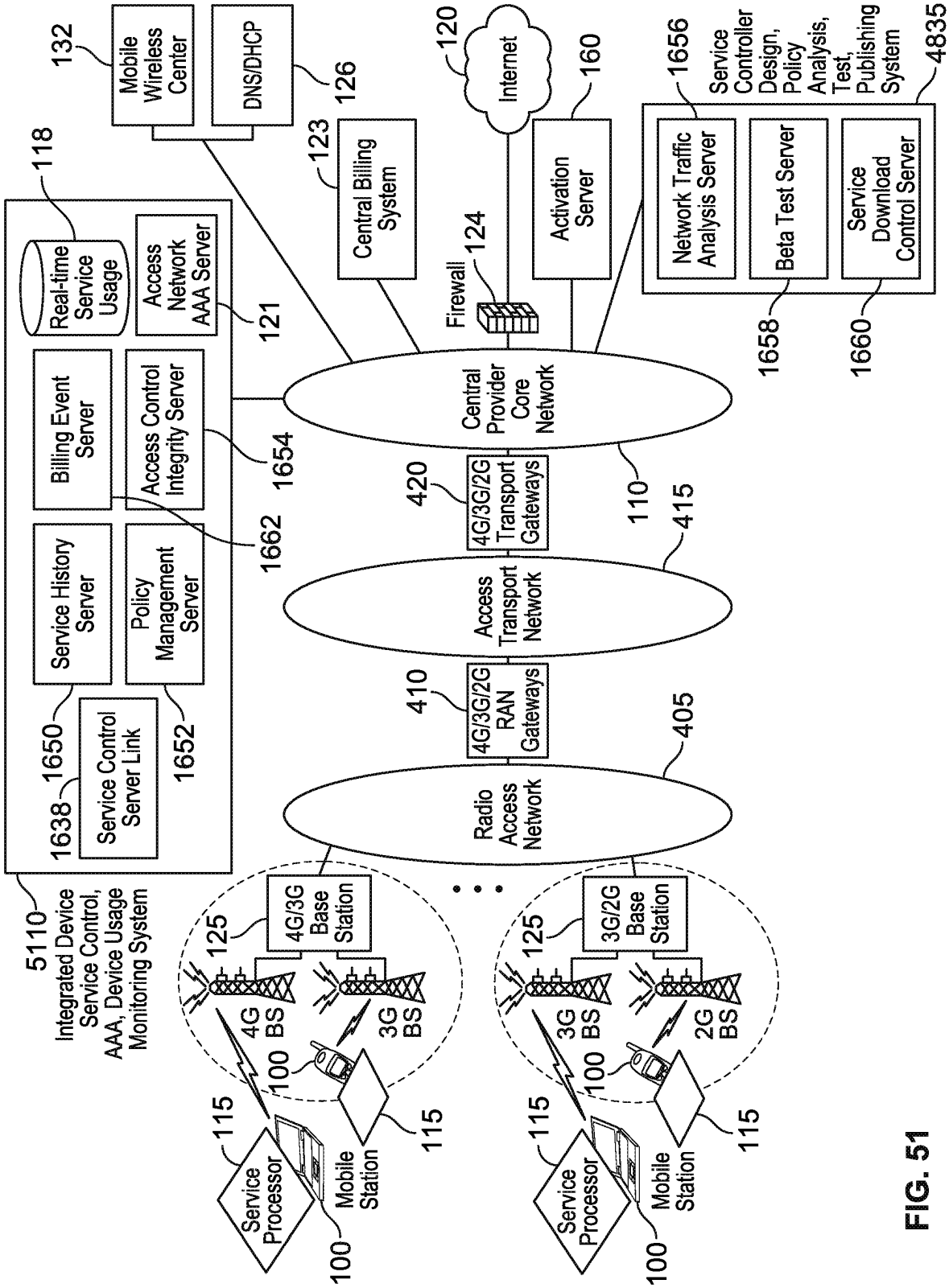

5110
Integrated Device Service Control, AAA, Device Usage Monitoring System
118
Real-time Service Usage
Access Network AAA Server
121
Billing Event Server
Access Control Integrity Server
1654
Service History Server
Policy Management Server
1662
1650
1652
1638
Service Control Server Link
132
Mobile Wireless Center
DNS/DHCP
126
123
Central Billing System
120
Internet
160
Activation Server
124
Firewall
1656
Service Controller Design, Policy Analysis, Test, Publishing System
4835
Network Traffic Analysis Server
Beta Test Server
Service Download Control Server
1658
1660
Central Provider Core Network
110
420
4G/3G/2G Transport Gateways
415
Access Transport Network
410
4G/3G/2G RAN Gateways
405
Radio Access Network
125
4G/3G Base Station
3G/2G Base Station
4G BS
3G BS
3G BS
2G BS
100
115
Service Processor
Mobile Station

FIG. 51

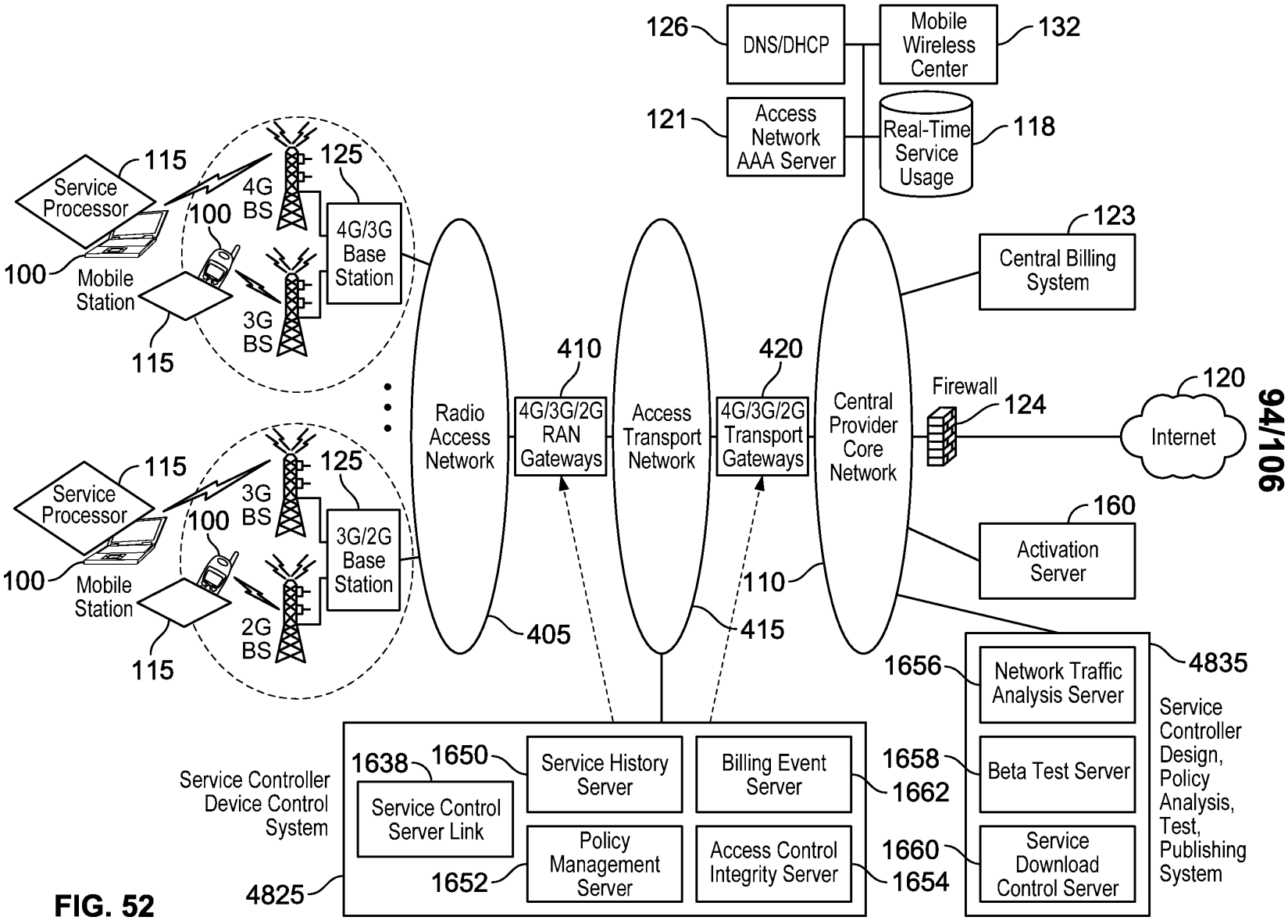

126
DNS/DHCP
Mobile Wireless Center
132
121
Access Network AAA Server
Real-Time Service Usage
118
123
Central Billing System
115
Service Processor
100
Mobile Station
4G BS
125
4G/3G Base Station
3G BS
410
420
Radio Access Network
4G/3G/2G RAN Gateways
Access Transport Network
4G/3G/2G Transport Gateways
Central Provider Core Network
Firewall
124
120
Internet
94/106
3G BS
3G/2G Base Station
2G BS
160
Activation Server
110
405
415
4835
1656
Network Traffic Analysis Server
Service Controller Design, Policy Analysis, Test, Publishing System
1658
Beta Test Server
1660
Service Download Control Server
1654
1662
1638
1650
Service Control Server Link
Service History Server
Billing Event Server
Service Controller Device Control System
1652
Policy Management Server
Access Control Integrity Server
4825

FIG. 52

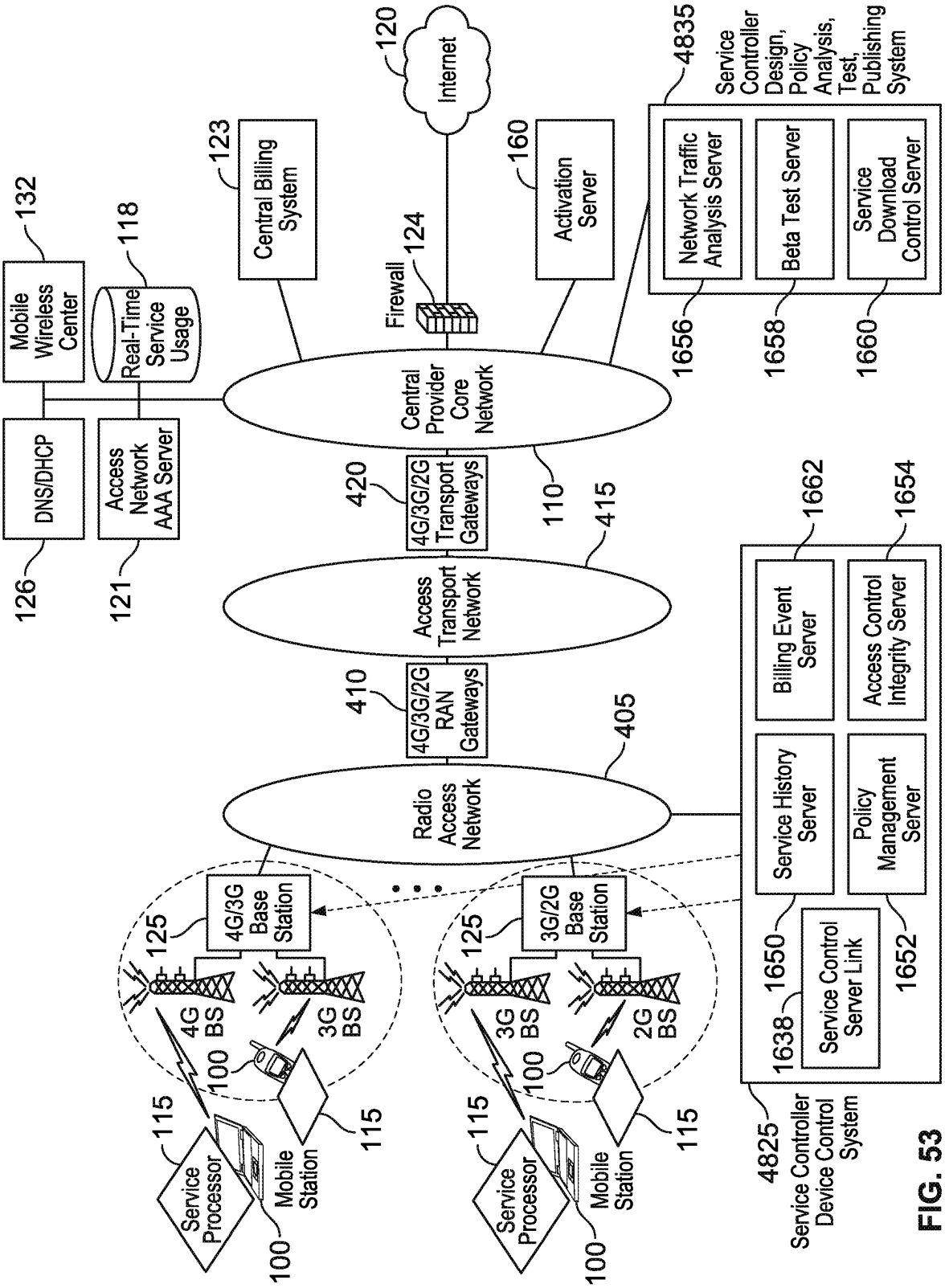

Mobile Wireless Center
132
Real-Time Service Usage
118
Central Billing System
123
Internet
120
Firewall
124
Activation Server
160
Service Controller Design, Policy Analysis, Test, Publishing System
4835
Network Traffic Analysis Server
Beta Test Server
Service Download Control Server
1656
1658
1660
DNS/DHCP
126
Access Network AAA Server
121
Central Provider Core Network
110
4G/3G/2G Transport Gateways
420
Access Transport Network
415
4G/3G/2G RAN Gateways
410
Radio Access Network
405
Billing Event Server
1662
Access Control Integrity Server
1654
Service History Server
Policy Management Server
Service Control Server Link
1650
1652
1638
4825
Service Controller Device Control System
4G/3G Base Station
3G/2G Base Station
125
4G BS
3G BS
3G BS
2G BS
100
115
Service Processor
Mobile Station

FIG. 53

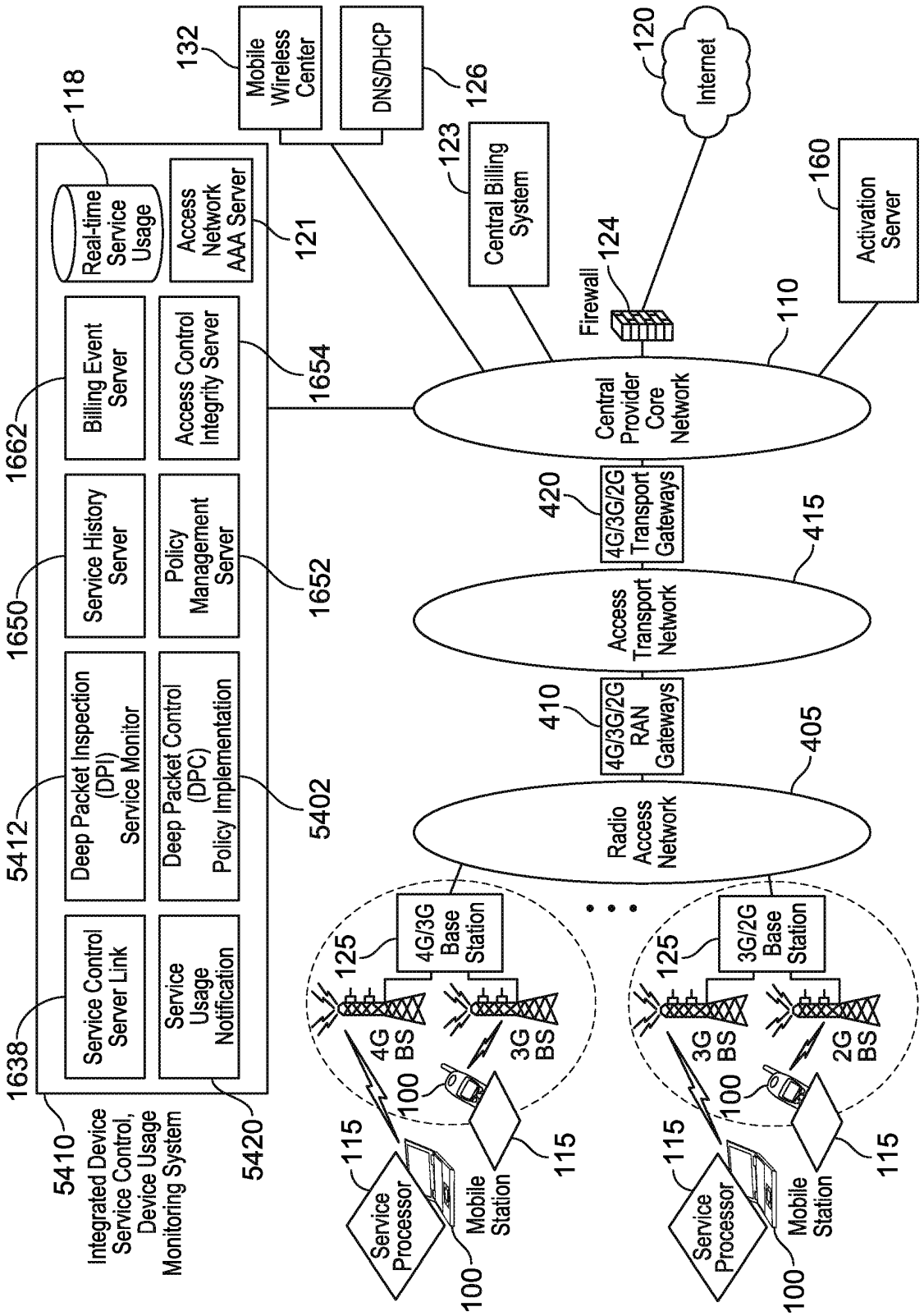

5410
Integrated Device Service Control, Device Usage Monitoring System
1638
Service Control Server Link
Service Usage Notification
5412
Deep Packet Inspection (DPI) Service Monitor
Deep Packet Control (DPC) Policy Implementation
5402
5420
1650
Service History Server
Policy Management Server
1652
1662
Billing Event Server
Access Control Integrity Server
1654
118
Real-time Service Usage
Access Network AAA Server
121
132
Mobile Wireless Center
DNS/DHCP
126
123
Central Billing System
Firewall
124
120
Internet
160
Activation Server
110
Central Provider Core Network
420
4G/3G/2G Transport Gateways
415
Access Transport Network
410
4G/3G/2G RAN Gateways
405
Radio Access Network
125
4G/3G Base Station
4G BS
3G BS
100
115
Service Processor
Mobile Station
125
3G/2G Base Station
3G BS
2G BS
100
115
Service Processor
Mobile Station

FIG. 54

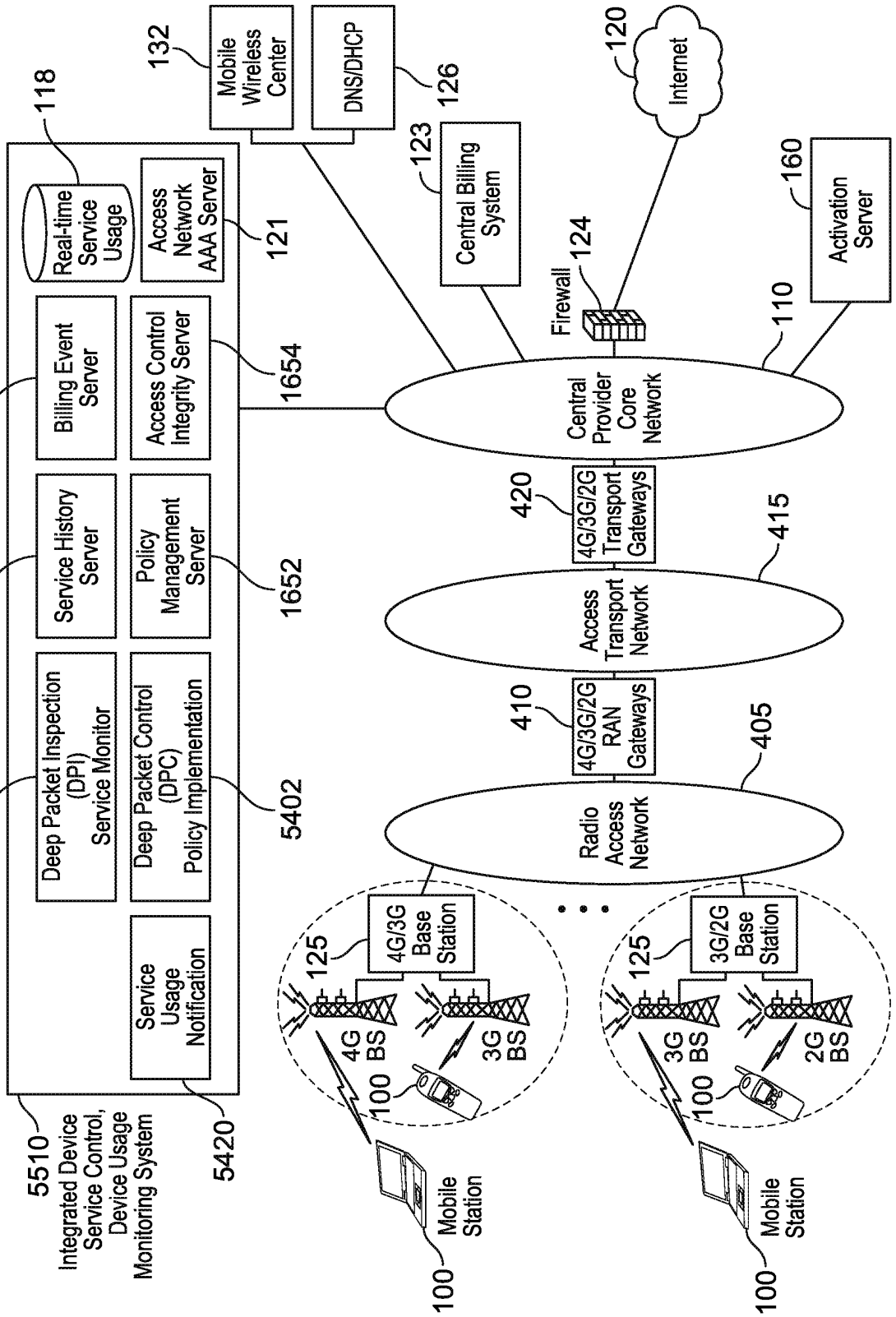

5510
Integrated Device Service Control, Device Usage Monitoring System
5420
5412
Deep Packet Inspection (DPI) Service Monitor
Service Usage Notification
1650
Service History Server
1662
Billing Event Server
118
Real-time Service Usage
5402
Deep Packet Control (DPC) Policy Implementation
1652
Policy Management Server
1654
Access Control Integrity Server
121
Access Network AAA Server
132
Mobile Wireless Center
DNS/DHCP
126
123
Central Billing System
120
Internet
Firewall
124
110
Central Provider Core Network
160
Activation Server
420
4G/3G/2G Transport Gateways
415
Access Transport Network
410
4G/3G/2G RAN Gateways
405
Radio Access Network
125
4G/3G Base Station
4G BS
3G BS
100
Mobile Station
125
3G/2G Base Station
3G BS
2G BS
100
Mobile Station

FIG. 55

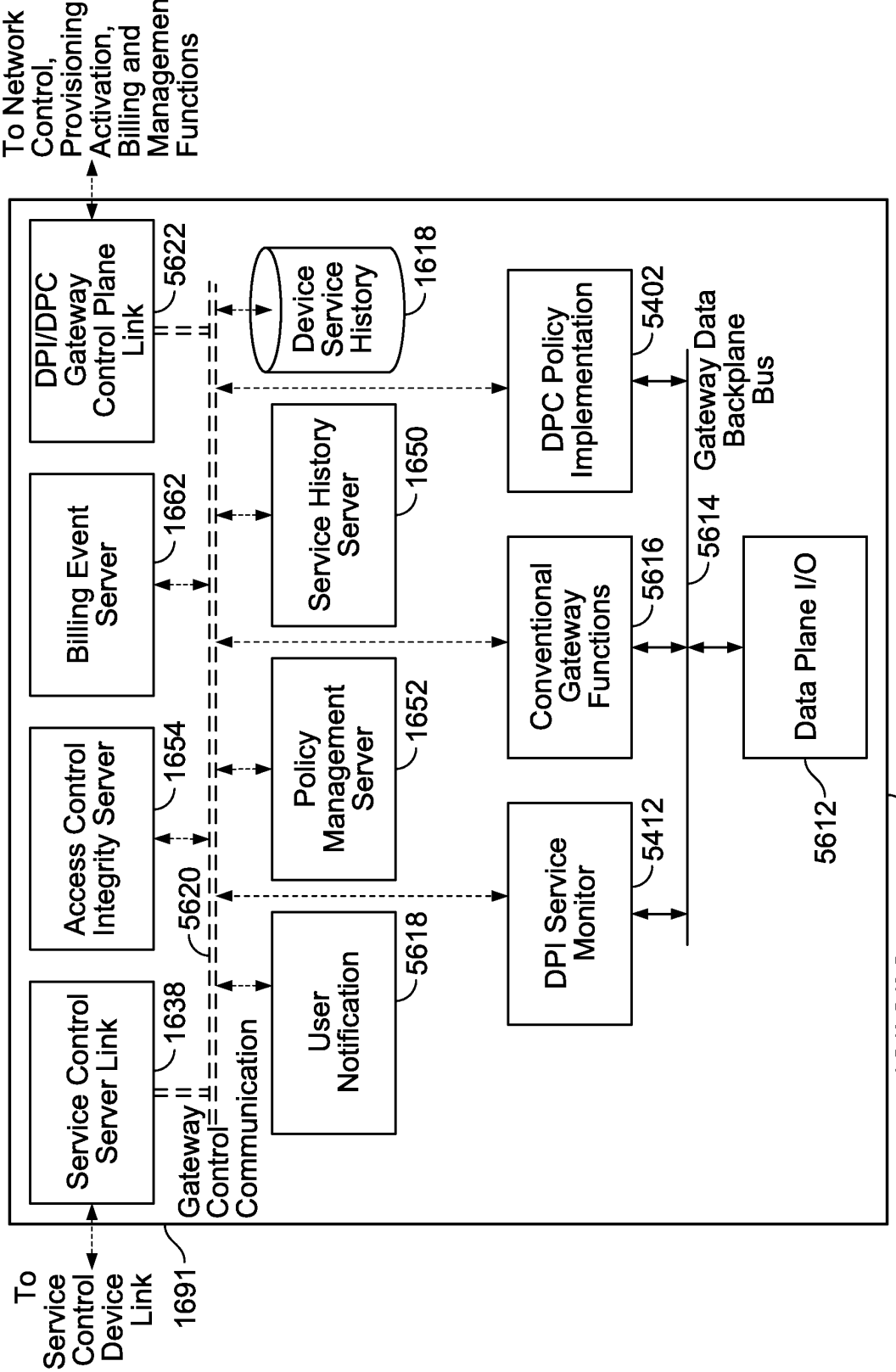

To Network Control, Provisioning, Activation, Billing and Management Functions
DPI/DPC Gateway Control Plane Link
5622
Device Service History
1618
Billing Event Server
1662
Service History Server
1650
DPC Policy Implementation
5402
Gateway Data Backplane Bus
5614
Access Control Integrity Server
1654
Policy Management Server
1652
Conventional Gateway Functions
5616
Data Plane I/O
5612
Service Control Server Link
1638
Gateway Control Communication
5620
User Notification
5618
DPI Service Monitor
5412
4G/3G/2G DPI/DPC Gateway
5610
To Service Control Device Link
1691

FIG. 56

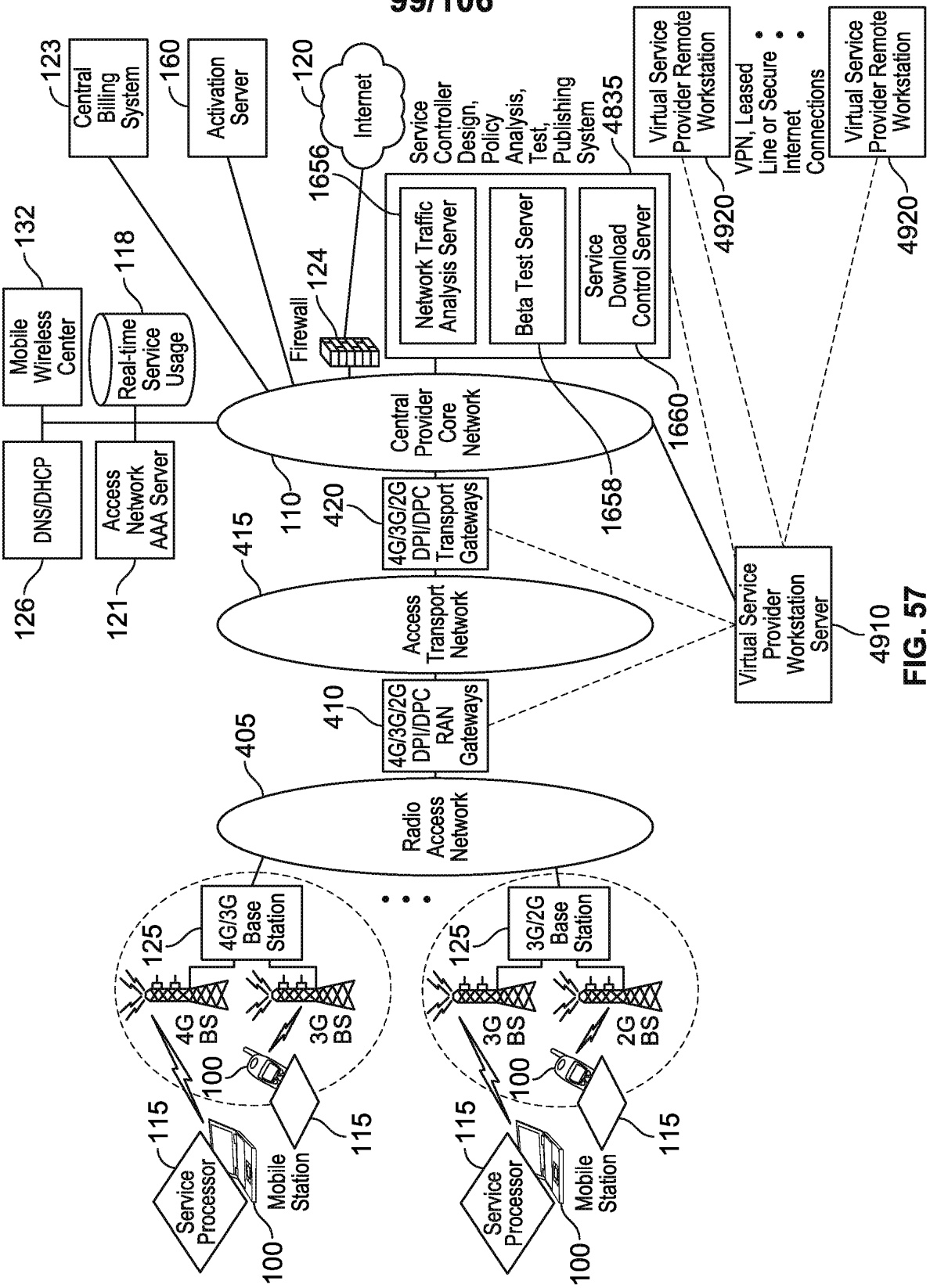

Central Billing System
123
Activation Server
160
Internet
120
Service Controller Design, Policy Analysis, Test, Publishing System
4835
Virtual Service Provider Remote Workstation
4920
VPN, Leased Line or Secure Internet Connections
Mobile Wireless Center
132
Real-time Service Usage
118
Firewall
124
1656
Network Traffic Analysis Server
Beta Test Server
Service Download Control Server
1660
1658
DNS/DHCP
126
Access Network AAA Server
121
Central Provider Core Network
110
4G/3G/2G DPI/DPC Transport Gateways
420
415
Access Transport Network
4G/3G/2G DPI/DPC RAN Gateways
410
405
Radio Access Network
Virtual Service Provider Workstation Server
4910
4G/3G Base Station
125
3G/2G Base Station
4G BS
3G BS
3G BS
2G BS
100
115
Service Processor
Mobile Station

FIG. 57

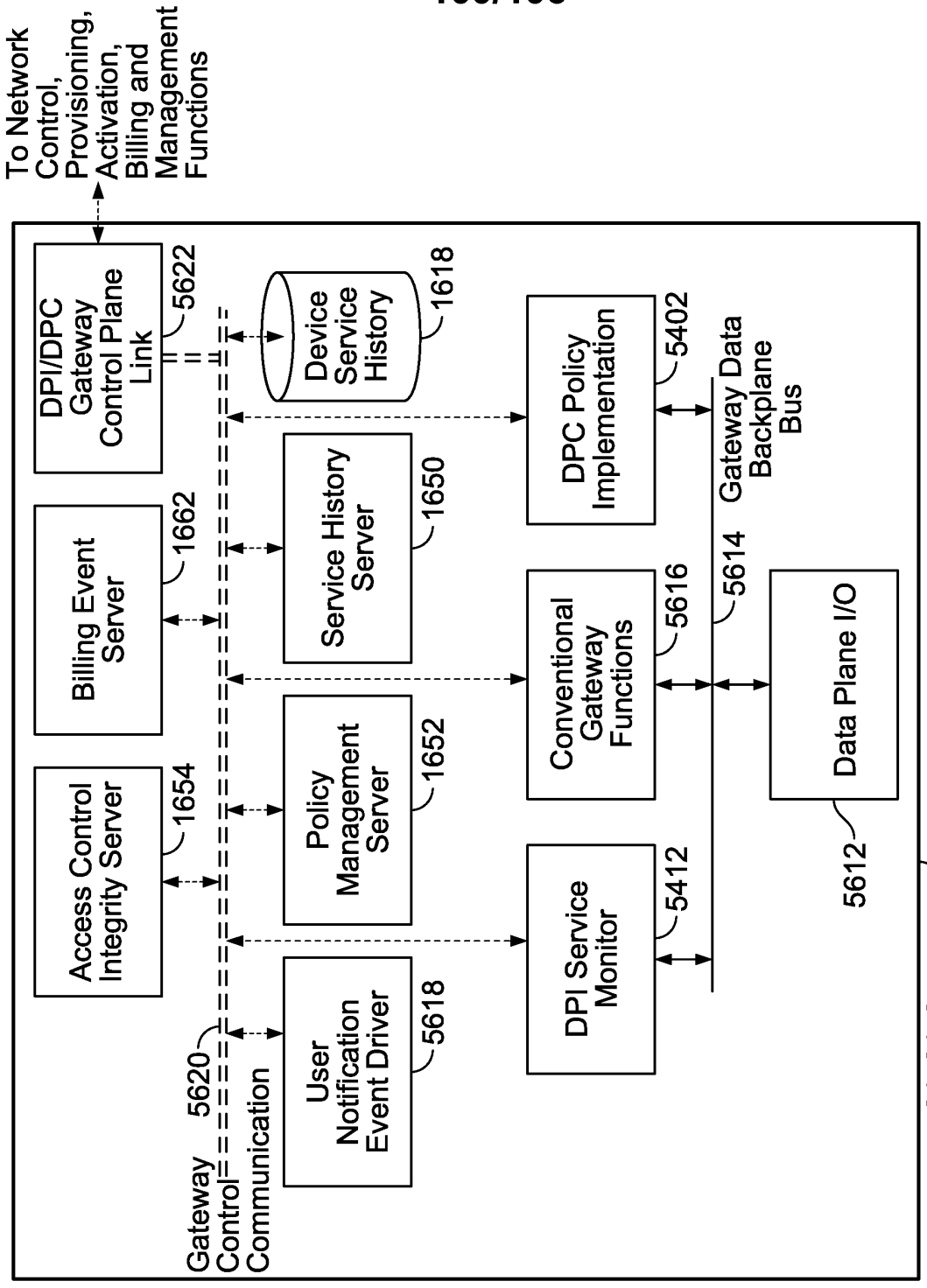

To Network Control, Provisioning, Activation, Billing and Management Functions
DPI/DPC Gateway Control Plane Link
5622
Device Service History
1618
Billing Event Server
1662
Service History Server
1650
DPC Policy Implementation
5402
Gateway Data Backplane Bus
Access Control Integrity Server
1654
Policy Management Server
1652
Conventional Gateway Functions
5616
5614
Data Plane I/O
User Notification Event Driver
5618
DPI Service Monitor
5412
5612
Gateway Control Communication
5620
4G/3G/2G DPI/DPC Gateway
5810

FIG. 58

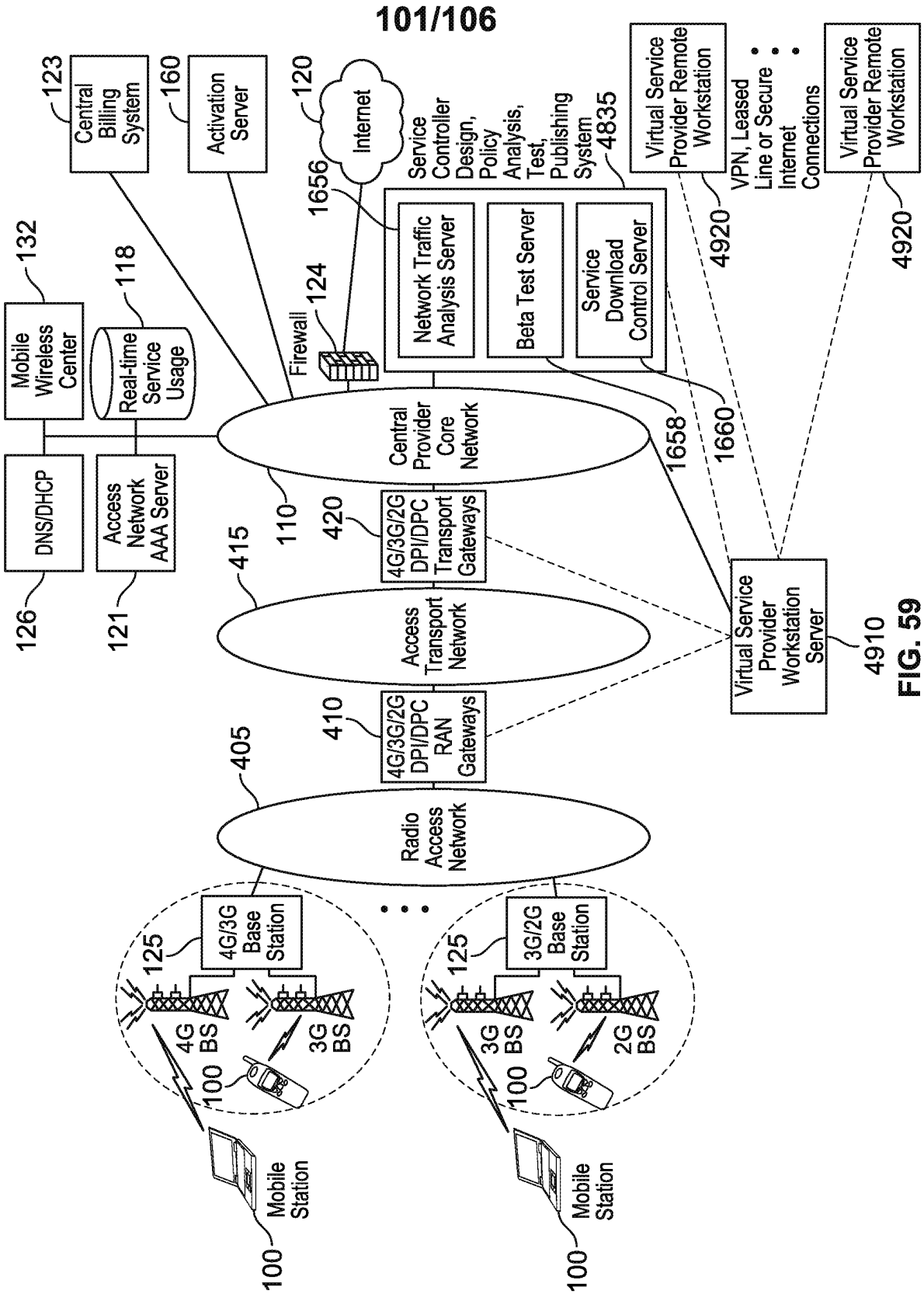

101/106
Central Billing System
123
Activation Server
160
Internet
120
Service Controller Design, Policy Analysis, Test, Publishing System
4835
Virtual Service Provider Remote Workstation
VPN, Leased Line or Secure Internet Connections
4920
Virtual Service Provider Remote Workstation
4920
1656
Network Traffic Analysis Server
Beta Test Server
Service Download Control Server
Mobile Wireless Center
132
Real-time Service Usage
118
Firewall
124
Central Provider Core Network
110
1658
1660
DNS/DHCP
126
Access Network AAA Server
121
4G/3G/2G DPI/DPC Transport Gateways
420
415
Access Transport Network
4G/3G/2G DPI/DPC RAN Gateways
410
405
Radio Access Network
Virtual Service Provider Workstation Server
4910
4G/3G Base Station
125
3G/2G Base Station
125
4G BS
3G BS
3G BS
2G BS
100
100
Mobile Station
Mobile Station
100
100

FIG. 59

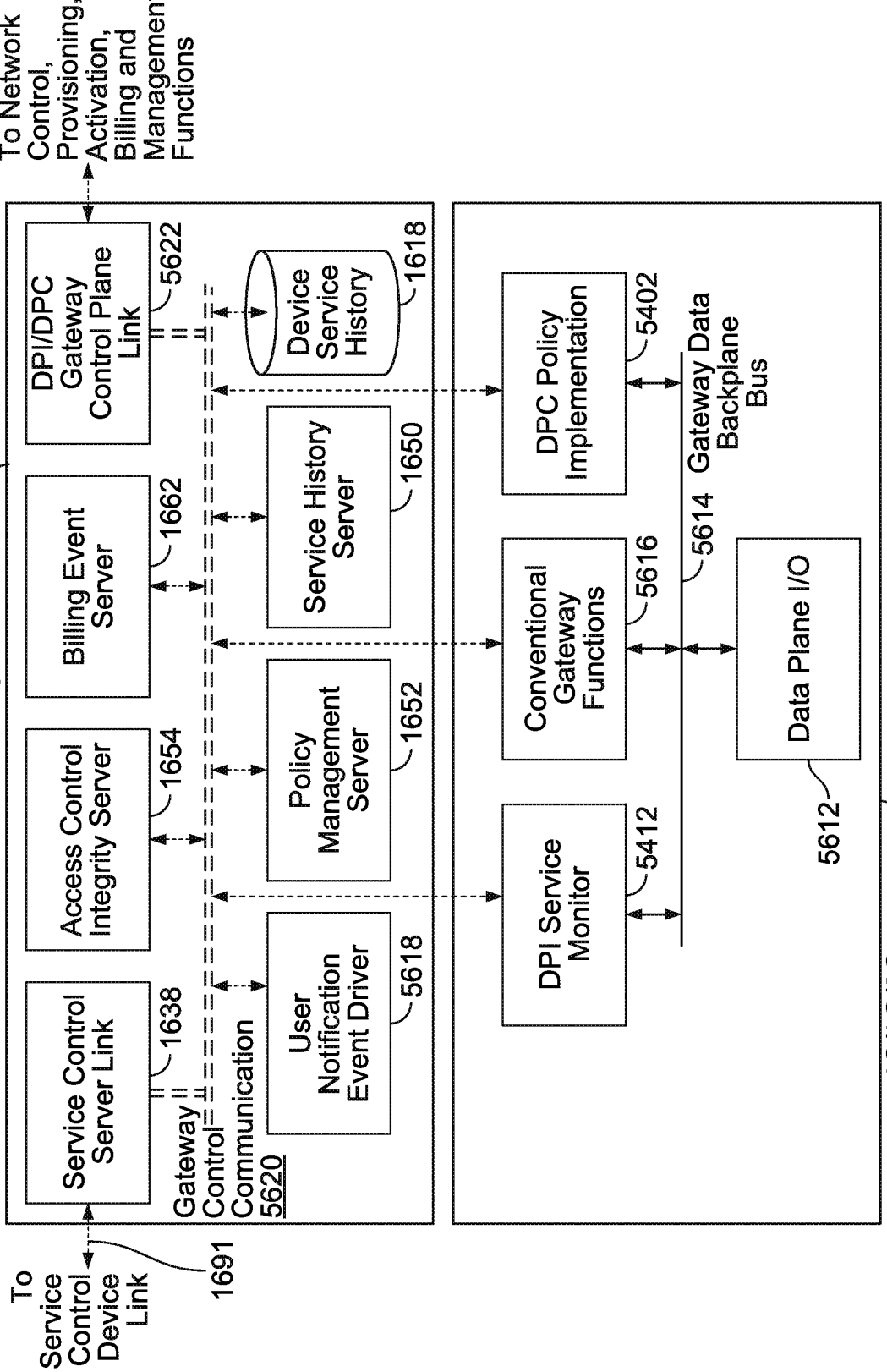

To Network Control, Provisioning, Activation, Billing and Management Functions
Service Controller Device Control System
6025
DPI/DPC Gateway Control Plane Link
5622
Billing Event Server
1662
Access Control Integrity Server
1654
Policy Management Server
1652
User Notification Event Driver
5618
Service Control Server Link
1638
Gateway Control Communication 5620
Device Service History
1618
Service History Server
1650
DPC Policy Implementation
5402
Conventional Gateway Functions
5616
DPI Service Monitor
5412
Gateway Data Backplane Bus
5614
Data Plane I/O
5612
4G/3G/2G DPI/DPC Gateway
6010
To Service Control Device Link
1691

FIG. 60

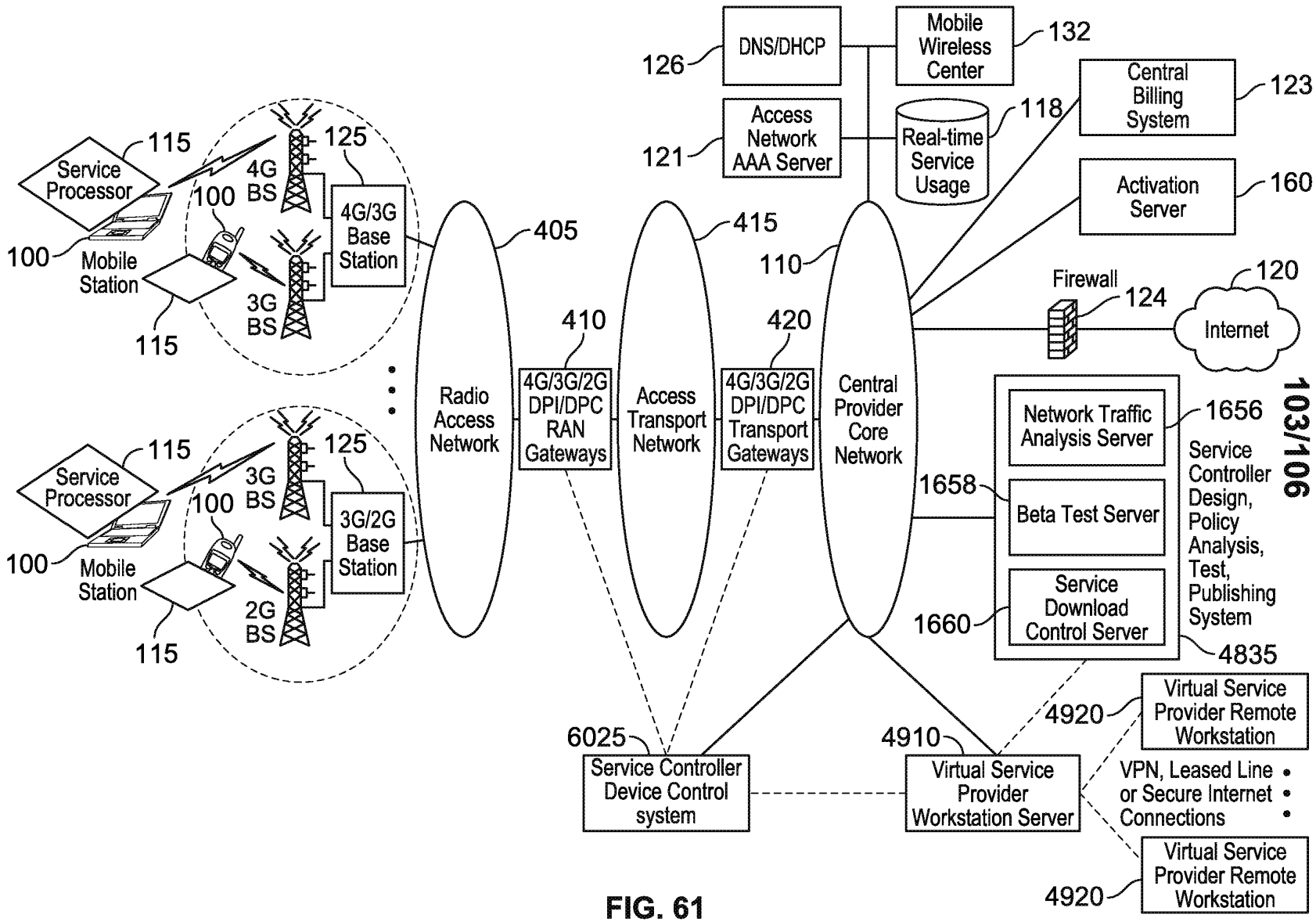

Service Processor
115
100
Mobile Station
4G BS
125
4G/3G Base Station
3G BS
Service Processor
3G BS
3G/2G Base Station
2G BS
Radio Access Network
405
4G/3G/2G DPI/DPC RAN Gateways
410
Access Transport Network
415
4G/3G/2G DPI/DPC Transport Gateways
420
Central Provider Core Network
110
DNS/DHCP
126
Mobile Wireless Center
132
Access Network AAA Server
121
Real-time Service Usage
118
Central Billing System
123
Activation Server
160
Firewall
124
Internet
120
Network Traffic Analysis Server
1656
Beta Test Server
1658
Service Download Control Server
1660
Service Controller Design, Policy Analysis, Test, Publishing System
4835
103/106
Service Controller Device Control system
6025
Virtual Service Provider Workstation Server
4910
Virtual Service Provider Remote Workstation
4920
VPN, Leased Line or Secure Internet Connections
Virtual Service Provider Remote Workstation
4920

FIG. 61

1048

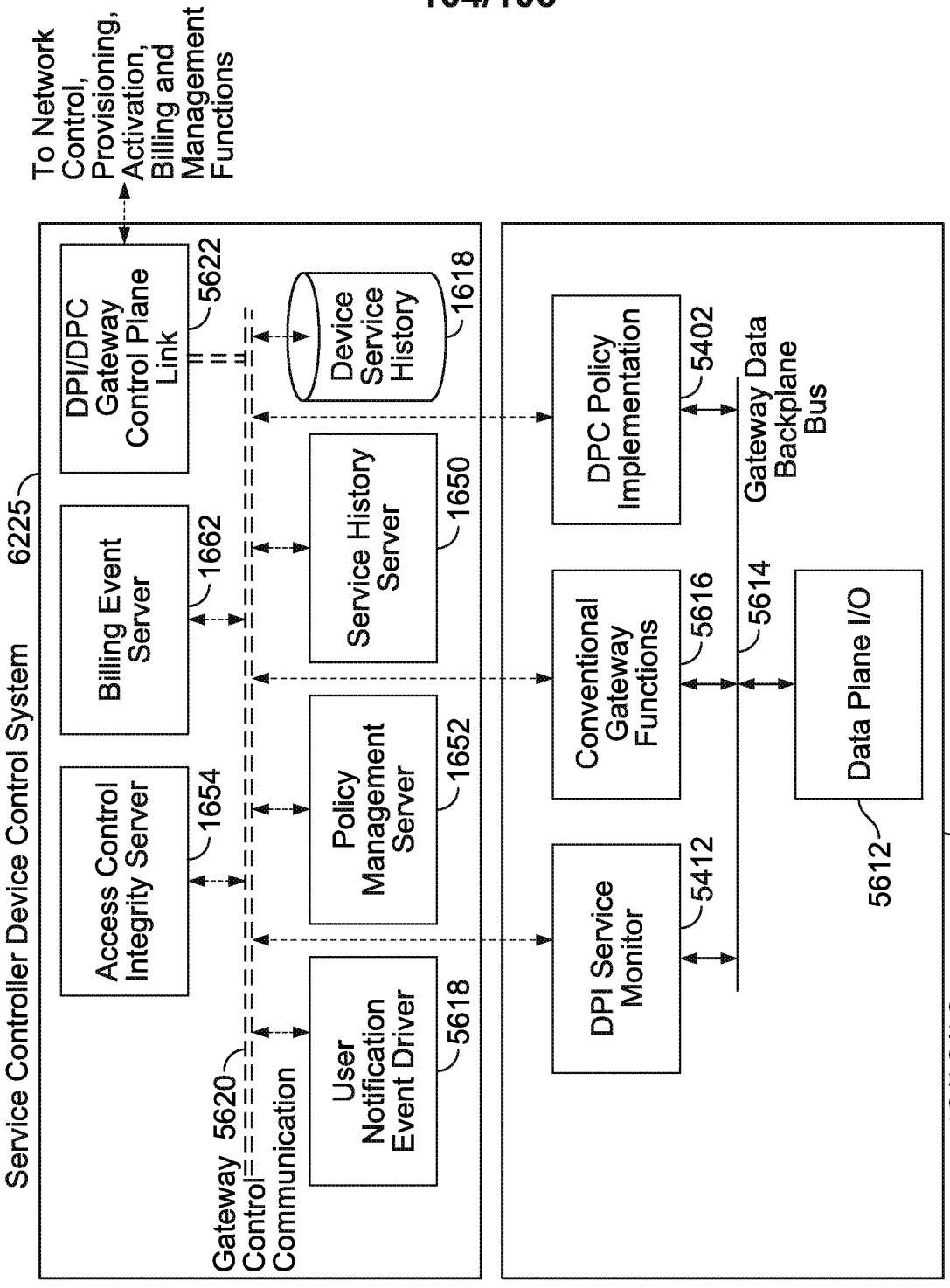

To Network Control, Provisioning, Activation, Billing and Management Functions
Service Controller Device Control System
6225
DPI/DPC Gateway Control Plane Link
5622
Billing Event Server
1662
Service History Server
1650
Device Service History
1618
Access Control Integrity Server
1654
Policy Management Server
1652
User Notification Event Driver
5618
Gateway Control Communication
5620
DPC Policy Implementation
5402
Gateway Data Backplane Bus
Conventional Gateway Functions
5616
5614
Data Plane I/O
DPI Service Monitor
5412
5612
4G/3G/2G DPI/DPC Gateway
6210

FIG. 62

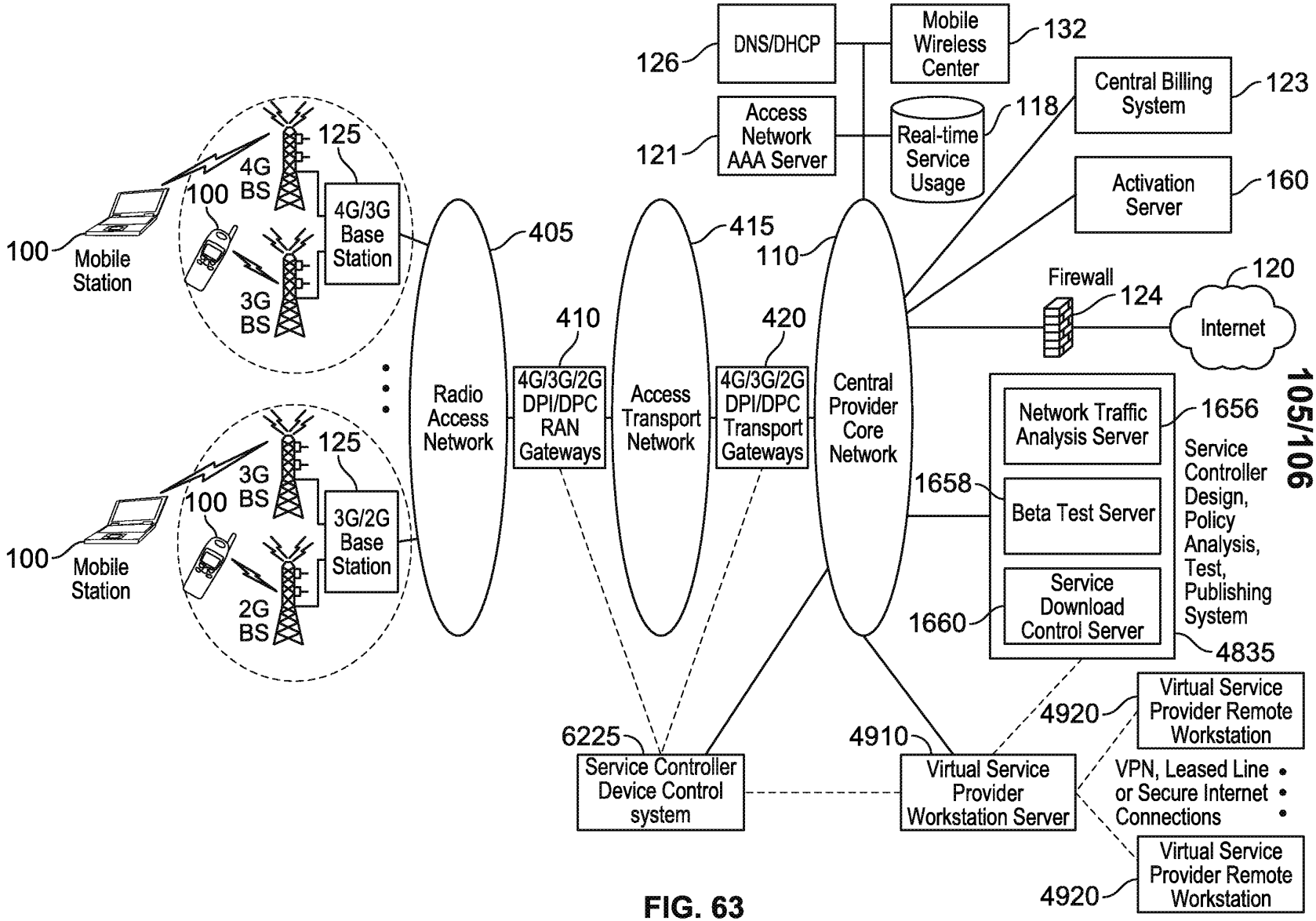

1050
100
Mobile Station
4G BS
125
4G/3G Base Station
3G BS
100
Mobile Station
3G BS
125
3G/2G Base Station
2G BS
Radio Access Network
405
4G/3G/2G DPI/DPC RAN Gateways
410
Access Transport Network
415
4G/3G/2G DPI/DPC Transport Gateways
420
Central Provider Core Network
110
126
DNS/DHCP
Mobile Wireless Center
132
121
Access Network AAA Server
Real-time Service Usage
118
Central Billing System
123
Activation Server
160
Firewall
124
Internet
120
105/106
Network Traffic Analysis Server
1656
1658
Beta Test Server
1660
Service Download Control Server
Service Controller Design, Policy Analysis, Test, Publishing System
4835
6225
Service Controller Device Control system
4910
Virtual Service Provider Workstation Server
4920
Virtual Service Provider Remote Workstation
VPN, Leased Line or Secure Internet Connections
4920
Virtual Service Provider Remote Workstation

FIG. 63

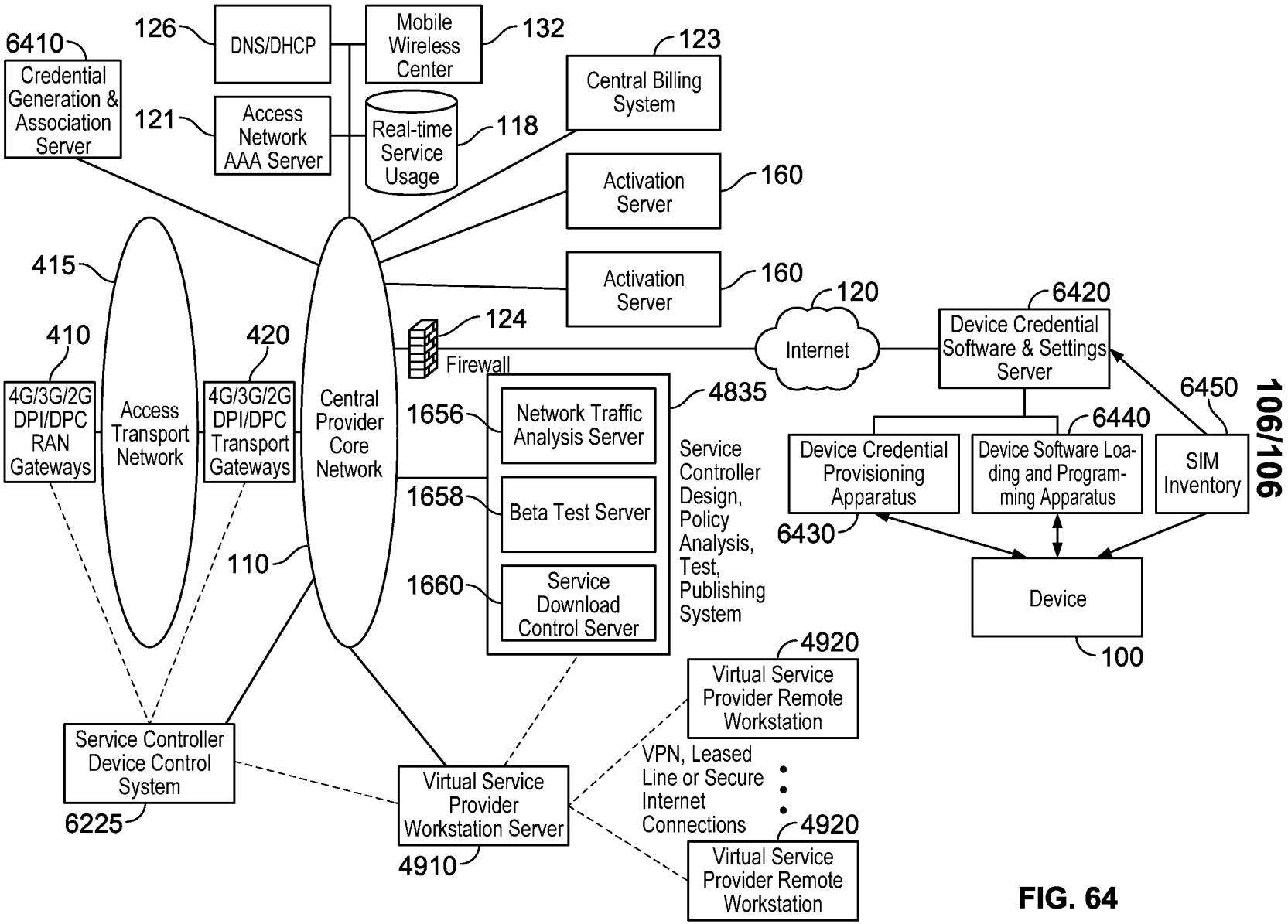

6410
Credential Generation & Association Server
126
DNS/DHCP
Mobile Wireless Center
132
123
Central Billing System
121
Access Network AAA Server
Real-time Service Usage
118
Activation Server
160
415
Activation Server
160
120
6420
410
420
124
Internet
Device Credential Software & Settings Server
Firewall
4G/3G/2G DPI/DPC RAN Gateways
Access Transport Network
4G/3G/2G DPI/DPC Transport Gateways
Central Provider Core Network
4835
1656
Network Traffic Analysis Server
6450
106/106
6440
Device Credential Provisioning Apparatus
Device Software Loading and Programming Apparatus
SIM Inventory
1658
Beta Test Server
Service Controller Design, Policy Analysis, Test, Publishing System
6430
110
1660
Service Download Control Server
Device
100
4920
Virtual Service Provider Remote Workstation
Service Controller Device Control System
VPN, Leased Line or Secure Internet Connections
Virtual Service Provider Workstation Server
6225
4910
4920
Virtual Service Provider Remote Workstation

FIG. 64

1051

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	Automated Device Provisioning and Activation
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Filer:	James E. Harris/Ann Taylor
Attorney Docket Number:	RALEP007C11C4

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility filing Fee (Electronic filing)	4011	1	70	70
Utility Search Fee	2111	1	300	300
Utility Examination Fee	2311	1	360	360
Pages:				
Utility Appl Size fee per 50 sheets >100	2081	4	200	800
Claims:				
Miscellaneous-Filing:				
Publ. Fee- Early, Voluntary, or Normal	1504	1	0	0

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**1530**

Electronic Acknowledgement Receipt	
EFS ID:	21868038
Application Number:	14667516
International Application Number:	
Confirmation Number:	5348
Title of Invention:	Automated Device Provisioning and Activation
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	James E. Harris/Ann Taylor
Filer Authorized By:	James E. Harris
Attorney Docket Number:	RALEP007C11C4
Receipt Date:	24-MAR-2015
Filing Date:	
Time Stamp:	19:14:45
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$1530
RAM confirmation Number	5466
Deposit Account	505876
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

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

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

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

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Application Data Sheet	P007C11C4_ADS.pdf	1561866 fca080cfa7fab4f469165e353939a0494e58fc54	no	7
Warnings:					
Information:					
2		P007C11C4_Spec.pdf	1093904 25b504b8d7e3f19fadc4efa7baf76ac048274bd1	yes	242

Multipart Description/PDF files in .zip description

Document Description	Start	End
Specification	1	240
Claims	241	241
Abstract	242	242

Warnings:					
Information:					
3	Oath or Declaration filed	P007C11C4_RaleighDecl.pdf	104311 70693a740200f34cca93e331daf36c35833318ed	no	1
Warnings:					
Information:					
4	Drawings-only black and white line drawings	P007C11C4_Drawings_Part1.pdf	10373531 e0fc5e83c7051baf9971ec66850158a151bbe2ed	no	54
Warnings:					
Information:					
5	Drawings-only black and white line drawings	P007C11C4_Drawings_Part2.pdf	8159440 2aa88e3fca51a61630c71981434904942cbd5b67	no	52
Warnings:					
Information:					
6	Fee Worksheet (SB06)	fee-info.pdf	38328 e9b07a1efcc1612744b408f94c1a89446bb68969	no	2

Warnings:	
Information:	
Total Files Size (in bytes):	21331380

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

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

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

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

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 14/667,516	Filing Date 03/24/2015	☐ To be Mailed

ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)		
FOR	NUMBER FILED	NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT	03/24/2015	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 18	Minus	** 20	= 0	X $40 =	0
	Independent (37 CFR 1.16(h))	* 1	Minus	***3	= 0	X $210 =	0
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	**0**

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

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
/DORRETTA BROOKS/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.