UNITED STATES
PATENT AND TRADEMARK OFFICE

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

ACKNOWLEDGEMENT OF LOSS OF ENTITLEMENT TO ENTITY STATUS DISCOUNT

APPLICATION #	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET #	REQUEST ID
15/582,350	04/28/2017	Gregory G. Raleigh	RALEP007C11C3C2C3C2	477681

The entity status change request below filed through Patent Center on 09/22/2025 has been accepted.

Certifications

APPLICANT CHANGING TO REGULAR UNDISCOUNTED FEE STATUS

Signature

I certify, in accordance with 37 CFR 1.4(d)(4), that I am one of the signatories making the entity status change.

Signature	Name	Registration #
/Farshad Farjami/	Farshad Farjami	41014

TARGET 1002

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/582,350	06/11/2019	10321320	RALEP007C11C3C2C3C2	7797

106963 7590 05/22/2019

Headwater Research LLC
1011 Pruitt Place
Tyler, TX 75703

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 280 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 Research LLC, Tyler, TX;

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

PART B - FEE(S) TRANSMITTAL

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

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

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

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

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

100963 7590 04/04/2019
Headwater Research LLC
1011 Pruitt Place
Tyler, TX 75703

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

Certificate of Mailing or Transmission

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

Jennifer Smith	(Typed or printed name)
[signature]	(Signature)
4-24-19	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/582,350	04/28/2017	Gregory G. Raleigh	RALEP007C11C3C2C3C2	7797

TITLE OF INVENTION: Wirless Network Buffered Message System

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$500	$0.00	$0.00	$500	07/05/2019

EXAMINER	ART UNIT	CLASS-SUBCLASS
RUDY, ANDREW J	3687	705-016000

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

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

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

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

1 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 must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE	(B) RESIDENCE: (CITY and STATE OR COUNTRY)
Headwater Research LLC	Tyler, TX

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

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

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

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

☒ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. 505876

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

☐ Applicant certifying micro entity status. See 37 CFR 1.29

☐ Applicant asserting small entity status. See 37 CFR 1.27

☐ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

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

Authorized Signature [signature] Date APRIL 24, 2019

Typed or printed name James E. Harris Registration No. 40013

PTOL-85 Part B (08-18) Approved for use through 01/31/2020 OMB 0651-0033 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Electronic Patent Application Fee Transmittal

Application Number:	15582350
Filing Date:	28-Apr-2017
Title of Invention:	Wirless Network Buffered Message System
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Filer:	James E. Harris/Jennifer Smith
Attorney Docket Number:	RALEP007C11C3C2C3C2

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	500	500

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

Electronic Acknowledgement Receipt	
EFS ID:	35814566
Application Number:	15582350
International Application Number:	
Confirmation Number:	7797
Title of Invention:	Wirless Network Buffered Message System
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	James E. Harris/Jennifer Smith
Filer Authorized By:	James E. Harris
Attorney Docket Number:	RALEP007C11C3C2C3C2
Receipt Date:	24-APR-2019
Filing Date:	28-APR-2017
Time Stamp:	11:57:19
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$500
RAM confirmation Number	042419INTEFSW00014441505876
Deposit Account	505876
Authorized User	Ann Taylor
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.20 (Post Issuance fees) 37 CFR 1.21 (Miscellaneous fees and charges)	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	Fee_Transmittal007C11C3C2C3C2.pdf	443581 6db4898f19af2225ba16571facc20f435b760363	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30356 ce36537f34f046111edafad22e51931c65ce9138	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	473937		

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 04/04/2019

Headwater Research LLC
1011 Pruitt Place
Tyler, TX 75703

EXAMINER
RUDY, ANDREW J

ART UNIT	PAPER NUMBER
3687	

DATE MAILED: 04/04/2019

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/582,350	04/28/2017	Gregory G. Raleigh	RALEP007C11C3C2C3C2	7797

TITLE OF INVENTION: Wirless Network Buffered Message System

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$500	$0.00	$0.00	$500	07/05/2019

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

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

HOW TO REPLY TO THIS NOTICE:

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

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

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

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

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

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

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

PART B - FEE(S) TRANSMITTAL

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

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

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

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

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

106963 7590 04/04/2019
Headwater Research LLC
1011 Pruitt Place
Tyler, TX 75703

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

Certificate of Mailing or Transmission

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

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/582,350	04/28/2017	Gregory G. Raleigh	RALEP007C11C3C2C3C2	7797

TITLE OF INVENTION: Wirless Network Buffered Message System

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$500	$0.00	$0.00	$500	07/05/2019

EXAMINER	ART UNIT	CLASS-SUBCLASS
RUDY, ANDREW J	3687	705-016000

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

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

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

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

1_____
2_____
3_____

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

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

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

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

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

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

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

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

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

❑ Applicant certifying micro entity status. See 37 CFR 1.29

❑ Applicant asserting small entity status. See 37 CFR 1.27

❑ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

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

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/582,350	04/28/2017	Gregory G. Raleigh	RALEP007C11C3C2C3C2	7797

106963 7590 04/04/2019

Headwater Research LLC
1011 Pruitt Place
Tyler, TX 75703

EXAMINER	
RUDY, ANDREW J	
ART UNIT	PAPER NUMBER
3687	

DATE MAILED: 04/04/2019

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

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

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

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

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

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

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

Privacy Act Statement

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

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

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

Notice of Allowability	**Application No.** 15/582,350	**Applicant(s)** Raleigh, Gregory G.	
	Examiner ANDREW JOSEPH RUDY	**Art Unit** 3687	**AIA (FITF) 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 August 8, 2017 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 areply 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

Notice of Pre-AIA or AIA Status

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

2. Applicant cancelled claim 1. Claims 2-19 are pending.

3. Applicant's claim for priority is assumed to correspond to the multiple priority documents contained in the Application submission. It is incumbent upon Applicant to correct the record if the material claimed in the present Application is not supported for the multiple priority documents.

Drawings

4. Applicant's Drawings submitted April 28, 2017 are acceptable.

Claim Rejections - 35 USC § 101

5. Claims 2-19 are not deemed adversely impacted under 35 U.S.C. § 101. Thus, no 35 USC § 101 rejection is deemed warranted.

Allowable Subject Matter

6. Claims 2- 19 are allowed.

7. The following is an examiner's statement of reasons for allowance: Claims 2-19 are allowed as all the cited prior art, either alone or in combination, does not disclose Applicant's inventive claim language.

Claims 2-19 have been reviewed in light of Alice Corporation Pty. Ltd. v. CLtweS Bank International, et al., 573 U. S. ___ (2014) and are not deemed invalidated by such. Again, no 35 USC § 101 rejection is deemed warranted.

Claims 2-19 are determined to be directed to patent-eligible subject matter and the Examiner does not consider any of the pending claims to be directed to an abstract idea. Even if the Examiner were to identify an abstract idea for any claim, then under a further analysis under Alice all claims would still be found to be patent eligible for the following reasons. The Examiner finds that when all of the elements of each claim are considered individually and as an ordered combination, each claim contains an inventive concept which is directed to an application, a particular application, or a special application, of the identified abstract idea. Further the Examiner finds that issuance of a patent for any claim would not preempt the identified abstract idea, or the field of the identified 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."

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

9. Applicant's nine (9) Information Disclosure Statements (IDS's) submitted have been reviewed. Note the attached IDS's.

10. 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.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nathan Uber, can be reached on 571-270-3923. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/ANDREW JOSEPH RUDY/

Primary Examiner

Art Unit 3687

Notice of References Cited	Application/Control No. 15/582,350	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-5751719-A	05-1998	Chen; Kuo-Wei Herman	H04L1/1809	370/394
*	B	US-7013469-B2	03-2006	Smith; Adam W.	G06F9/465	719/315
*	C	US-7707320-B2	04-2010	Singhai; Sandeep	H04L47/10	709/250
*	D	US-7885644-B2	02-2011	Gallagher; Michael D.	H04W4/90	455/414.2
*	E	US-7929446-B2	04-2011	Bozarth; Brad	H04L41/22	370/235
*	F	US-8401906-B2	03-2013	Ruckart; John	G06Q20/12	235/380
*	G	US-8611919-B2	12-2013	Barnes, Jr.; Melvin L.	G06Q10/1053	455/456.1
*	H	US-8761809-B2	06-2014	Faith; Patrick	G06F1/1694	455/456.6
*	I	US-9262370-B2	02-2016	Hofstaedter; Christian E.	G06F15/173	1/1
*	J	US-9615192-B2	04-2017	Raleigh; Gregory G.	G06Q10/06375	1/1
*	K	US-20070124077-A1	05-2007	Hedlund; RobertG JR.	G06Q10/087	701/300
*	L	US-20070242659-A1	10-2007	Cantu; Diana Maria	H04M11/007	370/352
*	M	US-20080183811-A1	07-2008	Kotras; Timothy W.	G06F16/954	709/203

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.

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/582,350	Raleigh, Gregory G.
	Examiner	**Art Unit**
	ANDREW JOSEPH RUDY	3687

CPC						
Symbol					**Type**	**Version**
H04W	/	12	/	08	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	I	2013-01-01
H04L	/	41	/	5003	I	2013-01-01
H04M	/	15	/	00	I	2013-01-01
H04M	/	15	/	58	I	2013-01-01
H04W	/	4	/	24	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
H04W	/	28	/	02	I	2013-01-01
H04L	/	47	/	2408	I	2013-01-01
H04L	/	67	/	306	I	2013-01-01
G06Q	/	40	/	12	I	2013-12-03
H04W	/	8	/	20	I	2013-01-01
H04W	/	28	/	12	I	2013-01-01
H04W	/	48	/	14	I	2013-01-01
H04W	/	88	/	08	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

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	18	
/ANDREW JOSEPH RUDY/ Primary Examiner, Art Unit 3687	28 March 2019	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	22A

U.S. Patent and Trademark Office — Part of Paper No.: 20190328

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/582,350	Raleigh, Gregory G.
	Examiner	Art Unit
	ANDREW JOSEPH RUDY	3687

CPC						
Symbol					Type	Version
H04W	/	24	/	08	I	2013-01-01
H04L	/	51	/	046	I	2013-01-01
H04W	/	4	/	12	I	2013-01-01
H04W	/	8	/	18	I	2013-01-01
H04W	/	72	/	0453	I	2013-01-01
H04L	/	47	/	20	I	2013-01-01
H04W	/	28	/	0215	I	2013-01-01
H04L	/	63	/	0236	I	2013-01-01
G06Q	/	10	/	06315	I	2013-01-01
H04L	/	41	/	0806	I	2013-01-01
H04L	/	41	/	5054	I	2013-01-01
H04M	/	15	/	80	I	2013-01-01
H04L	/	67	/	327	I	2013-01-01
H04L	/	9	/	3247	I	2013-01-01
H04L	/	63	/	0892	I	2013-01-01
H04L	/	67	/	145	I	2013-01-01
H04W	/	12	/	06	I	2013-01-01
H04L	/	67	/	26	I	2013-01-01
H04L	/	63	/	0853	I	2013-01-01
H04W	/	48	/	16	I	2013-01-01
H04W	/	4	/	50	I	2018-02-01
H04L	/	41	/	5025	A	2013-01-01
H04M	/	2215	/	0188	A	2013-01-01
H04W	/	8	/	02	A	2013-01-01
H04W	/	84	/	04	A	2013-01-01
H04W	/	84	/	12	A	2013-01-01
H04W	/	88	/	06	A	2013-01-01
H04L	/	67	/	34	A	2013-01-01
H04L	/	67	/	2819	A	2013-01-01
H04W	/	84	/	042	A	2013-01-01
H04L	/	41	/	0876	A	2013-01-01

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	18	
/ANDREW JOSEPH RUDY/ Primary Examiner, Art Unit 3687	28 March 2019	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	22A

U.S. Patent and Trademark Office — Part of Paper No.: 20190328

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/582,350	Raleigh, Gregory G.
	Examiner	**Art Unit**
	ANDREW JOSEPH RUDY	3687

CPC							
Symbol						**Type**	**Version**
Y02P	/	90	/	86		A	2015-11-01

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

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	18	
/ANDREW JOSEPH RUDY/ Primary Examiner, Art Unit 3687	28 March 2019	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	22A

U.S. Patent and Trademark Office — Part of Paper No.: 20190328

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/582,350	Raleigh, Gregory G.
	Examiner	**Art Unit**
	ANDREW JOSEPH RUDY	3687

INTERNATIONAL CLASSIFICATION					
CLAIMED					
H04W	/	12	/	08	
NON-CLAIMED					
	/		/		

US ORIGINAL CLASSIFICATION	
CLASS	**SUBCLASS**
709	224

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

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	18	
/ANDREW JOSEPH RUDY/ Primary Examiner, Art Unit 3687	28 March 2019	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	22A

U.S. Patent and Trademark Office — Part of Paper No.: 20190328

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/582,350	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

CLAIMS

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

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	18	
/ANDREW JOSEPH RUDY/ Primary Examiner, Art Unit 3687	28 March 2019	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	22A

U.S. Patent and Trademark Office — Part of Paper No.: 20190328

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/582,350	Raleigh, Gregory G.
	Examiner	Art Unit
	ANDREW JOSEPH RUDY	3687

CPC - Searched*		
Symbol	**Date**	**Examiner**
G06Q 10/06375 ; G06Q 20/20; G06Q 20/40; G06Q 30/0207; G06Q 30/0283; G06Q 30/0284; G06Q 30/04; G06Q 30/0601; G06Q 40/00; G06Q 30/0241; G06Q 40/12; G06Q 10/06315; G06Q 20/102	03/28/2019	AJR
H04W 4/50; H04W 28/02; H04W 12/08; H04W 8/02; H04W 8/20; H04W 28/12; H04W 48/14; H04W 4/24; H04W 28/0268; H04W 88/08; H04W 24/08; H04W 84/04; H04W 84/12; H04W 4/12; H04W 8/18; H04W 72/0453; H04W 28/0215; H04W 88/06; H04W 84/042; H04W 12/06; H04W 48/16	03/28/2019	AJR
H04L 12/14; H04L 41/0893; H04L 41/5003; H04L 41/5025; H04L 9/32; H04L 67/306; H04L 47/2408;H04L 63/0236; H04L 51/046; H04L 47/20; H04L 41/0806; H04L 41/5054; H04L 63/0853; H04L 67/34; H04L 67/2819; H04L 67/327; H04L 9/3247; H04L 63/0892; H04L 67/145; H04L 67/26; H04L 41/0876	03/28/2019	AJR
H04M 15/00; H04M 15/58; H04M 2215/0188; H04M 15/88; H04M 15/61 ; H04M 15/80;	03/28/2019	AJR
G06F 15/177	03/28/2019	AJR
Y02P 90/86	03/28/2019	AJR

CPC Combination Sets - Searched*		
Symbol	**Date**	**Examiner**

US Classification - Searched*			
Class	**Subclass**	**Date**	**Examiner**
235	376-383	03/28/2019	AJR
370	328, 395.21	03/28/2019	AJR
455	405, 406, 414.1, 432.1, 456.1	03/28/2019	AJR
705	16, 26.1	03/28/2019	AJR
709	217-226	03/28/2019	AJR
713	1, 152, 189	03/28/2019	AJR
726	1	03/28/2019	AJR

/ANDREW JOSEPH RUDY/ Primary Examiner, Art Unit 3687	

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/582,350	Raleigh, Gregory G.
	Examiner	Art Unit
	ANDREW JOSEPH RUDY	3687

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

Search Notes		
Search Notes	**Date**	**Examiner**
Inventor name search conducted.	03/25/2019	AJR
Continuity data reviewed.	03/25/2019	AJR
Bibliographic data updated.	03/28/2019	AJR

Interference Search			
US Class/CPC Symbol	**US Subclass/CPC Group**	**Date**	**Examiner**
G06Q	10/06375 ; 20/20; 20/40; 30/0207; 30/0283; 30/0284; 30/04; 30/0601; 40/00; 30/0241; 40/12; 10/06315; 20/102	03/25/2019	AJR
H04W	4/50; 28/02; 12/08; 8/02; 8/20; 28/12; 48/14; 4/24; 28/0268; 88/08; 24/08; 84/04; 84/12; 4/12; 8/18; 72/0453; 28/0215; 88/06; 84/042; 12/06; 48/16	03/28/2019	AJR
H04L	12/14; 41/0893; 41/5003; 41/5025; 9/32; 67/306; 47/2408; 63/0236; 51/046; 47/20; 41/0806; 41/5054; 63/0853; 67/34; 67/2819; 67/327; 9/3247; 63/0892; 67/145; 67/26; 41/0876	03/28/2019	AJR
H04M	15/00; 15/58; 2215/0188; 15/88; 15/61; 15/80;	03/28/2019	AJR

/ANDREW JOSEPH RUDY/ Primary Examiner, Art Unit 3687	

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

PTO/SB/08a (03-15)
Approved for use through 07/31/2016. 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	15582350
Filing Date	2017-04-28
First Named Inventor	Raleigh
Art Unit	2447
Examiner Name	not yet assigned
Attorney Docket Number	RALEP007C11C3C2C3C2

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	20010048738	A	2001-12-06	Baniak, Paul G. et al.	
	2	20010053694		2001-12-20	IGARASHI, Yoichiro et al.	
	3	20020022472		2002-02-21	WATLER et al.	
	4	20020049074	A	2002-04-25	Eisinger, Bernd et al.	
	5	20020116338		2002-08-22	GONTHIER, Jean-Charles et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	6	20020120370	A1	2002-08-29	Parupudi et al.	
	7	20020120540		2002-08-29	KENDE et al.	
	8	20020131404		2002-09-19	MEHTA et al.	
	9	20020138599	A1	2002-09-26	Dilman et al.	
	10	20020138601		2002-09-26	PIPONIUS et al.	
	11	20020154751	A1	2002-10-24	Thompson et al.	
	12	20020161601	A	2002-10-31	Nauer, Bernhard et al.	
	13	20020164983		2002-11-07	Raviv, Li-On et al.	
	14	20020176377		2002-11-28	HAMILTON, Thomas E.	
	15	20020188732	A1	2002-12-12	Buckman et al.	
	16	20020191573	A1	2002-12-19	Whitehill et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	17	20020199001		2002-12-26	WENOCUR et al.	
	18	20030004937		2003-01-02	SALMENKAITA et al.	
	19	20030005112		2003-01-02	KRAUTKREMER, Todd Joseph	
	20	20030013434		2003-01-16	ROSENBERG et al.	
	21	20030018524		2003-01-23	FISHMAN et al.	
	22	20030028623	A1	2003-02-06	Hennessey et al.	
	23	20030046396		2003-03-06	RICHTER et al.	
	24	20030050070		2003-03-13	MASHINSKY et al.	
	25	20030050837		2003-03-13	KIM, Do Sik	
	26	20030084321	A1	2003-05-01	Tarquini et al.	
	27	20030088671		2003-05-08	KLINKER et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	28	20030133408		2003-07-17	CHENG et al.	
	29	20030134650	A1	2003-07-17	Sundar et al.	
	30	20030159030	A1	2003-08-21	Evans, Junius A.	
	31	20030161265		2003-08-28	CAO et al.	
	32	20030171112		2003-09-11	Lupper, Alfred et al.	
	33	20030182420		2003-09-25	JONES et al.	
	34	20030182435		2003-09-25	REDLICH et al.	
	35	20030184793	A1	2003-10-02	Pineau, Richard A.	
	36	20030188006	A	2003-10-02	Bard, Steven R.	
	37	20030188117	A	2003-10-02	Yoshino et al.	
	38	20030220984		2003-11-27	JONES et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	39	20030224781		2003-12-04	MILFORD et al.	
	40	20030229900		2003-12-11	REISMAN, Richard	
	41	20030233332	A	2003-12-18	Keeler, James D. et al.	
	42	20030236745		2003-12-25	HARTSELL et al.	
	43	20040019539		2004-01-29	RAMAN et al.	
	44	20040021697		2004-02-05	BEATON et al.	
	45	20040030705		2004-02-12	BOWMAN-AMUAH, Michel K.	
	46	20040039792	A1	2004-02-26	Nakanishi, Tomoaki	
	47	20040044623		2004-03-04	WAKE et al.	
	48	20040047358		2004-03-11	CHEN et al.	
	49	20040054779	A1	2004-03-18	Takeshima et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	50	20040073672		2004-04-15	FASCENDA, Anthony C.	
	51	20040082346		2004-04-29	SKYTT et al.	
	52	20040098715		2004-05-20	AGHERA et al.	
	53	20040102182	A	2004-05-27	Reith, Lothar et al.	
	54	20040103193		2004-05-27	PANDYA et al.	
	55	20040107360		2004-06-03	HERRMANN et al.	
	56	20040127200		2004-07-01	SHAW et al.	
	57	20040127208	A1	2004-07-01	Nair et al.	
	58	20040132427		2004-07-08	Lee, Wan-Yeon et al.	
	59	20040133668	A1	2004-07-08	Nicholas III, Henry T.	
	60	20040137890	A1	2004-07-15	Kalke, Catherine	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	61	20040168052		2004-08-26	CLISHAM et al.	
	62	20040170191	A	2004-09-02	Guo et al.	
	63	20040176104	A1	2004-09-09	Arcens, Suzanne	
	64	20040198331		2004-10-07	COWARD et al.	
	65	20040203755		2004-10-14	BRUNET, Jeffrey et al.	
	66	20040203833	A	2004-10-14	Rathunde, Dale F. et al.	
	67	20040225561	A1	2004-11-11	Hertzberg et al.	
	68	20040225898	A	2004-11-11	Frost, D. et al.	
	69	20040236547		2004-11-25	RAPPAPORT et al.	
	70	20040243680	A1	2004-12-02	Mayer, Georg	
	71	20040243992	A	2004-12-02	Gustafson et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	72	20040249918		2004-12-09	SUNSHINE, Roger N.	
	73	20040255145	A	2004-12-16	Chow, Jerry	
	74	20040259534	A1	2004-12-23	Chaudhari et al.	
	75	20040260766	A1	2004-12-23	Barros et al.	
	76	20040267872	A1	2004-12-30	Serdy et al.	
	77	20050007993		2005-01-13	Chambers, Mahdi et al.	
	78	20050009499		2005-01-13	KOSTER, Karl	
	79	20050021995		2005-01-27	LAL et al.	
	80	20050041617	A1	2005-02-24	Huotari et al.	
	81	20050048950		2005-03-03	MORPER, Hans-Jochen	
	82	20050055291		2005-03-10	BEVENTE et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	83	20050055309		2005-03-10	WILLIAMS et al.	
	84	20050055595	A	2005-03-10	Frazer et al.	
	85	20050060266		2005-03-17	DEMELLO et al.	
	86	20050060525	A1	2005-03-17	Schwartz et al.	
	87	20050075115	A1	2005-04-07	Corneille et al.	
	88	20050079863	A	2005-04-14	Macaluso, Anthony G.	
	89	20050091505	A1	2005-04-28	Riley et al.	
	90	20050096024	A1	2005-05-05	Bicker et al.	
	91	20050097516		2005-05-05	DONNELLY et al.	
	92	20050107091		2005-05-19	VANNITHAMBY et al.	
	93	20050108075	A1	2005-05-19	Douglis et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	94	20050111463	A1	2005-05-26	Leung et al.	
	95	20050128967		2005-06-16	SCOBBIE, Donald MacGregor	
	96	20050135264	A1	2005-06-23	Popoff et al.	
	97	20050163320	A1	2005-07-28	Brown et al.	
	98	20050166043		2005-07-28	ZHANG et al.	
	99	20050183143		2005-08-18	ANDERHOLM et al.	
	100	20050186948	A	2005-08-25	Gallagher et al.	
	101	20050198377		2005-09-08	FERGUSON et al.	
	102	20050216421		2005-09-29	BARRY et al.	
	103	20050228985		2005-10-13	YLIKOSKI et al.	
	104	20050238046		2005-10-27	HASSAN et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	105	20050239447	A1	2005-10-27	Holzman et al.	
	106	20050245241	A1	2005-11-03	Durand et al.	
	107	20050246282		2005-11-03	NASLUND et al.	
	108	20050250508		2005-11-10	GUO et al.	
	109	20050250536	A1	2005-11-10	Deng et al.	
	110	20050254435		2005-11-17	MOAKLEY et al.	
	111	20050266825		2005-12-01	CLAYTON, Steve	
	112	20050266880		2005-12-01	GUPTA, Vivek G.	
	113	20060014519		2006-01-19	MARSH et al.	
	114	20060019632		2006-01-26	CUNNINGHAM et al.	
	115	20060020787	A1	2006-01-26	Choyi et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	116	20060026679		2006-02-02	ZAKAS, Philip H.	
	117	20060030306	A1	2006-02-09	Kuhn, Brian Gerald	
	118	20060034256		2006-02-16	ADDAGATLA et al.	
	119	20060035631	A1	2006-02-16	White et al.	
	120	20060040642		2006-02-23	BORIS et al.	
	121	20060045245		2006-03-02	AARON et al.	
	122	20060048223		2006-03-02	LEE et al.	
	123	20060068796	A	2006-03-30	Millen, Stephanie L. et al.	
	124	20060072451	A1	2006-04-06	Ross, Alan D.	
	125	20060072550	A1	2006-04-06	Davis et al.	
	126	20060072646		2006-04-06	FEHER, Kamilo	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	127	20060075506	A1	2006-04-06	Sanda et al.	
	128	20060085543		2006-04-20	HRASTAR et al.	
	129	20060095517	A1	2006-05-04	O'Connor et al.	
	130	20060098627	A1	2006-05-11	Karaoguz et al.	
	131	20060099970	A1	2006-05-11	Morgan et al.	
	132	20060112016		2006-05-25	ISHIBASHI, Yoshihito	
	133	20060114821	A1	2006-06-01	Willey et al.	
	134	20060114832	A	2006-06-01	Hamilton et al.	
	135	20060126562	A1	2006-06-15	Liu, Huitao	
	136	20060135144	A	2006-06-22	Jothipragasam, Premkumar	
	137	20060136882	A1	2006-06-22	Noonan et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	138	20060143066	A1	2006-06-29	Calabria	
	139	20060143098		2006-06-29	LAZARIDIS, Mihal	
	140	20060156398	A	2006-07-13	Ross et al.	
	141	20060160536	A	2006-07-20	Chou, Joey	
	142	20060165060		2006-07-27	DUA, Robin	
	143	20060168128	A	2006-07-27	Sistla et al.	
	144	20060173959	A	2006-08-03	Mckelvie et al.	
	145	20060174035	A	2006-08-03	Tufail, Mudassir	
	146	20060178917		2006-08-10	MERRIAM et al.	
	147	20060178918		2006-08-10	MIKURAK, Michael G.	
	148	20060182137	A1	2006-08-17	Zhou et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	149	20060183462		2006-08-17	KOLEHMAINEN, Mikko	
	150	20060190314		2006-08-24	HERNANDEZ, Rick	
	151	20060190987	A1	2006-08-24	Ohta et al.	
	152	20060199608		2006-09-07	DUNN et al.	
	153	20060200663	A1	2006-09-07	Thornton, Andrew J.	
	154	20060206709	A1	2006-09-14	Labrou et al.	
	155	20060206904		2006-09-14	WATKINS et al.	
	156	20060218395		2006-09-28	MAES, Stephane H.	
	157	20060233108		2006-10-19	KRISHNAN, Murali R.	
	158	20060233166		2006-10-19	BOU-DIAB et al.	
	159	20060236095		2006-10-19	SMITH et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	160	20060242685		2006-10-26	HEARD et al.	
	161	20060258341		2006-11-16	MILLER et al.	
	162	20060277590	A1	2006-12-07	Limont et al.	
	163	20060291419	A1	2006-12-28	McConnell et al.	
	164	20060291477		2006-12-28	CROAK et al.	
	165	20070005795	A1	2007-01-04	Gonzalez, Ruben	
	166	20070019670		2007-01-25	FALARDEAU, Eric	
	167	20070022289		2007-01-25	ALT et al.	
	168	20070025301	A	2007-02-01	Petersson et al.	
	169	20070033194	A	2007-02-08	Srinivas et al.	
	170	20070033197	A	2007-02-08	Scherzer, Shimon et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	171	20070036312		2007-02-15	CAI et al.	
	172	20070055694		2007-03-08	RUGE et al.	
	173	20070060200	A1	2007-03-15	Boris et al.	
	174	20070061243	A1	2007-03-15	Ramer et al.	
	175	20070061800	A1	2007-03-15	Cheng et al.	
	176	20070061878		2007-03-15	HAGIU, Costin et al. et al.	
	177	20070073899	A1	2007-03-29	Judge et al.	
	178	20070076616		2007-04-05	NGO et al.	
	179	20070093243		2007-04-26	KAPADEKAR et al.	
	180	20070100981		2007-05-03	ADAMCZYK et al.	
	181	20070101426		2007-05-03	LEE et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	182	20070104126		2007-05-10	CALHOUN et al.	
	183	20070109983	A	2007-05-17	Shankar, Rohit et al.	
	184	20070130283	A1	2007-06-07	Klein et al.	
	185	20070130315		2007-06-07	FRIEND et al.	
	186	20070140113		2007-06-21	GEMELOS, Steven	
	187	20070140145	A	2007-06-21	Kumar et al.	
	188	20070140275		2007-06-21	BOWMAN et al.	
	189	20070143824	A1	2007-06-21	Shahbazi, Majid	
	190	20070147317	A	2007-06-28	Smith et al.	
	191	20070147324		2007-06-28	McGary, Faith	
	192	20070155365	A	2007-07-05	Kim, Sung-Jun et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	193	20070165630	A1	2007-07-19	Rasanen et al.	
	194	20070168499	A	2007-07-19	Chu, Jing-Long	
	195	20070174490	A1	2007-07-26	Choi et al.	
	196	20070192460	A1	2007-08-16	Choi et al.	
	197	20070198656		2007-08-23	MAZZAFERRI et al.	
	198	20070201502	A1	2007-08-30	Abramson, Nathan	
	199	20070213054	A1	2007-09-13	Han, Seung-Wook	
	200	20070220251		2007-09-20	ROSENBERG et al.	
	201	20070226225		2007-09-27	YIU et al.	
	202	20070226775	A	2007-09-27	Andreasen et al.	
	203	20070234402	A1	2007-10-04	Khosravi et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	204	20070243862		2007-10-18	COSKUN et al.	
	205	20070248100		2007-10-25	ZUBERI et al.	
	206	20070254675		2007-11-01	ZORLU OZER et al.	
	207	20070255769	A1	2007-11-01	Agrawal et al.	
	208	20070255797	A1	2007-11-01	Dunn et al.	
	209	20070255848		2007-11-01	SEWALL et al.	
	210	20070257767	A1	2007-11-08	Beeson, Curt	
	211	20070259656	A	2007-11-08	Jeong, Jong Woo	
	212	20070259673		2007-11-08	WILLARS et al.	
	213	20070263558		2007-11-15	SALOMONE, Leonardo	
	214	20070266422	A1	2007-11-15	Germano et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	215	20070274327		2007-11-29	KAARELA et al.	
	216	20070280453		2007-12-06	Kelley, Sean S.	
	217	20070282896		2007-12-06	WYDROUG et al.	
	218	20070293191	A1	2007-12-20	Mir et al.	
	219	20070294395		2007-12-20	STRUB et al.	
	220	20070294410	A1	2007-12-20	Pandya et al.	
	221	20070297378	A1	2007-12-27	Poyhonen et al.	
	222	20070298764		2007-12-27	CLAYTON, Steve	
	223	20070299965	A1	2007-12-27	Nieh et al.	
	224	20070300252		2007-12-27	Acharya, Swarup et al.	
	225	20080005285		2008-01-03	ROBINSON et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	226	20080005561		2008-01-03	BROWN et al.	
	227	20080010379	A	2008-01-10	Zhao, Hang	
	228	20080010452		2008-01-10	HOLTZMAN et al.	
	229	20080018494	A1	2008-01-24	Waite et al.	
	230	20080022354	A	2008-01-24	Grewal, Karanvir et al.	
	231	20080025230	A	2008-01-31	Patel et al.	
	232	20080032715	A1	2008-02-07	Jia et al.	
	233	20080034063	A1	2008-02-07	Yee, Robert	
	234	20080034419	A	2008-02-07	Mullick et al.	
	235	20080039102		2008-02-14	SEWALL et al.	
	236	20080049630		2008-02-28	KOZISEK et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	237	20080050715	A1	2008-02-28	Golczewski et al.	
	238	20080051076		2008-02-28	O'Shaughnessy, John et al.	
	239	20080052387		2008-02-28	HEINZ et al.	
	240	20080056273	A	2008-03-06	Pelletier et al.	
	241	20080059474		2008-03-06	LIM, Keng	
	242	20080059743		2008-03-06	BYCHKOV et al.	
	243	20080060066		2008-03-06	WYNN et al.	
	244	20080062900		2008-03-13	RAO, Bindu Rama	
	245	20080064367		2008-03-13	NATH et al.	
	246	20080066149		2008-03-13	LIM, Keng	
	247	20080066150		2008-03-13	LIM, Keng	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	248	20080066181	A1	2008-03-13	Haveson et al.	
	249	20080070550	A	2008-03-20	Hose, David Alan	
	250	20080077705	A1	2008-03-27	Li et al.	
	251	20080080457	A1	2008-04-03	Cole, Terry L.	
	252	20080081606		2008-04-03	COLE, Terry L.	
	253	20080082643		2008-04-03	STORRIE et al.	
	254	20080083013		2008-04-03	SOLIMAN et al.	
	255	20080085707		2008-04-10	FADELL, Tony	
	256	20080089295	A	2008-04-17	Keeler, James D. et al.	
	257	20080089303	A1	2008-04-17	Wirtanen et al.	
	258	20080095339		2008-04-24	ELLIOTT et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	259	20080096559	A1	2008-04-24	Phillips et al.	
	260	20080098062		2008-04-24	BALIA, Hinal K.	
	261	20080109679		2008-05-08	WRIGHT et al.	
	262	20080120129	A	2008-05-22	Seubert et al.	
	263	20080120668		2008-05-22	Yau, Frank Chuen-Foo	
	264	20080120688		2008-05-22	QIU et al.	
	265	20080125079	A1	2008-05-29	O'Neil et al.	
	266	20080126287	A1	2008-05-29	Cox et al.	
	267	20080127304		2008-05-29	GINTER et al.	
	268	20080130534		2008-06-05	TOMIOKA, Tazuko	
	269	20080130656		2008-06-05	KIM et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	270	20080132201		2008-06-05	KARLBERG, Johan	
	271	20080132268		2008-06-05	CHOI-GROGAN et al.	
	272	20080134330		2008-06-05	KAPOOR et al.	
	273	20080139210	A	2008-06-12	Gisby et al.	
	274	20080147454		2008-06-19	WALKER et al.	
	275	20080160958		2008-07-03	ABICHANDANI et al.	
	276	20080162637		2008-07-03	ADAMCZYK et al.	
	277	20080162704		2008-07-03	POPLETT et al.	
	278	20080164304		2008-07-10	NARASIMHAN et al.	
	279	20080166993	A1	2008-07-10	Gautier et al.	
	280	20080167027		2008-07-10	GAUTIER et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	281	20080167033		2008-07-10	BECKERS, Michel	
	282	20080168275	A1	2008-07-10	DeAtley et al.	
	283	20080168523		2008-07-10	ANSARI et al.	
	284	20080177998		2008-07-24	APSANGI et al.	
	285	20080178300	A1	2008-07-24	Brown et al.	
	286	20080183812		2008-07-31	PAUL et al.	
	287	20080184127		2008-07-31	RAFEY et al.	
	288	20080189760		2008-08-07	ROSENBERG et al.	
	289	20080201266	A	2008-08-21	Chua et al.	
	290	20080207167		2008-08-28	BUGENHAGEN, Michael K.	
	291	20080212470		2008-09-04	CASTANEDA et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	292	20080212751	A1	2008-09-04	Chung, Simon	
	293	20080219268		2008-09-11	DENNISON, Larry R.	
	294	20080221951		2008-09-11	STANFORTH et al.	
	295	20080222692		2008-09-11	ANDERSSON et al.	
	296	20080225748		2008-09-18	KHEMANI et al.	
	297	20080229385		2008-09-18	FEDER et al.	
	298	20080229388		2008-09-18	MAES, Stephane H.	
	299	20080235511		2008-09-25	O'BRIEN, William G. et al.	
	300	20080240373		2008-10-02	WILHELM, Robert 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]

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	1	2688553	CA	A1	2008-12-04	Yoggie Security Systems, Inc.		
	2	101035308	CN	A	2006-03-09	Huawei Tech. Co. Ltd.		
	3	101080055	CN	A	2007-11-28	Tencent Technology (Shenzhen) Co., Ltd.		
	4	101115248	CN	A	2008-01-30	Lenovo Beijing Ltd.		
	5	101123553	CN	A	2007-09-11	SouTheast University		
	6	101127988	CN	A	2008-02-20	ZTE Corporation		
	7	101155343	CN	B	2006-09-29	Huawei Tech. Co. Ltd.		
	8	101183958	CN	A	2008-05-21	Huawei Tech. Co. Ltd.		
	9	101335666	CN	A	2008-12-31	Hangzhou H3C Technologies Co., Ltd.		
	10	101341764	CN	A	2009-01-07	Telefonaktiebolaget LM Ericsson		
	11	101815275	CN	A	2010-08-25	Yang, Liu		

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	12	1310401	CN	A	2001-08-29	Wang, Di Xing		
	13	1345154A	CN		2002-04-17	Datang Microelectronics Tech. Co.		
	14	1508734	CN	A	2004-06-30	Chinese Creative Corp.		
	15	1538730	CN	A	2004-10-20	Zhongxing Communication Co., Ltd.		
	16	1567818	CN	A	2005-01-19	Huawei Tech. Co. Ltd.		
	17	1801829	CN	A	2006-07-12	Kunda Computer Technology (Kunshan) Co., Ltd.		
	18	1802839	CN	A	2006-07-12	Motorola Inc.		
	19	1867024	CN	A	2006-11-22	Huawei Technologies Co., Ltd.		
	20	1878160	CN	A	2006-12-13	Huawei Technologies Co., Ltd.		
	21	1889777	CN	A	2006-07-19	Huawei Tech. Co. Ltd.		
	22	1937511	CN	A	2007-03-28	ZTE		

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	23	1289326	EP	A1	2003-03-05	Motorola, Inc.		
	24	1463238	EP		2004-09-29	Alcatel		
	25	1503548	EP	A1	2005-02-02	FG Microtec GmbH		
	26	1545114	EP	A1	2005-06-22	Alcatel		
	27	1739518	EP		2007-01-03	Research In Motion Limited		
	28	1772988	EP		2007-04-11	Huawei Technologies Co., Ltd.		
	29	1850575	EP	A1	2007-10-31	Research In Motion		
	30	1887732	EP	A1	2008-02-13	Huawei Technologies Co., Ltd.		
	31	1978772	EP		2008-10-08	British Telecommunications Public Limited Company		
	32	2007065	EP	A1	2008-12-24	Huawei Technologies Co., Ltd.		
	33	2005339247	JP	A	2005-12-08	Secured Communications		

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	34	2006041989	JP		2006-02-09	Fujitsu Ltd.		
	35	2006155263	JP	A	2006-06-15	NEC Corporation		
	36	2006197137	JP		2006-07-27	NTT Docomo Inc.		
	37	2006344007	JP	A	2006-12-21	Hitachi Ltd.		
	38	2007318354	JP	A	2007-12-06	Fujitsu Ten Ltd.		
	39	2008301121	JP	A	2008-12-11	Kyocera Corp.		
	40	2009111919	JP		2009-05-21	Kyocera Communications Systems		
	41	2009212707	JP	A	2009-09-17	Fujitsu Ltd.		
	42	2009218773	JP		2009-09-24	Advanced Telecommunication Research Institute Inte		
	43	2009232107	JP	A	2009-10-08	Fujitsu Ltd.		
	44	3148713	JP	B2	2001-03-26	ATR Kankyo Tekio Tsushin Kenkyusho		

EFS Web 2.1.17

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	45	0208863	WO		2002-01-31	Telemac Corp.		
	46	1998058505	WO		1998-12-23	Sonera Oy		
	47	1999027723	WO		1999-06-03	Telefonaktiebolaget LM Ericsson		
	48	1999065185	WO		1999-12-16	British Telecommunications Public Limited Company		
	49	2002045315	WO	A2	2002-06-06	Micromuse		
	50	2002067616	WO	A1	2002-08-29	Sonera Oyj		

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	"ASA/PIX: Allow Split Tunneling for VPN Clients on the ASA Configuration Example," Document ID 70917, January 10, 2008	
	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	

EFS Web 2.1.17

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	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	"Jentro Technologies launches Zenlet platform to accelerate location-based content delivery to mobile devices," The Mobile Internet, Boston, MA, Feb. 2008	
	6	"The Construction of Intelligent Residential District in Use of Cable Television Network," Shandong Science, Vol. 13, No. 2, June 2000	
	7	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	
	8	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	
	9	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	
	10	ALONISTIOTI et al., "Intelligent Architectures Enabling Flexible Service Provision and Adaptability," 2002	
	11	Amazon Technologies, Inc., "Kindle™ User's Guide," 3rd Edition, Copyright 2004-2009	
	12	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)	
	13	Blackberry Mobile Data System, version 4.1, Technical Overview, 2006	
	14	CHANDRASEKHAR et al., "Femtocell Networks: A Survey," June 28, 2008	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	15	CHAOUCHI et al., "Policy Based Networking in the Integration Effort of 4G Networks and Services," 2004 IEEE	
	16	Cisco Systems, Inc., "Cisco Mobile Exchange (CMX) Solution Guide: Chapter 2 - Overview of GSM, GPRS, and UMTS," November 4, 2008	
	17	Client Guide for Symantec Endpoint Protection and Symantec Network Access Control, 2007	
	18	DIKAIAKOS et al., "A Distributed Middleware Infrastructure for Personalized Services," November 24, 2003	
	19	Dixon et al., "Triple Play Digital Services: Comcast and Verizon (Digital Phone, Television, and Internet), August 2007	
	20	Ehnert, "Small application to monitor IP trafic on a Blackberry - 1.01.03 ", March 27, 2008; http://www.ehnert.net/MiniMoni/	
	21	European Commission, "Data Roaming Tariffs - Transparency Measures," obtained from EUROPA - Europe's Information Society Thematic Portal website, June 24, 2011: "http://ec.europa.eu/information_society/activities/roaming/data/measures/index_en.htm."	
	22	FAROOQ et al., "An IEEE 802.16 WiMax Module for the NS-3 Simulator," March 2-6, 2009	
	23	Fujitsu, "Server Push Technology Survey and Bidirectional Communication in HTTP Browser," January 9, 2008 (JP)	
	24	HAN et al., "Information Collection Services for Qos-Aware Mobile Applications," 2005	
	25	HARTMANN et al., "Agent-Based Banking Transactions & Information Retrieval - What About Performance Issues?" 1999	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	26	Hewlett-Packard Development Company, LP, "IP Multimedia Services Charging," white paper, January 2006	
	27	HOSSAIN et al., "Gain-Based Selection of Ambient Media Services in Pervasive Environments," Mobile Networks and Applications. 03 October 2008	
	28	Jing et al., "Client-Server Computing in Mobile Environments," GTE Labs. Inc., Purdue University, ACM Computing Surveys, Vol. 31, No. 2, June 1999	
	29	Kasper et al., "Subscriber Authentication in mobile cellular Networks with virtual software SIM Credentials using Trusted Computing," Fraunhofer-Institute for Secure Information Technology SIT, Darmstadt, Germany; ICACT 2008	
	30	Kassar et al., "An overview of vertical handover decision strategies in heterogeneous wireless networks," ScienceDirect, University Pierre & Marie Curie, Paris, France, 6/5/2007	
	31	Kim, "Free wireless a high-wire act; MetroFi needs to draw enough ads to make service add profits," San Francisco Chronicle, Aug. 21, 2006	
	32	KNIGHT et al., "Layer 2 and 3 Virtual Private Networks: Taxonomy, Technology, and Standarization Efforts," IEEE Communications Magazine, June 2004	
	33	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	
	34	KOUTSOPOULOU et al., "Middleware Platform for the Support of Charging Reconfiguration Actions," 2005	
	35	Kuntze et al., "Trustworthy content push," Fraunhofer-Institute for Secure Information Technology SIT; Germany; WCNC 2007 proceedings, IEEE	
	36	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	

EFS Web 2.1.17

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	37	LI, Yu, "Dedicated E-Reading Device: The State of the Art and The Challenges," Scroll, Vol. 1, No. 1, 2008	
	38	Loopt User Guide, metroPCS, 7/17/2008	
	39	Muntermann et al., "Potentiale und Sicherheitsanforderungen mobiler Finanzinformationsdienste und deren Systeminfrastrukturen," Chair of Mobile Commerce & Multilateral Security, Goethe Univ. Frankfurt, 2004	
	40	NetLimiter Lite 4.0.19.0; http://www.heise.de/download/netlimiter-lite-3617703.html from vol. 14/2007	
	41	NILSSON et al., "A Novel MAC Scheme for Solving the QoS Parameter Adjustment Problem in IEEE802.11e EDCA," February 2006	
	42	Nuzman et al., "A compund model for TCP connection arrivals for LAN and WAN applications," Oct. 22, 2002	
	43	Open Mobile Alliance (OMA), Push Architecture, Candidate Version 2.2; Oct. 2, 2007; OMA-AD-Push-V2_2-20071002-C	
	44	OPPLIGER, Rolf, "Internet Security: Firewalls and Bey," Communications of the ACM, May 1997, Vol. 40. No. 5	
	45	RAO et al., "Evolution of Mobile Location-Based Services," Communication of the ACM, December 2003	
	46	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	
	47	Rivadeneyra et al., "A communication architecture to access data services through GSM," San Sebastian, Spain, 1998	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	48	Sabat, "The evolving mobile wireless value chain and market structure," Nov. 2002	
	49	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	
	50	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	03/25/2019

*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.J.R./

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

PTO/SB/08a (03-15)
Approved for use through 07/31/2016. 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	15582350
Filing Date	2017-04-28
First Named Inventor	Raleigh
Art Unit	2447
Examiner Name	not yet assigned
Attorney Docket Number	RALEP007C11C3C2C3C2

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	7974624		2011-07-05	Gallagher, Michael D. et al.	
	2	7975184		2011-07-05	GOFF et al.	
	3	7978627		2011-07-12	TAYLOR, William Scott et al.	
	4	7978686	B2	2011-07-12	Goyal et al.	
	5	7979069	B2	2011-07-12	Hupp et al.	
	6	7984130		2011-07-19	BOGINENI et al.	
	7	7984511	B2	2011-07-19	Kocher Paul et al.	
	8	7986935		2011-07-26	D'SOUZA et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	9	7987496	B2	2011-07-26	Bryce et al.	
	10	7987510	B2	2011-07-26	Kocher et al.	
	11	7990049	B2	2011-08-02	Shioya, Shunsuke	
	12	8000276	B2	2011-08-16	Scherzer, Shimon et al.	
	13	8000318		2011-08-16	Wiley, William L. et al.	
	14	8005009		2011-08-23	McKee, Neil et al.	
	15	8005459		2011-08-23	BALSILLIE, Jim	
	16	8005726	B1	2011-08-23	Bao, Yulin	
	17	8005913	B1	2011-08-23	Carlander, Carrie	
	18	8005988		2011-08-23	MAES, Stephane H.	
	19	8010080		2011-08-30	THENTHIRUPERAI et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	20	8010081		2011-08-30	ROSKOWSKI, Steve	
	21	8010082	B2	2011-08-30	Sutaria et al.	
	22	8010990	B2	2011-08-30	Ferguson et al.	
	23	8015133		2011-09-06	WU et al.	
	24	8015234		2011-09-06	LUM et al.	
	25	8019687		2011-09-13	WANG et al.	
	26	8019820		2011-09-13	Son, Giyeong et al.	
	27	8019846	B2	2011-09-13	Roelens et al.	
	28	8019868		2011-09-13	RAO, Goutham et al.	
	29	8023425		2011-09-20	RALEIGH, Gregory G.	
	30	8024397		2011-09-20	ERICKSON, Richard R. et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	31	8027339	B2	2011-09-27	Short, Joel E. et al.	
	32	8031601	B2	2011-10-04	Feroz et al.	
	33	8032168	B2	2011-10-04	Ikaheimo, Jorma	
	34	8032409	B1	2011-10-04	Mikurak, Michael G.	
	35	8032899	B2	2011-10-04	Archer, Charles J. et al.	
	36	8036387	B2	2011-10-11	Kudelski et al.	
	37	8044792	B2	2011-10-25	Orr et al.	
	38	8045973	B2	2011-10-25	Chambers, Michael D.	
	39	8046449	B2	2011-10-25	Yoshiuchi, Hideya	
	40	8050275		2011-11-01	IYER, Jayaraman R.	
	41	8050690	B2	2011-11-01	Neeraj, Chawla	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	42	8050705	B2	2011-11-01	Sicher et al.	
	43	8059530		2011-11-15	Cole, Terry L.	
	44	8060463		2011-11-15	Spiegel, Joel R.	
	45	8064418	B2	2011-11-22	Maki, Lasse	
	46	8065365	B2	2011-11-22	Saxena et al.	
	47	8068824		2011-11-29	SHAN, Xueshan et al.	
	48	8068829	B2	2011-11-29	Lemond, Eric et al.	
	49	8073427	B2	2011-12-06	Koch et al.	
	50	8073721		2011-12-06	Lewis, Lundy	
	51	8078140	B2	2011-12-13	Baker, Matthew Donald et al.	
	52	8078163	B2	2011-12-13	Lemond, Eric et al.	

EFS Web 2.1.17

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	53	8085808	B2	2011-12-27	Brusca et al.	
	54	8086398	B2	2011-12-27	Sanchez et al.	
	55	8086497	B1	2011-12-27	Oakes III, Charles Lee	
	56	8086791	B2	2011-12-27	Caulkins, Jason	
	57	8090359		2012-01-03	Proctor Jr., James Arthur et al.	
	58	8090616		2012-01-03	Proctor Jr., James Arthur et al.	
	59	8094551		2012-01-10	HUBER, Kurt Donald et al.	
	60	8095112	B2	2012-01-10	Chow, Richard et al.	
	61	8095640	B2	2012-01-10	Guingo et al.	
	62	8095666		2012-01-10	SCHMIDT et al.	
	63	8098579		2012-01-17	Ray, Amar N. et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	64	8099077		2012-01-17	CHOWDHURY et al.	
	65	8099517		2012-01-17	JIA et al.	
	66	8102814		2012-01-24	RAHMAN, Shahriar I. et al.	
	67	8103285	B2	2012-01-24	Kalhan, Amit	
	68	8104080	B2	2012-01-24	Burns et al.	
	69	8107953	B2	2012-01-31	Zimmerman et al.	
	70	8108520		2012-01-31	Ruutu, Jussi et al.	
	71	8112435	B2	2012-02-07	Epstein et al.	
	72	8116223		2012-02-14	TIAN, Dan et al.	
	73	8116749		2012-02-14	Proctor Jr., James Arthur et al.	
	74	8116781	B2	2012-02-14	Chen, Xixian et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	75	8122128		2012-02-21	Burke, II, Robert M. et al.	
	76	8122249		2012-02-21	Falk, Rainer et al.	
	77	8125897	B2	2012-02-28	Ray et al.	
	78	8126123		2012-02-28	Cai, Yigang et al.	
	79	8126396	B2	2012-02-28	Bennett, James D.	
	80	8126476	B2	2012-02-28	Vardi, Yosef et al.	
	81	8126722		2010-02-28	ROBB, Terence Alan et al.	
	82	8130793	B2	2012-03-06	Edwards, Stephen K. et al.	
	83	8131256		2012-03-06	MARTTI, Jyrki et al.	
	84	8131281	B1	2012-03-06	Hildner et al.	
	85	8131840	B1	2012-03-06	Denker, Richard E.	

EFS Web 2.1.17

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	86	8131858	B2	2012-03-06	Agulnik et al.	
	87	8132256	B2	2012-03-06	Bari, Farooq	
	88	8134954	B2	2012-03-13	Godfrey, James A. et al.	
	89	8135388		2012-03-13	Gailloux, Michael A. et al.	
	90	8135392		2012-03-13	MARCELLINO et al.	
	91	8135657		2012-03-13	Kapoor, Harsh et al.	
	92	8140690	B2	2012-03-20	Ly et al.	
	93	8144591		2012-03-27	GHAI et al.	
	94	8145194	B2	2012-03-27	Yoshikawa et al.	
	95	8149823		2012-04-03	Turcan, Diane Brown et al.	
	96	8150394	B2	2012-04-03	Bianconi et al.	

EFS Web 2.1.17

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	97	8150431		2012-04-03	Wolovitz, Lionel et al.	
	98	8151205	B2	2012-04-03	Follmann et al.	
	99	8155155		2012-04-10	Chow, Albert T. et al.	
	100	8155620		2012-04-10	Wang, Jun et al.	
	101	8155666	B2	2012-04-10	Alizadeh-Shabdiz, Farshid	
	102	8155670		2012-04-10	Fullam, Scott et al.	
	103	8156206		2012-04-10	KILEY, Kevin J. et al.	
	104	8159520	B1	2012-04-17	Dhanoa et al.	
	105	8160056	B2	2012-04-17	Van der Merwe et al.	
	106	8160598	B2	2012-04-17	Savoor, Raghvendra	
	107	8165576		2012-04-24	Raju, Vishwanath et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	108	8166040	B2	2012-04-24	Brindisi, Richard G. et al.	
	109	8166554	B2	2012-04-24	John, Pramod	
	110	8170553		2012-05-01	BENNETT, James D.	
	111	8174378	B2	2012-05-08	Richman et al.	
	112	8174970	B2	2012-05-12	Adamczyk, Maria et al.	
	113	8175574	B1	2012-05-08	Panda et al.	
	114	8180881	B2	2012-05-15	Seo et al.	
	115	8180886	B2	2012-05-15	Overcash et al.	
	116	8184530		2012-05-22	SWAN, Tim L. et al.	
	117	8184590		2012-05-22	Rosenblatt, Ariel	
	118	8185093		2012-05-22	Jheng, Yu-Syuan et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	119	8185127	B1	2012-05-22	Cai, Zheng et al.	
	120	8185152		2012-05-22	GOLDNER, Alla	
	121	8185158		2012-05-22	Tamura, Motoshi et al.	
	122	8190122	B1	2012-05-29	Alexander et al.	
	123	8190675		2012-05-29	TRIBBETT, David	
	124	8191106	B2	2012-05-29	Choyi et al.	
	125	8191116		2012-05-29	Gazzard, Daryl	
	126	8191124	B2	2012-05-29	Wynn et al.	
	127	8194549	B2	2012-06-05	Huber et al.	
	128	8194553		2012-06-05	LIANG, Zhi Yong et al.	
	129	8194581	B1	2012-06-05	Schroeder et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	130	8195153	B1	2012-06-05	Frencel et al.	
	131	8195163	B2	2012-06-05	Gisby, Doug et al.	
	132	8195661	B2	2012-06-05	Kalavade, Asawaree	
	133	8196199	B2	2012-06-05	Hrastar et al.	
	134	8200163	B2	2012-06-12	Hoffman, George E.	
	135	8200200	B1	2012-06-12	Belser et al.	
	136	8200509	B2	2012-06-12	Kenedy, Andrew Alexander et al.	
	137	8200775		2012-06-12	MOORE, James F.	
	138	8200818	B2	2012-06-12	Freund et al.	
	139	8204190		2012-06-19	Bang, Jung-Hee et al.	
	140	8204505	B2	2012-06-19	Jin et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	141	8208788	B2	2012-06-26	Ando et al.	
	142	8208919		2012-06-26	KOTECHA, Lalit Ratilal	
	143	8213296		2012-07-03	SHANNON, Frank M. et al.	
	144	8213363		2012-07-03	Ying, Wen-Ping et al.	
	145	8214536		2012-07-03	ZHAO, Wen	
	146	8219134	B2	2012-07-10	Maharajh et al.	
	147	8223655	B2	2012-07-17	Heinz et al.	
	148	8224382		2012-07-17	Bultman, Michael J.	
	149	8224773		2012-07-17	Spiegel, Joel R.	
	150	8228818	B2	2012-07-24	Chase et al.	
	151	8229394	B2	2012-07-24	Karlberg, Johan	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	152	8229914	B2	2012-07-24	Ramer et al.	
	153	8233433	B2	2012-07-31	Kalhan, Amit	
	154	8233883		2012-07-31	De Froment, Eric	
	155	8233895		2012-07-31	Tysowski, Piotr Konrad	
	156	8238287		2012-08-07	Gopi, Paramesh et al.	
	157	8239520		2012-08-07	GRAH, Adrian	
	158	8242959	B2	2012-08-14	Mia, Rashidus S. et al.	
	159	8244241		2012-08-14	Montemurro, Michael	
	160	8249601	B2	2012-08-21	Emberson et al.	
	161	8254880	B2	2012-08-28	Aaltonen et al.	
	162	8254915		2012-08-28	Kozisek, Steven E.	

EFS Web 2.1.17

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	163	8255515		2012-08-28	MELMAN, David et al.	
	164	8255534	B2	2012-08-28	Assadzadeh, Alireza	
	165	8255689		2012-08-28	KIM, Eun Ah et al.	
	166	8259692	B2	2012-09-04	Bajko, Gabor	
	167	8264965	B2	2012-09-11	Dolganow et al.	
	168	8265004		2012-09-11	Toutonghi, Michael J.	
	169	8266681		2012-09-11	Deshpande, Sumit B. et al.	
	170	8270955	B2	2012-09-18	Ramer et al.	
	171	8270972	B2	2012-09-18	Otting, Marcia J. et al.	
	172	8271025	B2	2012-09-18	Brisebois et al.	
	173	8271045		2012-09-18	Parolkar, Satish et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	174	8271049		2012-09-18	SILVER, Andrew et al.	
	175	8271992	B2	2012-09-18	Chatley, Scott P. et al.	
	176	8275415	B2	2012-09-25	Huslak, Nicholas S.	
	177	8279067		2012-10-02	BERGER, Thomas R. et al.	
	178	8279864		2012-10-02	Wood, Daniel M.	
	179	8280354		2012-10-02	Smith, Christopher et al.	
	180	8284740		2012-10-09	O'CONNOR, Dennis M.	
	181	8285249	B2	2012-10-09	Baker, Matthew Donald et al.	
	182	8291238		2012-10-16	GINTER, Karl L. et al.	
	183	8291439	B2	2012-10-16	Jethi et al.	
	184	8296404		2012-10-23	McDysan, Dave et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	185	8300575	B2	2012-10-30	Willars, Per	
	186	8307067	B2	2012-11-06	Ryan, Nicholas M.	
	187	8315198	B2	2012-11-20	Corneille et al.	
	188	8315593	B2	2012-11-20	Gallant et al.	
	189	8315999	B2	2012-11-20	Chatley, Scott P. et al.	
	190	8320244	B2	2012-11-27	Muqattash et al.	
	191	8320949		2012-11-27	Matta, Sudheer Poorna Chandra	
	192	8325638		2012-12-04	Jin, Haipeng et al.	
	193	8325906	B2	2012-12-04	Fullarton et al.	
	194	8326319	B2	2012-12-04	Davis, Richard W.	
	195	8326828	B2	2012-12-04	Zhou et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	196	8331223	B2	2012-12-11	Hill et al.	
	197	8331293		2012-12-11	Sood, Kapil	
	198	8332375		2012-12-11	Chatley, Scott P. et al.	
	199	8339991	B2	2012-12-25	Biswas et al.	
	200	8340678	B1	2012-12-25	Pandey, Vinod	
	201	8340718		2012-12-25	Colonna, Massimo et al.	
	202	8346210	B2	2013-01-01	Balsan et al.	
	203	8347104	B2	2013-01-01	Pathiyal, Krishna K.	
	204	8347378	B2	2013-01-01	Merkin et al.	
	205	8350700		2013-01-08	Fast, Raymond D. et al.	
	206	8351592	B2	2013-01-08	Freeny Jr et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	207	8351898	B2	2013-01-08	Raleigh, Gregory G.	
	208	8352360	B2	2013-01-08	De Judicibus et al.	
	209	8352980		2013-01-08	Howcroft, Jerald Robert	
	210	8355696	B1	2013-01-15	Olding et al.	
	211	8356336	B2	2013-01-15	Johnston, Keith et al.	
	212	8358638	B2	2013-01-22	Scherzer, Tamir et al.	
	213	8358975	B2	2013-01-22	Bahl et al.	
	214	8363658		2013-01-29	Delker, Jason R. et al.	
	215	8363799	B2	2013-01-29	Gruchala et al.	
	216	8364806		2013-01-29	Short, Joel E. et al.	
	217	8370477		2013-02-05	Short, Joel E. et al.	

EFS Web 2.1.17

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	218	8370483	B	2013-02-05	Choong Jason et al.	
	219	8374090		2013-02-12	Morrill, Robert J. et al.	
	220	8374592		2013-02-12	Proctor, Jr. James A. et al.	
	221	8375128	B2	2013-02-12	Tofighbakhsh et al.	
	222	8375136	B2	2013-02-12	Roman et al.	
	223	8380247	B2	2013-02-19	Engstrom	
	224	8385199	B1	2013-02-26	Coward et al.	
	225	8385896		2013-02-26	Proctor Jr., James A. et al.	
	226	8385964	B2	2013-02-26	Haney, Richard D.	
	227	8386386		2013-02-26	Zhu, Kevin	
	228	8396929		2013-03-12	Helfman, Nadav et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	229	8402165	B2	2013-03-19	Deu-Ngoc et al.	
	230	8402540		2013-03-19	Kapoor, Harsh et al.	
	231	8406736	B2	2013-03-26	Das et al.	
	232	8407763	B2	2013-03-26	Weller et al.	
	233	8411587		2013-04-02	Curtis, William et al.	
	234	8411691	B2	2013-04-02	Aggarwal	
	235	8418168	B2	2013-04-09	Tyhurst et al.	
	236	8423016		2013-04-16	BUCKLEY, Adrian et al.	
	237	8429403		2013-04-23	Moret, Eric et al.	
	238	8437734		2013-05-07	Ray, Amar N. et al.	
	239	8442015	B2	2013-05-14	Behzad et al.	

EFS Web 2.1.17

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	240	8446831	B2	2013-05-21	Kwan et al.	
	241	8447607	B2	2013-05-21	Weider, Chris et al.	
	242	8447980		2013-05-21	Godfrey, James A. et al.	
	243	8448015	B2	2013-05-21	Gerhart, David	
	244	8461958	B2	2013-06-11	Saenz et al.	
	245	8463232	B2	2013-06-11	Tuli et al.	
	246	8468337	B2	2013-06-18	Gaur, Santosh P. et al.	
	247	8472371		2013-06-25	Bari, Farooq et al.	
	248	8477778		2013-07-02	Lehmann Jr., L. Curtis et al.	
	249	8483135		2013-07-09	Cai, Yigang et al.	
	250	8483694	B2	2013-07-09	Lewis et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	251	8484327	B2	2013-07-09	Werner et al.	
	252	8488597	B2	2013-07-16	Nie et al.	
	253	8489110	B2	2013-07-16	Frank et al.	
	254	8489720	B1	2013-07-16	Morford, Michael et al.	
	255	8494559	B1	2013-07-23	Malmi	
	256	8495181	B2	2013-07-23	Venkatraman et al.	
	257	8495227		2013-07-23	Kaminsky, David L. et al.	
	258	8495360		2013-07-23	Falk, Rainer et al.	
	259	8495700	B2	2013-07-23	Shahbazi, Majid	
	260	8503358	B2	2013-08-06	Hanson et al.	
	261	8503455	B2	2013-08-06	Heikens, Heico	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	262	8504032	B2	2013-08-06	Lott et al.	
	263	8504687	B2	2013-08-06	Maffione et al.	
	264	8504729		2013-08-06	Pezzutti, David A.	
	265	8505073	B2	2013-08-06	Taglienti et al.	
	266	8509082	B2	2013-08-13	Heinz, John M. et al.	
	267	8514927	B2	2013-08-20	Sundararajan et al.	
	268	8520589		2013-08-27	Bhatt, Yogesh et al.	
	269	8521110		2013-08-27	Rofougaran, Ahmadreza	
	270	8521775	B1	2013-08-27	Poh et al.	
	271	8522039	B2	2013-08-27	Hyndman et al.	
	272	8522249	B2	2013-08-27	Beaule, Stephane	

EFS Web 2.1.17

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	273	8522337	B2	2013-08-27	Adusumilli et al.	
	274	8523547	B2	2013-09-03	Pekrul, Merton W.	
	275	8526329	B2	2013-09-03	Mahany, Ronald L. et al.	
	276	8526350	B2	2013-09-03	Xue, Qi et al.	
	277	8527410	B2	2013-09-03	Markki et al.	
	278	8527662	B2	2013-09-03	Biswas et al.	
	279	8528068	B1	2013-09-03	Weglein et al.	
	280	8531954	B2	2013-09-10	McNaughton et al.	
	281	8532610	B2	2013-09-10	Manning Cassett et al.	
	282	8533775	B2	2013-09-10	Alcorn et al.	
	283	8538394	B2	2013-09-17	Zimmerman et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	284	8538421	B2	2013-09-17	Brisebois et al.	
	285	8538458	B2	2013-09-17	Haney, Richard D.	
	286	8539544	B2	2013-09-17	Garimella et al.	
	287	8543265	B2	2013-09-24	Ekhaguere et al.	
	288	8543814	B2	2013-09-24	Laitinen et al.	
	289	8544105	B2	2013-09-24	Mclean et al.	
	290	8548427	B2	2013-10-01	Chow et al.	
	291	8554876	B2	2013-10-08	Winsor, Gerald W.	
	292	8561138	B2	2013-10-15	Rothman, Michael M. et al.	
	293	8565746	B2	2013-10-22	Hoffman, George E.	
	294	8566236	B2	2013-10-22	Busch, James David	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	295	8571474	B2	2013-10-29	Chavez et al.	
	296	8571501	B2	2013-10-29	Miller et al.	
	297	8571598	B2	2013-10-29	Valavi, John J.	
	298	8571993	B2	2013-10-29	Kocher et al.	
	299	8572117	B2	2013-10-29	Rappaport, Theodore S.	
	300	8572256	B2	2013-10-29	Babbar, Uppinder Singh	

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.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	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	03/25/2019

*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.J.R./

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

PTO/SB/08a (03-15)
Approved for use through 07/31/2016. 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	15582350
Filing Date	2017-04-28
First Named Inventor	Raleigh
Art Unit	2447
Examiner Name	not yet assigned
Attorney Docket Number	RALEP007C11C3C2C3C2

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	8583499		2013-11-12	De Judicibus, Dario et al.	
	2	8589955	B2	2013-11-19	Roundtree et al.	
	3	8600895	B2	2013-12-03	Felsher, David Paul	
	4	8601125	B2	2013-12-03	Huang et al.	
	5	8605691	B2	2013-12-10	Soomro et al.	
	6	8634425	B2	2014-01-21	Gorti et al.	
	7	8635164	B2	2014-01-21	Rosenhaft et al.	
	8	8639215	B2	2014-01-28	McGregor et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	9	8644702	B1	2014-02-04	Kalajan, Kevin E.	
	10	8644813	B1	2014-02-04	Gailloux et al.	
	11	8645518	B	2014-02-04	David, Scott L.	
	12	8655357	B1	2014-02-18	Gazzard et al.	
	13	8660853	B2	2014-02-25	Robb et al.	
	14	8666395	B2	2014-03-04	Silver, Andrew	
	15	8667542	B1	2014-03-04	Bertz et al.	
	16	8670334	B	2014-03-11	Keohane et al.	
	17	8675852	B2	2014-03-18	Maes, Stephane H.	
	18	8676925	B	2014-03-18	Liu et al.	
	19	8693323		2014-04-08	McDysan, David E.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	20	8694772	B2	2014-04-08	Kao et al.	
	21	8700729	B2	2014-04-15	Dua, Robin	
	22	8701015	B2	2014-04-15	Bonnat, Pierre	
	23	8706863		2014-04-22	Fadell, Anthony	
	24	8713535	B2	2014-04-29	Malhotra et al.	
	25	8713641	B1	2014-04-29	Pagan et al.	
	26	8719397	B2	2014-05-06	Levi et al.	
	27	8719423	B2	2014-05-06	Wyld	
	28	8725899	B	2014-05-13	Short et al.	
	29	8730842	B2	2014-05-20	Collins et al.	
	30	8731519	B2	2014-05-20	Flynn et al.	

EFS Web 2.1.17

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	31	8732808	B2	2014-05-20	Sewall et al.	
	32	8739035	B2	2014-05-27	Trethewey, Jim	
	33	8744339	B2	2014-06-03	Halfmann et al.	
	34	8761711	B2	2014-06-24	Grignani et al.	
	35	8780857	B2	2014-07-15	Balasubramanian et al.	
	36	8787249	B2	2014-07-22	Giaretta et al.	
	37	8793304	B2	2014-07-29	Lu et al.	
	38	8811338	B2	2014-08-19	Jin et al.	
	39	8811991	B2	2014-08-19	Jain et al.	
	40	8819253	B2	2014-08-26	Simeloff et al.	
	41	8825109	B2	2014-09-02	Montemurro et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	42	8826411	B2	2014-09-02	Moen et al.	
	43	8831561	B2	2014-09-09	Sutaria et al.	
	44	8838752	B2	2014-09-16	Lor et al.	
	45	8855620	B2	2014-10-07	Sievers et al.	
	46	8862751	B2	2014-10-14	Faccin et al.	
	47	8875042	B2	2014-10-28	LeJeune et al.	
	48	8880047	B2	2014-11-04	Konicek et al.	
	49	8908516	B2	2014-12-09	Tzamaloukas et al.	
	50	8930238	B2	2015-01-06	Coffman et al.	
	51	8943551	B2	2015-01-27	Ganapathy et al.	
	52	8948726	B2	2015-02-03	Smith et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	53	8966018	B2	2015-02-24	Bugwadia et al.	
	54	8971912	B2	2015-03-03	Chou et al.	
	55	8977284	B2	2015-03-10	Reed, Mark J.	
	56	8995952	B1	2015-03-31	Baker et al.	
	57	9002342	B2	2015-04-07	Tenhunen et al.	
	58	9014973	B2	2015-04-21	Ruckart, John	
	59	9015331	B2	2015-04-21	Lai et al.	
	60	9030934	B2	2015-05-12	Shah et al.	
	61	9049010		2015-06-02	Jueneman et al.	
	62	9111088	B2	2015-08-18	Ghai et al.	
	63	9172553	B2	2015-10-27	Dawes et al.	

EFS Web 2.1.17

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	64	9325737	B2	2016-04-26	Gutowski et al.	
	65	9326173	B2	2016-04-26	Luft, Achim	
	66	9344557	B2	2016-05-17	Gruchala et al.	
	67	9367680	B2	2016-06-14	Mahaffey et al.	
	68	9413546	B2	2016-08-09	Meier et al.	
	69	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

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.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	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	03/25/2019

*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.J.R./

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

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

Application Number	15582350
Filing Date	2017-04-28
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP007C11C3C2C3C2

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	5915226	A	1999-06-22	Martineau	
	2	6246870	B1	2001-06-12	Dent et al.	
	3	6591098	B1	2003-07-08	Shieh et al.	
	4	6603975	B1	2003-08-05	Inouchi et al.	
	5	6959202	B2	2005-10-25	Heinonen et al.	
	6	7031733	B2	2006-04-18	Alminana et al.	
	7	7120133	B1	2006-10-10	Joo et al.	
	8	7315892	B2	2008-01-01	Freimuth et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3C2C3C2

	9	7548875	B2	2009-06-16	Mikkelsen et al.	
	10	7584298	B2	2009-09-01	Klinker et al.	
	11	7607041	B2	2009-10-20	Kraemer et al.	
	12	7610057	B2	2009-10-27	Bahl et al.	
	13	7620383	B2	2009-11-17	Taglienti et al.	
	14	7627600	B2	2009-12-01	Citron et al.	
	15	7668966	B2	2010-02-23	Klinker et al.	
	16	7681226	B2	2010-03-16	Kraemer et al.	
	17	7688792	B2	2010-03-30	Babbar et al.	
	18	7693107	B2	2010-04-06	De Froment, Eric	
	19	7774412	B1	2010-08-10	Schnepel, Soenke	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3C2C3C2

	20	7797019	B2	2010-09-14	Friedmann	
	21	7805522	B2	2010-09-28	Schlüter et al.	
	22	7813746	B2	2010-10-12	Rajkotia, Purva R.	
	23	7835275	B1	2010-11-16	Swan et al.	
	24	7853656	B2	2010-12-14	Yach et al.	
	25	7882560	B2	2011-02-01	Kraemer et al.	
	26	7930553	B2	2011-04-19	Satarasinghe et al.	
	27	7979889	B2	2011-07-12	Gladstone et al.	
	28	8024424	B2	2011-09-20	Freimuth et al.	
	29	8060017	B2	2011-11-15	Schlicht et al.	
	30	8090361	B2	2012-01-03	Hagan, Guy R.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3C2C3C2

	31	8149748	B2	2012-04-03	Bata et al.	
	32	8340625	B1	2012-12-25	Johnson et al.	
	33	8346923	B2	2013-01-01	Rowles et al.	
	34	8392982	B2	2013-03-05	Harris et al.	
	35	8413245	B2	2013-04-02	Kraemer et al.	
	36	8495743	B2	2013-07-23	Kraemer et al.	
	37	8504574	B2	2013-08-06	Dvorak et al.	
	38	8531995	B2	2013-09-10	Khan et al.	
	39	8559369	B2	2013-10-15	Barkan	
	40	8594665	B2	2013-11-26	Anschutz, Thomas	
	41	8620257	B2	2013-12-31	Qiu et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3C2C3C2

	42	8849297	B2	2014-09-30	Balasubramanian	
	43	8929374	B2	2015-01-06	Tönsing et al.	
	44	9137286	B1	2015-09-15	Yuan	
	45	9286469	B2	2016-03-15	Kraemer 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	20040024756	A1	2004-02-05	Rickard, John Terrell	

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	2010128391	WO	A2	2010-11-11	Bridgewater Systems 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]

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3C2C3C2

	1	Android Cupcake excerpts, The Android Open Source Project, Feb. 10, 2009	

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	03/25/2019

*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 2.1.18

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

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

PTO/SB/08a (03-15)
Approved for use through 07/31/2016. 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	15582350
Filing Date	2017-04-28
First Named Inventor	Gregory G. Raleigh
Art Unit	2447
Examiner Name	not yet assigned
Attorney Docket Number	RALEP007C11C3C2C3C2

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	6760417	B1	2004-07-06	Wallenius, Jukka	
	2	7539862	B2	2009-05-26	Edgett et al.	
	3	7721296	B2	2010-05-18	Ricagni, Giuseppe	
	4	7873346	B2	2011-01-18	Petersson et al.	
	5	7873540	B2	2011-01-18	Arumugam, Avin	
	6	8091087	B2	2012-01-03	Ali et al.	
	7	8146142	B2	2012-03-27	Lortz et al.	
	8	8190087	B2	2012-05-29	Fisher et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Gregory G. Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	9	8214890	B2	2012-07-03	Kirovski et al.	
	10	8285992	B2	2012-10-09	Mathur et al.	
	11	8588240	B2	2013-11-19	Ramankutty et al.	
	12	8676682	B2	2014-03-18	Kalliola, Janne	
	13	8818394	B2	2014-08-26	Bienas et al.	
	14	9064275	B1	2015-06-23	Lu et al.	
	15	9286604	B2	2016-03-15	Aabye et al.	
	16	9589117	B2	2017-03-07	Ali 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	20100284388	A1	2010-11-11	Fantini et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Gregory G. Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	2	20020099848	A1	2002-07-25	Lee, Hoon			

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]
	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	03/25/2019

*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.J.R./

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

PTO/SB/08a (03-15)
Approved for use through 07/31/2016. 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	15582350
Filing Date	2017-04-28
First Named Inventor	Gregory G. Raleigh
Art Unit	2447
Examiner Name	not yet assigned
Attorney Docket Number	RALEP007C11C3C2C3C2

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	7165040	B2	2007-01-16	Ehrman et al.	
	2	7656271	B2	2010-02-02	Ehrman et al.	
	3	8401968	B1	2013-03-19	Schattauer et al.	
	4	6535949	B1	2003-03-18	Parker, Kenneth W.	
	5	7809372	B2	2010-10-05	Rajaniemi, Jaakko	

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	20060101507	A1	2006-05-11	Camenisch, Ja L.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Gregory G. Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	2	20070171856	A1	2007-07-26	Bruce et al.	
	3	20110004917	A1	2011-01-06	Saisa 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	1098490	EP	A2	2001-05-09	Nortel Networks Ltd.		
	2	2026514	EP	A1	2009-02-18	Nokia Siemens Networks		
	3	2007129180	WO	A2	2007-11-15	Nokia Corp.		
	4	1942698	EP	A1	2008-07-09	Apple 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.	T[5]
	1		

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

EFS Web 2.1.17

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Gregory G. Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

EXAMINER SIGNATURE			
Examiner Signature	/ANDREW JOSEPH RUDY/	Date Considered	03/25/2019

*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.J.R./

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

PTO/SB/08a (03-15)
Approved for use through 07/31/2016. 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	15582350
Filing Date	2017-04-28
First Named Inventor	Raleigh
Art Unit	2447
Examiner Name	not yet assigned
Attorney Docket Number	RALEP007C11C3C2C3C2

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	7102620	B2	2006-09-05	Harries, Andrew Stanely Guy et al.	
	2	7110753	B2	2006-09-19	Campen, Kenneth Brian	
	3	7113780	B2	2006-09-26	Mckenna Daniel et al.	
	4	7113997		2012-09-26	Jayapalan, Jay et al.	
	5	7133386	B2	2006-11-07	Holur et al.	
	6	7133695	B2	2006-11-07	Beyda, William J.	
	7	7136361	B2	2006-11-14	Benveniste, Mathilde	
	8	7139569	B2	2006-11-21	Kato, Akira	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	9	7142876		2006-11-28	TROSSEN et al.	
	10	7149229	B1	2006-12-12	Leung, Kent K.	
	11	7149521	B2	2006-12-12	Sundar et al.	
	12	7151764	B1	2006-12-19	Heinonen et al.	
	13	7158792		2007-01-02	COOK et al.	
	14	7162237	B1	2007-01-09	Silver et al.	
	15	7167078		2007-01-23	POURCHOT, Shawn C.	
	16	7174156	B1	2007-02-06	Mangal, Manish	
	17	7174174		2007-02-06	BORIS et al.	
	18	7177919	B1	2007-02-13	Truong et al.	
	19	7180855		2007-02-20	LIN , Wei	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	20	7181017		2007-02-20	Nagel, Robert H. et al.	
	21	7191248	B2	2007-03-13	Chattopadhyay et al.	
	22	7197321		2007-03-27	ERSKINE et al.	
	23	7200112	B2	2007-04-03	Sundar et al.	
	24	7203169	B1	2007-04-10	Okholm, Jon et al.	
	25	7203721	B1	2007-04-10	Ben-Efraim et al.	
	26	7203752	B2	2007-04-10	Rice et al.	
	27	7212491		2007-05-01	Koga, Takahiro	
	28	7219123	B1	2007-05-15	Fiechter et al.	
	29	7222190	B2	2007-05-22	Klinker et al.	
	30	7222304	B2	2007-05-22	Beaton et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	31	7224968	B2	2007-05-29	Dobson et al.	
	32	7228354		2007-06-05	CHAMBLISS, David Darden et al.	
	33	7236780		2007-06-26	Benco, David S.	
	34	7242668	B2	2007-07-10	Kan et al.	
	35	7242920		2007-07-10	MORRIS, Robert P.	
	36	7245901		2007-07-17	McGREGOR et al.	
	37	7248570	B2	2007-07-24	Bahl et al.	
	38	7251218		2007-07-31	Jorgensen, Jacob W.	
	39	7260382	B1	2007-08-21	Lamb et al.	
	40	7266371	B1	2007-09-04	Amin et al.	
	41	7269157	B2	2007-09-11	Klinker et al.	

EFS Web 2.1.17

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	42	7271765	B2	2007-09-18	Stilp et al.	
	43	7272660	B1	2007-09-18	Powers et al.	
	44	7280816		2007-10-09	FRATTI et al.	
	45	7280818		2007-10-09	CLAYTON, Steve	
	46	7283561		2007-10-16	Picher-Dempsey, Heidi	
	47	7283963		2007-10-16	FITZPATRICK, John E. et al.	
	48	7286834	B2	2007-10-23	Walter	
	49	7286848	B2	2007-10-23	Vireday, Richard P. et al.	
	50	7289489		2007-10-30	KUNG et al.	
	51	7290283		2007-10-30	COPELAND III, John A.	
	52	7310424		2007-12-18	Gehring, Stephan Walter et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	53	7313237	B2	2007-12-25	Bahl, Paramvir et al.	
	54	7317699		2008-01-08	GODFREY et al.	
	55	7318111	B2	2008-01-08	Zhao, Wen	
	56	7320029	B2	2008-01-15	Rinne 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	7336960		2008-02-26	ZAVALKOVSKY et al.	
	61	7340772	B2	2008-03-04	Panasyuk et al.	
	62	7346410		2008-03-18	UCHIYAMA, Kenji	
	63	7349695		2008-03-25	OOMMEN et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	64	7353533		2008-04-01	WRIGHT et al.	
	65	7356011		2008-04-08	Waters, Christopher J.F. et al.	
	66	7356337		2008-04-08	FLORENCE, Shahar	
	67	7366497		2008-04-29	NAGATA, Hideaki	
	68	7366654	B2	2008-04-29	Moore, Robert C.	
	69	7369848	B2	2008-05-06	Jiang, Yue Jun	
	70	7369856	B2	2008-05-06	Ovadia, Shlomo	
	71	7373136		2008-05-13	WATLER et al.	
	72	7373179		2008-05-13	Stine, Ted et al.	
	73	7379731	B2	2008-05-27	Natsuno et al.	
	74	7388950		2008-06-17	ELSEY et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	75	7389412	B2	2008-06-17	Sharma et al.	
	76	7391724	B2	2008-06-24	Alakoski et al.	
	77	7395244	B1	2008-07-01	Kingsford, Bryan	
	78	7401338		2008-07-15	BOWEN et al.	
	79	7403763		2008-07-22	MAES, Stephane H.	
	80	7409447	B	2008-08-05	Assadzadeh, Alireza	
	81	7409569	B2	2008-08-05	Illowsky et al.	
	82	7411930	B2	2008-08-12	Montojo et al.	
	83	7418253		2008-08-26	KAVANAH, Alan	
	84	7418257		2008-08-26	Kim, Myong-Ju	
	85	7421004		2008-09-02	FEHER, Kamilo	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	86	7423971	B1	2008-09-09	Mohaban et al.	
	87	7428750	B1	2008-09-23	Dunn et al.	
	88	7440433	B2	2008-10-21	Rink et al.	
	89	7444669	B1	2008-10-28	Bahl, Paramvir et al.	
	90	7450591		2008-11-11	KORLING et al.	
	91	7450927		2008-11-11	CRESWELL et al.	
	92	7454191	B2	2008-11-18	Dawson et al.	
	93	7457265		2008-11-25	Julka, Vibhor et al.	
	94	7457870	B1	2008-11-25	Lownsbrough et al.	
	95	7460837	B2	2008-12-02	Diener, Neil R.	
	96	7466652	B2	2008-12-16	Lau et al.	

EFS Web 2.1.17

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	97	7472189		2008-12-30	Mallya, Arvind R. et al.	
	98	7478420	B2	2009-01-13	Wright, Michael et al.	
	99	7486185		2009-02-03	CULPEPPER et al.	
	100	7486658	B2	2009-02-03	Kumar, Rajneesh	
	101	7493659	B1	2009-02-17	Wu, Handong et al.	
	102	7496652		2009-02-24	Pezzutti, David	
	103	7499438		2009-03-03	Hinman, Brian L. et al.	
	104	7499537		2009-03-03	ELSEY et al.	
	105	7502672	B1	2009-03-10	Kolls, H. Brock	
	106	7505795	B1	2009-03-17	Lim et al.	
	107	7508799	B2	2009-03-24	Sumner et al.	

EFS Web 2.1.17

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	108	7512128	B2	2009-03-31	DiMambro et al.	
	109	7512131	B2	2009-03-31	Svensson et al.	
	110	7515608		2009-04-07	Yuan, Yuan et al.	
	111	7515926	B2	2009-04-07	Bu et al.	
	112	7516219		2009-04-07	MOGHADDAM et al.	
	113	7522576	B2	2009-04-21	Du et al.	
	114	7526541	B2	2009-04-28	Roese et al.	
	115	7529204	B2	2009-05-05	Bourlas, Yair et al.	
	116	7535880		2009-05-19	Hinman, Brian L. et al.	
	117	7536695	B2	2009-05-19	Alam et al.	
	118	7539132	B2	2009-05-26	Werner et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	119	7540408	B2	2009-06-02	Levine, Judah et al.	
	120	7545782		2009-06-09	Rayment, Stephen G. et al.	
	121	7546460		2009-06-09	Maes, Stephane H.	
	122	7546629		2009-06-09	ALBERT, Anthony et al.	
	123	7548976	B2	2009-06-16	Bahl, Paramvir et al.	
	124	7551922		2009-06-23	Roskowski, Steve et al.	
	125	7554983	B1	2009-06-30	Muppala, Suresh	
	126	7555757	B2	2009-06-30	Smith et al.	
	127	7561899	B2	2009-07-14	Lee, Changseok	
	128	7562213	B1	2009-07-14	Timms, Natalie	
	129	7564799	B2	2009-07-21	Holland et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	130	7565141		2009-07-21	Macaluso, Anthony G.	
	131	7574509	B2	2009-08-11	Nixon et al.	
	132	7574731		2009-08-11	FASCENDA, Anthony C.	
	133	7577431	B2	2009-08-18	Jiang, Yue Jun	
	134	7580356	B1	2009-08-25	Mishra et al.	
	135	7580857		2009-08-25	VanFLEET et al.	
	136	7583964	B2	2009-09-01	Wong, Gregory A.	
	137	7586871	B2	2009-09-08	Hamilton et al.	
	138	7593417		2009-09-22	Wang, James et al.	
	139	7593730	B2	2009-09-22	Khandelwal, Deepak et al.	
	140	7596373	B2	2009-09-29	Mcgregor, Christopher et al.	

EFS Web 2.1.17

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	141	7599288		2009-10-06	COLE, Raymond E. et al.	
	142	7599714	B2	2009-10-06	Kuzminskiy, Alexandr	
	143	7602746	B2	2009-10-13	Calhoun et al.	
	144	7609650		2009-10-27	ROSKOWSKI, Steve et al.	
	145	7609700		2009-10-27	Ying, Wen-Ping et al.	
	146	7610047	B2	2009-10-27	Hicks III et al.	
	147	7610328		2009-10-27	HAASE et al.	
	148	7610396	B2	2009-10-27	Taglienti et al.	
	149	7614051	B	2009-11-03	Glaum et al.	
	150	7616962	B2	2009-11-10	Oswal, Anand K. et al.	
	151	7617516		2009-11-10	HUSLAK et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	152	7620041		2009-11-17	Dunn, Jeffrey H. et al.	
	153	7620065		2009-11-17	FALARDEAU, Eric	
	154	7620162		2009-11-17	AARON et al.	
	155	7627314		2009-12-01	Carlson, Steven I. et al.	
	156	7627767	B2	2009-12-01	Sherman et al.	
	157	7627872	B2	2009-12-01	Hebeler et al.	
	158	7633438		2009-12-15	Tysowski, Piotr Konrad	
	159	7634388		2009-12-15	Archer, Charles J. et al.	Entire Document
	160	7636574		2009-12-22	Poosala, Viswanath	
	161	7636626	B2	2009-12-22	Oesterling et al.	
	162	7643411	B2	2010-01-05	Andreasen et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	163	7644151		2010-01-05	JERRIM, John et al.	
	164	7644267		2010-01-05	YLIKOSKI, Martti et al.	
	165	7647047		2010-01-12	MOGHADDAM et al.	
	166	7650137		2010-01-19	JOBS et al.	
	167	7653394	B2	2010-01-26	McMillin, Brian K.	
	168	7657920	B2	2010-02-02	Arseneau et al.	
	169	7660419	B1	2010-02-09	Ho, Jin-Meng	
	170	7661124	B2	2010-02-09	Ramanathan et al.	
	171	7664494	B2	2010-02-16	Jiang, Yue Jun	
	172	7668176		2010-02-23	Chuah, Mooi Choo	
	173	7668612	B	2010-02-23	Okkonen, Harri	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	174	7668903		2010-02-23	EDWARDS et al.	
	175	7676673	B2	2010-03-09	Weller et al.	
	176	7680086	B2	2010-03-16	Eglin	
	177	7684370	B2	2010-03-23	Kezys, Vytautas Robertas	
	178	7685131		2010-03-23	Batra, Vishal Singh et al.	
	179	7685254		2010-03-23	Pandya, Ashish A.	
	180	7685530	B2	2010-03-23	Sherrard et al.	
	181	7693720		2010-04-06	KENNEWICK et al.	
	182	7697540	B2	2010-04-13	Haddad et al.	
	183	7710932		2010-05-04	MUTHUSWAMY, Sivakumar et al.	
	184	7711848		2010-05-04	MAES, Stephane H.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	185	7719966	B2	2010-05-18	Luft et al.	
	186	7720206	B2	2010-05-18	Devolites et al.	
	187	7720464	B2	2010-05-18	Batta, Puneet	
	188	7720505		2010-05-18	GOPI et al.	
	189	7720960	B2	2010-05-18	Pruss, Richard Manfred et al.	
	190	7724716	B2	2010-05-25	Fadell, Anthony M.	
	191	7725570		2010-05-25	Lewis, Lundy	
	192	7729326		2010-06-01	Sekhar, Ramesh	
	193	7730123		2010-06-01	ERICKSON, Richard R. et al.	
	194	7734784		2010-06-08	ARAUJO et al.	
	195	7742406	B1	2010-06-22	Muppala, Suresh	

EFS Web 2.1.17

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	196	7746854		2010-06-29	AMBE, Shekhar et al.	
	197	7747240		2010-06-29	BRISCOE et al.	
	198	7747699		2010-06-29	PRUEITT et al.	
	199	7747730		2010-06-29	HARLOW, James D.	
	200	7752330	B2	2010-07-06	Olsen et al.	
	201	7756056	B2	2010-07-13	Kim et al.	
	202	7756534		2010-07-13	Anupam, Vinod et al.	
	203	7756757	B1	2010-07-13	Oakes III, Charles Lee	
	204	7760137	B2	2010-07-20	Martucci et al.	
	205	7760711	B1	2010-07-20	Kung et al.	
	206	7760861		2010-07-20	Croak, Marian et al.	

EFS Web 2.1.17

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	207	7765294	B2	2010-07-27	Edwards et al.	
	208	7769397	B2	2010-08-03	Funato et al.	
	209	7770785	B2	2010-08-10	Jha et al.	
	210	7774323	B2	2010-08-10	Helfman, Nadav	
	211	7774456	B1	2010-08-10	Lownsbrough, Derek Leigh et al.	
	212	7778176		2010-08-17	Morford, Michael Robert	
	213	7778643		2010-08-17	Laroia, Rajiv et al.	
	214	7792257	B1	2010-09-07	Vanier et al.	
	215	7792538		2010-09-07	Kozisek, Steven E.	
	216	7792708		2010-09-07	ALVA, Jessi	
	217	7797060	B2	2010-09-14	Grgic et al.	

EFS Web 2.1.17

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	218	7797204		2010-09-14	BALENT, Bruce F.	
	219	7797401		2010-09-14	STEWART et al.	
	220	7801523		2010-09-21	Kenderov, Stoyan	
	221	7801783	B2	2010-09-21	Kende et al.	
	222	7801985	B1	2010-09-21	Pitkow, Jim et al.	
	223	7802724		2010-09-28	Nohr, Steven Paul	
	224	7805140	B2	2010-09-28	Friday et al.	
	225	7805606	B2	2010-09-28	Birger et al.	
	226	7809351	B1	2010-10-05	Panda et al.	
	227	7817615	B1	2010-10-19	Breau et al.	
	228	7817983	B2	2010-10-19	Cassett et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	229	7822837		2010-10-26	URBAN et al.	
	230	7826427	B2	2010-11-02	Sood et al.	
	231	7826607	B1	2010-11-02	De Carvalho Resende et al.	
	232	7843831	B2	2010-11-30	Morrill et al.	
	233	7843843	B1	2010-11-30	Papp III et al.	
	234	7844034	B1	2010-11-30	Oh et al.	
	235	7844728		2010-11-30	ANDERSON, Thomas W. et al.	
	236	7848768		2010-12-07	OMORI et al.	
	237	7849161	B2	2010-12-07	Koch et al.	
	238	7849477	B2	2010-12-07	Cristofalo et al.	
	239	7853255	B2	2010-12-14	Karaoguz et al.	

EFS Web 2.1.17

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	240	7856226		2010-12-21	WONG, Ellis L. et al.	
	241	7860088	B2	2010-12-28	Lioy, Marcello	
	242	7865182		2011-01-04	Macaluso, Anthony G.	
	243	7865187	B2	2011-01-04	Ramer et al.	
	244	7868778		2011-01-11	KENWRIGHT, David Norris	
	245	7873001	B2	2011-01-18	Silver, Andrew	
	246	7873344		2011-01-18	BOWSER, Robert et al.	
	247	7873705		2011-01-18	KALISH, Dan	
	248	7877090		2011-01-25	Maes, Stephane H.	
	249	7881199		2011-02-01	KRSTULICH, Zlatko	
	250	7881697	B2	2011-02-01	Baker, Matthew Donald et al.	

EFS Web 2.1.17

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	251	7882029		2011-02-01	WHITE, Craig R.	
	252	7882247	B2	2011-02-01	Sturniolo et al.	
	253	7886047		2011-02-08	POTLURI, Dora	
	254	7889384	B2	2011-02-15	Armentrout et al.	
	255	7890084		2011-02-15	Dudziak, Thaddeus Jude et al.	
	256	7890111		2011-02-15	Bugenhagen, Michael K.	
	257	7894431	B2	2011-02-22	Goring et al.	
	258	7899039	B2	2011-03-01	Andreasen et al.	
	259	7899438	B2	2011-03-01	Baker, Matthew Donald et al.	
	260	7903553		2011-03-08	Liu, Enhui	
	261	7907970		2011-03-15	Park, Vincent D. et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	262	7911975		2011-03-22	DROZ, Patrick et al.	
	263	7912025		2011-03-22	Pattenden, Christopher E. S. et al.	
	264	7912056		2011-03-22	BRASSEM, Wayne	
	265	7920529		2011-04-05	MAHLER, Roger et al.	
	266	7921463		2011-04-05	Sood, Kapil et al.	
	267	7925740	B2	2011-04-12	Nath et al.	
	268	7925778	B1	2011-04-12	Wijnands et al.	
	269	7929959	B2	2011-04-19	DeAtley, Dallas et al.	
	270	7929960		2011-04-19	MARTIN et al.	
	271	7929973		2011-04-19	Zavalkovsky, Arthur et al.	
	272	7930327	B2	2011-04-19	Craft David et al.	

EFS Web 2.1.17

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	273	7930446	B2	2011-04-19	Kesselman, Alex et al.	
	274	7933274	B2	2011-04-26	Verma et al.	
	275	7936736	B2	2011-05-03	Proctor, Jr. et al.	
	276	7937069		2011-05-03	RASSAM, Frederic	
	277	7937450	B2	2011-05-03	Janik, Craig M.	
	278	7940685	B1	2011-05-10	Breslau, Lee et al.	
	279	7940751		2011-05-10	Hansen, Christopher J.	
	280	7941184		2011-05-10	PRENDERGAST et al.	
	281	7944948		2011-05-17	Chow, Albert T. et al.	
	282	7945238	B2	2011-05-17	Baker, Matthew Donald et al.	
	283	7945240		2011-05-17	KLOCK, Jacqueline et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	284	7945945		2011-05-17	Graham, Richard et al.	
	285	7948952		2011-05-24	HURTTA, Tuija et al.	
	286	7948953	B2	2011-05-24	Melkote, Keerti G. et al.	
	287	7948968		2011-05-24	Voit, Eric A. et al.	
	288	7949529		2011-05-24	WEIDER et al.	
	289	7953808		2011-05-31	SHARP et al.	
	290	7953877	B2	2011-05-31	Vemula et al.	
	291	7957020		2011-06-07	MINE, Ryuta et al.	
	292	7957381	B2	2011-06-07	Clermidy et al.	
	293	7957511		2011-06-07	DRUDIS et al.	
	294	7958029	B1	2011-06-07	Bobich et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	295	7962622		2011-06-14	Friend, John et al.	
	296	7965983		2011-06-21	SWAN, Tim et al.	
	297	7966405	B2	2011-06-21	Sundaresan et al.	
	298	7969950	B2	2011-06-28	Iyer, Pradeep J. et al.	
	299	7970350		2011-06-28	SHEYNMAN, Arnold	
	300	7970426		2011-06-28	Poe, Brian R. 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					

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.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	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	03/25/2019

*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.J.R./

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

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

Application Number	15582350
Filing Date	2017-04-28
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP007C11C3C2C3C2

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	6370139	B2	2002-04-09	Redmond	
	2	6732176	B1	2004-05-04	Stewart et al.	
	3	6842628	B1	2005-01-11	Arnold et al.	
	4	6970927	B1	2005-11-29	Stewart et al.	
	5	7200551	B1	2007-04-03	Senez	
	6	7433362	B2	2008-10-07	Mallya et al.	
	7	7467160	B2	2008-12-16	McIntyre	
	8	7505756	B2	2009-03-17	Bahl	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3C2C3C2

	9	7522549	B2	2009-04-21	Karaoguz et al.	
	10	7551921	B2	2009-06-23	Petermann	
	11	7606918	B2	2009-10-20	Holzman et al.	
	12	7644414	B2	2010-01-05	Smith et al.	
	13	7822849	B2	2010-10-26	Titus	
	14	7849170	B1	2010-12-07	Hargens et al.	
	15	7979896	B2	2011-07-12	McMurtry et al.	
	16	8108680	B2	2012-01-31	Murray	
	17	8266249	B2	2012-09-11	Hu	
	18	8463194	B2	2013-06-11	Erlenback et al.	
	19	8500533	B2	2013-08-06	Lutnick et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3C2C3C2

	20	8535160	B2	2013-09-17	Lutnick et al.	
	21	8595186	B1	2013-11-26	Mandyam et al.	
	22	8615507	B2	2013-12-24	VARADARAJULU et al.	
	23	8656472	B2	2014-02-18	McMurtry et al.	
	24	8804695	B2	2014-08-12	Branam	
	25	8845415	B2	2014-09-30	Lutnick et al.	
	26	8949382	B2	2015-02-03	Cornett et al.	
	27	8955038	B2	2015-02-10	Nicodemus et al.	
	28	9105031	B2	2015-08-11	Shen et al.	
	29	9313708	B2	2016-04-12	Nam et al.	
	30	9363285	B2	2016-06-07	Kitamura	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3C2C3C2

	31	9418381	B2	2016-08-16	Ahuja et al.	
	32	9501803	B2	2016-11-22	Bilac 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	20020013844	A1	2002-01-31	Garrett et al.	
	2	20020022483	A1	2002-02-21	Thompson et al.	
	3	20040019564	A1	2004-01-29	Goldthwaite et al.	
	4	20040116140	A1	2004-06-17	Babbar et al.	
	5	20040127256	A1	2004-07-01	Goldthwaite et al.	
	6	20040167958	A1	2004-08-26	Stewart et al.	
	7	20070111740	A1	2007-05-17	Wandel	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3C2C3C2

	8	20070191006	A1	2007-08-16	Carpenter	
	9	20070254646	A1	2007-11-01	Sokondar	
	10	20100069074	A1	2010-03-18	Kodialam et al.	
	11	20100113020	A1	2010-05-06	Subramanian et al.	
	12	20100142478	A1	2010-06-10	Forssell et al.	
	13	20150181628	A1	2015-06-25	Haverinen 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	20040053858	KR		2004-06-25	Electronics and Telecommunications Research Instit		

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.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3C2C3C2

	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	03/25/2019

*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 2.1.18

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

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

PTO/SB/08a (03-15)
Approved for use through 07/31/2016. 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	15582350
Filing Date	2017-04-28
First Named Inventor	Raleigh
Art Unit	2447
Examiner Name	not yet assigned
Attorney Docket Number	RALEP007C11C3C2C3C2

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	5131020	A	1992-07-14	Liebesny et al.	
	2	5283904		1994-02-01	CARSON, David G. et al.	
	3	5325532	A	1994-06-28	Crosswy et al.	
	4	5572528	A	1996-11-05	Shuen, Pauline	
	5	5577100		1996-11-19	McGREGOR et al.	
	6	5594777		1997-01-14	Makkonen, Matti et al.	
	7	5617539	A	1997-04-01	Ludwig et al.	
	8	5630159	A	1997-05-13	Zancho, William F.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	9	5633484	A	1997-05-27	Zancho, William F. et al.	
	10	5633868	A	1997-05-27	Baldwin et al.	
	11	5754953	A	1998-05-19	Briancon et al.	
	12	5774532	A	1998-06-30	Gottlieb et al.	
	13	5794142		1998-08-11	VANTTILA et al.	
	14	5814798	A	1998-09-29	Zancho, William F.	
	15	5889477		1999-03-30	Fastenrath, Ulrich	
	16	5892900		1999-04-06	GINTER et al.	
	17	5903845		1999-05-11	BUHRMANN et al.	
	18	5915008	A	1999-06-22	Dulman, Scott	
	19	5933778		1999-08-03	BUHRMANN et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	20	5940472		1999-08-17	NEWMAN et al.	
	21	5974439	A	1999-10-26	Bollella, Gregory	
	22	5983270	A	1999-11-09	Abraham et al.	
	23	6035281		2000-03-07	Crosskey, James P. et al.	
	24	6038452		2000-03-14	Strawczynski, Leo et al.	
	25	6038540	A	2000-03-14	Krist et al.	
	26	6047268		2000-04-04	BARTOLI et al.	
	27	6058434	A	2000-05-02	Wilt et al.	
	28	6061571	A	2000-05-09	Tamura, Hideo	
	29	6064878		2000-05-16	DENKER, John Stewart et al.	
	30	6078953		2000-06-20	VAID et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	31	6081591		2000-06-27	SKOOG, Frederick H.	
	32	6098878		2000-08-08	DENT et al.	
	33	6104700	A	2000-08-15	Haddock, Stephen R. et al.	
	34	6115823	A	2000-09-05	Velasco et al.	
	35	6119933	A	2000-09-19	Wong et al.	
	36	6125391	A	2000-09-26	Meltzer et al.	
	37	6141565	A	2000-10-31	Feuerstein et al.	
	38	6141686		2000-10-31	JACKOWSKI et al.	
	39	6148336		2000-11-14	THOMAS et al.	
	40	6154738		2000-11-28	CALL, Charles Gainor	
	41	6157636	A	2000-12-05	Voit et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	42	6185576	B1	2001-02-06	Mcintosh, Lowrie	
	43	6198915		2001-03-06	McGREGOR et al.	
	44	6219786	B1	2001-04-17	Cunningham et al.	
	45	6226277		2001-05-01	Chuah, Mooi Choo	
	46	6263055		2001-07-17	GARLAND et al.	
	47	6292828		2001-09-18	Williams, David L.	
	48	6317584		2001-11-13	ABU-AMARA et al.	
	49	6381316		2002-04-30	JOYCE, Simon James et al.	
	50	6393014	B1	2002-05-21	Daly et al.	
	51	6397259	B1	2002-05-28	Lincke et al.	
	52	6401113	B2	2002-06-04	Lazaridis et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	53	6418147		2002-07-09	WIEDEMAN, Robert A.	
	54	6438575	B1	2002-08-20	Khan et al.	
	55	6445777	B1	2002-09-03	Clark, Curtis	
	56	6449479		2002-09-10	SANCHEZ, Eduardo	
	57	6466984	B1	2002-10-15	Naveh et al.	
	58	6477670		2002-11-05	Ahmadvand, Nima	
	59	6502131		2002-12-31	VAID, Aseem et al.	
	60	6505114		2003-01-07	LUCIANI, Sergio	
	61	6510152	B1	2003-01-21	Gerszberg et al.	
	62	6522629	B1	2003-02-18	Anderson, Sr., Ronald D.	
	63	6532235		2003-03-11	BENSON et al.	

EFS Web 2.1.17

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	64	6532579		2003-03-11	SATO et al.	
	65	6535855	B1	2003-03-18	Cahill et al.	
	66	6539082		2003-03-25	LOWE et al.	
	67	6542500	B1	2003-04-01	Gerszberg et al.	
	68	6542992		2003-04-01	Peirce, Kenneth L. et al.	
	69	6546016	B1	2003-04-08	Gerszberg et al.	
	70	6563806		2003-05-13	YANO et al.	
	71	6570974	B1	2003-05-27	Gerszberg et al.	
	72	6574321		2003-06-03	COX et al.	
	73	6574465		2003-06-03	MARSH et al.	
	74	6578076	B1	2003-06-10	Putzolu, David Matthew	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	75	6581092		2003-06-17	MOTOYAMA, Tetsuro	
	76	6598034	B1	2003-07-22	Kloth, Axel K.	
	77	6601040	B1	2003-07-29	Kolls, H. Brock	
	78	6603969		2003-08-05	VUORISTO et al.	
	79	6606744		2003-08-12	MIKURAK, Michael G.	
	80	6628934	A	2003-09-30	Rosenberg et al.	
	81	6631122		2003-10-07	ARUNACHALAM, Vaidhyanathan et al.	
	82	6636721	B2	2003-10-21	Threadgill et al.	
	83	6639975		2003-10-28	O'NEAL et al.	
	84	6640097		2003-10-28	Corrigan, Louis et al.	
	85	6640334	B	2003-10-28	Rasmussen, John H.	

EFS Web 2.1.17

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	86	6650887		2003-11-18	McGREGOR et al.	
	87	6651101		2003-11-18	GAI et al.	
	88	6654786	B1	2003-11-25	Fox et al.	
	89	6654814		2003-11-25	Britton, Kathryn H. et al.	
	90	6658254		2003-12-02	PURDY et al.	
	91	6662014	B1	2003-12-09	Walsh, Patrick Jay	
	92	6678516		2004-01-13	Nordman, Ian et al.	
	93	6683853		2004-01-27	Kannas, Chris et al.	
	94	6684244		2004-01-27	GOLDMAN et al.	
	95	6690918	B2	2004-02-10	Evans et al.	
	96	6697821	B2	2004-02-24	Ziff et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	97	6725031		2004-04-20	WATLER et al.	
	98	6725256	B1	2004-04-20	Albal et al.	
	99	6735206	B1	2004-05-11	Oki et al.	
	100	6748195	B1	2004-06-08	Phillips, W. Garland	
	101	6748437	B1	2004-06-08	Mankude et al.	
	102	6751296	B1	2004-06-15	Albal et al.	
	103	6754470		2004-06-22	Hendrickson, Keith et al.	
	104	6757717	B1	2004-06-29	Goldstein, Leonid	
	105	6763000		2004-07-13	WALSH, Peter J.	
	106	6763226	B1	2004-07-13	McZeal Jr., Alfred	
	107	6765864		2004-07-20	NATARAJAN et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	108	6765925		2004-07-20	Sawyer, Wilson et al.	
	109	6782412		2004-08-24	BROPHY, Kevin et al.	
	110	6785889		2004-08-31	WILLIAMS, Peter	
	111	6792461	B1	2004-09-14	Hericourt, Olivier	
	112	6829596		2004-12-07	FRAZEE, Steve	
	113	6829696		2004-12-07	BALMER et al.	
	114	6839340		2005-01-04	Voit, Eric A. et al.	
	115	6873988	B2	2005-03-29	Herrmann et al.	
	116	6876653		2005-04-05	AMBE, Shekhar et al.	
	117	6879825	B1	2005-04-12	Daly, Brian Kevin	
	118	6882718	B1	2005-04-19	Smith, Benjamin V.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	119	6885997	B1	2005-04-26	Roberts, David T.	
	120	6901440	B1	2005-05-31	Bimm et al.	
	121	6920455		2005-07-19	WESCHLER, Paul	
	122	6922562		2005-07-26	Ward, Stephen L. et al.	
	123	6928280		2005-08-09	Xanthos, James et al.	
	124	6934249	B1	2005-08-23	Bertin, Olivier et al.	
	125	6934751	B2	2005-08-23	Jayapalan et al.	
	126	6947723		2005-09-20	Gurnani, Roger et al.	
	127	6947985	B2	2005-09-20	Hegli et al.	
	128	6952428		2005-10-04	NECKA et al.	
	129	6957067		2005-10-18	Iyer, Pradeep J. et al.	

EFS Web 2.1.17

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	130	6959393	B2	2005-10-25	Hollis et al.	
	131	6965667		2005-11-15	TRABANDT et al.	
	132	6965872		2005-11-15	Grdina, Jerome M.	
	133	6967958		2005-11-22	ONO, Yoshiyuki et al.	
	134	6970692	B2	2005-11-29	Tysor, Arthur James	
	135	6982733	B1	2006-01-03	McNally et al.	
	136	6983370	B2	2006-01-03	Eaton et al.	
	137	6996062	B1	2006-02-07	Freed et al.	
	138	6996076		2006-02-07	FORBES et al.	
	139	6996393		2006-02-07	Pyhalammi, Seppo et al.	
	140	6998985		2006-02-14	REISMAN et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	141	7002920		2006-02-21	Ayyagari, Deepak et al.	
	142	7007295	B1	2006-02-28	Rose et al.	
	143	7013469	B2	2006-03-14	Smith et al.	
	144	7017189	B1	2006-03-21	DeMello et al.	
	145	7024200		2006-04-04	McKENNA et al.	
	146	7024460	B2	2006-04-04	Koopmas et al.	
	147	7027055	B2	2006-04-11	Anderson et al.	
	148	7027408		2006-04-11	NABKEL et al.	
	149	7032072	B1	2006-04-18	Quinn et al.	
	150	7039027	B2	2006-05-02	Bridgelall, Raj	
	151	7039037		2006-05-02	Wang, Jiwei R. et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	152	7039403		2006-05-02	Wong, Gregory A.	
	153	7039713	B1	2006-05-02	Van Gunter, David et al.	
	154	7042988		2006-05-09	JUITT et al.	
	155	7043225	B1	2006-05-09	Patel et al.	
	156	7043226		2006-05-09	Yamauchi, Toshiaki	
	157	7043268	B2	2006-05-09	Yukie et al.	
	158	7047276	B2	2006-05-16	Liu et al.	
	159	7058022	B1	2006-06-06	Carolan et al.	
	160	7058968		2006-06-06	ROWLAND et al.	
	161	7068600		2006-06-27	CAIN, Joseph Bibb	
	162	7069248		2006-06-27	HUBER, Adriano	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	163	7082422	B1	2006-07-25	Zirngibl et al.	
	164	7084775	B1	2006-08-01	Smith, Michael R.	
	165	7092696		2006-08-15	HOSAIN et al.	
	166	7095754	B2	2006-08-22	Benveniste, Mathilde	

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	20080250053	A	2008-10-09	Aaltonen, Janne et al.	
	2	20080256593		2008-10-16	VINBERG et al.	
	3	20080259924	A1	2008-10-23	Gooch et al.	
	4	20080262798		2008-10-23	KIM, Eun Ah et al.	
	5	20080263348	A	2008-10-23	Zaltsman et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	6	20080268813		2008-10-30	MAES, Stephane H.	
	7	20080270212	A	2008-10-30	Blight et al.	
	8	20080279216	A1	2008-11-13	Sharif-Ahmadi et al.	
	9	20080282319	A1	2008-11-13	Fontijn et al.	
	10	20080293395	A1	2008-11-27	Mathews et al.	
	11	20080298230		2008-12-04	LUFT et al.	
	12	20080305793		2008-12-11	GALLAGHER et al.	
	13	20080311885		2008-12-18	DAWSON et al.	
	14	20080313315	A	2008-12-18	Karaoguz et al.	
	15	20080313730		2008-12-18	Iftimie, Sorin et al.	
	16	20080316923		2008-12-25	FEDDERS et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	17	20080318547		2008-12-25	BALLOU et al.	
	18	20080318550		2008-12-25	DeATLEY, Dallas	
	19	20080319879		2008-12-25	CARROLL et al.	
	20	20080320497	A1	2008-12-25	Tarkoma et al.	
	21	20090005000	A	2009-01-01	Baker, Matthew et al.	
	22	20090005005		2009-01-01	FORSTALL et al.	
	23	20090006116	A	2009-01-01	Baker, Matthew et al.	
	24	20090006200	A	2009-01-01	Baker, Matthew et al.	
	25	20090006229	A1	2009-01-01	Sweeney et al.	
	26	20090013157		2009-01-08	BEAULE, Stephane	
	27	20090016310	A1	2009-01-15	Rasal, Digambar L.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	28	20090036111	A1	2009-02-05	Danford et al.	
	29	20090042536	A1	2009-02-12	Bernard et al.	
	30	20090044185	A1	2009-02-12	Krivopaltsev, Eugene	
	31	20090046707	A1	2009-02-19	Smires et al.	
	32	20090046723		2009-02-19	RAHMAN, Reshad A. et al.	
	33	20090047989	A1	2009-02-19	Harmon et al.	
	34	20090048913	A1	2009-02-19	Shenfield et al.	
	35	20090049156	A1	2009-02-19	Aronsson et al.	
	36	20090049518	A1	2009-02-19	Roman et al.	
	37	20090054030		2009-02-26	GOLDS, David	
	38	20090065571	A1	2009-03-12	Jain, Deepak	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	39	20090067372		2009-03-12	SHAH, Keyur C. et al.	
	40	20090068984		2009-03-12	BURNETT, R. Alan	
	41	20090070379	A1	2009-03-12	Rappaport, Theodore R.	
	42	20090077622		2009-03-19	BAUM et al.	
	43	20090079699		2009-03-26	SUN, Jian	
	44	20090113514		2009-04-30	HU, Q. James	
	45	20090125619		2009-05-14	ANTANI, Snehal S.	
	46	20090132860	A1	2009-05-21	LIU et al.	
	47	20090149154	A1	2009-06-11	Bhasin et al.	
	48	20090157792		2009-06-18	Fiatal, Trevor	
	49	20090163173	A1	2009-06-25	Williams, Timothy D.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	50	20090172077		2009-07-02	ROXBURGH, David et al.	
	51	20090180391		2009-07-16	PETERSEN et al.	
	52	20090181662	A1	2009-07-16	Fleischman et al.	
	53	20090197585		2009-08-06	AARON, Jeffrey A.	
	54	20090197612	A1	2009-08-06	Kiiskinen, Arto	
	55	20090203352	A1	2009-08-13	Fordon et al.	
	56	20090217364	A1	2009-08-27	Salmela et al.	
	57	20090219170		2009-09-03	CLARK, Ryan C. et al.	
	58	20090248883		2009-10-01	SURYANARAYANA et al.	
	59	20090254857	A	2009-10-08	Romine et al.	
	60	20090257379		2009-10-15	ROBINSON et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	61	20090271514		2009-10-29	THOMAS et al.	
	62	20090282127	A	2009-11-12	Leblanc et al.	
	63	20090286507		2009-11-19	O'NEIL et al.	
	64	20090287921		2009-11-19	ZHU et al.	
	65	20090288140		2009-11-19	HUBER et al.	
	66	20090291665	A1	2009-11-26	Gaskarth et al.	
	67	20090299857		2009-12-03	BRUBAKER, Curtis M.	
	68	20090307696	A1	2009-12-10	Vals et al.	
	69	20090307746		2009-12-10	DI, Jinwen et al.	
	70	20090315735		2009-12-24	BHAVANI, Neeraj S. et al.	
	71	20090320110	A1	2009-12-24	NICOLSON et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	72	20100017506		2010-01-21	FADELL, Anthony	
	73	20100020822		2010-01-28	ZERILLO, Anthony J. et al.	
	74	20100027469		2010-02-04	GURAJALA, Ravindra Babu et al.	
	75	20100027559		2010-02-04	LIN, Hung-Ming et al.	
	76	20100030890	A	2010-02-04	Dutta et al.	
	77	20100041364		2010-02-18	LOTT, Robert Wayne et al.	
	78	20100041365	A1	2010-02-18	Lott et al.	
	79	20100042675		2010-02-18	FUJII, Hiroshi	
	80	20100043068		2010-02-18	VARADHAN et al.	
	81	20100071053		2010-03-18	ANSARI et al.	
	82	20100075666	A1	2010-03-25	Garner, Neil Robert	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	83	20100080202		2010-04-01	Hanson, Mark	
	84	20100082431		2010-04-01	RAMER et al.	
	85	20100103820		2010-04-29	FULLER et al.	
	86	20100121744	A1	2010-05-13	Belz et al.	
	87	20100131584		2010-05-27	Johnson, William J.	
	88	20100144310		2010-06-10	BEDINGFIELD, James Carlton	
	89	20100151866	A1	2010-06-17	Karpov et al.	
	90	20100153781		2010-06-17	HANNA, Stephen R.	
	91	20100167696	A	2010-07-01	Smith, Christopher David et al.	
	92	20100188975		2010-07-29	RALEIGH, Gregory G.	
	93	20100188990		2010-07-29	RALEIGH, Gregory G.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	94	20100188992		2010-07-29	RALEIGH, Gregory G.	
	95	20100188994		2010-07-29	RALEIGH, Gregory G.	
	96	20100190469	A1	2010-07-29	Vanderveen et al.	
	97	20100191576		2010-07-29	RALEIGH, Gregory G.	
	98	20100191612		2010-07-29	RALEIGH, Gregory G.	
	99	20100191846		2010-07-29	RALEIGH, Gregory G.	
	100	20100192170		2010-07-29	RALEIGH, Gregory G.	
	101	20100192212		2010-07-29	RALEIGH, Gregory G.	
	102	20100195503		2010-08-05	RALEIGH, Gregory G.	
	103	20100197268		2010-08-05	RALEIGH, Gregory G.	
	104	20100198698		2010-08-05	RALEIGH et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	105	20100198939		2010-08-05	RALEIGH, Gregory G.	
	106	20100241544		2010-09-23	Benson, Dan et al.	
	107	20100248719	A1	2010-09-30	Scholaert, Hugh	
	108	20100284327	A	2010-11-11	Miklos, Gyorgy	
	109	20100287599	A1	2010-11-11	He et al.	
	110	20100325420		2010-12-23	KANEKAR, Tushar	
	111	20110013569	A	2011-01-20	Scherzer, Shimon et al.	
	112	20110019574	A	2011-01-27	Malomsoky et al.	
	113	20110081881	A	2011-04-07	Baker, Matthew Donald et al.	
	114	20110082790	A	2011-04-07	Baker, Matthew Donald et al.	
	115	20110110309	A	2011-05-12	Bennett, James D.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	116	20110126141		2011-05-26	KING et al.	
	117	20110145920	A1	2011-06-16	Mahaffey et al.	
	118	20110159818	A	2011-06-30	Scherzer, Shimon et al.	
	119	20110173678		2011-07-14	KAIPPALLIMALIL, John et al.	
	120	20110264923	A	2011-10-27	Kocher et al.	
	121	20120020296	A	2012-01-26	Scherzer, Shimon et al.	
	122	20120144025	A1	2012-06-07	Melander et al.	
	123	20120166364	A1	2012-06-28	Ahmad et al.	
	124	20120196644	A	2012-08-02	Scherzer, Shimon et al.	
	125	20120238287	A	2012-09-20	Scherzer, Shimon	
	126	20130029653	A	2013-01-31	Baker, Matthew Donald et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	127	20130058274	A	2013-03-07	Scherzer, Shimon et al.	
	128	20130065555	A	2013-03-14	Baker, Matthew Donald et al.	
	129	20130072177	A1	2013-03-21	Ross et al.	
	130	20130084835	A	2013-04-04	Scherzer, Shimon et al.	
	131	20130144789		2013-06-06	Aaltonen, Janne et al.	
	132	20130326356	A9	2013-12-05	Zheng et al.	
	133	20140073291	A1	2014-03-13	Hildner et al.	
	134	20140241342	A1	2014-08-28	Constantinof, Cristian	

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	2002093877	WO	A1	2002-11-21	Nokia Corp.		

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	2	2003014891	WO		2003-02-20	The Boeing Company		
	3	2003017063	WO	A2	2003-02-27	Apogee Networks		
	4	2003017065	WO	A2	2003-02-27	Apogee Networks		
	5	2003058880	WO		2003-07-17	Telia AB		
	6	2004028070	WO		2004-04-01	Credant Technologies, Inc.		
	7	2004064306	WO		2004-07-29	Motorola Inc.		
	8	2004077797	WO		2004-09-10	Boston Communications Group, Inc. (Erskine)		
	9	2004095753	WO		2004-11-04	Motorola Inc.		
	10	2005008995	WO		2005-01-27	Starhub Ltd.		
	11	2005053335	WO	A1	2005-06-09	Nokia Corp.		
	12	2005083934	WO	A1	2005-09-09	Research In Motion Ltd.		

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	13	2006004467	WO		2006-01-12	Telefonaktiebolaget LM Ericsson		
	14	2006004784	WO	A1	2006-01-12	Japan Communications Inc.		
	15	2006012610	WO	A2	2006-02-02	Citrix Systems, Inc.		
	16	2006050758	WO		2006-05-18	Telefonaktiebolaget LM Ericsson		
	17	2006073837	WO		2006-07-13	Symbol Technologies, Inc.		
	18	2006077481	WO		2006-07-27	TrueContext Corporation		
	19	2006093961	WO	A1	2006-09-08	Kyocera Wireless Corp.		
	20	2006120558	WO		2006-11-16	Nokia Corp.		
	21	2006130960	WO		2006-12-14	Mobidia, Inc.		
	22	2007001833	WO		2007-01-04	Symbol Technologies, Inc.		
	23	2007014630	WO		2007-02-08	Telefonaktiebolaget LM Ericsson		

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	24	2007018363	WO		2007-02-15	Upresto, Inc.		
	25	2007053848	WO		2007-05-10	Mobile Armor, LLC		
	26	2007068288	WO		2007-06-21	Telefonaktiebolaget LM Ericsson		
	27	2007069245	WO		2007-06-21	Yoggie Security Systems, Inc.		
	28	2007097786	WO	A	2007-08-30	Sony Ericsson Mobile Communications AB		
	29	2007107701	WO		2007-09-27	British Telecommunications Public Limited Company		
	30	2007120310	WO		2007-10-25	Qualcomm Inc.		
	31	2007124279	WO		2007-11-01	Cisco Technology, Inc., et al.		
	32	2007126352	WO		2007-11-08	Telefonaktiebolaget LM Ericsson		
	33	2007133844	WO	A	2007-11-22	Camiant, Inc.		
	34	2008017837	WO		2008-02-14	Symbian Software Limited		

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	35	2008051379	WO		2008-05-02	Verizon Services Corp.		
	36	2008066419	WO		2008-06-05	Telefonaktiebolaget LM Ericsson		
	37	2008080139	WO		2008-07-03	Integrated Mobile, Inc.		
	38	2008080430	WO		2008-07-10	Telecom Italia S.P.A.		
	39	2008099802	WO		2008-08-21	NEC Corporation		
	40	2009008817	WO	A1	2009-01-15	Ericsson		
	41	2009091295	WO	A1	2009-07-23	Telefonaktiebolaget LM Ericsson		
	42	2010088413	WO		2010-08-05	Headwater Partners I LLC		

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	STEGLICH, Stephan, "I-Centric User Interaction," November 21, 2003	

EFS Web 2.1.17

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	2	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	
	3	VAN EIJK, et al., "GigaMobile, Agent Technology for Designing Personalized Mobile Service Brokerage," July 1, 2002	
	4	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	
	5	Windows7 Power Management, published April 2009	
	6	ZHU et al., "A Survey of Quality of Service in IEEE 802.11 Networks," IEEE Wireless Communications, August 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	03/25/2019

*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.J.R./

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. 7797

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
15/582,350	04/28/2017 RULE	705	3687	RALEP007C11C3C2C3C2

APPLICANTS
Headwater Research LLC, Tyler, TX;

INVENTORS
Gregory G. Raleigh, Woodside, CA;

**** CONTINUING DATA ***************************
This application is a CON of 15/239,398 08/17/2016 PAT 9641957
which is a CON of 14/979,233 12/22/2015 PAT 9532161
which is a CON of 14/667,353 03/24/2015 PAT 9232403
which 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 **
05/05/2017

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

ADDRESS
Headwater Research LLC
1011 Pruitt Place
Tyler, TX 75703
UNITED STATES

TITLE
Wirless Network Buffered Message System

FILING FEE RECEIVED	FEES: Authority has been given in Paper	❑ All Fees
1600	No._____ to charge/credit DEPOSIT ACCOUNT	❑ 1.16 Fees (Filing)
	No._____ for following:	❑ 1.17 Fees (Processing Ext. of time)
		❑ 1.18 Fees (Issue)
		❑ Other _____
		❑ Credit

BIB (Rev. 05/07).

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

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

Application Number	15582350
Filing Date	2017-04-28
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP007C11C3C2C3C2

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	6370139	B2	2002-04-09	Redmond	
	2	6732176	B1	2004-05-04	Stewart et al.	
	3	6842628	B1	2005-01-11	Arnold et al.	
	4	6970927	B1	2005-11-29	Stewart et al.	
	5	7200551	B1	2007-04-03	Senez	
	6	7433362	B2	2008-10-07	Mallya et al.	
	7	7467160	B2	2008-12-16	McIntyre	
	8	7505756	B2	2009-03-17	Bahl	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3C2C3C2

	9	7522549	B2	2009-04-21	Karaoguz et al.	
	10	7551921	B2	2009-06-23	Petermann	
	11	7606918	B2	2009-10-20	Holzman et al.	
	12	7644414	B2	2010-01-05	Smith et al.	
	13	7822849	B2	2010-10-26	Titus	
	14	7849170	B1	2010-12-07	Hargens et al.	
	15	7979896	B2	2011-07-12	McMurtry et al.	
	16	8108680	B2	2012-01-31	Murray	
	17	8266249	B2	2012-09-11	Hu	
	18	8463194	B2	2013-06-11	Erlenback et al.	
	19	8500533	B2	2013-08-06	Lutnick et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3C2C3C2

	20	8535160	B2	2013-09-17	Lutnick et al.	
	21	8595186	B1	2013-11-26	Mandyam et al.	
	22	8615507	B2	2013-12-24	VARADARAJULU et al.	
	23	8656472	B2	2014-02-18	McMurtry et al.	
	24	8804695	B2	2014-08-12	Branam	
	25	8845415	B2	2014-09-30	Lutnick et al.	
	26	8949382	B2	2015-02-03	Cornett et al.	
	27	8955038	B2	2015-02-10	Nicodemus et al.	
	28	9105031	B2	2015-08-11	Shen et al.	
	29	9313708	B2	2016-04-12	Nam et al.	
	30	9363285	B2	2016-06-07	Kitamura	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3C2C3C2

	31	9418381	B2	2016-08-16	Ahuja et al.	
	32	9501803	B2	2016-11-22	Bilac 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	20020013844	A1	2002-01-31	Garrett et al.	
	2	20020022483	A1	2002-02-21	Thompson et al.	
	3	20040019564	A1	2004-01-29	Goldthwaite et al.	
	4	20040116140	A1	2004-06-17	Babbar et al.	
	5	20040127256	A1	2004-07-01	Goldthwaite et al.	
	6	20040167958	A1	2004-08-26	Stewart et al.	
	7	20070111740	A1	2007-05-17	Wandel	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3C2C3C2

	8	20070191006	A1	2007-08-16	Carpenter	
	9	20070254646	A1	2007-11-01	Sokondar	
	10	20100069074	A1	2010-03-18	Kodialam et al.	
	11	20100113020	A1	2010-05-06	Subramanian et al.	
	12	20100142478	A1	2010-06-10	Forssell et al.	
	13	20150181628	A1	2015-06-25	Haverinen 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	20040053858	KR		2004-06-25	Electronics and Telecommunications Research Instit		

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	15582350
	Filing Date	2017-04-28
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3C2C3C2

	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	15582350
	Filing Date	2017-04-28
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3C2C3C2

CERTIFICATION STATEMENT

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

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

OR

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

See attached certification statement.

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

☒ A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/James E. Harris/	Date (YYYY-MM-DD)	2018-07-25
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.

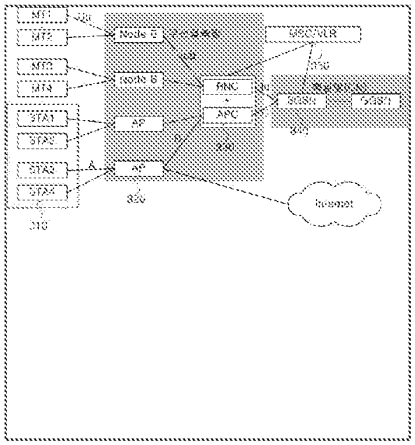
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine 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.

무선랜과 셀룰러 망의 연동 시스템 및 방법, 그프로그램이 저장된 기록매체

system for linking of wireless and cellular networkand method thereof, its program storing recordingmedium

(51) Int. CL	H04W 48/18(2009.01.01) H04W 88/06(2009.01.01) H04W 84/12(2009.01.01) H04L 29/06(2006.01.01)
(52) CPC	H04W 48/18(2013.01) H04W 88/06(2013.01) H04W 84/12(2013.01) H04L 29/06(2013.01)
(21) Application No.(Date)	1020020080313 (2002.12.16)
(71) Applicant	Electronics and Telecommunications Research Institute
(11) Registration No.(Date)	1004830210000 (2005.04.04)
(65) Unex. Pub. No.(Date)	1020040053858 (2004.06.25)
(11) Publication No.(Date)	(2005.04.15)
(86) Int'l Application No.(Date)	
(87) Int'l Unex. Pub. No.(Date)	
(30) Priority info. (Country / No. / Date)	
Legal Status	**Ended**
Examination Status	Decision to grant (General)
Trial Info	
Kind/Right of Org. Application	/
Right of Org. Application No.(Date)	
Related Application No.	
Request for an examination(Date)	Y(2002.12.16)
Number of examination claims	34



Abstract (Translated from Korean) PURPOSE: An interworking system between a WLAN(Wireless LAN) and a cellular phone network is provided to operate an IEEE802.11 physical layer and an AP(Access Point) according to an 802.11e MAC protocol that improves a QoS function, thereby supporting service mobility and supporting dual modes by selectively

interworking a WLAN and a cellular network.CONSTITUTION: A wireless station(310) maintains profile information in the same information type as a mobile terminal, and supports dual modes to connect with a WLAN or to be operated by interworking with a cellular network. If the wireless station(310) requests a call setup and transceives data after the call setup, APs(320) wirelessly connect with the wireless station(310) by using an 802.11 physical layer and an 802.11e MAC function, receive data and a control signal, and transmit the data and the control signal to an APC(330). The APC(330) maintains information necessary for interworking with the cellular network by accessing the APs(320), and connects with an MSC/VLR(350) and an SGSN(340) of the cellular network.© KIPO 2004

10-2004-0053858

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.[7]
H04L 12/46

(11) 공개번호 10-2004-0053858
(43) 공개일자 2004년06월25일

(21) 출원번호 10-2002-0080313
(22) 출원일자 2002년12월16일

(71) 출원인 한국전자통신연구원
대전 유성구 가정동 161번지
(72) 발명자 성낙운
대전광역시유성구구성동373-1번지
박남훈
대전광역시유성구어은동한빛아파트120동1001호
(74) 대리인 유미특허법인

심사청구 : 있음

(54) 무선랜과 셀룰러 망의 연동 시스템 및 방법, 그프로그램이 저장된 기록매체

요약

본 발명은 이동단말기나 무선 단말기와 핵심망 사이에서 유기적으로 연결되는 셀룰러 망의 무선접속망에 적용되는 무선랜과 셀룰러 망의 연동 시스템 및 방법, 그 프로그램이 저장된 기록매체에 관한 것으로서, 본 발명은 상기 셀룰러 망의 무선 접속망은 무선 접속망 내에서 동일한 인터페이스로 접속하고, 무선랜을 위한 규격을 이용하여 상기 무선 단말기와 무선 접속하여 데이터 및 제어신호를 출력하는 다수의 접속장치, 다수의 접속 장치와 연결되어 접속장치로부터의 데이터 및 제어신호를 전달받아 이를 상기 핵심망으로 전달하고, 핵심망과 무선접속망에서와 동일한 방식으로 접속하는 접속 제어장치를 포함함으로써, 무선랜을 위해 IEEE 802.11 물리계층과, 서비스 품질 기능을 향상시킨 802.11e MAC 프로토콜에 따라 무선 접속 구간을 운용함으로써 서비스의 이동성을 지원할 수 있고, 서비스에 따라 무선랜과 셀룰러 망에 선택적 연동할 수 있어 듀얼 모드 지원이 가능하고, 또한 호 설정을 위한 제어 신호의 실시간 전송 및 사용자 트래픽의 서비스 품질을 보장할 수 있는 효과가 있다.

대표도

도4

색인어

선랜, 셀룰러 망, 무선접속망, 핵심망, 접속장치(AP), 접속제어장치(APC)

명세서

도면의 간단한 설명

도 1은 일반적인 패킷 서비스를 제공하는 W-CDMA 네트워크의 구성을 도시한 것이다.

도 2는 종래 기술에 따른 실시예의 IEEE(Institute of Electrical and Electronics Engineers) 802.11 네트워크의 구성을 도시한 것이다.

도 3은 셀룰러 망 중에서 광대역 코드분할 다중접속(W-CDMA) 망의 접속 인터페이스 구조를 도시한 것이다.

도 4는 본 발명에 따른 실시예의 무선랜과 셀룰러 망의 연동 시스템의 구성을 도시한 것이다.

도 5는 도 3에 의한 W-CDMA 프로토콜의 제어평면 구조를 도시한 것이다.

도 6은 도 3에 의한 W-CDMA 프로토콜의 사용자 평면 구조를 도시한 것이다.

도 7은 도 4에 의한 802.11e 무선랜과 셀룰러 망 중 W-CDMA 망 연동 네트워크의 제어평면 프로토콜 구조를 도시한 것이다.

도 8은 도 4에 의한 802.11e 무선랜과 셀룰러 망 중 W-CDMA 망 연동 네트워크의 사용자 평면 프로토콜 구조를 도시한 것이다.

도 9는 본 발명에 따른 실시예의 무선랜과 셀룰러 망의 연동 방법에 따른 신호 및 데이터 전송 절차를 도시한 것이다.

발명의 상세한 설명

발명의 목적

발명이 속하는 기술분야 및 그 분야의 종래기술

본 발명은 무선랜과 셀룰러 망의 연동 시스템 및 방법, 그 프로그램이 저장된 기록매체에 관한 것으로, 보다 상세하게는 IEEE 802.11를 이용하여 무선랜과 셀룰러 망을 연동하기 위한 무선랜과 셀룰러 망의 연동 시스템 및 방법, 그 프로그램이 저장된 기록매체에 관한 것이다.

도 1은 일반적인 패킷 서비스를 제공하는 W-CDMA 네트워크의 구성을 도시한 것이다.

도 1을 참고하면, 이동통신 가입자는 노트북이나 일반 개인용 컴퓨터와 같은 종단 장치(Terminal Equipment)(10)를 사용하여 이동 전화기(Mobile Terminal, MT)(20)에 접속하여 인터넷 등의 패킷 데이터 서비스를 제공받는다.

이동 전화기(20)는 에어 인터페이스(Air Interface)를 통해 무선 접속망(UMTS Terrestrial Radio Access Network, UTRAN)(30)에 접속하고, UTRAN(30)은 ATM(Asynchronous Transfer Mode) 또는 인터넷 프로토콜 망(IP)을 통하여 SGSN(Serving GPRS Support Node)(40)에 접속하며, SGSN(40)은 GGSN(Gateway GPRS Support Node)(50)를 통하여 외부 공중망(Public Data Network, PDN)(70)과 접속된다.

여기서, UMTS는 Universal Mobile Telecommunication System의 약어이고, GPRS는 General Packet Radio Service의 약어이다.

또한, 이동교환기(Mobile Switching Center, MSC)(60)는 UTRAN(30), SGSN(40), GGSN(50)과 통신하면서 이동통신 가입자에게 회선 교환 서비스를 제공하고, 이동 전화기(20)의 위치를 추적한다. 이때, MSC(60)는 이동 전화기(20)의 위치 추적을 위해 가입자 및 이동 전화기(20) 정보를 보관하는 방문자 위치 등록기(Visitor Location Register, VLR)와 연동된다.

도 2는 종래 기술에 따른 실시예의 IEEE(Institute of Electrical and Electronics Engineers) 802.11 네트워크의 구성을 도시한 것이다.

도 2를 참고하면, 다수의 무선 단말기(Mobile Station, STA1)(110)는 노트북이나 PDA(Personal Digital Assistant) 등을 이용하여 하나의 CF(Coordination Function)에 의해서 제어되는 BSS(Basic Service Set)(130)를 이루고, 이는 다시 AP(Access Point)(120)를 통하여 다른 BSS와 DS(Distribution System)(140)를 거쳐 연결된다.

이러한 구조로 이루어진 종래의 셀룰러(Cellular) 망과 802.11 무선랜 망은 현재 별개의 망으로 중복 구축되고 있는 실정이다. 이는 셀룰러 망이 넓은 서비스 영역과 높은 이동성을 지원하지만 서비스 속도가 느리고 비용이 고가인 반면에, 무선랜 망은 좁은 서비스 영역과 낮은 이동성을 지원하지만 비교적 높은 서비스 속도와 저렴한 서비스 비용으로 급속히 확산되고 있기 때문이다.

따라서 종래 기술에 따른 실시예에서는 셀룰러 망과 802.11 무선랜 망의 장점을 이용하여 연동할 수 있는 방안이 아직 제시되지 않고 있으며, 기존의 802.11a/b 망은 셀룰러 망에서 요구하는 QoS(서비스 품질, Quality of Service)를 제공할 수 없는 문제점이 있다.

또한, 종래 기술에 따른 실시예에서 무선랜 망과 셀룰러 망간의 실시간 호 설정이 지원되지 않으며, 서비스의 이동성도 지원되지 않는다는 문제점도 있다.

발명이 이루고자 하는 기술적 과제

본 발명은 위의 문제점을 해결하기 위한 것으로, 본 발명의 목적은 셀룰러 망의 무선 접속망을 무선랜으로 내체하여 셀룰러 망과 무선랜이 연동하여 망간 서비스 이동성과 서비스 품질을 보장하기 위한 무선랜과 셀룰러 망의 연동 시스템 및 방법, 그 프로그램이 저장된 기록매체를 제공하는 것이다.

발명의 구성 및 작용

상기한 바와 같은 목적을 실현하기 위한 본 발명에 따른 무선랜과 셀룰러 망의 연동 시스템의 특징은, 이동단말기나 무선 단말기와 핵심망 사이에서 유기적으로 연결되는 셀룰러 망의 무선접속망에 적용되는 무선랜과 셀룰러 망의 연동 시스템에 있어서, 상기 무선 접속망 내에서 동일한 인터페이스로 접속하고, 무선랜을 위한 규격을 이용하여 상기 무선 단말기와 무선 접속하여 데이터 및 제어신호를 출력하는 다수의 접속장치; 상기 다수의 접속 장치와 연결되어 상기 접속장치로부터의 데이터 및 제어신호를 전달받아 이를 상기 핵심망으로 전달하고, 상기 핵심망과 무선접속망에서와 동일한 방식으로 접속하는 접속 제어장치를 포함한다.

상기 무선 단말기는 무선랜을 위한 규격에서 사용하는 특정 프로토콜 기능과 셀룰러 망에서 사용하는 프로토콜 기능, 및 인터넷 통신 프로토콜 기능을 가진다.

상기 무선 단말기의 프로토콜 중에서 무선 접속구간에서 이용되는 계층(Layer)2 이하의 PDCP(Packet Data Convergence Protocol), RRC(Radio Resource Control), RLC(Radio Link Control)/MAC(Media Access Control) 프로토콜이 IEEE(Institute of Electrical and Electronics Engineers) 802.11e MAC(Medium Access Control) 프로토콜로 대체하고, 나머지 PMM(Packet Mobility Management) 및 SM(Session Management) 프로토콜은 그대로 채용한다.

상기 무선 단말기의 프로토콜 중에서 무선 접속 구간에 이용되는 RRM(Radio Resource Management) 기능을

16-2

추가하여 무선 자원관리 및 이동성을 지원하도록 한다.

상기 무선 단말기는 셀룰러 망 접속을 위해 필요한 프로파일 정보를 상기 이동 단말기와 같은 정보 형태로 유지한다.

상기 무선 단말기는 상기 셀룰러 망에 연동하여 운용되거나 무선랜에 접속하여 운용되도록 듀얼 모드(Dual mode)를 지원한다.

상기 접속장치의 무선랜을 위한 규격은 IEEE(Institute of Electrical and Electronics Engineers) 802.11 물리계층과 802.11e MAC(Medium Access Control) 계층을 이용한다.

상기 접속장치와 접속 제어장치는 유선으로 접속한다. 상기 접속 제어장치는, 상기 무선접속망의 RNC(Radio Network Controller) 기능을 포함한다. 상기 접속 제어장치는, 상기 셀룰러 망과의 연동에 필요한 정보를 유지하며 상기 셀룰러 망 내의 MSC(Mobile Switching Center)/VLR(Visitor Location Register)에 접속한다.

상기 접속장치와 접속 제어장치간의 제어신호는, 상기 무선랜을 위한 규격인 IEEE 802.11e MAC의 기능 중 HCF(Hybrid Coordination Function) 기능 중 HCF Controlled channel access 기능, 또는 PCF(Point Coordination Function) 기능을 이용하여 실시간 전송되도록 한다.

상기 접속장치와 접속 제어장치간의 데이터 전송은, 사용자의 서비스 품질을 고려하여 HCF contention-based channel access(EDCF) 기능을 이용하여 전송한다.

상기 접속장치와 접속 제어장치간의 데이터 전송은, 사용자의 서비스 품질을 고려하지 않고 DCF(Distributed Coordination Function) 기능을 이용하여 전송한다.

상기 접속 제어장치와 무선 단말기는 무선랜과 상기 셀룰러 망간의 이동성을 지원하기 위해 버티컬 핸드오프(Vertical Hand-off) 기능을 지원한다.

한편, 본 발명에 따른 무선랜과 셀룰러 망의 연동 시스템의 특징은, 이동단말기나 무선 단말기와 핵심망 사이에서 유기적으로 연결되는 셀룰러 망의 무선접속망에 적용되는 무선랜과 셀룰러 망의 연동 방법에 있어서, a) 상기 무선 단말기를 초기화하고 상기 무선 단말기와 셀룰러 망, 또는 상기 무선 단말기와 무선랜 간 호 설정을 수행하는 단계; b) 상기 a) 단계에서 호 설정 후, 상기 무선 단말기와 셀룰러 망간 데이터를 전송하는 단계; 및 c) 상기 b) 단계에서 데이터 전송이 완료되면, 설정된 호를 해제하는 단계를 포함한다.

상기 a) 단계 내지 c) 단계는, 상기 무선 단말기와 무선 접속하여 데이터 전송을 수행하는 접속장치가 무선랜을 위해 IEEE(Institute of Electrical and Electronics Engineers) 802.11 물리계층과 802.11e MAC(Medium Access Control) 계층을 이용한다.

상기 접속장치는 802.11e 스펙에 의해 CP(Contention Period) 또는 CFP(Contention Free Period)에 상관없이 CCI(Controlled Contention Interval)을 야기하기 위해 부정기적으로 'CC(Controlled Contention) Control Frame'을 상기 무선 단말기로 전송한다.

상기 CC에는 CCI 내의 CCOP(Controlled Contention OPportunity)의 수(Nccop)와, 각 CCOP의 주기 시간(Duration time) 값을 포함한다.

상기 a) 단계는,

가) 상기 무선 단말기가 메시지 전달을 위해 상기 셀룰러 망에서 야기되는 'CC Control Frame'의 수신을 대기하는 단계; 나) 상기 무선 단말기가 'CC Control Frame'을 수신하면, 'RR(Reservation Request) Frame'을 상기 셀룰러 망으로 전송하여 무선 자원을 예약하는 단계; 다) 상기 나) 단계를 통해 CCI(Controlled Contention Interval) 동안 다수의 무선 단말기로부터'RR Frame'를 전송받은 셀룰러 망은 다음 CCI에 전송하는 'CC Frame'에 해당 무선 단말기의 무선 자원 예약 알림(Ack) 메시지를 전송하는 단계; 라) 상기 셀룰러 망이 'RR Frame'을 승인한 무선 단말기에 대하여 무선 전송 기회를 부여하는 단계; 마) 상기 라) 단계에서 무선 전송 기회를 부여받은 무선 단말기는 상기 셀룰러 망의 핵심망에 등록 절차를 수행하는 단계; 및 바) 상기 마) 단계에서 등록 절차가 완료된 무선 단말기는 데이터 전송을 위해 상기 셀룰러 망과의 세션 연결 설정을 요구하는 단계를 포함한다.

상기 나) 단계에서 'RR Frame'은 TID(Traffic ID)와 무선 전송 기회 기간 값을 포함한다.

상기 다) 단계에서 'Ack 메시지'를 전송받은 무선단말기는 'CC Frame'의 피드백 필드(Feedback Filed) 내 자신의 식별 값으로 무선 자원 예약 요구의 승인을 확인한다.

상기 마) 단계에서 무선 단말기의 등록 절차를 수행하는 단계는, ㄱ) 상기 셀룰러 망의 무선접속망 내에서 상기 무선 단말기와 무선 접속되는 접속장치에 전송된 무선 단말기의 'Attach Request'메시지가 상기 접속장치와 접속되는 접속 제어장치에 전송되는 단계; ㄴ) 상기 ㄱ) 단계에서 'Attach Request'메시지를 전송받은 접속 제어장치는 이 메시지를 상기 핵심망으로 전달하고, 상기 핵심망으로부터 전달되는 'Attach Request/Reject'메시지를 상기 접속장치로 전송하는 단계; 및 ㄷ) 상기 ㄴ) 단계를 통해 접속장치는 'Attach Request/Reject'메시지를 '(QoS Data+)CF-Poll+CF-Ack Frame'을 통하여 상기 무선 단말기로 전송하는 단계를 포함한다.

마) 상기 바) 단계를 통해 상기 무선 단말기의 세션 연결 절차와 등록 절차 사이에 일정 시간 이상이 소요되면, 상기 무선 단말기는 이전의 무선 전송 기회를 종료하고 다시 상기 셀룰러 망으로 다른 무선 전송 기회를 부여받기 위해 세션 연결 제어 메시지를 상기 셀룰러 망으로 전송하는 단계를 포함한다.

상기 바) 단계에서 무선 단말기의 세션 연결 설정 단계는, ㄱ) 상기 무선 단말기는 'QoS Data Frame'을 이용하여 'Active PDP Context Request' 메시지를 상기 셀룰러 망의 무선 접속망으로 전송하는 단계; ㄴ) 상기 ㄱ) 단계를 통해 무선접속망에 전달된 메시지는 핵심망의 SM(Session Management) 계층에 전달되어 데이터 경로 설정에 대한 준비가 이루어지는 단계; 및 ㄷ) 상기 ㄴ) 단계를 통해 핵심망의 SM 계층은

16-3

'Activate PDP Context Accept/Reject' 메시지를 상기 무선 접속망을 거쳐 'CF-Poll-Ack Frame'을 통해 상기 무선 단말기로 전달하는 단계를 포함한다.

상기 ㄷ) 단계에서 'Activate PDP Context Accept'메시지를 수신한 무선 단말기는 데이터 경로 설정 요구가 이루어졌음을 확인하고, 무선접속망에 설정된 무선 전송의 기회를 해제한다.

상기 b) 단계는,

상기 a) 단계에서 호 설정이 이루어지면, 상기 무선 단말기는 IEEE 802.11의 DCF(Distributed Coordination Function) 기능, 또는 사용자의 서비스 품질을 고려하여 HCF contention-based channel access(EDCF) 기능을 이용하여 상기 셀룰러 망으로 데이터를 전송한다.

상기 무선 단말기와 셀룰러 망 내에서 무선으로 접속되는 접속장치 간의 데이터 전송은, IEEE 802.11e 스펙에 규정된 CSMA/CA(Carrier Sensing Multiple Access/Collision Avoidance) 알고리즘에 따라 이루어지고, 각 데이터 트래픽에 대한 우선순위는 MAC 계층의 스케줄러에 의해 제어된다.

상기 c) 단계는,

가) 상기 b) 단계에서 데이터 전송이 종료되면, 상기 무선 단말기와 셀룰러 망의 핵심망간 설정된 세션을 종료하기 위해 무선접속망의 호 설정을 예약하는 단계; 나) 상기 가) 단계를 통해 핵심망은 이전에 설정된 데이터 경로를 해제하여 셀룰러 망의 세션을 종료하는 단계; 및 다) 상기 나) 단계에서 세션이 종료되면, 상기 무선 단말기는 전송할 데이터의 유무에 따라 세션을 재설정하거나 등록 해제 절차를 수행하는 단계을 포함한다.

상기 가) 단계는,

ㄱ) 상기 무선 단말기가 메시지 전달을 위해 상기 셀룰러 망에서 아기되는 'CC Control Frame'의 수신을 대기하는 단계; ㄴ) 상기 무선 단말기가 'CC Control Frame'을 수신하면, 'RR(Reservation Request) Frame'을 상기 셀룰러 망으로 전송하여 무선 자원을 예약하는 단계; ㄷ) 상기 ㄴ) 단계를 통해 CCI(Controlled Contention Interval) 동안 다수의 무선 단말기로부터'RR Frame'를 전송받은 셀룰러 망은 다음 CCI에 전송하는 'CC Frame'에 해당 무선 단말기의 무선 자원 예약 알림(Ack) 메시지를 전송하는 단계; ㄹ) 상기 셀룰러 망이 'RR Frame'을 승인한 무선 단말기에 대하여 무선 전송 기회를 부여하는 단계; 및 ㅁ) 상기 ㄹ) 단계에서 무선 전송 기회를 부여받은 무선 단말기는 상기 셀룰러 망의 핵심망에 등록 절차를 수행하는 단계를 포함한다.

상기 나) 단계는, ㄱ) 상기 무선 단말기는 셀룰러 망의 핵심망으로부터 'Deactivate PDP Context Request'메시지를 전달받아 'QoS Data Frame'을 통해 무선접속망으로 전달하는 단계; ㄴ) 상기 ㄱ) 단계에서 무선접속망으로 전달된 메시지는 다시 핵심망으로 전달되므로 상기 핵심망이 이전에 설정된 데이터 경로를 해제한 후에 'Deactivate PDP Context Accept'메시지를 무선접속망으로 전송하는 단계; 및 ㄷ) 상기 ㄴ) 단계에서 메시지를 전송받은 무선 접속망은 'CF-Poll+CF-Ack'을 이용하여 상기 무선 단말기로 전송하는 단계를 포함한다.

상기 다) 단계는, 상기 무선 단말기가 전송할 데이터가 있을 경우에 세션을 재설정하기 위한 절차를 수행하고, 상기 무선 단말기가 전송할 데이터가 없을 경우에 상기 셀룰러 망과의 접속을 종료하기 위해 등록 해제 절차를 수행한다.

상기 무선단말기의 등록 해제 절차는, 상기 무선 단말기의 'Detach Request'메시지가 핵심망으로 전달하여 상기 핵심망으로부터 'Detach Accept'메시지가 상기 무선 접속망으로 수신되면, 상기 무선 접속망이 제어 메시지 전달을 위한 무선 전송의기회가 종료되었음을 상기 무선 단말기로 알린다.

상기 무선 단말기가 셀룰러 망에 연동하여 운영되거나, 무선랜에 접속하여 운영되는 듀얼 모드로 동작한다. 상기 듀얼 모드 지원과 선택은 자동으로 설정 가능하고, 비콘(beacon) 프레임을 이용하여 방송될 수 있다.

무선랜과 셀룰러 망의 연동을 위한 프로그램이 저장된 기록매체의 특징은, 이동단말기나 무선 단말기와 핵심망 사이에서 유기적으로 연결되는 셀룰러 망의 무선접속망에 적용되는 무선랜과 셀룰러 망의 연동을 위해, 상기 무선 단말기를 초기화하고 상기 무선 단말기와 셀룰러 망, 또는 상기 무선 단말기와 무선랜 간 호 설정을 수행하는 제1 기능; 상기 호 설정 후, 상기 무선 단말기와 셀룰러 망간 데이터를 전송하는 제2 기능; 및 상기 데이터 전송이 완료되면, 설정된 호를 해제하는 제3 기능을 포함한다.

이하 첨부된 도면을 참조하여 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자가 본 발명을 용이하게 실시할 수 있는 바람직한 실시예를 상세히 설명하면 다음과 같다.

도 3은 셀룰러 망 중에서 광대역 코드분할 다중접속(W-CDMA) 망의 접속 인터페이스 구조를 도시한 것이다.

도 3에서, Iu는 핵심망(Core Network, CN)과 무선접속망(UTRAN) 사이의 인터페이스이고, Iur은 UTRAN의 RNC(Radio Network Controller) 사이의 논리적인 인터페이스이며, Iub는 RNC와 노드B 사이의 인터페이스를 각각 나타낸다. 한편, Uu는 UTRAN과 이동국(User Equipment, UE) 사이의 무선 인터페이스를 나타낸다.

여기서, 노드B(Node B)는 하나 또는 그 이상의 셀에서 UE로부터 무선 송수신을 책임지고 있는 논리적인 노드로서, 각각의 셀들을 제어하는 셀 제어장치(Cell Controller)가 포함되어 있다.

도 4는 본 발명에 따른 실시예의 무선랜과 셀룰러 망의 연동 시스템의 구성을 도시한 것이다.

도 4에 도시된 바와 같이, 본 발명에 따른 실시예의 시스템은 이동단말기나 무선단말기(Mobile Station, STA)와 핵심망(CN) 사이에서 유기적으로 연결되는 셀룰러 망의 무선접속망에 적용되고, 무선 접속망 내에 노드B, RNC, 외에 접속장치(Access Point)(320)와 접속 제어장치(Access Point Controller)(330)를 포함하고 있다.

이때, 접속장치(320)는 노드B를 대체한 것이고, 접속 제어장치(330)는 무선접속망 내의 RNC를 대체하거나,

16-4

기존의 RNC 기능에 접속 제어 기능을 포함하도록 RNC를 재설계한 것일 수도 있다.

또한, 접속장치(320)와 접속 제어장치(330)는 유선으로 접속된다.

무선 단말기(310)는 IEEE 802.11 물리계층과 802.11e MAC 계층 프로토콜 기능을 가지며, 계층 3에서 셀룰러 프로토콜 기능(예를 들어, W-CDMA의 PMM, SM 등)을 가지며, 그 상위에 일반적인 인터넷 통신 프로토콜 기능을 갖는다.

한편, 무선 단말기(310)는 셀룰러 망 접속을 위해 필요한 프로파일 정보를 이동 단말기(Mobile Terminal)와 같은 정보 형태로 유지고, 무선 단말기(310)는 셀룰러 망에 연동하여 운용되거나 무선랜에 접속하여 운용되도록 듀얼 모드(Dual mode)를 지원한다.

무선 단말기(310)가 호 설정을 요구하고 호 설정 이후의 데이터를 송수신하면, 접속장치(320)는 무선 단말기(310)와 802.11 물리 계층과 802.11e MAC 기능을 이용하여 무선 접속하여 데이터 및 제어 신호를 수신하고, 이를 접속 제어장치(330)에 전달한다.

이때, 접속장치(320)는 접속 제어장치(330)와 셀룰러 망의 BTS와 BSC 간, 노드 B와 RNC간의 Iub 접속처럼 ATM 프로토콜을 이용하여 접속할 수 있으며, 다른 인터넷 망을 이용하여 접속할 수도 있다.

접속 제어장치(330)는 접속장치와 접속하여 셀룰러 망과의 연동에 필요한 정보를 유지하며 필요시 셀룰러 망의 MSC/VLR(350), SGSN(340) 등에 접속할 수 있다.

이러한 접속 제어장치(330)는 핵심망과 무선접속망간의 인터페이스와 동일한 방식으로 접속하여 다수의 접속장치(320)로부터 데이터 및 제어신호를 전달받아 이를 핵심망으로 전달한다.

한편, 접속 제어장치와 무선 단말기는 무선랜과 상기 셀룰러 망간의 이동성을 지원하기 위해 버티컬 핸드오프(Vertical Hand-off) 기능을 지원한다.

위에서 살펴본 바와 같이, 무선 접속 구간이 기존의 셀룰러 망에서 이용되던 프로토콜을 대신하여 802.11 MAC의 기능에 서비스 품질(QoS) 기능을 향상시킨 802.11e MAC 프로토콜에 따라 운용되고 있다.

도 5는 도 3에 의한 W-CDMA 프로토콜의 제어평면 구조를 도시한 것이고, 도 6은 도 3에 의한 W-CDMA 프로토콜의 사용자 평면 구조를 도시한 것이다. 그리고 도 7은 도 4에 의한 802.11e 무선랜과 셀룰러 망 중 W-CDMA 망 연동 네트워크의 제어평면 프로토콜 구조를 도시한 것이고, 도 8은 도 4에 의한 802.11e 무선랜과 셀룰러 망 중 W-CDMA 망 연동 네트워크의 사용자 평면 프로토콜 구조를 도시한 것이다.

도 5 내지 도 8에 나탄 있듯이, 본 발명에 따른 실시예에서는 노드B와 이동단말기(MT)간 인터페이스, 즉 Uu 인터페이스만이 802.11e를 사용하는 무선랜 구간으로 대체됨을 알 수 있다.

따라서 무선 단말기(310)의 프로토콜 중에서 무선 접속구간에서 이용되는 계층(Layer)2 이하의 PDCP(Packet Data Convergence Protocol), RRC(Radio Resource Control), RLC(Radio Link Control)/MAC(Media Access Control) 프로토콜이 IEEE(Institute of Electrical and Electronics Engineers) 802.11e MAC(Medium Access Control) 프로토콜로 대체하고, 나머지 PMM(Packet Mobility Management) 및 SM(Session Management) 프로토콜은 그대로 채용한다.

그리고 무선 단말기(310)의 프로토콜 중에서 무선 접속 구간에 이용되는 RRM(Radio Resource Management) 기능을 추가하여 무선 자원관리 및 이동성을 지원하도록 한다.

이와 같이 구성되는 본 발명에 따른 실시예의 무선랜과 셀룰러 망의 연동 시스템의 서비스 이용은 제어 신호를 이용한 호 설정 과정과 호 설정 이후의 데이터 전송 과정으로 이루어진다.

먼저, 제어 신호는 실시간 전송을 위해 IEEE 802.11e MAC의 기능 중 HCF(Hybrid Coordination Function) 기능 중 HCF Controlled channel access 기능, 또는 PCF(Point Coordination Function) 기능을 이용하도록 한다.

다음, 데이터 전송 과정은 사용자의 서비스 품질을 고려하여 HCF contention-based channel access(EDCF) 기능을 이용하여 전송하거나, 또는 사용자의 서비스 품질을 고려하지 않고 DCF(Distributed Coordination Function) 기능을 이용하여 전송한다.

도 9는 본 발명에 따른 실시예의 무선랜과 셀룰러 망의 연동 방법에 따른 신호 및 데이터 전송 절차를 도시한 것이다.

도 9는 무선단말기(STA)와 HC(Hybrid Coordinator) 사이의 신호 및 데이터 전송 절차에 관한 것으로서, 802.11e 무선랜에서 HC의 기능은 일반적으로 AP의 기능에 포함된 것으로 간주하고, 도 9에서 무선랜의 호 설정 절차는 이미 이루어져 있는 것으로 가정한다.

먼저, HC는 802.11e 스펙에 의하면 CP(Contention Period)나 CFP(Contention Free Period)에 상관없이 CCI(Controlled Contention Interval)를 야기하기 위하여 부정기적으로 'CC(Controlled Contention) Control Frame'을 전송한다.

이때 CC에는 CCI내의 CCOP(Controlled Contention OPportunity)의 수(Nccop)와 각 CCOP의 'duration time' 값을 포함하고 있다(S100).

한편, 셀룰러 망에 접속하고자 하는 무선단말기(STA)는 HC에 의해 야기되는 CC Control Frame의 수신을 대기한다. CC Control Frame을 수신한 경우에, 무선 단말기(310)는 RR(Reservation Request) frame을 HC로 전송한다.

이때, RR Frame은 TID(Traffic ID)와 TXOP(Transmission OPportunity) duration 값 등을 포함하고 있다(S110).

CCI 동안 여러 무선 단말기(STA)로부터 RR Frame을 수신한 HC는 다음 CCI에 전송하는 CC Frame을 이용하여

16-5

ACK 메시지를 전송하게 된다. 이때 무선 단말기는 CC Frame의 Feedback Field 내의 자신의 AID 값으로 무선 자원 예약 요구가 승인된 것을 확인한다(S120).

HC는 RR을 승인한 무선 단말기(STA)에 대하여 (QoSData+)CF-Poll 메시지를 전송하여 TXOP, 즉 무선 전송의 기회를 부여한다. 이를 수신한 무선 단말기는 QoS Data 프레임을 이용하여 셀룰러 망의 핵심망에 무선 단말기의 등록 절차를 수행한다.

접속장치(320)에 전송된 셀룰러 망 제어 메시지인 Attach Request 메시지는 접속 제어장치(330)를 거쳐 핵심망에 전달된다. 그리고 핵심망으로부터 응답된 Attach Accept 또는 Attach Reject 메시지는 다시 접속 제어장치(330)를 거쳐 접속장치(320)로 전달되며, 여기서 전달된 메시지는 (QoS Data+)CF-Poll+CF-Ack Frame을 통하여 무선단말기로 전송된다.(S130~S150).

무선 단말기(STA)는 등록 절차 이후 데이터 전송의 필요가 있을 때마다 셀룰러 망과의 세션 연결 설정을 요구한다. 이때 세션 연결 절차와 무선 단말기 등록 절차 사이에 시간이 길어질 경우에, 기존의 TXOP를 종료하고 다시 S110~S940의 절차를 거쳐 다른 TXOP를 이용하여 세션 연결 제어 메시지를 전송할 수 있다.

무선 단말기(310)는 접속장치(320)로 세션 연결 설정을 위하여 QoS Data Frame을 이용하여 Activate PDP Context Request 메시지를 전송한다. 접속장치(320)로 전달된 메시지는 접속 제어장치(330)를 거쳐 핵심망의 SM(Session Management) 계층까지 전달되어 데이터 경로 설정이 되도록 한다.

데이터 경로 설정에 대한 준비가 이루어지며, SGSN의 SM 계층은 Activate PDP Context Accept 또는 Reject 메시지를 응답한다. 응답된 메시지는 다시 접속 제어장치(330)를 거쳐 접속장치(320)로 전달되며, 다시 CF-Poll-Ack Frame을 통하여 무선단말기(310)로 최종 전달된다.

이때 무선단말기는 Activate PDP Context Accept 메시지를 수신하는 경우, 데이터 경로 설정 요구가 이루어졌음을 확인하고, 무선접속망에 설정된 TXOP를 해제한다. 이는 CF-End 메시지를 전송함으로써 이루어진다(S160~S190).

앞에서의 절차로 호 설정이 이루어지면, 무선단말기(STA)는 데이터를 전송할 수 있는데, 무선 단말기는 802.11의 DCF 기능에 따라 전송 될 수 있으며 또는 QoS의 보장을 위하여 EDCF 기능에 의해 전송될 수 있다.

이때 무선접속망 ,즉 무선 단말기와 AP간의 데이터 전송은 802.11e 스펙에 규정된 CSMA/CA(Carrier Sensing Multiple Access/Collision Avoidance) 알고리즘에 따라 이루어지며, QoS를 보장하기 위하여 EDCF 기능을 이용할 수 있다. 각 데이터 트랙픽에 대한 우선순위는 MAC 계층의 스케줄러(scheduler)에 의해 제어되는 것으로 본다(S200).

데이터 전송을 종료하고, 현재 셀룰러 망의 핵심망과 설정된 세션을 종료하고자 하는 경우에, 이를 위하여 다시 무선 접속망의 호 설정을 예약해야 하며, 이때 호 설정의 과정은 S100~S130의 과정과 동일하다(S210~S240).

셀룰러 망의 세션 종료를 위하여 무선 단말기는 SM 계층으로부터 Deactivate PDP Context Request 메시지를 전달받아 QoSData Frame에 담아 접속장치(320)로 전송한다.

접속장치(320)로 전달된 메시지는 접속 제어장치(330)를 거쳐 핵심망의 SM 계층으로 전달된다. 이 메시지를 수신한 핵심망의 SGSN은 기존에 설정된 데이터 경로를 해제하고, Deactivate PDP Context Accept로 응답한다. 이 메시지는 접속 제어장치(330)를 거쳐 접속장치(320)로 전달되며, 다시 CF-Poll+CF-Ack Frame을 이용하여 무선단말기로 전달된다(S260~S270).

한편, 세션을 종료한 무선 단말기는 다시 전송할 데이터가 있을 경우 S110에서 S210까지의 절차를 통해 세션을 재설정하고 데이터를 전송할 수 있다. 만약 셀룰러 망과의 접속을 종료하고자 하는 경우에, 무선단말기는 등록 해제 절차를 수행한다.

이때 등록 해제 메시지, 즉 Detach Request 메시지는 핵심망으로 전달되고, 이에 대한 응답 메시지 즉 Detach Accept 메시지를 수신함으로써 이루어진다.

마지막으로 HC는 제어 메시지 전달을 위한 TXOP가 종료되었음을 CF-End Frame을 전송하여 알린다(S280~S310).

한편 무선 단말기는 기존의 802.11e MAC은 기존의 802.11 MAC의 기능에 QoS 기능을 더한 것이므로 도4에서 제시한 바와 같이 기존의 무선랜에 접속하여 필요한 서비스를 지원 받을 수 있다.

이러한 이중 모드 지원과 선택은 사용자의 관여 없이 자동적으로 설정 가능하다. 이러한 서비스의 유형은 비콘(Beacon) 프레임을 이용하여 방송(broadcasting)될 수 있다.

상기 도면과 발명의 상세한 설명은 단지 본 발명의 예시적인 것으로서, 이는 단지 본 발명을 설명하기 위한 목적에서 사용된 것이지 의미한정이나 특허청구범위에 기재된 본 발명의 범위를 제한하기 위하여 사용된 것은 아니다. 그러므로 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다. 따라서 본 발명의 진정한 기술적 보호 범위는 첨부된 특허청구범위의 기술적 사상에 의해 정해져야 할 것이다.

발명의 효과

본 발명에 의한 무선랜과 셀룰러 망의 연동 시스템 및 방법, 그 프로그램이 저장된 기록매체는 무선랜을 위해 IEEE 802.11 물리계층과, 서비스 품질 기능을 향상시킨 802.11e MAC 프로토콜에 따라 무선 접속 구간을 운용함으로써 서비스의 이동성을 지원할 수 있고, 서비스에 따라 무선랜과 셀룰러 망에 선택적 연동할 수 있어 듀얼 모드 지원이 가능한 효과가 있다.

또한, 본 발명에 의한 무선랜과 셀룰러 망의 연동 시스템 및 방법, 그 프로그램이 저장된 기록매체는 호

16-6

설정을 위한 제어 신호의 실시간 전송 및 사용자 트래픽의 서비스 품질을 보장할 수 있는 효과가 있다.

(57) 청구의 범위

청구항 1

이동단말기나 무선 단말기와 핵심망 사이에서 유기적으로 연결되는 셀룰러 망의 무선접속망에 적용되는 무선랜과 셀룰러 망의 연동 시스템에 있어서,

상기 무선 접속망 내에서 동일한 인터페이스로 접속하고, 무선랜을 위한 규격을 이용하여 상기 무선 단말기와 무선 접속하여 데이터 및 제어신호를 출력하는 다수의 접속장치;

상기 다수의 접속 장치와 연결되어 상기 접속장치로부터의 데이터 및 제어신호를 전달받아 이를 상기 핵심망으로 전달하고, 상기 핵심망과 무선접속망에서와 동일한 방식으로 접속하는 접속 제어장치

을 포함하는 무선랜과 셀룰러 망의 연동 시스템.

청구항 2

제 1 항에 있어서,

상기 무선 단말기는 무선랜을 위한 규격에서 사용하는 특정 프로토콜 기능과 셀룰러 망에서 사용하는 프로토콜 기능, 및 인터넷 통신 프로토콜 기능을 가지는 것을 특징으로 하는 무선랜과 셀룰러 망의 연동 시스템.

청구항 3

제 2 항에 있어서,

상기 무선 단말기의 프로토콜 중에서 무선 접속구간에서 이용되는 계층(Layer)2 이하의 PDCP(Packet Data Convergence Protocol), RRC(Radio Resource Control), RLC(Radio Link Control)/MAC(Media Access Control) 프로토콜이 IEEE(Institute of Electrical and Electronics Engineers) 802.11e MAC(Medium Access Control) 프로토콜로 대체하고, 나머지 PMM(Packet Mobility Management) 및 SM(Session Management) 프로토콜은 그대로 채용하는 것을 특징으로 하는 무선랜과 셀룰러 망의 연동 시스템.

청구항 4

제 2 항에 있어서,

상기 무선 단말기의 프로토콜 중에서 무선 접속 구간에 이용되는 RRM(Radio Resource Management) 기능을 추가하여 무선 자원관리 및 이동성을 지원하도록 하는 것을 특징으로 하는 무선랜과 셀룰러 망의 연동 시스템.

청구항 5

제 1 항에 있어서,

상기 무선 단말기는 셀룰러 망 접속을 위해 필요한 프로파일 정보를 상기 이동 단말기와 같은 정보 형태로 유지하는 것을 특징으로 하는 무선랜과 셀룰러 망의 연동 시스템.

청구항 6

제 1 항에 있어서,

상기 무선 단말기는 상기 셀룰러 망에 연동하여 운용되거나 무선랜에 접속하여 운용되도록 듀얼 모드(Dual mode)를 지원하는 것을 특징으로 하는 무선랜과 셀룰러 망의 연동 시스템.

청구항 7

제 1 항에 있어서,

상기 접속장치의 무선랜을 위한 규격은 IEEE(Institute of Electrical and Electronics Engineers) 802.11 물리계층과 802.11e MAC(Medium Access Control) 계층을 이용하는 것을 특징으로 하는 무선랜과 셀룰러 망의 연동 시스템.

청구항 8

제 1 항에 있어서,

상기 접속장치와 접속 제어장치는 유선으로 접속하는 것을 특징으로 하는 무선랜과 셀룰러 망의 연동 시스템.

청구항 9

제 1 항에 있어서,

상기 접속 제어장치는,

상기 무선접속망의 RNC(Radio Network Controller) 기능을 포함하는 것을 특징으로 하는 무선랜과 셀룰러 망의 연동 시스템.

청구항 10

16-7

제 1 항에 있어서,

상기 접속 제어장치는, 상기 셀룰러 망과의 연동에 필요한 정보를 유지하며 상기 셀룰러 망 내의 MSC(Mobile Switching Center)/VLR(Visitor Location Register)에 접속하는 것을 특징으로 하는 무선랜과 셀룰러 망의 연동 시스템.

청구항 11

제 1 항에 있어서,

상기 접속장치와 접속 제어장치간의 제어신호는,

상기 무선랜을 위한 규격인 IEEE 802.11e MAC의 기능 중 HCF(Hybrid Coordination Function) 기능 중 HCF Controlled channel access 기능, 또는 PCF(Point Coordination Function) 기능을 이용하여 실시간 전송되도록 하는 것을 특징으로 하는 무선랜과 셀룰러 망의 연동 시스템.

청구항 12

제 1 항에 있어서,

상기 접속장치와 접속 제어장치간의 데이터 전송은, 사용자의 서비스 품질을 고려하여 HCF contention-based channel access(EDCF) 기능을 이용하여 전송하는 것을 특징으로 하는 무선랜과 셀룰러 망의 연동 시스템.

청구항 13

제 1 항에 있어서,

상기 접속장치와 접속 제어장치간의 데이터 전송은, 사용자의 서비스 품질을 고려하지 않고 DCF(Distributed Coordination Function) 기능을 이용하여 전송하는 것을 특징으로 하는 무선랜과 셀룰러 망의 연동 시스템.

청구항 14

제 1 항에 있어서,

상기 접속 제어장치와 무선 단말기는 무선랜과 상기 셀룰러 망간의 이동성을 지원하기 위해 버티컬 핸드오프(Vertical Hand-off) 기능을 지원하는 것을 특징으로 하는 무선랜과 셀룰러 망의 연동 시스템.

청구항 15

이동단말기나 무선 단말기와 핵심망 사이에서 유기적으로 연결되는 셀룰러 망의 무선접속망에 적용되는 무선랜과 셀룰러 망의 연동 방법에 있어서,

a) 상기 무선 단말기를 초기화하고 상기 무선 단말기와 셀룰러 망, 또는 상기 무선 단말기와 무선랜 간 호 설정을 수행하는 단계;

b) 상기 a) 단계에서 호 설정 후, 상기 무선 단말기와 셀룰러 망간 데이터를 전송하는 단계; 및

c) 상기 b) 단계에서 데이터 전송이 완료되면, 설정된 호를 해제하는 단계

를 포함하는 무선랜과 셀룰러 망의 연동 방법.

청구항 16

제 15 항에 있어서,

상기 a) 단계 내지 c) 단계는,

상기 무선 단말기와 무선 접속하여 데이터 전송을 수행하는 접속장치가 무선랜을 위해 IEEE(Institute of Electrical and Electronics Engineers) 802.11 물리계층과 802.11e MAC(Medium Access Control) 계층을 이용하는 것을 특징으로 하는 무선랜과 셀룰러 망의 연동 방법.

청구항 17

제 16 항에 있어서,

상기 접속장치는 802.11e 스펙에 의해 CP(Contention Period) 또는 CFP(Contention Free Period)에 상관없이 CCI(Controlled Contention Interval)을 야기하기 위해 부정기적으로 'CC(Controlled Contention) Control Frame'을 상기 무선 단말기로 전송하는 것을 특징으로 하는 무선랜과 셀룰러 망의 연동 방법.

청구항 18

제 17 항에 있어서,

상기 CC에는 CCI 내의 CCOP(Controlled Contention OPportunity)의 수(Nccop)와, 각 CCOP의 주기 시간(Duration time) 값을 포함하는 것을 특징으로 하는 무선랜과 셀룰러 망의 연동 방법.

청구항 19

제 15 항에 있어서,

상기 a) 단계는,

16-8

가) 상기 무선 단말기가 메시지 전달을 위해 상기 셀룰러 망에서 야기되는 'CC Control Frame'의 수신을 대기하는 단계;

나) 상기 무선 단말기가 'CC Control Frame'을 수신하면, 'RR(Reservation Request) Frame'을 상기 셀룰러 망으로 전송하여 무선 자원을 예약하는 단계;

다) 상기 나) 단계를 통해 CCI(Controlled Contention Interval) 동안 다수의 무선 단말기로부터'RR Frame'를 전송받은 셀룰러 망은 다음 CCI에 전송하는 'CC Frame'에 해당 무선 단말기의 무선 자원 예약 알림(Ack) 메시지를 전송하는 단계;

라) 상기 셀룰러 망이 'RR Frame'을 승인한 무선 단말기에 대하여 무선 전송 기회를 부여하는 단계;

마) 상기 라) 단계에서 무선 전송 기회를 부여받은 무선 단말기는 상기 셀룰러 망의 핵심망에 등록 절차를 수행하는 단계; 및

바) 상기 마) 단계에서 등록 절차가 완료된 무선 단말기는 데이터 전송을 위해 상기 셀룰러 망과의 세션 연결 설정을 요구하는 단계;

를 포함하는 무선랜과 셀룰러 망의 연동 방법.

청구항 20

제 19 항에 있어서,

상기 나) 단계에서 'RR Frame'은 TID(Traffic ID)와 무선 전송 기회 기간 값을 포함하는 것을 특징으로 하는 무선랜과 셀룰러 망의 연동 방법.

청구항 21

제 19 항에 있어서,

상기 다) 단계에서 'Ack 메시지'를 전송받은 무선단말기는 'CC Frame'의 피드백 필드(Feedback Filed) 내 자신의 식별 값으로 무선 자원 예약 요구의 승인을 확인하는 것을 특징으로 하는 무선랜과 셀룰러 망의 연동 방법.

청구항 22

제 19 항에 있어서,

상기 마) 단계에서 무선 단말기의 등록 절차를 수행하는 단계는,

ㄱ) 상기 셀룰러 망의 무선접속망 내에서 상기 무선 단말기와 무선 접속되는 접속장치에 전송된 무선 단말기의 'Attach Request'메시지가 상기 접속장치와 접속되는 접속 제어장치에 전송되는 단계;

ㄴ) 상기 ㄱ) 단계에서 'Attach Request'메시지를 전송받은 접속 제어장치는 이 메시지를 상기 핵심망으로 전달하고, 상기 핵심망으로부터 전달되는 'Attach Request/Reject'메시지를 상기 접속장치로 전송하는 단계; 및

ㄷ) 상기 ㄴ) 단계를 통해 접속장치는 'Attach Request/Reject'메시지를 '(QoS Data+)CF-Poll+CF-Ack Frame'을 통하여 상기 무선 단말기로 전송하는 단계

를 포함하는 무선랜과 셀룰러 망의 연동 방법.

청구항 23

제 19 항에 있어서,

마) 상기 바) 단계를 통해 상기 무선 단말기의 세션 연결 절차와 등록 절차 사이에 일정 시간 이상이 소요되면, 상기 무선 단말기는 이전의 무선 전송 기회를 종료하고 다시 상기 셀룰러 망으로 다른 무선 전송 기회를 부여받기 위해 세션 연결 제어 메시지를 상기 셀룰러 망으로 전송하는 단계를 포함하는 무선랜과 셀룰러 망의 연동 방법.

청구항 24

제 19 항에 있어서,

상기 바) 단계에서 무선 단말기의 세션 연결 설정 단계는,

ㄱ) 상기 무선 단말기는 'QoS Data Frame'을 이용하여 'Active PDP Context Request' 메시지를 상기 셀룰러 망의 무선 접속망으로 전송하는 단계;

ㄴ) 상기 ㄱ) 단계를 통해 무선접속망에 전달된 메시지는 핵심망의 SM(Session Management) 계층에 전달되어 데이터 경로 설정에 대한 준비가 이루어지는 단계; 및

ㄷ) 상기 ㄴ) 단계를 통해 핵심망의 SM 계층은 'Activate PDP Context Accept/Reject' 메시지를 상기 무선 접속망을 거쳐 'CF-Poll-Ack Frame'을 통해 상기 무선 단말기로 전달하는 단계

를 포함하는 무선랜과 셀룰러 망의 연동 방법.

청구항 25

제 24 항에 있어서,

16-9

상기 ㄷ) 단계에서 'Activate PDP Context Accept'메시지를 수신한 무선 단말기는 데이터 경로 설정 요구가 이루어졌음을 확인하고, 무선접속망에 설정된 무선 전송의 기회를 해제하는 것을 특징으로 하는 무선랜과 셀룰러 망의 연동 방법.

청구항 26

제 15 항에 있어서,

상기 b) 단계는,

상기 a) 단계에서 호 설정이 이루어지면, 상기 무선 단말기는 IEEE 802.11의 DCF(Distributed Coordination Function) 기능, 또는 사용자의 서비스 품질을 고려하여 HCF contention-based channel access(EDCF) 기능을 이용하여 상기 셀룰러 망으로 데이터를 전송하는 것을 특징으로 하는 무선랜과 셀룰러 망의 연동 방법.

청구항 27

제 26 항에 있어서,

상기 무선 단말기와 셀룰러 망 내에서 무선으로 접속되는 접속장치 간의 데이터 전송은, IEEE 802.11e 스펙에 규정된 CSMA/CA(Carrier Sensing Multiple Access/Collision Avoidance) 알고리즘에 따라 이루어지고, 각 데이터 트래픽에 대한 우선순위는 MAC 계층의 스케줄러에 의해 제어되는 것을 특징으로 하는 무선랜과 셀룰러 망의 연동 방법.

청구항 28

제 15 항에 있어서,

상기 c) 단계는,

가) 상기 b) 단계에서 데이터 전송이 종료되면, 상기 무선 단말기와 셀룰러 망의 핵심망간 설정된 세션을 종료하기 위해 무선접속망의 호 설정을 예약하는 단계;

나) 상기 가) 단계를 통해 핵심망은 이전에 설정된 데이터 경로를 해제하여 셀룰러 망의 세션을 종료하는 단계; 및

나) 상기 나) 단계에서 세션이 종료되면, 상기 무선 단말기는 전송할 데이터의 유무에 따라 세션을 재설정하거나 등록 해제 절차를 수행하는 단계

을 포함하는 무선랜과 셀룰러 망의 연동 방법.

청구항 29

제 28 항에 있어서,

상기 가) 단계는,

ㄱ) 상기 무선 단말기가 메시지 전달을 위해 상기 셀룰러 망에서 아기되는 'CC Control Frame'의 수신을 대기하는 단계;

ㄴ) 상기 무선 단말기가 'CC Control Frame'을 수신하면, 'RR(Reservation Request) Frame'을 상기 셀룰러 망으로 전송하여 무선 자원을 예약하는 단계;

ㄷ) 상기 ㄴ) 단계를 통해 CCI(Controlled Contention Interval) 동안 다수의 무선 단말기로부터'RR Frame'를 전송받은 셀룰러 망은 다음 CCI에 전송하는 'CC Frame'에 해당 무선 단말기의 무선 자원 예약 알림(Ack) 메시지를 전송하는 단계;

ㄹ) 상기 셀룰러 망이 'RR Frame'을 승인한 무선 단말기에 대하여 무선 전송 기회를 부여하는 단계; 및

ㅁ) 상기 ㄹ) 단계에서 무선 전송 기회를 부여받은 무선 단말기는 상기 셀룰러 망의 핵심망에 등록 절차를 수행하는 단계

것을 특징으로 하는 무선랜과 셀룰러 망의 연동 방법.

청구항 30

제 28 항에 있어서,

상기 나) 단계는,

ㄱ) 상기 무선 단말기는 셀룰러 망의 핵심망으로부터 'Deactivate PDP Context Request'메시지를 전달받아 'QoS Data Frame'을 통해 무선접속망으로 전달하는 단계;

ㄴ) 상기 ㄱ) 단계에서 무선접속망으로 전달된 메시지는 다시 핵심망으로 전달되므로 상기 핵심망이 이전에 설정된 데이터 경로를 해재한 후에 'Deactivate PDP Context Accept'메시지를 무선접속망으로 전송하는 단계; 및

ㄷ) 상기 ㄴ) 단계에서 메시지를 전송받은 무선 접속망은 'CF-Poll+CF-Ack'을 이용하여 상기 무선 단말기로 전송하는 단계

를 포함하는 무선랜과 셀룰러 망의 연동 방법.

청구항 31

16-10

제 28 항에 있어서,

상기 다) 단계는,

상기 무선 단말기가 전송할 데이터가 있을 경우에 세션을 재설정하기 위한 절차를 수행하고, 상기 무선 단말기가 전송할 데이터가 없을 경우에 상기 셀룰러 망과의 접속을 종료하기 위해 등록 해제 절차를 수행하는 것을 특징으로 하는 무선랜과 셀룰러 망의 연동 방법.

청구항 32

제 31 항에 있어서,

상기 무선단말기의 등록 해제 절차는,

상기 무선 단말기의 'Detach Request'메시지가 핵심망으로 전달하여 상기 핵심망으로부터 'Detach Accept'메시지가 상기 무선 접속망으로 수신되면, 상기 무선 접속망이 제어 메시지 전달을 위한 무선 전송의기회가 종료되었음을 상기 무선 단말기로 알리는 것을 특징으로 하는 무선랜과 셀룰러 망의 연동 방법.

청구항 33

제 15 항에 있어서,

상기 무선 단말기가 셀룰러 망에 연동하여 운영되거나, 무선랜에 접속하여 운영되는 듀얼 모드로 동작하는 것을 특징으로 하는 무선랜과 셀룰러 망의 연동 방법.

청구항 34

제 33 항에 있어서,

상기 듀얼 모드 지원과 선택은 자동으로 설정 가능하고, 비콘(beacon) 프레임을 이용하여 방송될 수 있는 것을 특징으로 하는 무선랜과 셀룰러 망의 연동 방법.

청구항 35

이동단말기나 무선 단말기와 핵심망 사이에서 유기적으로 연결되는 셀룰러 망의 무선접속망에 적용되는 무선랜과 셀룰러 망의 연동 방법을 구현한 프로그램이 저장된 기록매체에 있어서,

무선 단말기를 초기화하고 상기 무선 단말기와 셀룰러 망, 또는 상기 무선 단말기와 무선랜 간 호 설정을 수행하는 제1 기능;

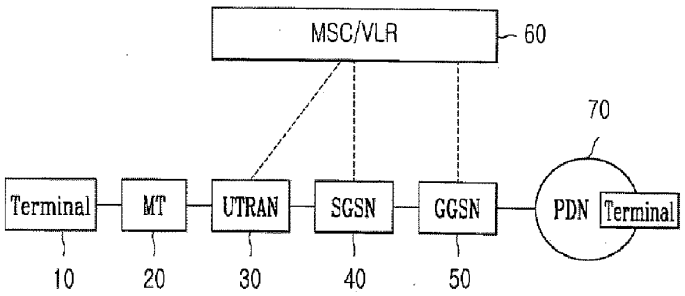
상기 호 설정 후, 상기 무선 단말기와 셀룰러 망간 데이터를 전송하는 제2 기능; 및

상기 데이터 전송이 완료되면, 설정된 호를 해제하는 제3 기능

을 포함하는 프로그램이 저장된 기록매체.

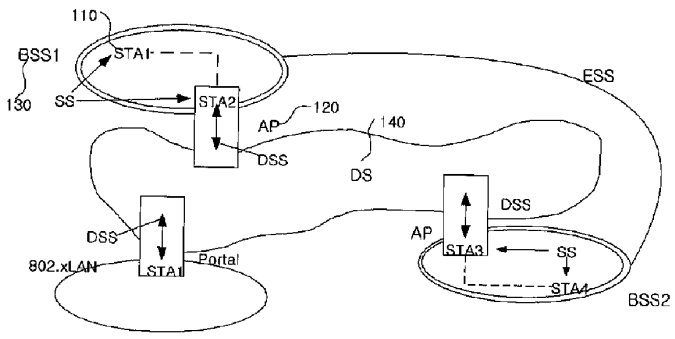
도면

도면1

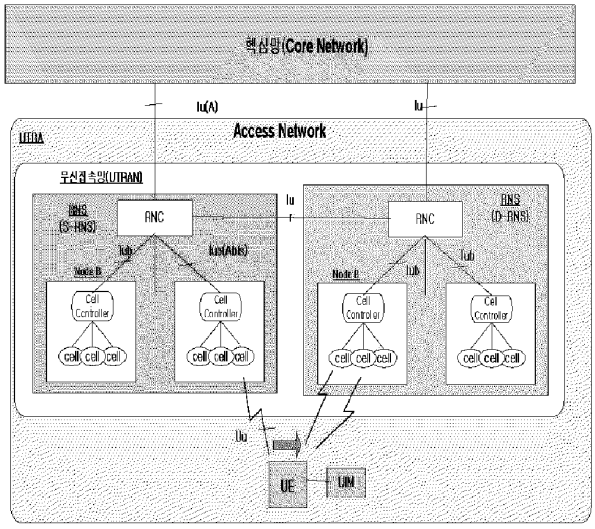


16-11

도면2

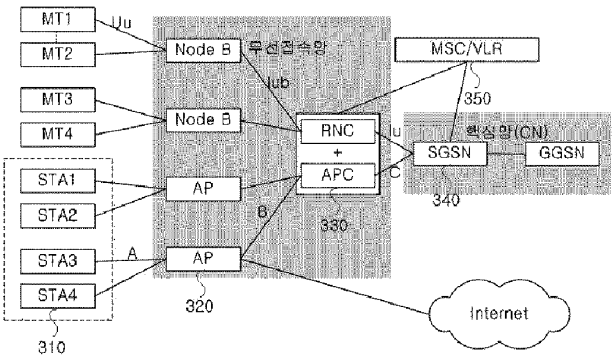

110
BSS1
STA1
130
SS
STA2
ESS
120
AP
140
DSS
DS
DSS
AP
STA3
SS
STA4
BSS2
DSS
802.xLAN
STA1
Portal

도면3

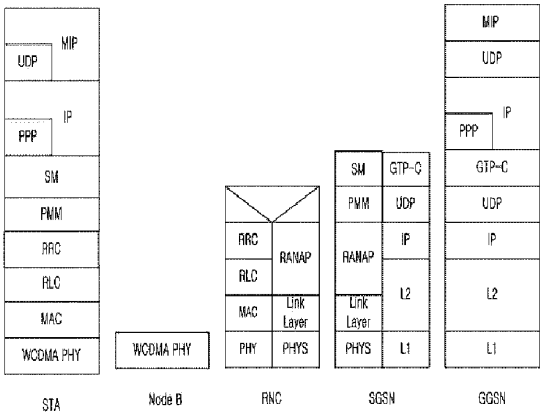

핵심망(Core Network)
Iu(A)
Iu
UTRA
Access Network
무선접속망(UTRAN)
RNS
(S-RNS)
RNC
Iub
Iur(Abis)
Node B
Cell Controller
cell
Iu
RNC
RNS
(D-RNS)
Iub
Node B
Cell Controller
cell
Iu
UE
UIM

16-12

도면4



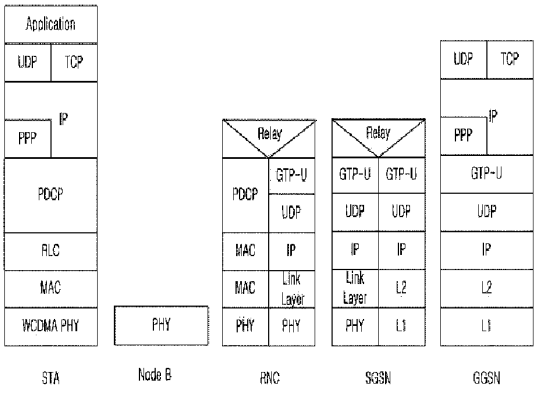
도면5



제어 평면

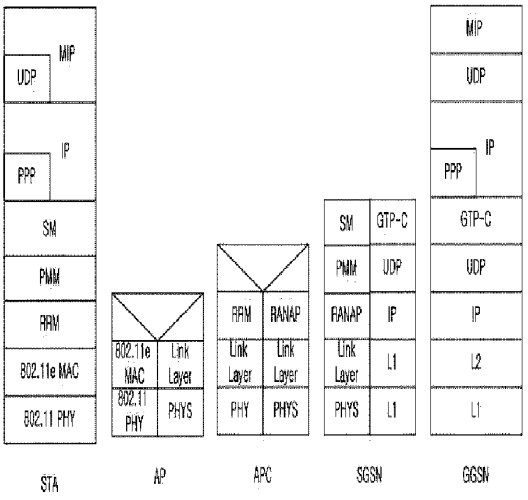
16-13

도면6



사용자 평면

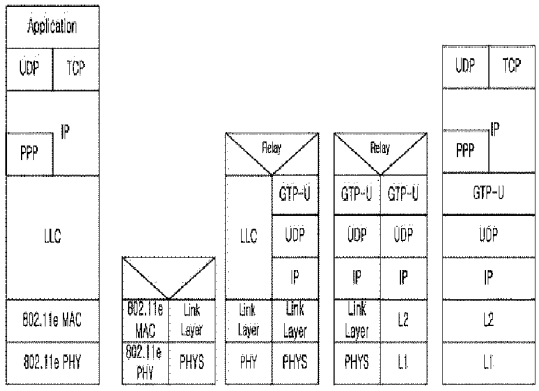
도면7



제어 평면

16-14

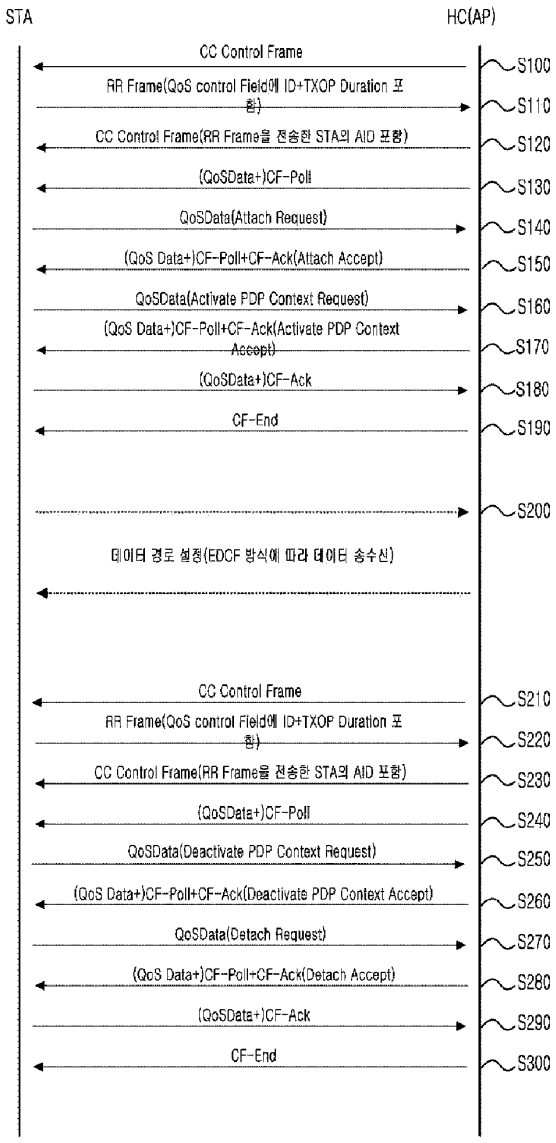
도면8



사용자 평면

16-15

도면9


STA
HC(AP)
CC Control Frame
S100
RR Frame(QoS control Field에 ID+TXOP Duration 포함)
S110
CC Control Frame(RR Frame을 전송한 STA의 AID 포함)
S120
(QoSData+)CF-Poll
S130
QoSData(Attach Request)
S140
(QoS Data+)CF-Poll+CF-Ack(Attach Accept)
S150
QoSData(Activate PDP Context Request)
S160
(QoS Data+)CF-Poll+CF-Ack(Activate PDP Context Accept)
S170
(QoSData+)CF-Ack
S180
CF-End
S190
S200
데이터 경로 설정(EDCF 방식에 따라 데이터 송수신)
CC Control Frame
S210
RR Frame(QoS control Field에 ID+TXOP Duration 포함)
S220
CC Control Frame(RR Frame을 전송한 STA의 AID 포함)
S230
(QoSData+)CF-Poll
S240
QoSData(Deactivate PDP Context Request)
S250
(QoS Data+)CF-Poll+CF-Ack(Deactivate PDP Context Accept)
S260
QoSData(Detach Request)
S270
(QoS Data+)CF-Poll+CF-Ack(Detach Accept)
S280
(QoSData+)CF-Ack
S290
CF-End
S300

16-16

Electronic Acknowledgement Receipt	
EFS ID:	33279175
Application Number:	15582350
International Application Number:	
Confirmation Number:	7797
Title of Invention:	Wirless Network Buffered Message System
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:	RALEP007C11C3C2C3C2
Receipt Date:	25-JUL-2018
Filing Date:	28-APR-2017
Time Stamp:	14:01:31
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)	P007C11C3C2C3C2.pdf	1054557 fb028062f1da3eebf056e51e3df440eeb0aa6987	no	8

Warnings:

Information:					
2	Foreign Reference	2102.pdf	1166143 22bd19b8fca35bc95ff2f7d6607b582f7d7d807d	no	18
Warnings:					
Information:					
			Total Files Size (in bytes):	2220700	

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 (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

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

Application Number	15582350
Filing Date	2017-04-28
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP007C11C3C2C3C2

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	5915226	A	1999-06-22	Martineau	
	2	6246870	B1	2001-06-12	Dent et al.	
	3	6591098	B1	2003-07-08	Shieh et al.	
	4	6603975	B1	2003-08-05	Inouchi et al.	
	5	6959202	B2	2005-10-25	Heinonen et al.	
	6	7031733	B2	2006-04-18	Alminana et al.	
	7	7120133	B1	2006-10-10	Joo et al.	
	8	7315892	B2	2008-01-01	Freimuth et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3C2C3C2

	9	7548875	B2	2009-06-16	Mikkelsen et al.	
	10	7584298	B2	2009-09-01	Klinker et al.	
	11	7607041	B2	2009-10-20	Kraemer et al.	
	12	7610057	B2	2009-10-27	Bahl et al.	
	13	7620383	B2	2009-11-17	Taglienti et al.	
	14	7627600	B2	2009-12-01	Citron et al.	
	15	7668966	B2	2010-02-23	Klinker et al.	
	16	7681226	B2	2010-03-16	Kraemer et al.	
	17	7688792	B2	2010-03-30	Babbar et al.	
	18	7693107	B2	2010-04-06	De Froment, Eric	
	19	7774412	B1	2010-08-10	Schnepel, Soenke	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3C2C3C2

	20	7797019	B2	2010-09-14	Friedmann	
	21	7805522	B2	2010-09-28	Schlüter et al.	
	22	7813746	B2	2010-10-12	Rajkotia, Purva R.	
	23	7835275	B1	2010-11-16	Swan et al.	
	24	7853656	B2	2010-12-14	Yach et al.	
	25	7882560	B2	2011-02-01	Kraemer et al.	
	26	7930553	B2	2011-04-19	Satarasinghe et al.	
	27	7979889	B2	2011-07-12	Gladstone et al.	
	28	8024424	B2	2011-09-20	Freimuth et al.	
	29	8060017	B2	2011-11-15	Schlicht et al.	
	30	8090361	B2	2012-01-03	Hagan, Guy R.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3C2C3C2

	31	8149748	B2	2012-04-03	Bata et al.	
	32	8340625	B1	2012-12-25	Johnson et al.	
	33	8346923	B2	2013-01-01	Rowles et al.	
	34	8392982	B2	2013-03-05	Harris et al.	
	35	8413245	B2	2013-04-02	Kraemer et al.	
	36	8495743	B2	2013-07-23	Kraemer et al.	
	37	8504574	B2	2013-08-06	Dvorak et al.	
	38	8531995	B2	2013-09-10	Khan et al.	
	39	8559369	B2	2013-10-15	Barkan	
	40	8594665	B2	2013-11-26	Anschutz, Thomas	
	41	8620257	B2	2013-12-31	Qiu et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3C2C3C2

	42	8849297	B2	2014-09-30	Balasubramanian	
	43	8929374	B2	2015-01-06	Tönsing et al.	
	44	9137286	B1	2015-09-15	Yuan	
	45	9286469	B2	2016-03-15	Kraemer 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	20040024756	A1	2004-02-05	Rickard, John Terrell	

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	2010128391	WO	A2	2010-11-11	Bridgewater Systems 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]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3C2C3C2

	1	Android Cupcake excerpts, The Android Open Source Project, Feb. 10, 2009	

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	15582350
	Filing Date	2017-04-28
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3C2C3C2

CERTIFICATION STATEMENT

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

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

OR

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

See attached certification statement.

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

☒ A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/James E. Harris/	Date (YYYY-MM-DD)	2018-05-10
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.

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
11 November 2010 (11.11.2010)

PCT

(10) International Publication Number
WO 2010/128391 A2

(51) International Patent Classification:
H04W 28/02 (2009.01)

(21) International Application Number:
PCT/IB2010/001084

(22) International Filing Date:
3 May 2010 (03.05.2010)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/175,316 4 May 2009 (04.05.2009) US

(71) Applicant *(for all designated States except US)*: **BRIDGEWATER SYSTEMS CORP.** [CA/CA]; 303 Terry Fox Drive, Suite 500, Ottawa, Ontario K2K 3J1 (CA).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **MOMTAHAN, Parham** [CA/CA]; 281 Lincoln Heights Road, Ottawa, Ontario K2B 5L7 (CA). **FREEN, Russ** [CA/CA]; 5 Clemow Avenue, Ottawa, Ontario, K1S 2A9 (CA).

(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, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, 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, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, 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 (Rule 48.2(g))*

(54) Title: SYSTEM AND METHODS FOR MOBILE DEVICE-BASED DATA COMMUNICATIONS COST MONITORING AND CONTROL

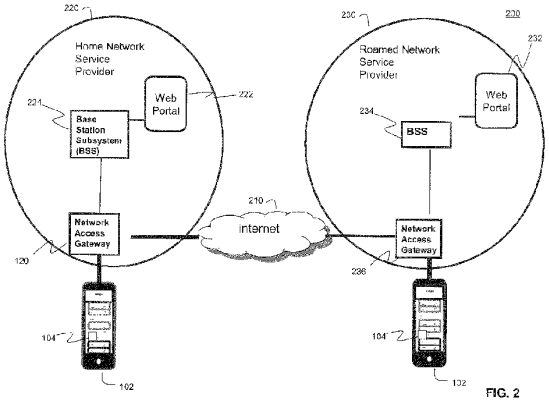


FIG. 2

(57) Abstract: Systems and methods for providing device-based data communications cost monitoring and controls are provided. In an embodiment, the method operates by receiving a registration request associated with a subscriber session, determining current data usage associated with the subscriber, and receiving data usage thresholds. The method further comprises receiving quotas associated with the subscriber session and collecting data usage information associated with the subscriber session. The method sends a notification to the subscriber when a predetermined quota is exceeded during the subscriber session and controls data usage. The system cost monitoring and control system comprises a usage policy server and a usage policy application. The usage policy application allows a subscriber to alter terms of a subscription. The usage policy application displays current data usage information on a per-network and per-application basis using subscriber profile information, subscriber session information, and prior subscriber usage history provided by the usage policy server.

WO 2010/128391 A2

System and Methods for Mobile Device-Based Data Communications Cost Monitoring and Control

FIELD OF THE INVENTION

[0001] The present invention relates generally to communications networks, more particularly, to monitoring and controlling data communications costs within wireless communications networks.

BACKGROUND

[0002] Portable computing devices such as laptop computers, personal data assistants (PDAs), smart phones and the like are in common usage, many featuring data communications support, powerful processors, larger and more colorful displays, and wireless networking and internet browsing capabilities. These advances in mobile technology have resulted in a dramatic increase in the volume of data communicated on wireless networks. These advances, coupled with subscribers seeking expanded mobility, will drive subscribers install and run data-hungry applications on their mobile devices. Data traffic is growing due to a combination of increasing market share of data-centric portable devices such as IPHONE™ and BLACKBERRY™ devices, lower wireless data subscription costs, higher wireless data throughput, and easier mobile access to data-intensive applications and rich content such as video. These trends are driving ever-increasing demands for wireless data communications.

[0003] Typically, users gain access to wireless data networks by purchasing a subscription plan from a service provider. In response to the explosive growth in mobile data traffic, service providers currently offer a wide variety of wireless subscription plan features such as actual usage plans, flat-rate plans, bandwidth caps that limit the amount of data per month for a mobile device, pre-paid and post-paid data plans. These plans typically impose limits on subscriber bandwidth consumption, often combined with additional fees for exceeding those limits. Bandwidth caps can alleviate network congestion by reducing overall mobile data traffic, but these caps reduce the attractiveness of data service for subscribers.

[0004] In a flat rate subscription plan a subscriber pays a fee for a billing cycle and is entitled to a set amount of network usage (i.e., a usage quota) during the billing cycle. For example, a subscriber may pay $30 for a month and be entitled to 500 minutes of network time. The usage quota can be specified as a time per billing cycle amount (e.g., 500 minutes per month) or as a data volume per billing cycle amount (e.g., 40 Mega Bytes per month). In some flat rate subscription plans, the usage quota is unlimited.

[0005] In an actual usage subscription plan a subscriber pays a set rate based on the actual amount of network usage during a billing cycle. For example, a user may pay $1 per minute of network usage. Actual usage plans can have incentives/penalties based on a subscriber's usage during a billing cycle. For example, in a subscription plan a subscriber may pay $1 per Mega Byte (MB) for the first 50 MBs and $2 per Mega Byte (MB) for every MB used beyond 50 MBs during the billing cycle. Subscription plans can combine aspects of flat rate plans and usage plans. For example, a subscriber may pay $30 per month for 40 MBs of wireless data usage and $1 per MB for every minute used after 40 MBs.

[0006] In the plans described above, as well as other subscriber plans, it is useful for a subscriber to be able to monitor his/her usage against one or more quotas.

[0007] Given the increasing versatility of mobile devices, it is helpful to implement a means by which these mobile devices can be used to monitor and control data communication costs, and to improve the subscriber experience.

[0008] Previous methods for network data communications cost monitoring and control are largely provider-centric, leaving the user with limited options to control and monitor costs. For example, a subscriber may be able to display cumulative consumption in MBs for the current month to determine if a monthly quota has been exceeded, but the subscriber cannot dynamically control and manage data communications costs without permanently changing his/her subscription plan. Provider-centric systems monitor usage and may allow subscribers to access usage information via a provider's web server, but they do not allow subscribers to set real time usage controls. For example, provider-centric systems do not allow subscribers to set data usage thresholds, quotas, or

caps on their devices each day based upon prior usage. Prior network data control techniques result in extra charges (i.e., due to roaming) and surprise data charges for subscribers who exceed bandwidth caps.

[0009] In prior systems, subscribers must rely on providers to monitor and control data usage. When a portable device moves to another provider network (i.e., roam), the amount of data usage information is limited to what the network the device is roaming in provides. For example, subscribers may not know what data charges (i.e., tariffs) apply while roaming. Prior techniques can result in excessive fees for subscribers who have unknowingly exceeded their plan's data quotas or caps. Subscribers cannot dynamically manage and control data costs for current data connections from their portable devices. In prior systems, subscribers only have data usage information in terms of overall volume of data used for all applications on a device, rather than the amount of data user per application. This lack of device-centric control and transparency limits the subscriber experience and causes subscribers to unnecessarily curtail their data usage.

[0010] What is therefore needed are systems and methods for providing device-based data communications cost monitoring and controls on a per application basis. What is further needed are systems and methods to allow subscribers to monitor and control expenditures on data services by providing proactive notification when subscribers are approaching bandwidth caps. What is also needed are systems and methods to allow subscribers to modify their plans either temporarily or permanently depending on their needs by providing add-on service availability (i.e., the ability to dynamically raise a bandwidth cap temporarily).

SUMMARY OF THE INVENTION

[0011] Embodiments of the present invention provide systems and methods that improve data communication usage and cost monitoring operations. An embodiment of the invention includes a system for monitoring and control of the

data usage that is based on a subscriber's device. Methods are disclosed that use a distributed system that runs on user equipment and mobile devices.

[0012] In an embodiment, a system provides subscribers with access to real-time information about data usage, and are given warnings to they are close to reaching bandwidth caps. The system notifies subscribers when they are close to reaching bandwidth caps or quotas and offers subscribers an opportunity to upgrade to a next service tier.

[0013] The invention also provides a method for managing data usage by allowing subscribers to gradually reduce download speeds, block some types of traffic, redirect device connection to on-portal applications, or select a new Quality of Service (QoS) level in order to manage bandwidth consumption. In this way, the invention makes different options available to subscribers, and lets them decide how to best-manage data usage according to their needs and priorities.

[0014] The invention additionally includes methods that use a distributed usage monitoring and control system that comprises applications that run on user devices.

[0015] Embodiments of the invention also include methods for performing cost monitoring and control on a per-application basis.

[0016] In an embodiment, the invention includes a centralized system for global monitoring and control of a plurality of mobile devices from a single, cross-provider (i.e., global) perspective.

[0017] Subscription data is used to calculate the likelihood of exceeding a quota (i.e., a quota breach) at a given time and this information is provided to a user of a mobile device. US Application No. 12/186,831, filed August 06, 2008 and entitled "Usage Measurement Collection and Analysis to Dynamically Regulate Customer Network Usage," describes methods and systems for calculating the likelihood of a quota breach. The present application includes the capabilities described therein. According to an embodiment of the present invention, a notification is sent to a subscriber when it is determined that a quota breach is likely to occur. In a related embodiment, subscribers are given the opportunity to

change a service tier associated with their subscription in order to prevent a likely quota breach.

[0018] In an embodiment, a service provider can present 'special offers' to a subscriber that provide the subscriber with an opportunity to change a service tier associated with their subscription. In further embodiments, acceptance of special offers can change service tiers associated with a subscriber's home network or roamed networks. According to embodiments of the invention, special offers can be sent to a subscriber by their home network service provider or roamed network service providers and are presented on the subscriber's mobile device.

[0019] In embodiments, both dynamic and static subscriber characteristics relative to a current usage session can be used to allow a subscriber to proactively manage data usage. Dynamic characteristics can be dynamic relative to the start of a usage session or relative to the usage session generally. An example of a dynamic characteristic relative to the start of a usage session is the type of data requested and the mobile applications requesting data. An example of a dynamic characteristic relative to the usage session is the total amount of data usage.

[0020] In a further embodiment, a subscriber characteristic used in data usage calculations includes knowledge of peak usage patterns (e.g., on peak/off-peak, weekdays).

[0021] It is an objective of the present invention that it may be incorporated into any mobile device capable of data communications.

[0022] In another embodiment, when a subscriber is roaming and the roaming traffic is not routed through the subscriber's home service provider home agent router or network access gateway, an interaction between the roamed service provider and home service provider occurs so that the home service provider has the information needed to control data usage in the roamed or visited network.

[0023] Another objective of the invention is to provide flexible policy descriptions for network service provider (carrier) charging plans. A further objective of the invention is to provide flexible tariff distribution. According to an embodiment of the invention, distribution of flexible policy descriptions associated to network service provider charging plans is achieved by using a

provider-based architecture. In an embodiment, a provider-dependent (i.e., carrier-based) architecture is also used to distribute tariffs associated with network service providers.

[0024] Further embodiments, features, and advantages of the invention, as well as the structure and operation of the various embodiments of the invention are described in detail below with reference to accompanying present drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0025] The accompanying drawings, which are incorporated herein and form a part of the specification, illustrate the present invention and, together with the description, further serve to explain the principles of the invention and to enable a person skilled in the pertinent art to make and use the invention.

[0026] FIG. 1 depicts an exemplary operating environment for providing network data communications cost monitoring and controls within a communications network, according to embodiments of the present invention.

[0027] FIG. 2 depicts an exemplary operating environment for providing data communications cost monitoring and controls in a roaming scenario including multiple communications networks, in accordance with an embodiment of the present invention.

[0028] FIG. 3 illustrates a provider independent system architecture for providing data communications cost monitoring and controls within a communications network, in accordance with an embodiment of the present invention.

[0029] FIG. 4 illustrates a provider-based system architecture for providing data communications cost monitoring and controls within a communications network, in accordance with an embodiment of the present invention.

[0030] FIG. 5 depicts an exemplary message flow diagram for a method providing data communications cost monitoring and controls when the provider-based architecture provided in FIG. 4 is used, according to an embodiment of the present invention.

[0031] FIG. 6 provides a method for monitoring and controlling data usage in accordance with the present invention.

[0032] FIGs. 7-11 depict a graphical user interface (GUI) for a mobile device to display data usage, edit usage limits, define tariffs, and accept offers to change service tiers, according to embodiments of the invention.

[0033] FIG. 12 depicts an exemplary computer system on which methods and systems herein may be implemented, according to embodiments of the present invention.

[0034] The present invention will now be described with reference to the accompanying drawings. In the drawings, like reference numbers can indicate identical or functionally similar elements. Additionally, the left-most digit(s) of a reference number may identify the drawing in which the reference number first appears.

DETAILED DESCRIPTION OF THE INVENTION

Mobile Environment

[0035] FIG. 1 provides an exemplary operating environment 100 for providing an adaptive window size for network data communications cost monitoring and controls, according to embodiments of the present invention. Operating environment 100 includes user equipment 102, network access gateway 120, optional service controller 130, policy controller 140, subscriber data repository 150, usage policy server 160, and application server farm 170. Operating environment 100 provides a simplified diagram of a communications network to illustrate the concepts of data communications cost monitoring and controls. As would be recognized by persons of skill in the art, embodiments of the present invention can be used in any type of communications network (e.g., wireline, wireless, or hybrid networks).

[0036] User equipment 102 is any device that provides a user access to one or more networks. User equipment 102 can include, but is not limited to, a

computer such as user equipment 102a, a personal digital assistant (PDA) such as user equipment 102b, a wireless phone such as user equipment 102c, a smart phone, other wireless mobile devices, and/or wired communications devices.

[0037] Access network 110 is a communications network that couples user equipment 102 to a packet data network (not shown). Access network 110 may be a third generation partnership project (3GPP) access network or a non-3GPP access network. Exemplary 3GPP access networks include the UMTS terrestrial radio access network (UTRAN) and the GSM EDGE radio access network (RAN). Other access networks include, but are not limited to, WiFi, WiMAX, CDMA2000, GSM, and UMTS.

[0038] Network access gateway 120 provides an interface between access network 110 and a packet data network (not shown). In a 3GPP network, network access gateway 120 may be the Gateway General Packet Radio Service (GPRS) Support Node (GGSN). Note that network access gateway 120 may also act as a policy enforcement point.

[0039] Policy controller 140, at a high level, includes subscriber profiles and network policies needed to manage network resources, such as bandwidth, according to a subscriber, session, and/or application. A service provider may apply a policy based on business rules associated with a variety of factors (e.g., service tiers and/or dynamic parameters such as time of day).

[0040] Policy controller 140 includes a policy and charging rules function (PCRF) 142 and a quota manager 144. For example, in a 3GPP network, PCRF 142 acts as a decision point for policy and charging control of service data flows. PCRF 142 is configured to select and provide the applicable policy and charging control decisions to the policy control enforcement point.

[0041] Usage policy server 160 works in conjunction with policy controller 140 to extend policy and charging control of service data flows to user equipment 102. These data flows may be monitored and controlled on a per subscriber, per user equipment, or per application basis. For example, control and metering of data flows from applications hosted in application server farm 170 to user equipment 102a may be performed by usage policy server 160. Alternatively,

control and metering of data flows for a particular subscriber using user equipment 102a may be performed by usage policy server without regard to the applications being invoked by the subscriber. Similarly, control and metering of data flows between a pool of related subscribers (i.e., subscribers in the same family, organization, or corporation) using user equipment 102a-c may be performed by usage policy sever 160, regardless of the applications involved in the data flows. Although the exemplary environment 200 depicts usage policy server 160 as a separate server from policy controller 140, as would be understood by those skilled in the relevant art(s) usage policy server 160 may be implemented as software residing in policy controller 140. Conversely, policy controller 140 may comprise software residing on usage policy server 160

[0042] According to an embodiment of the invention, a subscriber using user equipment 102 can set usage limits in mobile usage policy application 104 running on user equipment 102. For example, a subscriber using user equipment 102a can use mobile policy application 104a to set total daily usage limits in Mega Bytes (MBs), which are communicated to usage policy server 160 via access network 110, network access gateway 120, and policy controller 140. Subscribers can also set data usage notification and stop thresholds in mobile usage policy application 104. Upon reaching a notification threshold (i.e., 400 MBs in the example embodiment depicted in FIG. 7), a subscriber will receive a notification on user equipment 102. At that point, the subscriber can optionally can set a new, higher usage limit in mobile usage policy application 104, or choose to curtail data usage. Upon reaching a stop threshold (i.e., 600 MBs in the example embodiment depicted in FIG. 7), a subscriber will be unable to use additional data services on user equipment 102 until a higher usage limit is set in mobile usage policy application 104 or server-side usage policy application 164.

[0043] Usage policy server 160 provides usage policy data to policy controller 140. Quota manager 144 is configured to collect data communications usage and cost data. Quota manager 144 provides data communications cost monitoring and data to user equipment 102a-c via network access gateway 120 and access network 110. If the subscriber exceeds a data usage cap or threshold, quota

manager 144 provides this information to user equipment 102a-c and usage policy server 160. In an embodiment, server-side usage policy application 164 running on usage policy server 160 allows subscribers to set data usage controls via a web portal (See FIGs. 2 and 3). Data usage controls include, but are not limited to, total daily usage thresholds, total hourly usage thresholds, per-application usage thresholds, per-device usage thresholds, and thresholds based on data sources (i.e., Uniform Resource Locator/URL addresses or Internet Protocol/IP addresses). In an alternative embodiment, a mobile usage policy application 104 running on user equipment 102 allows subscribers using user equipment 102 to set data usage controls, such as, but not limited to the thresholds mentioned above directly on user equipment 102.

[0044] Quota manager 144 is configured to set adaptive fair usage windows according to a variety of techniques including, but not limited to, using pre-defined value or values, calculating windows based on one or more formulas, and/or determining window based on how quickly previous windows were violated. These techniques are described in further detail in US Application No. 61/153,910, filed February 19, 2009, and entitled "Adaptive Window Size for Network Fair Usage Controls." The capabilities described therein are included in the current application.

[0045] Policy controller 140 is coupled to subscriber data repository 150. Subscriber data repository 150 includes a subscriber profile database 152, a subscriber state database 154, and a subscriber usage database 156. Although depicted as three separate databases in FIG. 1, a person of ordinary skill in the art will recognize that subscriber profile, subscriber state, and subscriber usage data may be stored in any number of databases.

[0046] Policy controller 140 is further coupled to network access gateway 120. In an embodiment, the interface between policy controller 140 and network access gateway 120 is a Gy interface.

[0047] Subscriber state database 154 includes information that identifies and defines a subscriber's network session. Subscriber state information includes the subscriber identifier for the session. In embodiments of the invention, subscriber

identifiers may be one or more of a Mobile Subscriber ISDN Number (MSISDN), a Mobile Identification Number (MIN), a Private Identifier, information about the network such as the IP address the subscriber is currently using and what network or networks to which the subscriber is currently connected, device information such as the device being used and the version of the software, location and roaming information, and other unique state information.

[0048] When a subscriber connects to any network, the core elements of the network assign an Internet Protocol (IP) address to the subscriber. At that time, the subscriber session begins and subscriber state information is created, derived and captured. For example, state information is typically generated either through RADIUS accounting or through interactions with the dynamic host control protocol (DHCP) service on a network. The accounting message feeds are generated to a Remote Authentication Dial In User Service (RADIUS) engine or an authentication, authorization and accounting (AAA) service from core network elements.

[0049] Subscriber profile database 152 includes static information about the subscriber. This information may include the service tier (e.g., gold, silver, bronze) assigned to the subscriber. In an embodiment of the invention, service tiers are associated with Quality of Service (QoS) levels.

[0050] Subscriber usage database 156 includes static and dynamic information related to the subscriber's history. The subscriber's history includes, but is not limited to the subscriber's data usage history. In embodiments of the present invention, subscriber usage database 156 may store information about the amount of data used on a per-application basis by the subscriber's user equipment 102 in previous sessions. Usage policy server 160 uses the per-application usage data from prior sessions to inform the subscriber about which applications running on user equipment 102 have consumed the most bandwidth or data based on previous behavior patterns.

[0051] According to an embodiment of the invention, a carrier or provider-based infrastructure is used wherein the service provider infrastructure provides data metering and control. In this architecture, usage policy server and server-side

usage policy application 164 are used to control and meter data usage on user equipment 102.

[0052] In another embodiment, a carrier-independent is used whereby metering and control is performed on user equipment 102 using mobile usage policy application 104. In this embodiment, some centralized functions are performed by policy controller 140 and usage policy server 160, such as controlling data usage policies across multiple user equipment 102a-c. In this embodiment, longer-term historical storage of usage information occurs in subscriber usage database 156 within subscriber data repository 150.

[0053] In an embodiment, a hybrid architecture gathers usage data on user equipment 102 but long-term storage of the usage data occurs in subscriber usage database 156 within subscriber data repository 150. In this way, centralization is performed within a service provider infrastructure. This architecture is useful for the roaming scenario depicted in FIG. 2 and described below.

[0054] FIG. 2 depicts an exemplary operating environment 200 for providing data communications cost monitoring and controls while roaming. Although the exemplary environment 200 depicts two network service providers, home network service provider 220 and roamed network service provider 230, as would be understood by those skilled in the relevant art(s), user equipment 102 may connect to a plurality of roamed network service providers 230 while roaming.

[0055] FIG. 2 is described with continued reference to the operating environment of FIG. 1. However, environment 200 is not limited to that embodiment.

[0056] Mobile data costs for a subscriber using user equipment 102 may be based on data volume used within a period. For example, a subscriber's subscription may entail a charge of $60 up to a 1Giga Byte (GB) cap of data access each month with a $3 per MB charge after the 1GB cap has been exceeded. Data costs also vary based on the home network service provider 220 that user equipment 102 is homed in or connected to. Typically, data costs increase when user equipment 102 is roaming in roamed network service provider 230. Due to these and other dynamic factors that can increase data costs, embodiments of the

present invention enable subscribers to monitor and control expenditure on data services on user equipment 102 on a real time basis.

[0057] In accordance with a 'provider-centric' embodiment of the invention, monitoring and control of usage and charging for data is performed by methods and systems that reside within home network service provider 220 and remain under the control of home network service provider 220. In the provider-centric embodiment, home network access gateway 120 and roamed network access gateway 236 monitor and control packet traffic between user equipment 102 and the Internet 210. Home network access gateway 120 and roamed network access gateway 236 generate usage accounting records that are input to off-line or on-line (prepaid) billing and reporting systems residing in base station subsystems 224 and 234. Examples of home network access gateway 120 and roamed network access gateway 236 include, but are not limited to gateway GPRS Support Node (GGSN), Packet Data Serving Node (PDSN), Deep Packet Inspection (DPI), and "Evolved NodeB (eNodeB).

[0058] Home network service provider 220 and roamed network service provider 230 may provide visibility of data usage records via a website user interface to subscribers that log in to check their account via web portals 222 and 232.

[0059] According to an embodiment, subscribers can monitor and control their data usage via web portals 222 and 232. For example, subscribers can select service extensions, data usage boosts, a lower bandwidth service, or other alternatives via home network web portal 222 and/or roamed network web portal 232. These changes are then passed to usage policy server 160 and propagated to server-side usage policy application 164. In an alternative embodiment, changes made via home network web portal 222 and roamed network web portal 232 are propagated to mobile usage policy application 104 resident on user equipment 102.

[0060] In another embodiment, when a subscriber is roaming and the roaming traffic is not routed through the subscriber's home service network provider 220 home agent or home network access gateway 120, an interaction between a usage policy server 160 in roamed network service provider 230 and a usage policy

server 160 in home network service provider 220 is initiated. This interaction between the respective usage policy servers includes a request being sent from usage policy server 160 in home network service provider 220 to a usage policy server 160 in roamed network service provider 230. According to an embodiment, the request is for information that home network service provider 220 needs in order to affect data usage controls for user equipment 102 while it is accessing data in roamed network service provider 230.

[0061] In an embodiment, to prevent unexpectedly high roaming charges from roamed network service provider 230, a subscriber using user equipment 102 may select, using usage policy application 104 to be barred from all or some data applications while roaming in the network of roamed network service provider 230. For instance, a subscriber using a mobile device such as user equipment 102 may wish to avoid the high cost of data services while they are outside the coverage area of home network service provider 220, but retain the data service when they are not roaming.

[0062] According to an embodiment, while user equipment 102 is using roamed network service provider 230, a subscriber may opt to have certain applications from application server farm 170 blocked.

[0063] Operators of home network service provider 220 and roamed network service provider 230 can detect access to on- or off-portal applications, and they typically choose to charge less, or impose no data fees, for access to on-portal applications from user equipment 102. In an embodiment, a subscriber may choose to select only on-portal applications (either in home network service provider 220 or roamed network service provider 230) in order to reduce data usage and costs.

[0064] In instances when access network 110 depicted in FIG. 1 becomes congested, an embodiment of the invention provides real-time traffic information from access network 110 and, more specifically, from individual base station subsystems 224 and 234 which enables operators of home network service provider 220 or roamed network service provider 230 to identify areas of congestion within their respective access networks 110. Policy controller 140

includes operator tools to contain congestion in real-time by temporarily enforcing more stringent policies (i.e., not allowing bursting behavior, or assigning lower priority to subscribers with low-tier service plans).

[0065] In an embodiment, in order to prevent 'bill shock' due to exceeding data quotas and in order to extend usage control to subscribers, mobile usage policy application 104 works in conjunction with policy controller 140 to provide proactive notifications to user equipment 102 when subscribers are nearing bandwidth usage thresholds or data roaming charge limits in roamed network service provider 230. Subscribers can then be given choices in real-time in mobile usage policy application 104, such as a service extension, a data usage boost, a lower bandwidth service, or other alternatives. In addition, operators of home network service provider 220 or roamed network service provider 230 can extend control to subscribers to set personalized usage caps that can be updated in real-time based on personal financial limits, or to boost roaming data usage while a subscriber is traveling.

Data Monitoring and Control Systems

[0066] FIG. 3 illustrates an architecture for a system 300 for providing data communications cost monitoring and controls within a communications network, in accordance with an embodiment of the present invention. System 300 is provider independent in that the architecture is distributed between user equipment 102 and a usage policy server 160.

[0067] FIG. 3 is described with continued reference to the operating environments of FIGs. 1 and 2. However, system 300 is not limited to those embodiments.

[0068] In an embodiment, monitoring and control of the data usage is based on user equipment 102 using mobile usage policy application 104, instead of within the infrastructure of home network service provider 220 or roamed network service providers 230. This distributed system runs on user equipment 102 and usage policy server 160. In system 300, the charging/cost monitoring and control

can be performed down to the level of the individual applications 306 running on user equipment 102. Applications 306 may include, but are not limited to games, social networking applications, Voice over Internet Protocol (VOIP) applications such as Skype, and wireless access to data-intensive web sites that host multimedia content such as video.

[0069] According to an embodiment, a device usage control subsystem (executes on user equipment 102 and monitors data flows (denoted as 1-4) on user equipment 102. The device usage control subsystem comprises the following components: local store 308, application controller 310, and mobile usage policy application 104. These components are described in the following paragraphs.

[0070] Application controller 310 is installed to mediate between applications 306 and communication stack 312 of user equipment 102. In an embodiment, communication stack 312 is a Transmission Control Protocol (TCP)/Internet Protocol (TCP/IP) stack. Application controller 310 presents a virtual socket layer to applications 306. Application controller 310 also counts how many bytes each application 306 sends and receives (denoted as data flow 1). Application controller 310 also stores the data usage on a per-application basis in local store 308 (denoted as data flow 4). Application controller 310 checks for application data usage threshold limits defined in the local store by the mobile usage policy application 104. In an alternative embodiment, application controller 310 checks for application data usage threshold limits defined in the global store 368 by the server-side usage policy application 164, which can be accessed via calls to Application Programming Interface (API) 366.

[0071] In an embodiment, data usage information for a single device is stored in a data store, such as local store 308 on user equipment 102. 2. Local store 308 may use non-volatile storage on user equipment 102 to hold information such as, but not limited to, data usage for each application 306, data budgets, thresholds, tariff information, and statistics regarding highest budget applications 306. Each of these types of information is described below.

[0072] Each of the types of information described below may optionally be stored in local store 308 on user equipment 102. The information described

below may also be periodically imported from or exported information to global store 368 residing on one or more usage policy servers 160.

[0073] Data 'budgets' for applications 306 or groups of applications 306 can be set in mobile usage policy application 104 or server-side usage policy application 164. In an embodiment, after reaching its budgeted allocation for a given period, an application 306 is capped or blocked from further data network usage. According to this embodiment until that period is elapsed (or the budget is changed or over-ridden by a subscriber), application 306 will be blocked from performing additional data transactions, thereby allowing the subscriber to control data costs that may otherwise cause 'bill shock.'

[0074] Thresholds for applications 306 are kept, whereby the subscriber is notified that an application 306 or group of applications 306, if a subscriber has set a threshold of 75% for an application 306, when that application 306 has consumed 75% of its data budget, the subscriber will receive a notification at user equipment 102.

[0075] Tariffs comprise information kept for each known potential roamed network service provider 230 in which the subscriber can roam, so that the user has control over which roamed network service provider 230 would be most cost-effective to use. Tariff information pertaining to a plurality of roamed network service providers 230 may be stored in a local store 308 on user equipment 102. Tariff data for each roamed network service provider 230 may reside in a database or data store on usage policy server 160, such as global store 368.

[0076] According to an embodiment, local store 308 may periodically import or export tariff information via data flows 5 and 6, respectively, to global store 368 residing on one or more usage policy servers 160 associated with one or more roamed network service providers 230. Tariff information stored in global store 368 and a plurality of local stores 308 can be used to provide flexible tariff distribution. In an embodiment of the invention, a carrier-based architecture is used to distribute tariffs stored in global store 368 and local stores 308.

[0077] Statistics regarding highest budget applications 306 include cumulative data usage information kept in order to meter and display subscribers, user

equipment 102, and/or applications 306 using highest budgeted amount of data for a give period. For example, statistics may be kept on a single user equipment 102 regarding applications 306 on a particular user equipment 102 which have used the largest amount of data. Statistics may also be compiled on usage policy server 160 regarding data usage for a plurality of subscribers and/or user equipment 102.

[0078] In accordance with an embodiment of the invention, data usage pertaining to a plurality of subscribers is stored in a data store on usage policy server 160, such as global store 368. According to an embodiment, local store 308 may periodically import or export information via data flows 5 and 6, respectively, to global store 368 residing on one or more usage policy servers 160 associated with one or more network service providers.

[0079] According to an embodiment, the types of data described in the following paragraphs are modeled by usage policy application 104 and stored in a local store such as local store 308.

[0080] Usage entity data, including, but not limited to data identifying a network service provider such as home network service provider 220, network type (WiFi, 3G, etc.), user equipment 102 device type, device group, subscriber or user, user group, application 306, and groups of applications 306 may be stored in local store 308.

[0081] Quota information, such as a quota expressed in MBs or GBs and cost for additional quota levels, may be modeled by usage policy application 104 and stored in a local store such as local store 308. Quotas may be modeled and stored on the network service provider level, subscriber level, subscriber group level, for each application 306, and for groups of applications 306.

[0082] Threshold information such as the percentage of a quota reached in a period (i.e., monthly, weekly, and/or daily) may also be stored in local store 308. Thresholds may be modeled and stored on the network service provider level, subscriber level, subscriber group level, for each application 306, and for groups of applications 306.

[0083] Information regarding data costs incurred may also be modeled by usage policy application 104 and stored in a local store such as local store 308. Data costs may be modeled and stored on the network service provider level, subscriber level, subscriber group level, for each application 306, and for groups of applications 306.

[0084] Usage intervals may be stored be stored in local store 308 on a daily, weekly, and monthly basis. Usage intervals pertaining to a plurality of subscribers and user equipment 102 may also be stored in global store 368.

[0085] Tariff information for a plurality of networks regarding data prices (i.e., expressed as cost per Byte, MB, or GB) may also be stored in a local store such as local store 308. Tariff information is collected and stored on a network level.

Mobile Usage Policy Application

[0086] With continued reference to FIG. 3, in an embodiment, mobile usage policy application 104 provides the functionality described in the following paragraphs.

[0087] Mobile usage policy application 104 provides a user interface for monitoring and control (denoted as data flow 3). An exemplary user interface is provided in FIGs. 7-11, which are described in detail below.

[0088] Mobile usage policy application 104 also defines the data and policies that application controller 310 and local store 308 require (denoted as data flow 2 in FIG. 3).

[0089] The following are the types of data usage policies defined by mobile usage policy application 104 for application controller 310 on user equipment 102.

[0090] Mobile usage policy application 104 can set data usage quotas, thresholds (including alert and stop thresholds), allowable maximum tariffs (i.e., tariff limits expressed in terms of maximum acceptable costs per Byte, MB, or GB), allowable network service providers (i.e., allowed roamed network service providers 230 for a given subscriber, user equipment 102 and/or application 306),

and allowable network tariff minimums. For example, mobile usage policy application 104 may only allow a given subscriber, user equipment 102, or application 306 to access a roamed network service provider 230 tariff less than a certain currency amount per storage unit (i.e., US dollars per MB or GB).

Usage Policy Server and Server Side Usage Policy Application

[0091] In an embodiment, usage policy server 160 hosts server side usage policy application 164, global store 368, a Global Policy Controller, and web portal 222.

[0092] Global store 368 optionally collects data usage information from local stores 308 from a plurality of user equipment 102. In an embodiment, global store 368 comprises a database that provides rolled up, or per user equipment 102, per-subscriber, per-application 306 breakdowns, or views of usage data within various contexts. These contexts may include, but are not limited to, corporations, organizations (i.e., departments), and a subscriber. The level of granularity of data stored in global store 368 allows subscribers and network administrators to run data queries and generate reports regarding data usage for a single subscriber, single user equipment 102, groups of subscribers, and related sets of user equipment 102 (i.e., user equipment leased by an organization or corporations) for a given period. In an embodiment, these queries and reports can be accessed via web portal 222.

[0093] Global store 368 on usage policy server 160 optionally stores and distributes the per user equipment 102 information. In this way, usage policy server 160 can be used to provide centralized provisioning of user equipment 102.

[0094] Global policy controller 370 is an application on usage policy server 160 that enables access to global store 368 and drives global store 368 to collect information from a plurality of user equipment 102 (denoted as data flow 5). Global policy controller 370 also drives global store 368 to provision information to a plurality of user equipment 102 (denoted as data flow 5).

Provider Based System

[0095] FIG. 4 illustrates an architecture for a provider-based system 400 for providing data communications cost monitoring and controls within a communications network, in accordance with an embodiment of the present invention.

[0096] FIG. 4 is described with continued reference to FIGs. 1-3. However, system 400 is not limited to those embodiments.

[0097] In the embodiment of system 400, the infrastructure of a network service provider provides data usage metering and control. Usage policy server 160 provides interface 404 to subscribers using user equipment 102 to allow subscribers to monitor and control charging for data usage.

[0098] In an embodiment the data usage metering and control is web based and accessed via web portal 222. Alternatively, data usage metering and control is device application based using interface 404 invoked locally on user equipment 102. Interface 404 allows the device to register with usage policy server 160 (denoted as data flow 1). After registration, user equipment 102 is synchronized with usage policy server 160 and local store 308 is updated (denoted as data flow 2).

[0099] Usage policy server 160 also allows subscribers and network administrators to access web interface via web portal 222 to fetch values for data usage attributes (denoted as data flow 3) such as, but not limited to thresholds and quotas on a per application 306, home network service provider 220, roamed network service provider 230, or subscriber basis.

[0100] Usage policy server 160 also stores usage data for all registered user equipment 102 in subscriber usage database 156 for a given period (e.g., 2 months).

[0101] Usage policy server 160 then registers with online and offline charging systems such as policy and charging rules function (PCRF) 142. In embodiments, the charging systems may include AAA and other protocols, capable of receiving data usage information for user equipment 102.

[0102] According to an embodiment, PCRF 142 receives a bulk registration request from usage policy server 160 (denoted as data flow 4). The bulk registration request comprises data usage information for a plurality of user equipment 102 that has registered with usage policy server 160. The data usage information contains threshold and stoppage policies based on criteria such as data volume and the characteristics of roamed network service provider 230.

[0103] System 400 can be used to provide flexible policy descriptions for a network service provider's charging plan. For example, a network service provider can furnish its policy and charging rules from PCRF 142 via usage policy server 160. The provider-based architecture illustrated in FIG. 4 enables distribution of flexible policy descriptions corresponding to network service provider charging plans via data flows between PCRF 142 and usage policy server 160.

[0104] System 400 and the provider-based architecture depicted in FIG. 4 can also be used to provide flexible tariff distribution. Tariffs comprise information kept for each known potential roamed network service provider 230 in which a subscriber can roam. Access to this information on user equipment 102 is useful when a subscriber wants to determine which potential roamed network service provider 230 will be most cost-effective to use. Tariff information pertaining to a plurality of roamed network service providers 230 may reside in a database or data store on usage policy server 160 to be distributed to a plurality of user equipment 102.

[0105] PCRF 142 accesses usage information forwarded by one or more network access gateways 120. In an embodiment, this usage information is received by network access gateway 120 via a radio access network (RAN) 406. PCRF 142 sends usage stream information comprising current data usage information for user equipment 102 to usage policy server 160 (denoted as data flow 5).

[0106] Usage policy server 160 requests that PCRF 142 control usage (i.e., affect bearer channel) for user equipment 102 once a stoppage decision is made by PCRF 142 (denoted as data flow 6).

Data Monitoring and Control Methods

[0107] FIG. 5 depicts an exemplary message flow diagram for a method 500 for providing data communications cost monitoring and controls when the provider-based architecture provided in FIG. 4 is used, according to an embodiment of the present invention. FIG. 5 is described with continued reference to FIG. 4. However, method 500 is not limited to that embodiment.

[0108] In step 505, a subscriber, using interface 404 on user equipment 102 enters data needed to make an initial request to register user equipment 102. In another embodiment, this step is performed by a subscriber accessing a web based user interface via web portal 222 on usage policy server 160.

[0109] In step 510, the user equipment 102 device registration request is sent to usage policy server 160.

[0110] In step 520, data from subscriber usage database 156 is sent from usage policy server 160 to user equipment 102 in order to synchronize. In this step, user equipment 102 is synchronized with usage policy server 160 and local store 308 is updated.

[0111] In step 530, a request to fetch values for data usage attributes is sent from user equipment 102 to usage policy server 160. Attribute/value pairs fetched in this step may include application, subscriber, and/or network-based thresholds and quotas.

[0112] In step 540, a bulk registration request is sent from usage policy server 160 to PCRF 142. In this step, a bulk registration request from usage policy server 160 comprising data usage information for a plurality of user equipment 102 that has registered with usage policy server 160 is forwarded to PCRF 142. In an embodiment, the data usage information contains threshold and stoppage policies based on criteria such as data volume and the characteristics of a home network service provider 220 or a roamed network service provider 230.

[0113] In step 545, PCRF 142 sends usage stream information comprising current data usage information for user equipment 102 to usage policy server 160.

[0114] In step 550, usage policy server 160 sends a request to PCRF 142. In this step, a request to control data usage for user equipment 102 is sent based upon a stoppage decision made by PCRF 142.

[0115] FIG. 6 depicts a flowchart 600 of an exemplary method for monitoring and controlling data usage, according to embodiments of the present invention.

[0116] FIG. 6 is described with continued reference to FIGs. 1-5. However, flowchart 600 is not limited to those embodiments.

[0117] In step 610, a user equipment 102 device registration request is sent to a usage policy server 160. In an embodiment this step is performed using interface 404 on user equipment 102. In another embodiment, this step is performed by a subscriber accessing a web based user interface via web portal 222 on usage policy server 160.

[0118] In step 620, user equipment 102 is synchronized and updated using data from subscriber usage database 156 sent from usage policy server 160. In this step, local store 308 is updated.

[0119] In step 630, values for data usage thresholds and attributes are requested from user equipment 102. In an embodiment, thresholds and attribute/value pairs are tunable or editable on user equipment using interface 404. Attribute/value pairs may include application, subscriber, and/or network-based thresholds and quotas. Thresholds may include percentage usage levels beyond which a notification is to be sent to a subscriber using user equipment 102.

[0120] In step 640, bulk registration is performed. The bulk registration includes collecting data usage information for a plurality of user equipment 102 that has registered with a usage policy server 160. The data usage information comprises threshold and stoppage policies based on criteria such as data volume and the characteristics of network service providers.

[0121] In step 650, the usage stream for a subscriber is updated. In this step, usage stream information comprising current data usage information for user equipment 102 may be sent to a usage policy server 160.

[0122] In step 660, a determination whether an attribute value obtained in step 630 has been exceeded. In this step, a determination is made whether any

attribute value has been exceeded, such as a daily MB cap, a cap by an application 306 running on user equipment 102, a cap for user equipment 102, and/or an overall data cap for a subscriber

[0123] If an attribute has not been exceeded, operation proceeds to step 665. If threshold has been exceeded, operation proceeds to step 670.

[0124] In step 665, a determination whether a threshold value obtained in step 630 has been exceeded. In this step, a determination is made whether any threshold has been exceeded, such as a percentage threshold regarding daily usage in MBs, has been reached.

[0125] If a threshold has been exceeded, operation proceeds to step 670. If threshold has not been exceeded, operation proceeds to step 680.

[0126] In step 670, a notification is sent to subscriber. In this step, a notification may comprise a prompt in interface 404, an email message, a Short Messaging Service (SMS) message, a subscriber notification posted via web portal 222, or any other notification capable of notifying a subscriber that a threshold has been exceeded.

[0127] In step 675, after the notification sent in step 670 has been received by a subscriber, a determination is made whether a service characteristic has been changed. In this step, a subscriber, in response to the notification sent in step 670, can optionally change a service tier associated with their subscription in order to alleviate either an exceeded threshold determined in step 665 or an exceeded attribute determined in step 660. In this step, an upgrade to a next service tier can be made when a subscriber is close to reaching bandwidth caps or thresholds.

[0128] If a service characteristic is modified, operation proceeds to step 680. If a service characteristics are unchanged, operation proceeds to step 685.

[0129] In step 680, current total data usage is determined for user equipment 102. In this step, data usage for applications 306 running on user equipment 102 may also be determined. After collection and calculation of data usage information is performed in this step, control is passed back to step 650.

[0130] In step 680, data usage is controlled on user equipment 102 after a subscriber opted to not modify service characteristics in step 675 and the method ends.

Example Graphical User Interfaces

[0131] FIGs. 7-11 depict a graphical user interface (GUI) for a mobile device to display data usage, edit usage limits, define tariffs, and accept special offers to change service tiers, according to embodiments of the invention.

[0132] In an embodiment of the present invention, mobile usage policy application 104 may include the exemplary interface illustrated in FIGs. 7-11. FIGs. 7-11 are described with continued reference to the embodiments illustrated in FIGs. 1-4. However, FIGs. 7-11 are not limited to those embodiments. Throughout FIGs. 7-11, displays are shown with various hyperlinks, command regions, 'turn wheels', buttons, 'slide bars', and data entry fields, which are used to initiate action, invoke routines, enter data, view data, or invoke other functionality. For brevity, only the differences occurring within the figures, as compared to previous or subsequent ones of the figures, are described below.

[0133] FIG. 7 illustrates a data usage interface 700 that allows a subscriber to view home data used 702 in home network service provider 220 as compared roamed data used 704 while roaming in roamed network service provider 230 for a given period. In the exemplary embodiment illustrated in FIG. 7, the period is 1 month (e.g., April), but as would as would be understood by those skilled in the relevant art(s) interface 700 could display other data usage periods (i.e., hourly, daily, weekly, etc). In an embodiment, interface 404 comprises interface 700.

[0134] A subscriber can set "Notify" and "Stop" limits by selecting, using input device 710, limits button 706. Similarly, a subscriber can display and set tariffs by selecting, using input device 710, tariffs button 708. Interface 700 also displays total data usage 712.

[0135] FIG. 8 illustrates a usage limits interface 800 that allows a subscriber to set data usage limits in home network service provider 220 and in roamed

network service providers 230. According to an embodiment of the invention, interface 404 comprises interface 800. A subscriber, using input device 710 or a touch screen interface within interface 800 can change usage limits 802 for one or more network service providers. In an embodiment, usage limits 802 are changeable by scrolling through different values by using 'turn wheels' within interface 800. After one or more usage limits 802 have been changed, new usage limits 802 may be saved when a subscriber, using input device 710 or a touch screen interface within interface 800 selects save button 804. Current, updated usage data is displayed when a subscriber, using input device 710 or a touch screen interface within interface 800, selects usage button 806.

[0136] FIG. 9 illustrates a tariffs interface 900 that allows a subscriber to display and define tariffs 902 for home network service provider 220 and for roamed network service providers 230. In embodiment of the invention, interface 404 comprises interface 900. In an embodiment, some pre-set tariffs 902 are provided by the network service providers and other tariffs 902 are editable by the subscriber in interface 900 in cases where the subscriber knows the tariff 902 and a network service providers cannot know the tariff.

[0137] FIG. 10 illustrates an interface 1000 for displaying data usage. Interface 1000 is an alternative embodiment of interface 700 depicted in FIG. 7. A subscriber, using slide bars 1006, can set "Notify" and "Stop" limits. According to an embodiment, a subscriber can display special offers by selecting, using input device 710, special offers button 1008. An exemplary interface for displaying and selecting special offers is described below with reference to FIG. 11.

[0138] FIG. 11 illustrates an interface 1100 for displaying special offers presented to a subscriber by a home network service provider 220 and/or roamed network service providers 230. In an embodiment, some special offers 1102 are provided by the home network service provider 220 and other special offers 1102 are offered by roamed network service providers 230. In the exemplary embodiment depicted in FIG. 11, special offers 1102 can include offers to increase the number of Short Messaging Service (SMS) text messages the

subscriber can send and receive, a 'DayPass' on a roamed network, and a 'TopUp and Go' offer to provide a certain amount of additional data usage and/or calling minutes. In an embodiment, special offers 1102 may be offered to a user for free or may be offered for sale to the subscriber. In an embodiment, a subscriber can select special offers by selecting, using input device 710, links displayed with special offers 1102. Interface 1100 also displays total data usage 712.

Example Computer System Implementation

[0139] In an embodiment of the present invention, the methods and systems of the present invention described herein are implemented using well-known computers, such as a computer 1200 shown in FIG. 12. The computer 1200 can be any commercially available and well-known computer capable of performing the functions described herein, such as computers available from International Business Machines, Apple, Sun, HP, Dell, Cray, etc.

[0140] Computer 1200 includes one or more processors (also called central processing units, or CPUs), such as processor 1210. Processor 1210 is connected to communication bus 1220. Computer 1200 also includes a main or primary memory 1230, preferably random access memory (RAM). Primary memory 1230 has stored therein control logic (computer software), and data.

[0141] Computer 1200 may also include one or more secondary storage devices 1240. Secondary storage devices 1240 include, for example, hard disk drive 1250 and/or removable storage device or drive 1260. Removable storage drive 1260 represents a floppy disk drive, a magnetic tape drive, a compact disk drive, an optical storage device, tape backup, ZIP drive, JAZZ drive, etc.

[0142] Removable storage drive 1260 interacts with removable storage unit 1270. As will be appreciated, removable storage drive 1260 includes a computer usable or readable storage medium having stored therein computer software (control logic) and/or data. Removable storage drive 1260 reads from and/or writes to the removable storage unit 1270 in a well-known manner.

[0143] Removable storage unit 1270, also called a program storage device or a computer program product, represents a floppy disk, magnetic tape, compact disk, optical storage disk, ZIP disk, JAZZ disk/tape, or any other computer data storage device. Program storage devices or computer program products also include any device in which computer programs can be stored, such as hard drives, ROM or memory cards, etc.

[0144] In an embodiment, the present invention is directed to computer program products or program storage devices having software that enables computer 1200, or multiple computer 1200s to perform any combination of the functions described herein

[0145] Computer programs (also called computer control logic) are stored in main memory 1230 and/or the secondary storage devices 1240. Such computer programs, when executed, direct computer 1200 to perform the functions of the present invention as discussed herein. In particular, the computer programs, when executed, enable processor 1210 to perform the functions of the present invention. Accordingly, such computer programs represent controllers of the computer 1200.

[0146] Computer 1200 also includes input/output/display devices 1280, such as monitors, keyboards, pointing devices, etc.

[0147] Computer 1200 further includes a communication or network interface 1290. Network interface 1290 enables computer 1200 to communicate with remote devices. For example, network interface 1290 allows computer 1200 to communicate over communication networks, such as LANs, WANs, the Internet, etc. Network interface 1290 may interface with remote sites or networks via wired or wireless connections. Computer 1200 receives data and/or computer programs via network interface 1290. The electrical/magnetic signals having contained therein data and/or computer programs received or transmitted by the computer 1200 via network interface 1290 also represent computer program product(s).

[0148] The invention can work with software, hardware, and operating system implementations other than those described herein. Any software, hardware, and

operating system implementations suitable for performing the functions described herein can be used.

Conclusion

[0149] While various embodiments of the present invention have been described above, it should be understood that they have been presented by way of example only, and not limitation. It will be understood by those skilled in the relevant art(s) that various changes in form and details may be made therein without departing from the spirit and scope of the invention as defined in the appended claims. It should be understood that the invention is not limited to these examples. The invention is applicable to any elements operating as described herein. Accordingly, the breadth and scope of the present invention should not be limited by any of the above-described exemplary embodiments, but should be defined only in accordance with the following claims and their equivalents.

WHAT IS CLAIMED IS:

1. A method for providing data communications cost monitoring and control for a subscriber session, comprising:

receiving, at a usage policy server, a registration request associated with the subscriber session;

determining current data usage associated with the subscriber session;

receiving, at the usage policy server, one or more data usage thresholds and one or more quotas associated with the subscriber session;

collecting, at the usage policy server, data usage information associated with the subscriber session;

sending a notification to a subscriber when the subscriber exceeds a pre-determined quota during the subscriber session; and

controlling data usage for the subscriber session when the subscriber exceeds a pre-determined quota during the subscriber session

2. The method of claim 1, wherein the notification is one or more of an email message, a Short Messaging Service (SMS) message, and a prompt in a user interface.

3. The method of claim 1, wherein determining current data usage comprises:

retrieving subscriber profile data from a subscriber data repository; and

determining the whether a quota has been exceeded based on a service tier associated with the subscriber.

4. The method of claim 1, further comprising:

sending a notification to the subscriber when a pre-determined threshold is exceeded during the subscriber session.

5. The method of claim 4, wherein the notification is one or more of an email message, a Short Messaging Service (SMS) message, and a prompt in a user interface.

6. The method of claim 1, further comprising:

storing data usage information in a subscriber data repository.

7. The method of claim 1, further comprising:

receiving, at the usage policy server, a request to change a service tier associated with the subscriber session; and

updating a subscriber profile based upon a requested service tier change request.

8. The method of claim 1, further comprising:

receiving, at the usage policy server, a request to change a threshold associated with the subscriber session; and

updating a subscriber profile based upon a requested threshold change request.

9. The method of claim 1, further comprising:

receiving, at the usage policy server, a request to change a quota associated with the subscriber session; and

updating a subscriber profile based upon a requested quota change request.

10. The method of claim 1, wherein the one or more quotas comprise a maximum amount data usage for a period, a maximum amount of data usage for an application, a maximum amount of data usage for a group of applications, and a maximum amount of data usage for a mobile device associated with the subscriber.

11. The method of claim 1, wherein the one or more data usage thresholds comprise a percentage of data usage as compared to a quota.

12. A system for providing data communications cost monitoring and control for a subscriber session, comprising:

a usage policy server configured to receive a registration request associated with the subscriber session;

a usage policy application configured to determine current data usage associated with the subscriber session;

a receiving module configured to receive one or more data usage thresholds and one or more quotas associated with the subscriber session;

a collection module configured to collect data usage information associated with the subscriber session;

a notification module configured to notify a subscriber when the subscriber exceeds a pre-determined quota during the subscriber session; and

a control module configured to limit data usage for the subscriber session when the subscriber exceeds a pre-determined quota during the subscriber session.

13. The system of claim 12 further comprising a data usage limit module configured to receive and display modifications to data usage limits associated with the subscriber session.

14. The system of claim 13, wherein the data usage limit module is further configured receive and display modifications to data usage limits associated with one or more applications running on a mobile device.

15. The system of claim 14, wherein the data usage limit module is further configured to run on a web server.

16. The system of claim 14, wherein the data usage limit module is further configured to run on a mobile device.

17. The system of claim 12 further comprising a tariff definition module configured to receive modifications to tariffs associated with one or more network service providers.

18. The system of claim 17, wherein the tariff definition module is further configured to display modified tariffs associated with associated with one or more network service providers.

19. The system of claim 18, wherein the tariff definition module is further configured to run on a web server.

20. The system of claim 18, wherein the tariff definition module is further configured to run on a mobile device.

21. The system of claim 12 further comprising a special offer module configured to receive and display special offers to alter a service tier associated with the subscriber session.

22. The system of claim 21, wherein the special offer module is further configured receive and display special offers from a home network service provider associated with the subscriber session.

23. The system of claim 21, wherein the special offer module is further configured receive and display special offers from a roamed network service provider associated with the subscriber session.

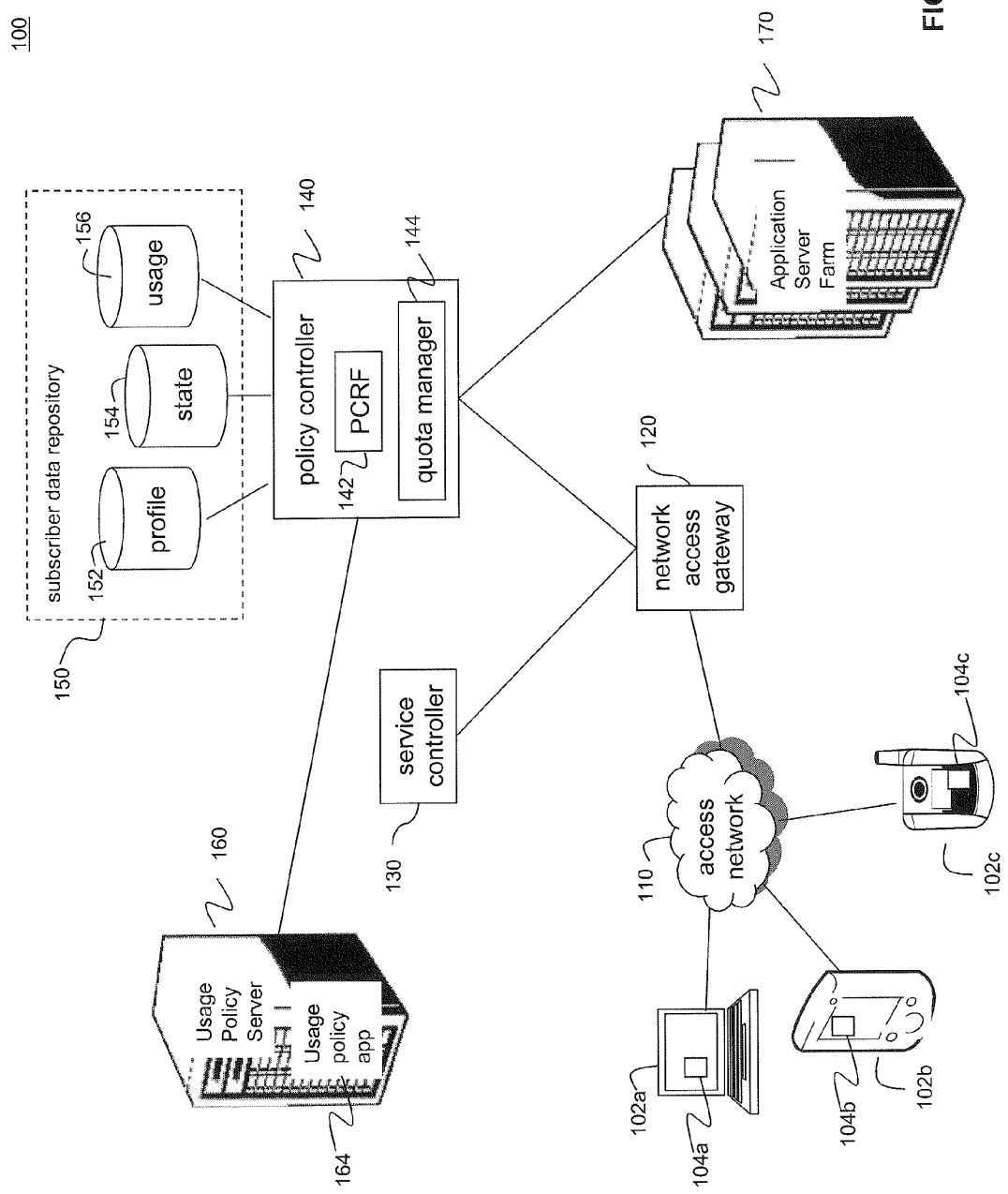

100
subscriber data repository
usage
state
profile
156
154
152
150
policy controller
PCRF
142
140
quota manager
144
Application Server Farm
170
network access gateway
120
service controller
130
Usage Policy Server
Usage policy app
160
164
access network
110
102a
104a
104b
102b
104c
102c

FIG. 1

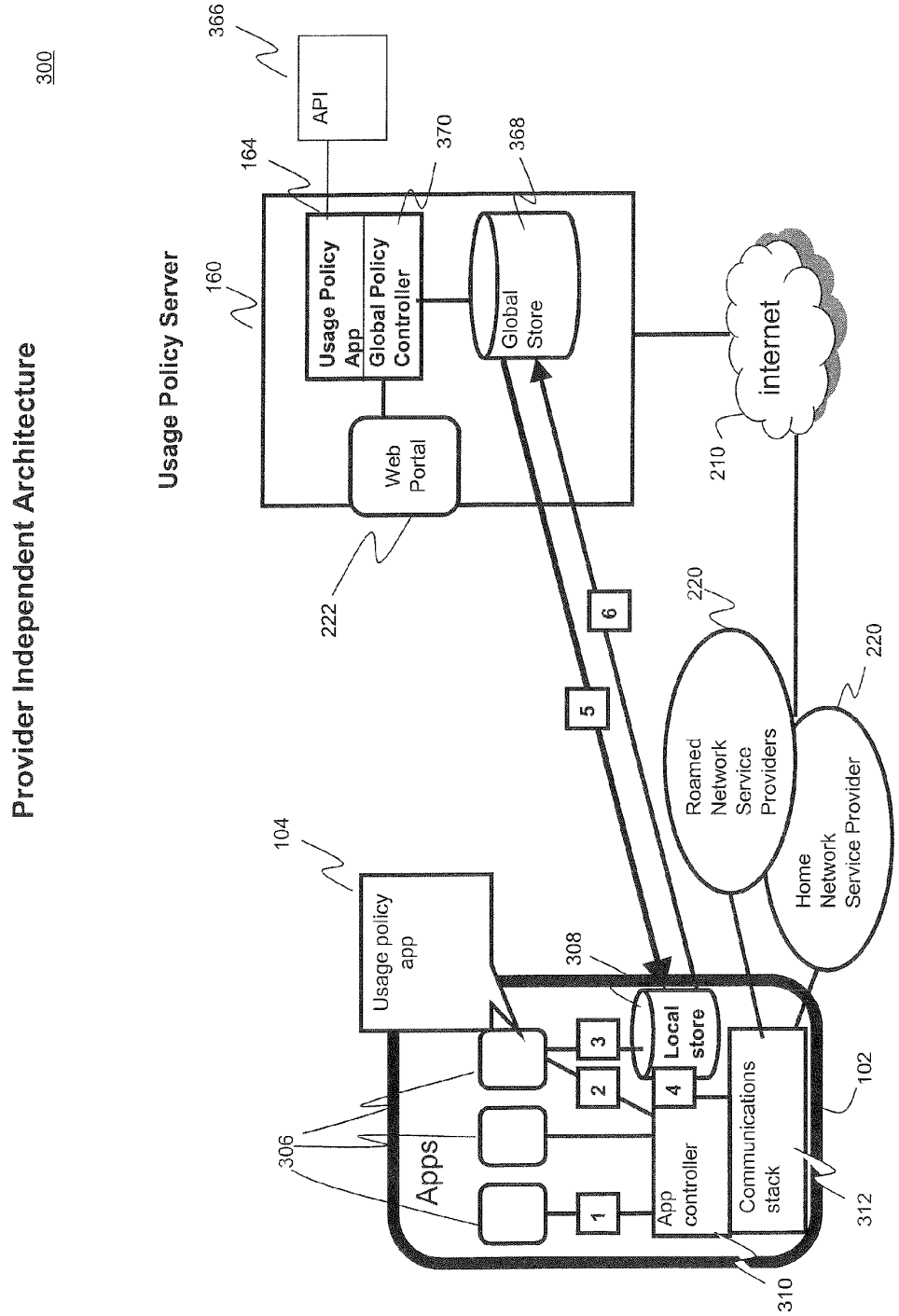

Provider Independent Architecture
300
Usage Policy Server
160
API
366
164
Usage Policy App
Global Policy Controller
370
Global Store
368
Web Portal
222
internet
210
220
Roamed Network Service Providers
Home Network Service Provider
220
104
Usage policy app
308
Local store
Apps
306
App controller
Communications stack
102
312
310
1
2
3
4
5
6

FIG. 3

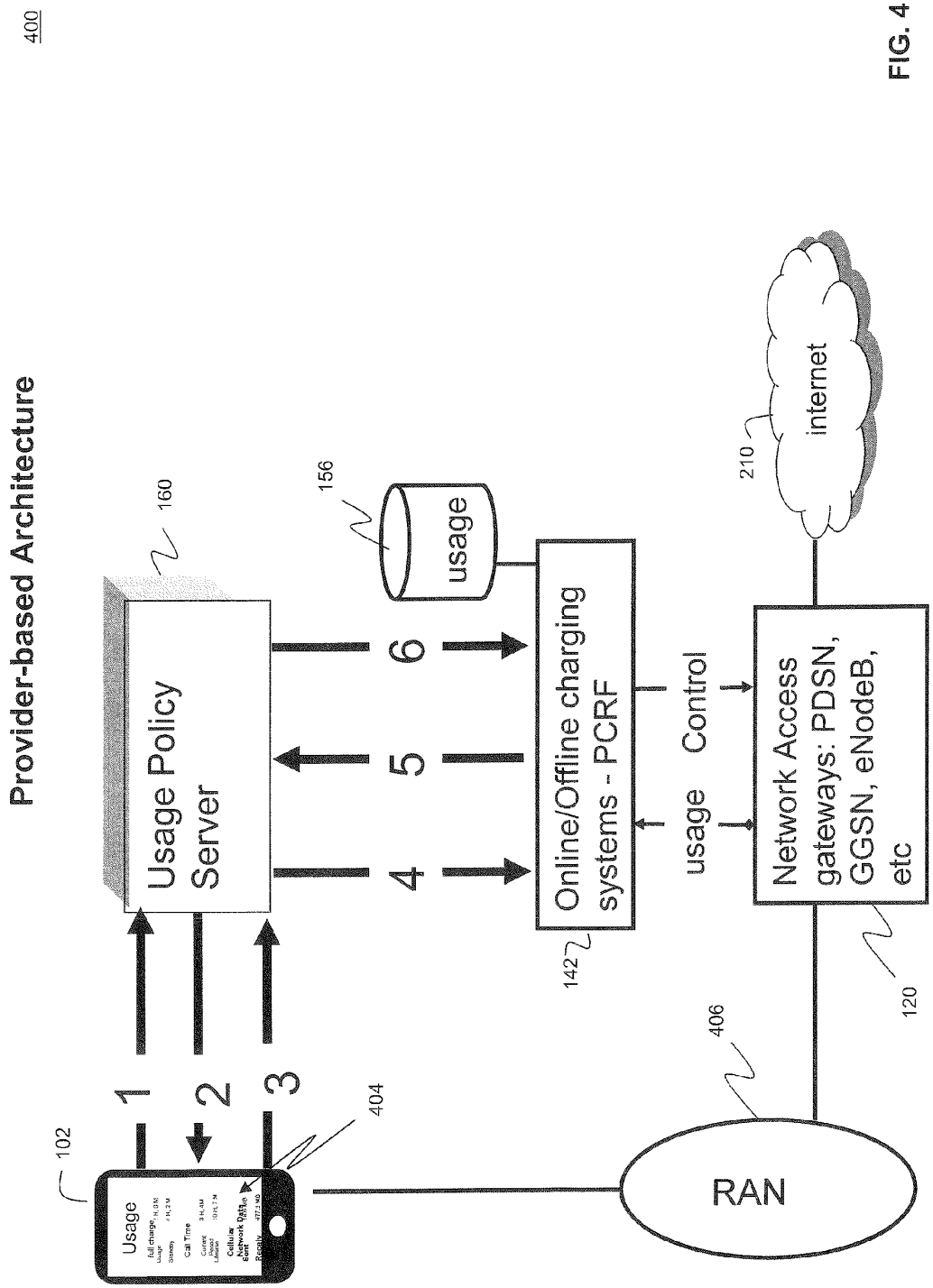

400
Provider-based Architecture
102
Usage
Call Time
Cellular Network Data
Ready
1
2
3
404
160
Usage Policy Server
4
5
6
156
usage
Online/Offline charging systems - PCRF
142
usage
Control
406
RAN
Network Access gateways: PDSN, GGSN, eNodeB, etc
120
210
internet

FIG. 4

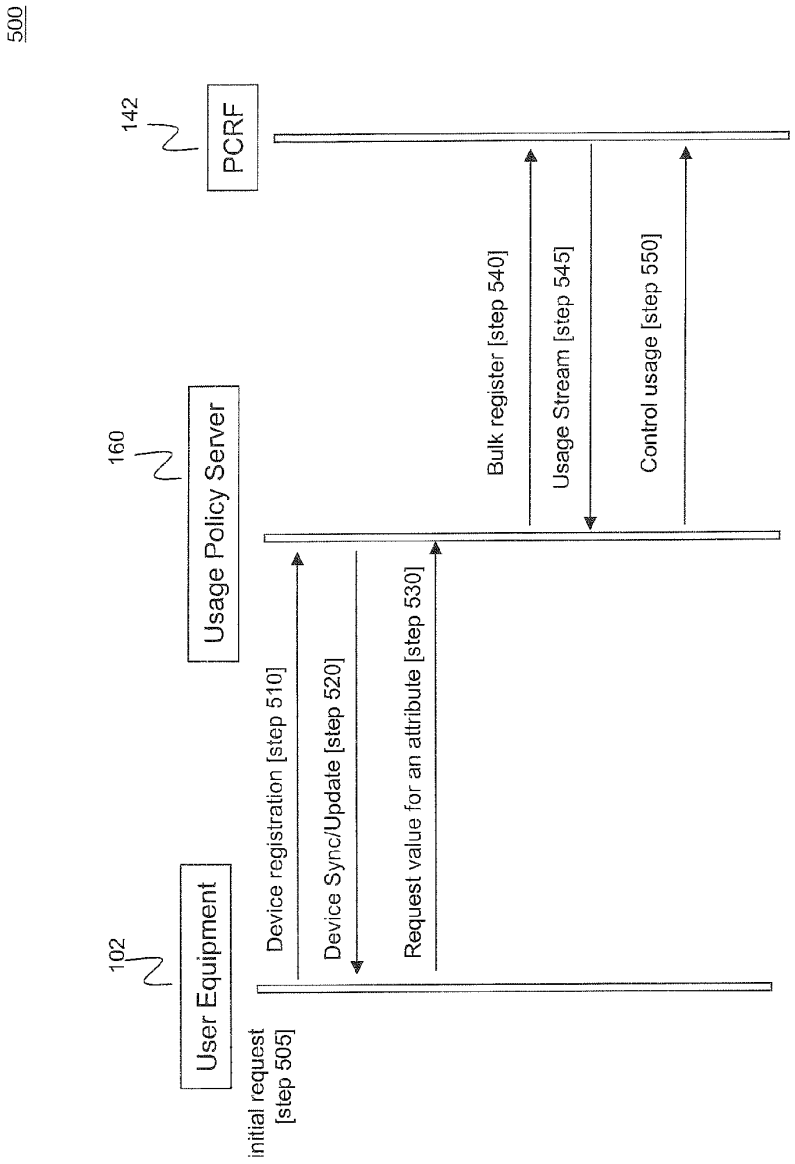

500
102
User Equipment
160
Usage Policy Server
142
PCRF
initial request [step 505]
Device registration [step 510]
Device Sync/Update [step 520]
Request value for an attribute [step 530]
Bulk register [step 540]
Usage Stream [step 545]
Control usage [step 550]

FIG. 5

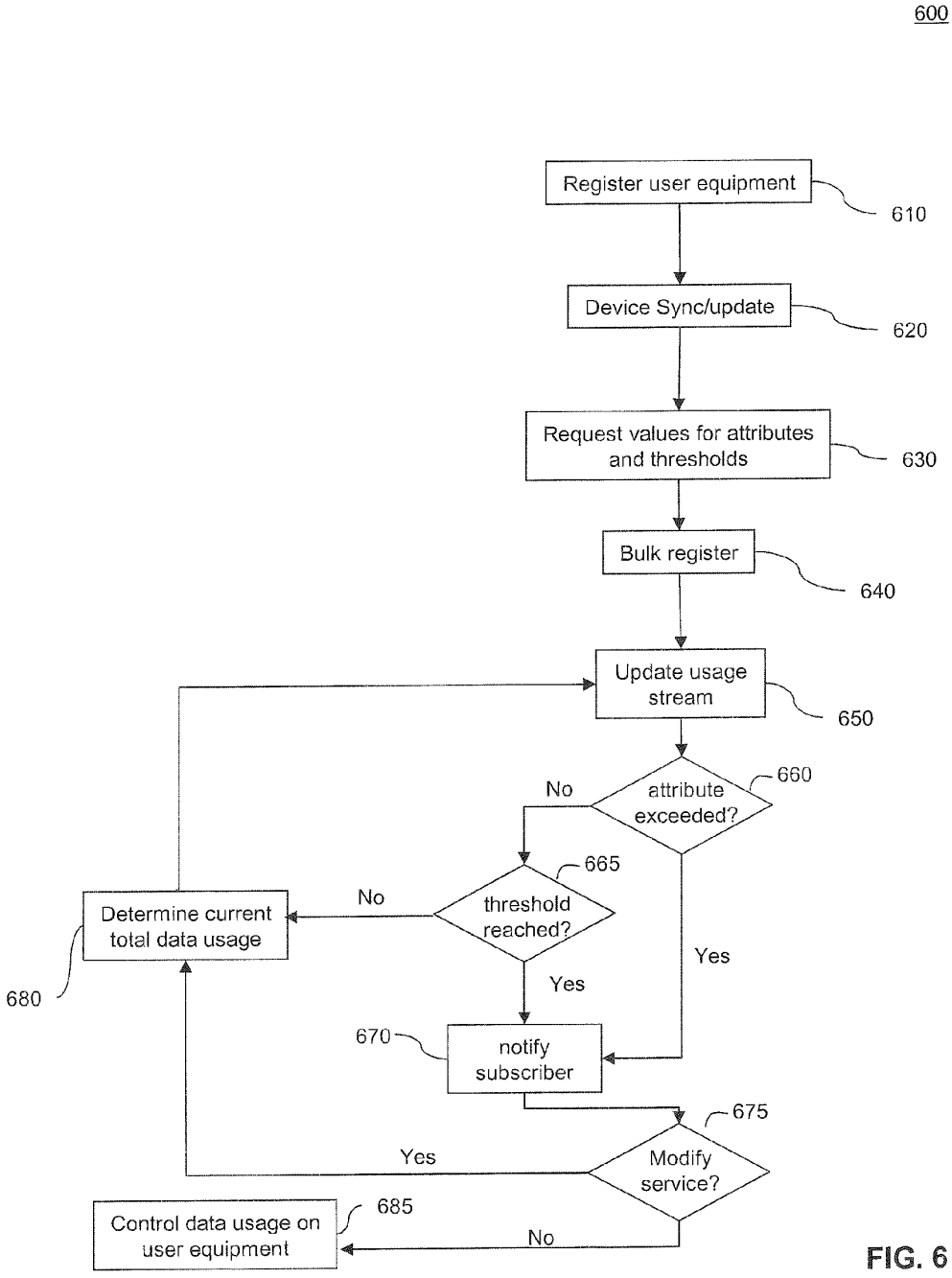

600
Register user equipment
610
Device Sync/update
620
Request values for attributes and thresholds
630
Bulk register
640
Update usage stream
650
attribute exceeded?
660
No
665
threshold reached?
No
Yes
Determine current total data usage
680
Yes
670
notify subscriber
675
Modify service?
Yes
Control data usage on user equipment
685
No

FIG. 6

Roaming Screen

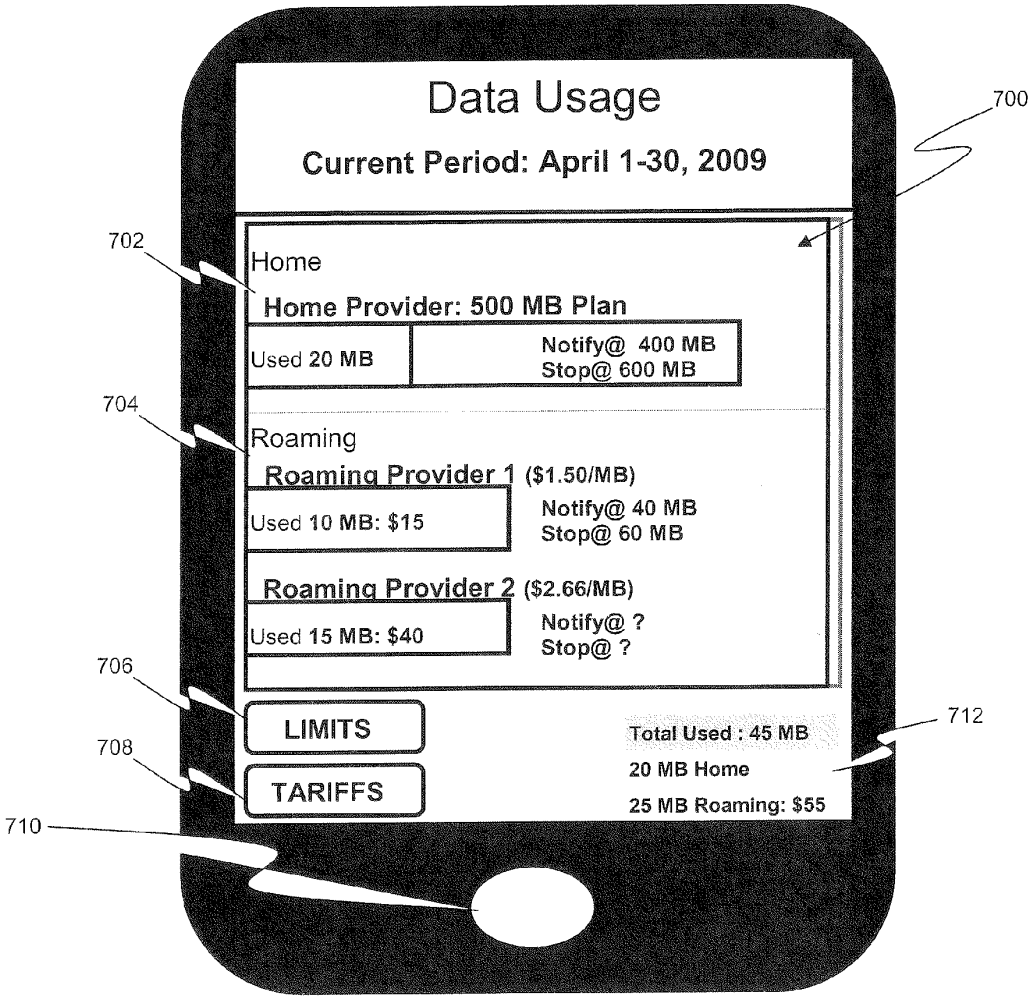


FIG. 7

Setting Usage Limits

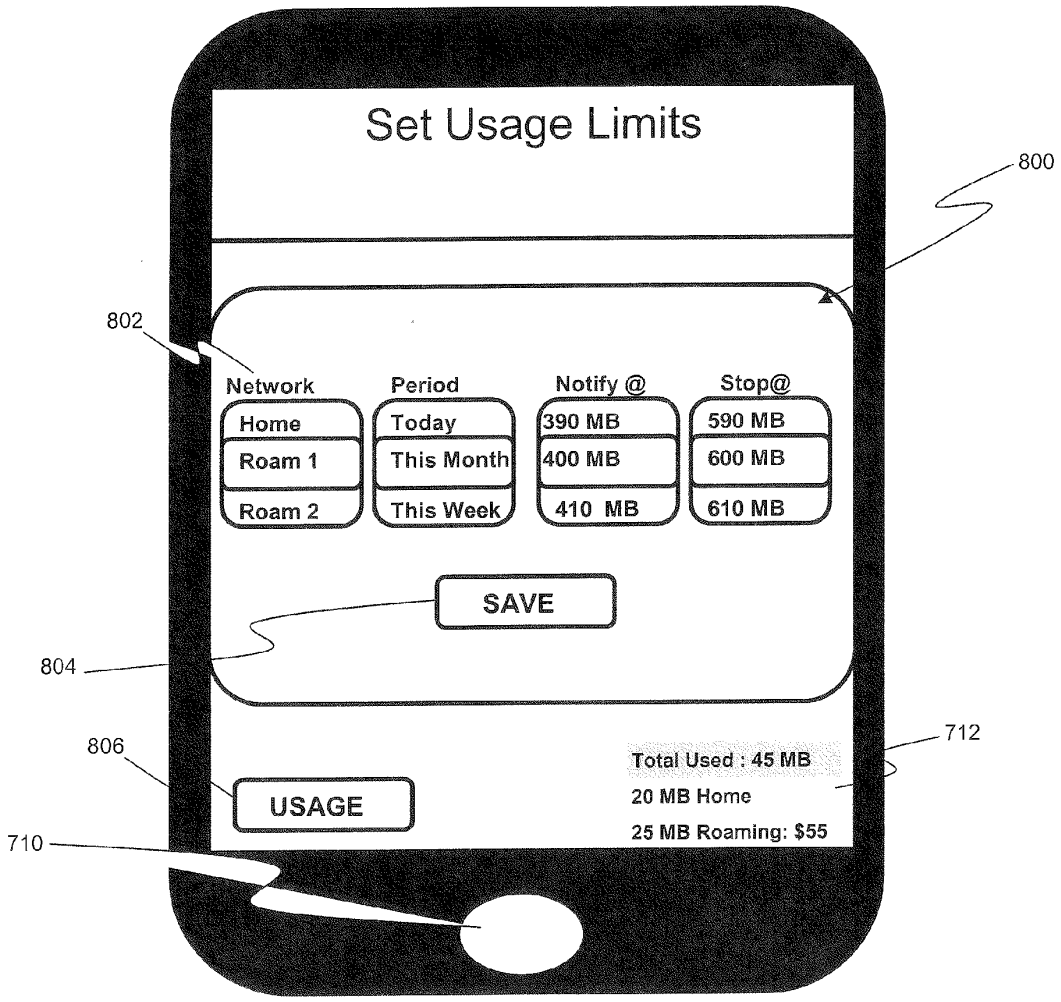


FIG. 8

Defining Tariff

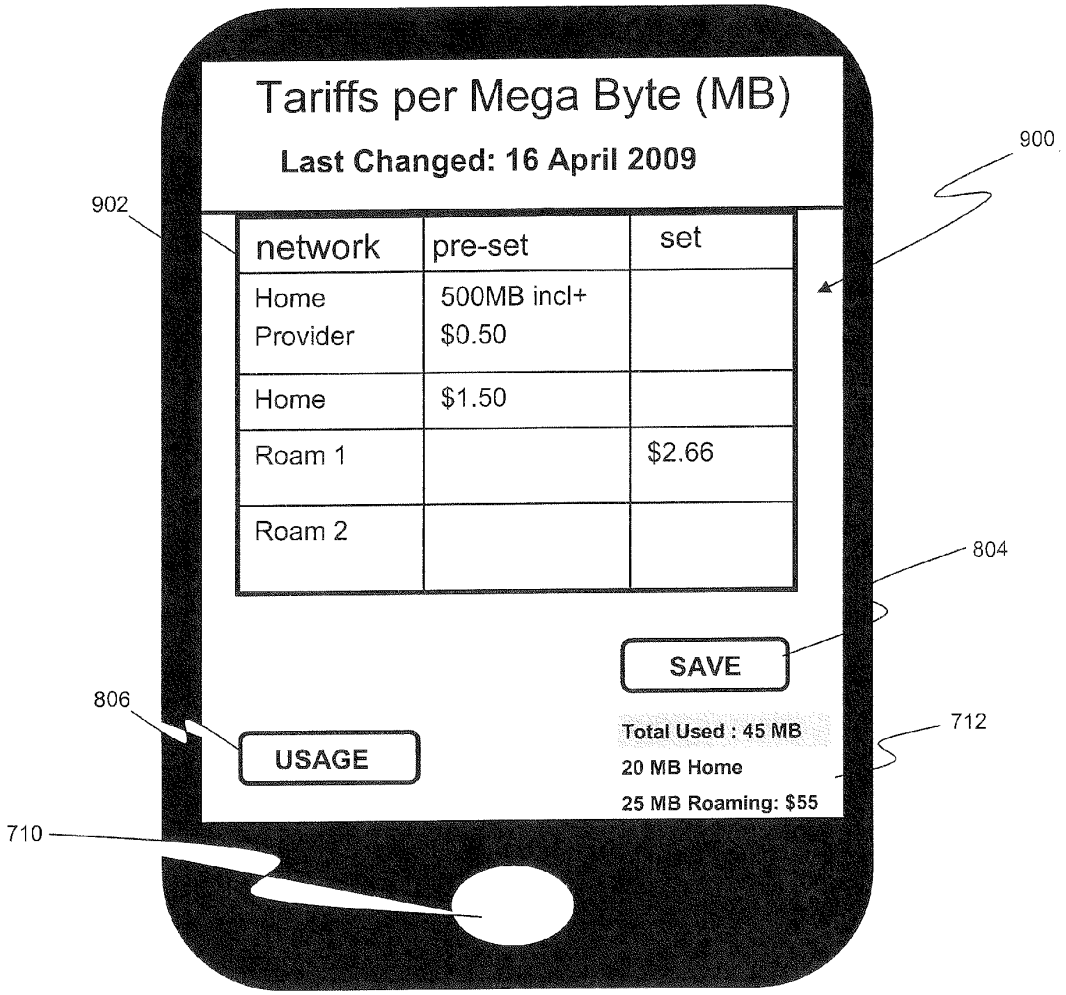


FIG. 9

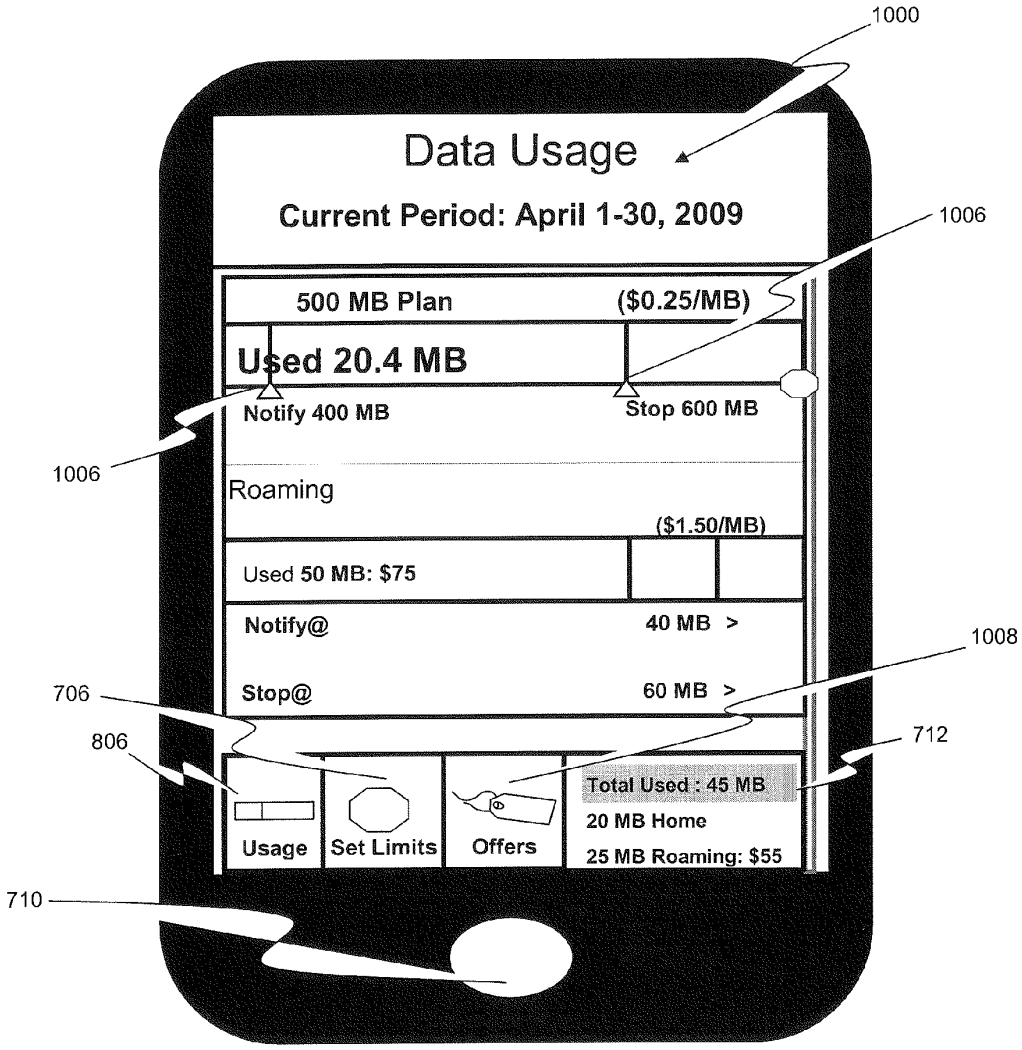

1000
Data Usage
Current Period: April 1-30, 2009
1006
500 MB Plan
($0.25/MB)
Used 20.4 MB
Notify 400 MB
Stop 600 MB
1006
Roaming
($1.50/MB)
Used 50 MB: $75
Notify@
40 MB >
1008
706
Stop@
60 MB >
806
712
Total Used : 45 MB
20 MB Home
25 MB Roaming: $55
Usage
Set Limits
Offers
710

FIG. 10

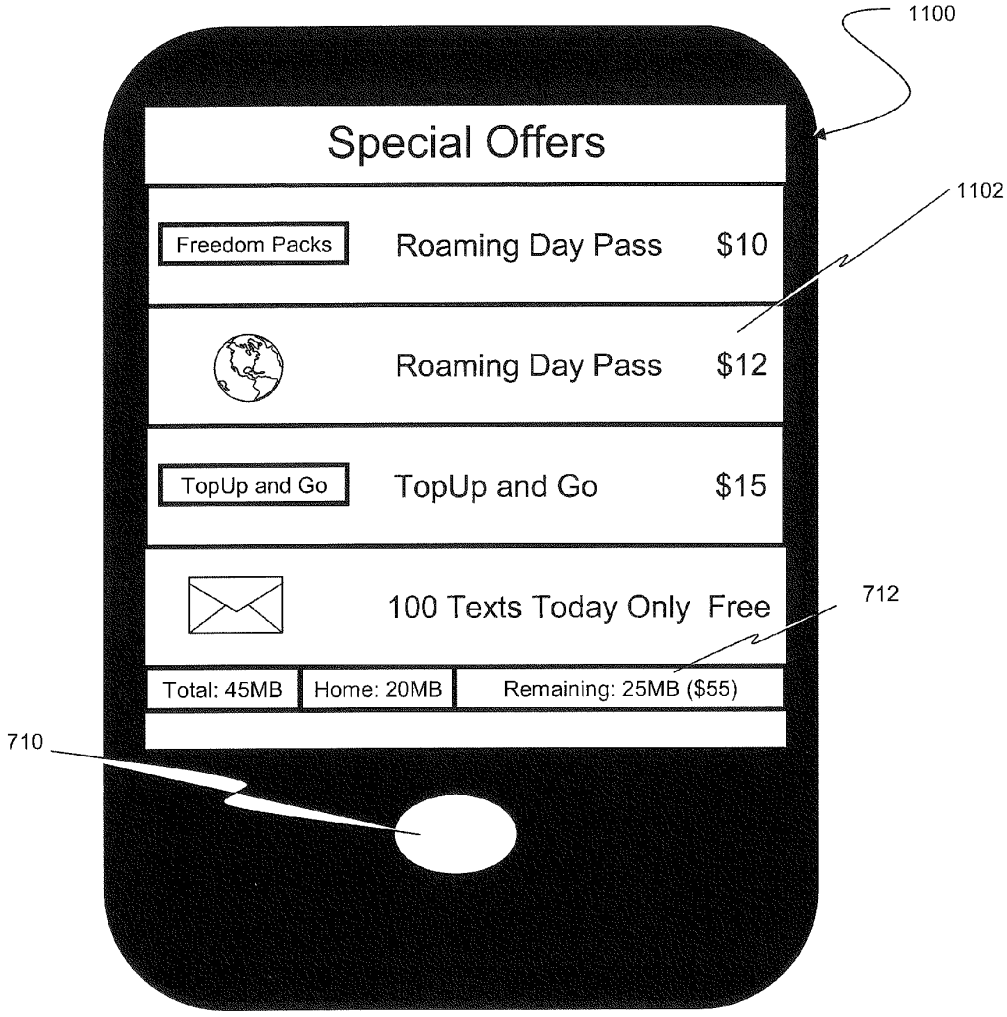

1100
Special Offers
1102
Freedom Packs
Roaming Day Pass $10
Roaming Day Pass $12
TopUp and Go
TopUp and Go $15
100 Texts Today Only Free
712
Total: 45MB
Home: 20MB
Remaining: 25MB ($55)
710

FIG. 11

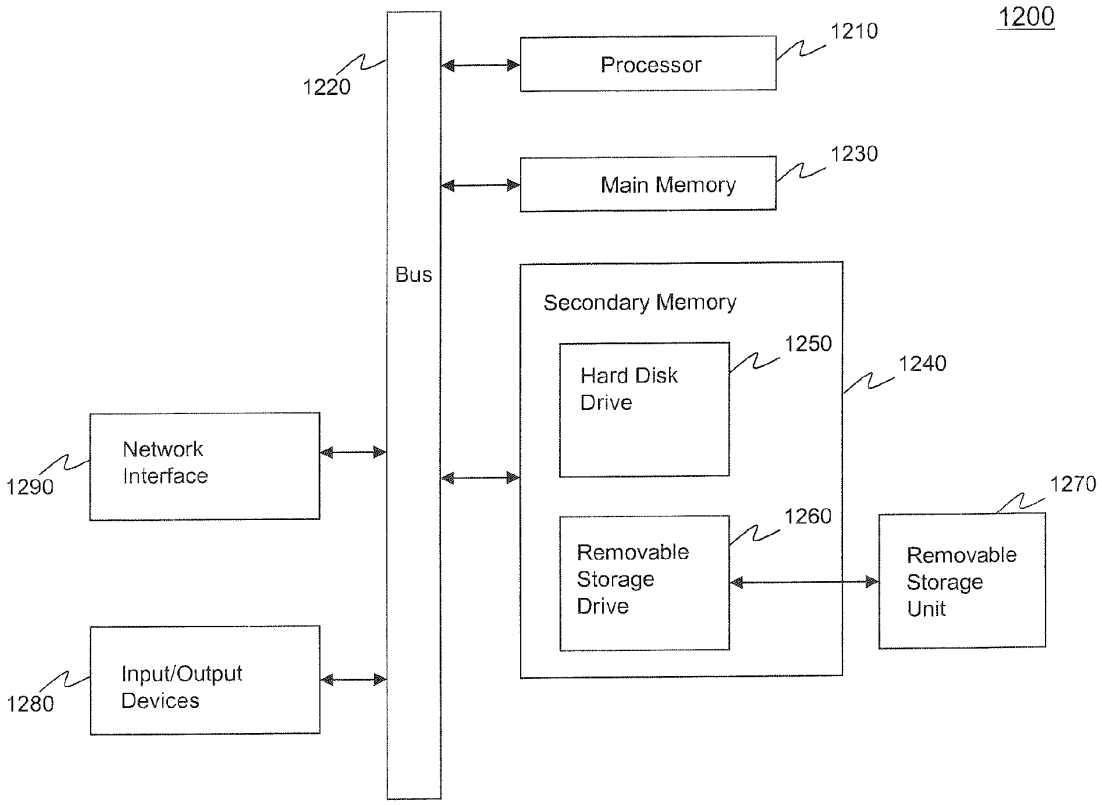

1200
1210
Processor
1220
1230
Main Memory
Bus
Secondary Memory
1250
Hard Disk Drive
1240
Network Interface
1290
1270
1260
Removable Storage Drive
Removable Storage Unit
Input/Output Devices
1280

FIG. 12

Electronic Acknowledgement Receipt	
EFS ID:	32588365
Application Number:	15582350
International Application Number:	
Confirmation Number:	7797
Title of Invention:	Wirless Network Buffered Message System
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:	RALEP007C11C3C2C3C2
Receipt Date:	10-MAY-2018
Filing Date:	28-APR-2017
Time Stamp:	13:13:18
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)	P007C11C3C2C3C2_IDS.pdf	1054624 0c721ed7aead6be4ab9025edf697b0495b913adb	no	8

Warnings:

Information:					
2	Foreign Reference	2099.pdf	4611633 bf9b948271be5b11856ba065b36bab8ca2c283b0	no	47
Warnings:					
Information:					
3	Non Patent Literature	3070.pdf	800138 a01751f11a1220082d7b94238b19e29ecf57278e	no	37
Warnings:					
Information:					
			Total Files Size (in bytes):	6466395	

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 (03-15)
Approved for use through 07/31/2016. 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	15582350
Filing Date	2017-04-28
First Named Inventor	Gregory G. Raleigh
Art Unit	2447
Examiner Name	not yet assigned
Attorney Docket Number	RALEP007C11C3C2C3C2

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	7165040	B2	2007-01-16	Ehrman et al.	
	2	7656271	B2	2010-02-02	Ehrman et al.	
	3	8401968	B1	2013-03-19	Schattauer et al.	
	4	6535949	B1	2003-03-18	Parker, Kenneth W.	
	5	7809372	B2	2010-10-05	Rajaniemi, Jaakko	

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	20060101507	A1	2006-05-11	Camenisch, Ja L.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Gregory G. Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	2	20070171856	A1	2007-07-26	Bruce et al.	
	3	20110004917	A1	2011-01-06	Saisa 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	1098490	EP	A2	2001-05-09	Nortel Networks Ltd.		
	2	2026514	EP	A1	2009-02-18	Nokia Siemens Networks		
	3	2007129180	WO	A2	2007-11-15	Nokia Corp.		
	4	1942698	EP	A1	2008-07-09	Apple 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.	T[5]
	1		

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Gregory G. Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

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	15582350
	Filing Date	2017-04-28
	First Named Inventor	Gregory G. Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

CERTIFICATION STATEMENT

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

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

OR

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

See attached certification statement.

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

☒ A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/James E. Harris/	Date (YYYY-MM-DD)	2018-02-08
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.

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

(11) EP 1 098 490 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
09.05.2001 Bulletin 2001/19

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

(21) Application number: **00309735.9**

(22) Date of filing: **03.11.2000**

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

(30) Priority: **05.11.1999 US 434628**

(71) Applicant: **Nortel Networks Limited**
Montreal, Quebec H2Y 3Y4 (CA)

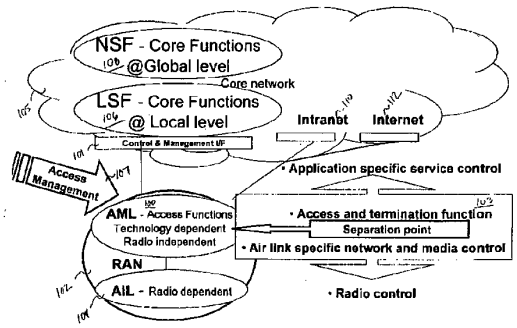
(72) Inventors:
- **Amin, Rajesh B.**
  Desoto, Texas 75115 (US)
- **Hanley, Donald V.**
  McKinney, Texas 75075 (US)
- **Morrow, Glenn C.**
  Plano, Texas 75075 (US)
- **Allahyar, John**
  Dallas, Texas 75252 (US)

(74) Representative: **Mackenzie, Andrew Bryan et al**
Sommerville & Rushton,
45 Grosvenor Road
St Albans, Herts. AL1 3AW (GB)

(54) An architecture for an IP centric distributed network

(57) A method and system to for a communications network architecture for an Internet Protocol centric wireless network for a first user to communicate to a destination, the architecture comprising: a network service function layer within the wireless network. The network service function layer can include: a policy management server; an authorization server; a service accounting server; an authentication, authorization and accounting server; an unified directory within a directory server; a security gateway; and a mobility manager. The architecture also includes a local service function layer associated with the network service function layer. The local service function layer can include: an access accounting server; an authentication, authorization and accounting server; a security gateway; a policy enforcement server; a mobility manager; a network management server; and a wireless gateway. The architecture also includes an access management layer associated with the local service function layer. The access management layer can include: a location tracking server; a connection management server; a protocol server; an access management server; a policy enforcement server; a network management server; and a resource management server. The architecture also includes an access interface layer associated with the access management layer. The access interface layer can include: a channel management server; a policy enforcement server; an administration and maintenance server; and a radio frequency server.

FIGURE 1



Printed by Jouve, 75001 PARIS (FR)

EP 1 098 490 A2

BNSDOCID: <EP_____1098490A2_I_>

Description

FIELD OF THE INVENTION

[0001] The invention relates generally to computers and, more particularly, to an architecture for an Internet Protocol centric distributed network and a method and apparatus for such a network.

BACKGROUND OF THE INVENTION

[0002] Recently, wireless communication devices have become more and more popular as a method of communicating from one point to another. Cellular Radio is one, and probably the most popular, method of wireless communication. The original and still, most common Cellular Mobile Telephone System is a low-powered, duplex, radio/telephone which operates between 800 and 900 mHz for TDMA and 1800 and 1900 mHz for CDMA, using multiple transceiver sites linked up to a central computer for coordination. The geographic region served by a cellular system is subdivided into areas called cells. Each cell has a central base station and two sets of assigned transmission frequencies; one set is used by the base station, and the other by mobile telephones. To prevent radio interference, each cell uses frequencies different from those used by its surrounding cells, but cells sufficiently distant from each other can use the same frequencies. When a mobile telephone leaves one cell and enters another, the telephone call is transferred from one base station and set of transmission frequencies to the next using a computerized switching system. The first cellular telephone system began operation in Tokyo in 1979, and the first U.S. system began operation in 1983 in Chicago.

[0003] The earlier system have been focused on providing mostly voice services with some capability of providing data communications as well. However, recently, the need for a network designed with other services in mind other than just voice has arisen. The network should be able to provide access to different application layer protocols such as Session Initiation Protocol, H.323, and Internet Protocol to name a few.

SUMMARY OF THE INVENTION

[0004] In contrast to the prior art, the present invention provides a distributed IP centric system and method for wireless access to an internet protocol (IP) based network, wherein the system and method is independent from technology used in accessing the network. The system also uses the application layer to send messages between the access layer and the IP network. The access layer also includes distributed IP based functionality and the flexibility to be incorporated into distributed servers on a Local Area Network (LAN). The access layer also includes the capability to support establishing and maintaining the wireless link and mobility services to the mobile station through the access layers along with simultaneous IP access to public domain services. The access layer also handles connection management independent from the hardware used (such as ATM, Ethernet, etc.).

[0005] To this end, in one embodiment the method and system include a communications network architecture for an Internet Protocol centric wireless network for a first user to communicate to a destination, the architecture comprising: a network service function layer within the wireless network. The network service function layer can include: a policy management server; an authorization server; a service accounting server; an authentication, authorization and accounting server; an unified directory within a directory server; a security gateway; and a mobility manager. The architecture also includes a local service function layer associated with the network service function layer. The local service function layer can include: an access accounting server; an authentication, authorization and accounting server; a security gateway; a policy enforcement server; a mobility manager; a network management server; and a wireless access gateway. The architecture also includes an access management layer associated with the local service function layer. The access management layer can include: a location tracking server; a connection management server; a protocol server; an access management server; a policy enforcement server; a network management server; and a resource management server. The architecture also includes an access interface layer associated with the access management layer. The access interface layer can include: a channel management server; a policy enforcement server; an administration and maintenance server; and a radio frequency server.

[0006] Therefore, in accordance with the previous summary, objects, features and advantages of the present invention will become apparent to one skilled in the art from the subsequent description and the appended claims taken in conjunction with the accompanying drawings.

BNSDOCID: <EP_____1098490A2_I_>

BRIEF DESCRIPTION OF THE DRAWINGS

[0007]

Figure 1 is a diagram of separating wireless access from the Core Network;
Figure 2 is a diagram of the LSF/NSF (core) Layer functional service components;
Figure 3 is a diagram of the Radio Access Network Layer functional service components;
Figure 4 is a diagram of the Mobile Terminal Layer functional service components;
Figure 5 is a diagram of Protocol layers and interactions;
Figure 6 is a diagram of Service layer interfaces;
Figure 7 illustrates the connectivity of the Access Management Layer;
Figure 8 is a diagram of AML functional components;
Figure 9 is a diagram illustrating step 1 of the access session establishment procedure;
Figure 10 is a diagram illustrating step 2 of the access session establishment procedure;
Figure 11 is a diagram illustrating step 3 of the access session establishment procedure;
Figure 12 is a diagram illustrating step 4 of the access session establishment procedure;
Figure 13 is a diagram of the service session invocation procedure;
Figure 14 is a diagram of the functional component interaction sequence flow;
Figure 15 is a diagram of an overview of an access scenario at the AIL-AML;
Figure 16 is a diagram of an QoS change request;
Figure 17 is a diagram of use of default QoS to establish call/session;
Figure 18 is a diagram of a call/session invocation request;
Figure 19 is a diagram of power up registration;
Figure 20 is a diagram of the use of default parameters; and
Figure 21 is a diagram of an example implementation of the various layers of the architecture of the preferred embodiment.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0008] The present invention can be described with several examples given below. It is understood, however, that the examples below are not necessarily limitations to the present invention, but are used to describe typical embodiments of operation. Additionally, a list of abbreviations and a glossary will be listed first to facilitate a better understanding of the invention.

Abbreviations

[0009]

AAA	Authorization Authentication Accounting
AIL	Access Interface Layer
AML	Access Management Layer
ATM	Asynchronous Transfer Mode
CDMA	Code Division Multiplex Access
CN	Core Network
COA	Care Of Address
COPS	Common Open policy Service
dB	data Base
DHCP	Dynamic Host Configuration Protocol
DNS	Directory Name System
DEN	Directory Enabled Networking
DS	Directory Server
FR	Frame Relay
HDLC	High Level Data Link Control
IP	Internet Protocol
ITU	International Telecommunication Union
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LDP	Local Decision Point

BNSDOCID: <EP_____1098490A2_I_>

LSF	Local Serving Function
L1	Layer 1
L2	Layer 2
L3	Layer 3
MH	Mobile Host
MM	Mobility Manager
MPLS	Multi-protocol Label Switching
MS	Mobile Station
NGWN	Next Generation Wireless Network
NSF	Network Serving Function
OSI	Open System Interconnection
PDP	Policy Decision Point
PPP	Point to Point Protocol
PSTN	Public Switched Telephone Network
RADIUS	Remote Authentication Dial-In User Service
RAN	Radio Access Network
RF	Radio Frequency
RSVP	Resource Reservation Protocol
RTCP	Real Time Control Protocol
RTP	Real Time Protocol
QoS	Quality of Service
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SMS	Short Message Service
SS	Session Server
TCP	Transmission Control Protocol
UAC	User Agent Client
UAS	User Agent Server
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunication System
UWN	Unified Wireless Network
WAG	Wireless Access Gateway

Definition of terms

[0010] UWN: The Unified Wireless Networks is the IP centric core-network consisting of LSF and NSF network components. The UWN is assumed to be independent of air interface technology. The interfaces between system components of the UWN are based on the LAN/WAN technology and uses client server architecture.

[0011] 2G: The current wireless network components are referred to as the second-generation components. The 2G-network component uses industry-defined protocols and interfaces to communicate between the system and network components.

[0012] 3G: The future wireless network components evolved from the 2G components are referred to as the third generation components. In the description of the preferred embodiment it is assumed that the 3G will be backward compatible to the 2G. For an example, 3G mobile (voice mode) terminal is capable to act as 2G mobile (voice mode) in voice call support. In addition, 3G will be able to support new standards for making a multi-media call using newly defined standards. The gateway devices may be used to support 2G and 3G components.

[0013] NG: The future wireless network components that evolve from the 3G components are referred to as the Next Generation components. The NG components are assumed to take full advantage of the IP centric network infrastructure and eliminate the need of gateway devices. End devices will become smarter with the capability of communicating without the need for the gateway or mapping functions.

[0014] NSF: The NSF is one of the network components of the UWN architecture. It consists of several system components. These components may include legacy components through the necessary interfaces or their functional equivalent suitable to the IP centric environment. Some of these components are HLR, SCP, Unified Directory, AAA server, SN, IP Service Platform (provides value added applications to the client), etc. Network Serving Function (NSF) is the global home component of the UWN that owns the mobile user's subscription.

[0015] LSF: The LSF is one of the network components of the UWN architecture. It consists of several system components. Some of these components are CS, MM, CD, DHCP, DNS, Gateway devices, etc. The Local Serving function (LSF) is the serving component of the UWN that provides services to local and visiting wireless subscriber in that area.

BNSDOCID: <EP_____1098490A2_I_>

[0016] RAN: The Radio Access Network is the system component of the wireless network that provides radio control functions used in transmitting and receiving control and data information between mobiles and core network. The RAN itself is air technology dependent. However, it is evolving to provide independent functionality towards the IP centric core network. On this basis, RAN is assumed to have distinct radio interface and access management components. The radio management components provides the radio independent functionality towards the IP centric core network.

[0017] AML: The Access Management Layer is the service layer of the RAN that consists of radio management and access management components.

[0018] AIL: The Access Interface Layer is the service layer of the RAN that consists of air link interface handling components.

[0019] WAG: The Wireless Access Gateway is the entity that interfaces with the wireless access network such as 3G RAN and provides controlling capabilities to facilitate the RAN resources to meet users' requirements such as bandwidth management and also to interface with the intranet or Internet components.

[0020] WGW: The Wireless GateWay is the entity that interfaces and provides gateway functionality between the traditional wireless access such as BSC and the IP centric network. The WGW is assumed to provide merely tunneling capabilities to transport messages such as DTAP or BSMAP between IP centric network and the traditional 2G-access controller. This definition is not used in the description of the preferred embodiment. However, it is provided just to differentiate the meaning of WGW with the WAG described earlier.

[0021] UAC: User Agent Client is the first entity within the wireless network that assumes responsibility on behalf of the user to communicate with the core network or external network components. The UAC facilitates the activities in the ingress direction. Typically, the UAC is capable of communicating to the external servers directly. However, in some instances the UAC may convey such need to the UAC proxy.

[0022] UAS: User Agent Server is the entity that receives requests from the UAC or the UAC proxy. It facilitates the activity in the egress direction.

[0023] UAC proxy: User Agent Client Proxy takes responsibilities on behalf of the UACs to send appropriate requests to the server.

[0024] UAS proxy: User Agent Server proxy is the first entity within the wireless network that assumes the terminating responsibility on behalf of the receiving user. However, it has the ability to forward or redirect the call/session to other external components. The UAS-proxy facilitates the activities in the egress direction. Typically, the UAS proxy is capable of communicating to the terminating user directly. However, in most instances the UAS-proxy just conveys such information to the UAS that in turn communicates to the end user.

[0025] Ingress: This term is used for those activities that occur in direction from the mobile host to the network.

[0026] Egress:This term is used for those activities that occur in direction from the network to the mobile host.

[0027] Outgoing call/session: This term is used as defined by the bellcore documents. This term is used for the call/session activities that originated from the mobile host and progresses to other network through the serving network.

[0028] Incoming call/session:This term is used as defined by the Bellcore documents. This term is used for the call/session activity that originates from the external network and progresses to the mobile host through the serving network.

Introduction

[0029] The distributed IP centric Wireless Internet - NGWN architecture is centered around IP mobility management, call/session management, and network management. The scope of the description of the preferred embodiment is to explore call/session management services.

[0030] The call/session management services consist of three functions. These functions are: 1) establishing an access session between the mobile host and the serving network; 2) an invocation of a service session by the end user; and 3) facilitating network resources to establish point to point or point to multi-point virtual connection.

[0031] The establishment of an access session attaches the mobile host to the serving network. During the establishment, subscribers' are authenticated and granted either a specifically requested, or a default, bandwidth with the desired quality of service. Once the access session is established, the mobile host becomes IP capable and can reach, or be reached, any other devices. The access session remains active while the mobile host is attached to the serving network..

[0032] Once the access session is established, the user can invoke a service session. The user is provided with user capabilities and network preferences to use services from the serving network or externally accessed services. Although the user is provided with many choices of service invocation, the one of the main components is call/session control services. The management of call/session control is distributed to a set of appropriate servers (functions) within the access management and Local Service Function (LSF) network service layers. This distribution allows access relevant activities to be coupled with the access dependent service layers, and policy decision making activities coupled with the access independent layers. The services originated at the application level are configured with the appropriate application servers at the LSF service layer. In addition, call/session control services are part of the access management

BNSDOCID: <EP_____1098490A2_I_>

services that aids to facilitate in establishing point to point and point to multi-point virtual connections.

[0033] The main components of the Unified Wireless Networks (UWN) consist of IP mobility management components, call/session management components, network management control, and gateway devices that interface with other systems supporting different protocols. The network management control functionality is also important but dependent on the full definition on the other components. The gateway functionality is also required along with the other appropriate components of the UWN.

[0034] The description of the preferred embodiment focuses on the functional components of the call/session management services. These functional components are distributed in distinct network service layers based on their role. The network access and user service related functional components are distributed in the access management and service management layers respectively. Further; the service management layer is distributed into a local network service layer and a global network service layer.

[0035] Thus, realization of functional components and their appropriate separation into access and service layers have allowed separating network access and service management functions from the media transport. This enabled the end user to have choice of using serving network services or to use external Internet services. Detailed procedures to establish the access session and invoke the service session are discussed below.

Objectives/Requirements

[0036] The call/session management tasks are expected to achieve objectives for three basic functions. These functions are comprised of first, establishing, maintaining and terminating an *access session* between mobile host and the serving network. Second, providing network services to the mobile host that allows a mobile host to establish a *service session*. And third, facilitating transport resources of the serving network to establish a *transport session* based on the mobile hosts' need of bandwidth with a desired quality of service. The desired objectives to achieve these three functions are described below. Moreover, the call/session management functions are real time sensitive where access of decision making information and propagation delay through the network infrastructure plays an important and critical role. Additional objectives related to performance, capacity, and scalability are also identified for real time and other similar issues.

Access, Service, and Transport Session Objectives

[0037] These three basic functions of the call/session management services are identified and elaborated to distinctly depict the differences within the Wireless Internet.

Access Related Objectives

[0038] An establishment of an access session enables the mobile host to establish a point of presence at the local serving network. During access session establishment, subscriber management services are executed. These services include admission policy control decision, provisioning of default air link resources, and establishing the virtual packet channel that allows mobile hosts to interface with the external Internet network. The following paragraphs describe the access related objectives in detail.

[0039] Any access dependent requirements for subscriber management services should be identified. The subscriber management services include authentication, authorization, usage selection and usage constraints associated with subscriber.

[0040] User authentication and authorization are based on digital certificates/signatures, and is provided by an authentication server.

[0041] Usage selection and user constraints are based on the subscriber profile and network policy.

[0042] Provisioning the local serving functions with access and usage profile in order to provide allowed access and usage services to the mobile host.

[0043] Handling of flexible bandwidth provisioning and supporting requirements.

[0044] Handling of accounting requirements based on flat rate, per packet, time used, and/or Quality of Service provided.

[0045] Handling of data speed requirements of up to 144 kb/s for vehicular users, up to 384 kb/s for outdoor to indoor mobility, and up to 2 Mb/s for indoor and Pico cell environments. Handling of Quality of Service requirements.

Service Session Related Objectives

[0046] The service session enables an end user to use services provided by the serving network. Also, an end user can use the serving network services to dynamically change network transport resources. That will allow an end user

BNSDOCID: <EP_____1098490A2_I_>

to access globally available network services at the required bandwidth for a desired quality of service. The following paragraphs describe a few objectives.

[0047] Identify serving network services to facilitate use of access network application servers to provide services independent from the subscriber's home network.

[0048] Identify any interaction needed in providing global network services that are based on service level agreements between other networks (home or third party).

[0049] Identify serving networks' role in enabling end user to form a private network within the scope of serving the Wireless Internet.

[0050] Identify scheme for reporting network resource usage.

[0051] Establishing and managing voice, paging, Short Message Service (SMS), and circuit and packet data oriented services (e.g. multi-media conference, on-line subscription, etc.).

[0052] Service capabilities related to information and functionality such as dynamic negotiation of QoS, use of Intranet service and use of communication resources.

Transport Related Objectives

[0053] The transport session activities enable the mobile host to use the network's air and virtual packet channel path resources. The following paragraphs describe a few identified objectives.

[0054] Establishing bearer connection path for an air link and virtual packet channel using serving network's resources.

[0055] Facilitating Point to Point, Point to Multi-point and Multi-point to multi-point connection.

[0056] Facilitating use of underlying network infrastructure resources such as ATM, FR, or Ethernet.

[0057] Facilitating use of payload coding/decoding task identified by the payload mediation function of the local serving function.

Other Related Objectives

[0058] The following paragraphs describe a few more important objectives.

[0059] Performance objectives :

[0060] Minimum packet delay; ITU recommends roundtrip delay less than 300 ms.

[0061] Minimum packet loss, such that no noticeable degrade in voice quality and the performance of fax.

[0062] Maximum throughput via a virtual connection

[0063] Optimized bandwidth distribution

Challenges

[0064] An identification of the Call/Session management functions and objectives for the newly defined NGWN are relatively straightforward. However, the feasibility of such objectives to implement and achieve quality of traditional networks in the newly defined Wireless Internet is not an easy task;. it is a paradigm shift. It involves many unknowns and challenges. An attempt is made here to list such challenges in this section along with the solutions in subsequent sections.

[0065] Identify interfaces and signaling objectives between mobile host and network components. More precisely between:

[0066] Mobile host and network's access management layer (AML) functional components to establish access session.

[0067] Mobile host and network's local service layer functional (LSF) components to establish service session.

[0068] Mobile host and home network service layer functional components (NSF) to establish Virtual Home Environment.

[0069] Achieve distributed transparencies for applications.

[0070] Achieve optimized information caching significant to established clusters and domains.

[0071] Reduce dependencies for availability and reliability of network components due to network problems, server problems and faulty software.

[0072] Achieve scheme to reach neighboring domains directly avoiding hierarchical intervention.

[0073] Identify both connection oriented and transaction-oriented services.

[0074] Identify inter-working between non-IP access network and IP-based core network.

BNSDOCID: <EP_____1098490A2_I_>

Architectural Framework: Emphasizing Call/Session Management components

[0075] This section establishes context for the call/session management services. An architectural framework is illustrated mainly emphasizing the functional service layers and components. It starts with separation of functional boundaries and later decomposes functional components in detail. The interfaces and interactions between network entities and inter-working between functional service layer components is described below. However, in order to illustrate the separation of functional layers and the respective inter-working between layers, the description will not flow from figure 1 through figure 8 sequentially, but will refer to the figures out of order. However, the elements are numbered consistently throughout figures 1 through 8 so as to help the understanding of the description.

Architectural overview

[0076] The NGWN/Wireless Internet is an IP centric distributed Local Area Network (LAN) based architecture. The network components in this architecture are functionally separated as required to fulfill the need of wireless telecommunication and is also suitable to integrate with other data and telecommunication networks.

[0077] The NGWN architecture provides the separation of applications/services control that interacts with the end user and management of the physical infrastructure. Figure 1 identifies the separation of wireless access 102 from the core network 105 at the access management layer 107. Figures 2 through 4 illustrate the distributed architecture with suggested functional service components. The main focus of interest is on the functional service components at the LSF 106/NSF 108 network layer and the Radio Access Network Layer 102. Figure 2 identifies the core functional service components associated with the LSF 106/NSF 108 network layer. Figure 3 identifies the access interface and access management specific functional service components. As shown in figure 2, the WAG functional components 200, 202 provide the bridge function between the local service layer 106 and the access management service layer 100.

[0078] Now referring to figures 1 and 2, the WAG component 101 that is attached to the LSF network 106 represents the access gateway point for the technology dependent functional components. Multiple access gateway points 202 can be attached to the LSF network 106. This provides flexibility in network scalability. The detailed functionality of the WAG components is represented by the Access Management Layer components 100 and shown in figure 3. The LSF 106/NSF 108 service layer functional components on one side of the WAG provide the application specific controlling functions. The access side 104 of the WAG provides the technology dependent access functions.

[0079] The access points 200 and 202 shown in figure 2 as the Wireless Access Gateway, separate the network in two distinct layers. First, the LSF106 /NSF 108 network layer that consists of common core functional service components required for telecommunication network. Second, the Radio Access Network layer that is partitioned into Access Interface Layer (AIL) 104 and Access Management Layer (AML) 100 consists of access interface and access management specific functional service components. Through out the description of the preferred embodiment, an access point that is attached to the LSF 106/NSF 108 (core) network layer is referred for wireless access point. The separate access point is required because of the different air technologies used for wireless access. Likewise, any other technology such as a wireline telecommunication system or a LAN based system can be attached to the LSF/NSF network layer. For different types of access points attached to the core network, the appropriate corresponding controlling core functional service components can be added and configured into the network.

[0080] The LSF/NSF service layers provide the core network functions. Some of the core network functions are listed in Appendix B. Depending on the scalability requirement of the network, the functional service components within the LSF 106 and NSF 108 network layers can be distributed or consolidated based on the desired hierarchy.

[0081] The access management layer 100 as shown in figure 3 provides the controlling functionality relevant to access management and RF management activities. Please note that the RF management activities and access management activities are part of the Radio Access Network layer 102. However, only RF management activities are closely coupled with the AIL 104 and access management 100 activities are closely coupled with the core network. Thus, it is possible to separate the access management activities from the RAN layer. Another major activity is the connection management function. The RAN also provides other associated functions such as local decision making domain specific database, resource control for radio resources, transmission facilities associated with the connection management function, and network management activities. These functions are illustrated in more detail in figure 8. The RF management function of the AML interfaces with the AIL service components and service components within the AML. It performs functions such as channel management, resource management at the AIL level, and policy decision functionality with respect to the AIL needs. The access management functions of the AML interfaces with the core components towards the network side and service components within the AML. The major access management function includes the ingress and egress activities that take place through the access point. Figure 8 shows distributed access management functions. The 'Access' function 800 provides ingress activities, while 'Termination' 802 and 'Paging' 804 functions provide an egress activities. The layer 3 protocol signaling messages between the mobile host and the serving network received at the AIL are distributed to the pre-configured functional service components. The layer 3 protocol

BNSDOCID: <EP_____1098490A2_I_>

signaling accomplishes basic inter-working activities with the terminal device. Some of such activities include mobility management activities, location updating, radio resource selection, power control adjustments 806, and channel assignment and reassignments. Also, it may include network layer (L3) originated call control and supplementary services as traditionally used in legacy mobile systems. The AML components are pre-configured to communicate with the AIL components and tunnels appropriate signaling and data information.

The AIL components provide the radio access functions.

[0082] Now referring back to figure 1, the AML 100 is the dividing point 103 between the core network 105 and access dependent controlling functions 102 and 104. The components within the access management layer 100 take the role equivalent to the policy enforcement while the LSF 106/NSF 108 (core) service layer components provide the role equivalent to the policy decision. In order to expedite the policy decision and also to take advantage of the distributed infrastructure, the WAG (the access point attached to the LSF network) domain database is considered at the AML, which facilitates the policy and subscriber related default parameters and access related status information.

[0083] The functionality of various functional components in each service layer is out of the scope to describe in the description of the preferred embodiment. However, Appendix A provides a brief description for some of these components. The access management functional component as shown in figure 3 plays an important role in providing call/session management services. The distribution of access management component functionality along with other AML components is described in figure 8. The access management component performs ingress and egress activities. Logically, access management functions can be further distributed into access (origination) function for ingress activities and termination 802 and paging 804 functions for egress activities. These functions can be physically located in a single (access management) server 800. However, they can be distributed in different servers as they provide distinctly independent functionality. These functional service components are capable of sending/receiving application level messages (from/to user) as well as layer 3 protocol messages over IP (from/to AIL) that take place between the mobile host and the serving network. The detailed functions of these components are described later. However, a brief description is provided here to establish context.

[0084] The access management 800 of the AML takes the role of user agent in the network domain. Within the access management function 800, the access function takes the role of user agent client. With respect to the call/session management service perspective, this functional component handles ingress activities such as registration and origination. Similarly, the termination function 802 takes the role of user agent server and provides the proxy functions for egress activities. The paging function 804 is the further distribution of the egress activities that is associated with the users at the cell level 808. The location-tracking function (defined as handoff function later) handles handoff activities. The location-tracking function interfaces with the LSF service layer component - mobility manager for periodic location update, and inter system (WAG to WAG domain) and inter network domain controlling functions such as handoff.

Interfaces between network entities

[0085] The functional service components are distributed in appropriate network service layers as shown in figure 2 and figure 3 that interact with each other using various interfaces. Although the logical interface model is not shown in the figures, the lower layer (L1-L2) interfaces (shown in figure 5) are assumed to be Ethernet. The interface at the transport layer is either TCP or UDP that is based on the delay sensitivity and reliability requirement. The "other" in figure 5 indicates the support of application level framing (ALF) and support of timer associated with transport layer protocols in order to enhance transaction level capabilities such as controlling congestion and canceling transactions. Application layer protocols are text based and based on the currently being defined Internet protocols.

[0086] The logical interface model includes primary control and data path interfacing to the Wireless Internet. Unlike the LAN based application interfaces in most interfaces mentioned in this model, the air link interface is a specific interface. The mobile host interfaces at the serving network on the technology dependent air interface uses network layer protocol messaging. The radio access interface layer, as shown in figure 3, terminates the network layer air technology dependent messages. Based on the type of messages received at the access interface layer, they are distributed to the pre-configured functional components at the access management layer. Detailed procedures are explained later in the description of the preferred embodiment.

[0087] Although the details of the Mobile Terminal Layer are not discussed much in the description of the preferred embodiment, figure 4 shows an example of how the functionality of the mobile host can be separated into two layers: a wireless interface layer and a mobile application layer.

BNSDOCID: <EP_____1098490A2_I_>

Application inter-working

[0088] Figure 5 depicts the protocol layers and interactions between network entities. It establishes the main context for application interactions between various network components. It shows the protocol interfaces between OSI layers that inter-work to accommodate air interface and LAN based connectivity. The description of the preferred embodiment only focuses on activities that take place above the transport layer in case of LAN based architecture and at the network layer in case of air interface.

[0089] The following sections describe the interactions between mobile host and access network components, mobile host and local serving function components, and mobile host and home network components.

Interactions between mobile host and access network

[0090] The Access Management Layer and the Access Interface Layer are the part of the Radio Access Network. The AML service components provide the access dependent control functions. The technology dependent network layer (L3) protocol terminates at this point. The AML service components are logically distributed into different functions as shown in figure 8. A signaling distributor between AIL and AML distributes messages to the pre-configured functional components (servers). With respect to the call/session management services, the access, termination and paging functions play an important role. These components interface with the LSF service components in order to provide services to the AIL and the mobile host. The LSF service components interface with the NSF service components in order to provide services to the access management components.

[0091] The following interactions occur between the mobile host and the access management service layer:

[0092] The AML components interact with the network layer of the mobile host to establish an access session. (L3/IP between AIL and AML)

[0093] The AML components interact with the AIL components to bring the mobile host on the traffic channel.

[0094] The AML components interact through the connection management component to establish point to point protocol path that allows the mobile host to access any other IP capable devices.

[0095] The network preferred call/session control services are handled through the access management components.

[0096] Handoff, power control, and paging functions related handshakes with the mobile host are controlled by the AML components.

[0097] Interactions between mobile host and CN/LSF network service components

[0098] The LSF network service components provide specific services to the access management components during establishment of an access session and service session with the mobile host.

[0099] The subscriber management and policy decision services are provided during an access session establishment with the mobile host.

[0100] The policy decision services are provided during user session invocation.

[0101] Intranet services are provided by the LSF service components through the specialized application servers.

[0102] Interactions between mobile host and CN-NSF/Global network Service components

[0103] The NSF network service components provide services to the LSF network service components during establishment of an access session with the mobile host.

[0104] The subscriber management services are provided during an access session establishment with the mobile host.

[0105] Facilitate to publicly available server accesses.

[0106] Direct home network accesses.

[0107] Interactions between network service layers

Inter-working between service layer components

[0108] The access management layer components and the LSF/NSF service layer components are the main network components that play the significant role in controlling call/session management. The functional components within an access management layer are the edge components through which mobile users in a area accesses the core network for access establishment service, service session invocation service and intranet services or external network access services. The AML is comprised of many distributed functions. These functions are explored in subsequent sections including access (Origination: User Agent Client), termination (Termination: User Agent server), protocol servers (optionally at AML but not at LSF service layer), power control, resource control, handoff, paging, and connection management (Transport Network). The functions within LSF/NSF network service layer include service broker, session server, payload mediation, and AAA+ (accounting, authorization, and authentication) servers. The components are described in greater detail later.

BNSDOCID: <EP_____1098490A2_I_>

[0109] How these components interact with each other as well as with end user and establish an access session, service session and transport session is also described later in the text. The access function facilitate to establish an *access session* that interact with the mobility manager to provide the functionality and the context needed to grant and support the user in accessing NGWN - Wireless Intranet services. Typical access functions performed by the network domain include an establishment of an authentication, authorization, usage selection, and usage constraints. At the end of establishing access session, the serving network is configured and provisioned with the subscriber's profile to provide appropriate access role, and usage role to the end user. Further, appropriate access functions are instantiated within the access management layer that interacts with mobile host to facilitate service session invocation and monitoring usage functions of the network resources. These instantiated functions interact with the session and accounting servers during the service session. The access functions within the AML take the role of User Agent in the network domain.

[0110] The session server component of the LSF/NSF network service layer facilitates establishment and maintenance of a *service session*. It provides the functionality needed to satisfy end users' request for desired services. The functional components within the LSF/NSF network service layer provide services to the access management layer and to the end user in establishing functionality and context involved in the negotiations of parties, configuration and QoS to be associated to the execution of a service. These services are unlike the call model services that facilitate in establishing connection-less or connection oriented call/session.

[0111] The AML of a particular domain must establish an association with the session server of the LSF/NSF network service layer in order to provide call/session services to a mobile. It is possible for the AML to have association with multiple session servers. However, the AML must associate with a single session server to complete initiated transaction. It is also possible to have many transactions during call/session establishment. During each transaction the AML may use a different session server. This implies that the AML maintains call/session states.

[0112] The session server provides services such as address translation, location service, and bandwidth management and admission policy control. It interacts with the AML for instantiated access functions to provide desired call control and other session services to the mobile host.

[0113] The session server is capable of accessing any of the AML components. This enables the session server to update the domain specific local database within the AML, monitor resources and achieve flexibility (optional) to manage connections for traffic. Updating local domain database provides necessary intelligence to the AML components to perform default capabilities quickly and efficiently. Also, the session server uses services from home (global) network components (NSF) for the purpose of authentication, authorization, accounting, policy related decisions, and globally provided services. The session server performs the function of redirect server in terms of SIP context (SIP Session Initiation Protocol - RFC 2543) or similar to gatekeeper function in terms of H.323 context for the call/session control services.

[0114] The connection management component of the AML provides the function of establishing *transport session* that establishes an end-to-end virtual connection, and handles multi-point and multi-media connections. It interacts with the session and accounting servers for policy and usage monitoring and reporting functions.

Call/Session management specific: components, services, and procedures

[0115] This section describes call/session management relevant functional service components within each network service layer and services and procedures that establish access session and transport sessions. The service components within an access management layer of the RAN layer and service components within the local service layer of the LSF/NSF network services layer plays an important role in providing call/session management services.

Access Management Layer (AML) components

[0116] The AML functional component position is between the radio access interface layer and the core network components as shown in figure 1 and figure 7. The AML component performs controlling and policy enforcement functions. It controls activities that take place at the access interface layer. Also, it controls interface activities associated with the user during access session establishment and service session invocation. It controls connection management activities that establish and monitor the point to point and point to multi-point virtual packet channels.

[0117] The network and user specific preferences are executed here based on the policy decision provided by the LSF/NSF network layer service components. The local domain database is updated with limited relevant information during access session establishment and service session invocation that expedites real time critical policy decision execution. For an example, an origination request arriving at the access management server examines the requested bandwidth with the allowed default permission through the local domain database. If the requested bandwidth matches with the allowed default, an access management server facilitates the requested bandwidth through the resource control function of the AML. If the requested bandwidth is other than default, an access management server may consult

BNSDOCID: <EP_____1098490A2_I_>

with the session server to take further action.

[0118] These functions can be physically distributed in different servers within the AML as network capacity demands. The AML functions (i.e. components) are pre-configured with the local service layer components to provide services to the mobile host during access session establishment. Additional components are instantiated and configured at the end of access session establishment. This is done based on the capabilities granted to the users and network capabilities to provide additional services.

[0119] Figure 6 illustrates how some of the components within each layer interfaces to some of the other components and is only meant to illustrate an example of the components described in detail throughout the description of the preferred embodiment.

[0120] Figure 7 illustrates the respective position of AML in Wireless Internet. Figure 8 illustrates the functional components within the AML. The functional components within the AML are pre-configured with a signaling router that interfaces between AIL and AML. The signaling packet to/from the radio access interface layer arbitrates at the signaling distribution function of the AML and distributes to the pre-configured AML components based on the type of signaling (e.g. related to call/session processing, mobility management, supplementary services, radio resource, etc.). An access function plays an important role in ingress direction while termination and the paging functions play an important role in egress direction. The access function takes the role of user agent on behalf of the end user. An access function involves in initial dialog with the mobile host. At network layer, the mobile host communicates with the access function using network layer messages. Intelligence at the access function uses local domain database in performing default services. For higher-level policy decisions, it accesses the session server at the LSF network service layer.

Activities of the AML components are described below:

[0121] **Access function** - Access function takes care of ingress related call/session management activities. These activities include registration and origination. An access function is the first signaling termination point with respect to ingress call establishment. It executes the policy enforcement functions. The access function of the AML takes the role of a user agent in a serving network. It interfaces with the mobile host to provide access session establishment service. During initial registration, it interacts with the mobility manager of the LSF network layer component that facilitates the subscriber management services. Upon successful completion of the subscriber management services through the mobility manager, the local domain database is updated with user and network preferences. The local domain database provides the local decision point functions. This expedites the domain specific activities during service session invocation and through out the active access session.

[0122] Further, an access function facilitates the establishment of a traffic path (establish PPP link) between the mobile host and the connection management component. The purpose of this action is to establish an access session between the mobile host and the serving network. The access function of the AML does this in two steps. First, the access function interacts with the RF management (resource control as shown in figure 8) component to bring the mobile on a traffic channel. Second, the access function interacts with the connection management component through which the PPP protocol messages handshake to establish IP address service point at the mobile host. The mobile host can negotiate the choice of IP address to be used; either network provided or mobile provided. This establishes the transparencies between the mobile host and the serving network. The access function informs the session server of the LSF network layer about the completion of the access session.

[0123] At this point, the session server has direct addressing capability to the mobile host to provide user capabilities and network preferences. Based on the usage and preferences granted to the mobile host, an appropriate service session manager function is instantiated within the access management layer domain. The user application interacts with the service session manager for service invocation and network service requests.

[0124] The access function takes the role of either user agent client or user agent client proxy depending on the need that is based on the capability of the mobile host. Please note that access function implies that the activities may be provided by an instantiated session server manager or handed over to the appropriate protocol servers. When the mobile host is capable to control call/session-handling activities, the mobile host takes the role of user agent client. The access function provides the role of user client proxy if requested. The mobile host has choice not to use access function as client proxy and may contact any desired client proxy or directly to the end user agent server. The mobile host keeps track of state machine. If the mobile host requests to the access function to aid in further call/session-handling activities, the access function takes the role of user agent client proxy. In this case, the access function is taking role of client proxy may interacts with the session server that provides the role of redirect server. Also, the access function can play role in two possible modes. First, an idle mode in which it provides call/session-handling transaction services when requested but do not keep track of call/session state machines. Second, an active mode, in which access function provides call/session-handling transaction services and keep track of call/session state machine.

[0125] When the mobile host is not capable of handling call/session activities, the access function receives request from the mobile host. The access function takes the role of user agent client, interacts with the session server for

BNSDOCID: <EP_____1098490A2_I_>

admission control and policy decision if required. The access function performs the outgoing call/session activities. The access function keeps track of state machine.

[0126] Termination and paging function - Termination function handles egress activities related to the incoming service session (call control activities) requests. Why do we need the termination function? In an IP environment, with the fact that each IP capable mobile host is addressed by a specific IP address, an external caller when trying to reach a mobile host in a Wireless Internet, it can reach directly without any intervention from the wireless access. However, this is only true when the mobile host is attached to the serving system using its permanent IP address. Because of the transient characteristics of the mobile host it is more suitable to assign a domain specific IP address within the Wireless Internet. In this case, once the domain specific address is made globally available by linking with the mobile host's home then the external caller only needs to find domain specific termination-proxy server. The termination-proxy server associates the current location of the callee within that domain with the current paging server (user agent server).

[0127] Thus, the termination function acts as a user agent proxy server for the user agent servers associated within the AML (notice cloud shown in figure 8). The termination function provides the first signaling termination point with respect to egress call establishment. It executes the policy enforcement functions. The local domain database provides the local decision point functions. This expedites the domain specific activities during termination service session establishment. The termination function interacts with domain database to get information for handling incoming request. If the end-user is not recognized, it interacts with the session server of the LSF component to take further action. In terms of SIP context (SIP RFC 2543), the session server performs function similar to the redirect server. Similarly, in H.323 context, the session server performs function similar to the gatekeeper. The termination function uses services from the session server and mobility server of the core network for various services that may include authentication during termination, current location information and policy-related decision.

[0128] If the end-user is recognized (i.e. registered within this domain) and the requested service is allowed, the termination function directs the request to the appropriate paging function (user agent server) to page the end-user or activate the traffic path from either standby or dormant mode. The paging functions (user agent servers) are associated with the unique cells within the access management domain serving area. The paging functional component keeps track of the call/session state machine as it is acting as a user agent server on behalf of the mobile host.

[0129] The termination and paging function interacts with the RF management server (resource manager) to establish a radio link connection. As mobile host is attached to the serving network, a domain specific IP address is already assigned. So in terms of SIP context (SIP RFC 2543), this IP address is returned in the contact header when returning response to the INVITE message. The termination or paging function interacts with the connection management function to establish a transport session.

[0130] Protocol servers (or functions) - The access management functions are closely coupled with the protocol servers or functions. The protocol functions are the different code points within the system specific to the type of protocol (such as SIP, H.225, H.245, RSVP, MPLS, etc.) used for the specific activities (such as session establishment, quality of service request, secure virtual path establishment, mobility specific, etc.). These functions can be part of the access management functions and instantiated for each service session invoked. Or, these functions can be separated in different servers and access management functions can hand over the specific requests to these servers as needed. The role of these servers varies depending on the type of protocols. For an example, in SIP context, such server provides functional role as proxy server. Similarly, in H.323 context, such server provides functional role as H.323 gateway.

[0131] The location of these protocol functions or servers is not appropriate at the LSF network layer as they are closely coupled with the access management activities. For the simplest network hierarchy, these functions or servers can be associated with one WAG (access point) domain. As network scalability increases, i.e., additional access points are added, other access points can access these servers established at a single geographically convenient location. Alternatively, it is possible to locate these protocol servers along with other Intranet application servers.

[0132] Once access management hand over request to the appropriate protocol servers, these servers create direct links with the end user and takes the responsibility to interact with the connection management functions to establish appropriate transport session.

[0133] Connection management function - The connection management function is the part of the AML component. It provides the third and final phase of the call/session management services that facilitates in establishing transport session. It receives transport session establishment request from the access (user agent client) function or instantiated session service manager during the outgoing service session establishment. Similarly, the termination (UAS proxy server) and/or paging function (user agent server) requests transport session establishment during incoming service session establishment. Based on the request, the connection management function facilitates to establish the point to point or point to multi-point virtual packet channel. The connection management function monitors and records usage activities. Like session service manager, the connection session manager is instantiated for each transport session establishment. The connection session manager for the transport session takes care of providing required quality of service and use of appropriate network infrastructure as described earlier.

BNSDOCID: <EP_____1098490A2_I_>

[0134] **Configuration Manager** - the configuration management function at the AML service layer facilitates reconfiguration of AML service layer components. It also facilitates location tracking (handoff) with addresses of neighboring location tracking components that are used for handoff activities during movement from one AML to another AML.

[0135] **LSF/NSF network service layer components** - There are many functional components that are involved in providing call/session management services. However, only some of these are significant for the purpose of the description of the preferred embodiment and described here.

[0136] **Session server** - The session server is one of the call/session management service components at the local service layer. The primary function of the session server is to interact with the AML service components to provide call/session management services. More precisely, it interacts with the access function and the termination function within the access management server of the AML service layer. Also, it interacts with the connection management function at the AML for usage monitoring and recording purpose. Once the access session is established between the mobile host and the serving access network, the access function interacts with the session server. At this time, the session server may configure the mobile host with available network preferences and users granted capabilities. Also, the session server provides important IP addresses to the mobile host (possibly using html) that can provide value-added services. The call control services are some of the many other services the mobile host can invoke. The session server at the LSF service layer along with access and termination functions at the AML service layer provides most of the call/session control services. The typical functions facilitated by the session server includes address resolution, call/session admission control, policy control decisions and access accounting control.

[0137] Other issues such as address translation and finding terminating proxy servers are not explored here. However, it is important to mention that the session server is assumed to perform functions similar to the redirect server identified within the SIP component definition (SIP RFC 2543). An identification of functionality for admission policy control and bandwidth management is the challenge with respect to the 3rd generation infrastructure. In addition to these, the role of session server in providing location-based applications and its interactions with the mobility manager server is also a challenge. These issues are differed at this time.

[0138] **Database management (directory services)** - The call/session functions related to a subscriber are typically based on the subscriber's profile. Such information in wireless network is typically centrally located at the subscriber's home NSF layer or at global level. In order to take advantage of the distributed network, subscriber's profile and related information need to be distributed in appropriate domains. Such distribution should be to a level where access point dependent components (e.g. session server, MM server) and radio dependent components (e.g. functional components within the AML) can take necessary decision independently. Such distribution will expedite the call/session processing and reduce the lengthy delay involved in accessing centrally located database and hence improve performance.

[0139] **Call/Session management services** - The ultimate objective of the Wireless Internet is to provide the end user an access through the network, provide choice of user desired services (Intranet or external Internet, etc.), and finally, the control and monitor capability for network resources used. The call/session management services facilitate these objectives. Three basic functions were briefly identified earlier. These functions are listed in the following paragraphs again.

Establishing an access session between the mobile host and the serving network

[0140] The establishment of an access session facilitates the mobile host to attach to the serving network. During the establishment, subscribers' are authenticated and granted for requested or default bandwidth with desired quality of service. The local decision point within the access management layer is updated and appropriate service components get configured. Once the access session is established, the mobile host becomes IP capable enabling access to/from any other device. The access session remains active at all times as long as the mobile host remains attached to the serving network.

An invocation of a service session by the end user

[0141] The user can invoke a service session. The call/session control service is one of many services that the user can invoke. The session server at the LSF service layer facilitates the call/session management control activities. At this point network becomes capable of providing basic call/session control services. However, the network is also capable of providing simple to complex services.

[0142] The user is provided with user capabilities and network preferences to use desired services from the serving network or access external services. Based on the user capabilities and network preferences with respect to the type of user, the network configures itself to respond to the user service invocation.

[0143] For example, in the management of basic call/session control services, the session server manager is instantiated at the access management layer that provides the user interface for call/session control services. While at the LSF service layer, instance of a session can be created at the accounting server to handle accounting activities for

BNSDOCID: <EP_____1098490A2_I_>

any service session. Similarly, for any other service, the appropriate session manager can be instantiated to respond to that specific desired service. The application servers are configured at the LSF service layer.

[0144] This allows the ability to keep access relevant activities coupled with the access dependent service layers, and policy decision making activities at the access independent layers. Also, this allows flexibility to provide mixture of independent services and add new services.

Facilitating network resources to establish point to point or point to multi-point virtual connection

[0145] Distinction between the call/session control services and other applications/services is emphasized throughout the specification for clarification purposes. The call/session control services are the part of the access management services that facilitate establishing point to point and point to multi-point virtual connections.

[0146] **Access session establishment** - The mobile host establishes point of attachment with the serving network. The mobile hosts on power up or during idle state periodically sends registration or location update request to the serving network. The access interface layer components facilitate an air link communication with the mobile host. Upon receiving registration request, AIL distributes it to an access management server component within the AML. The access management server consists of many functions. They are identified in figure 8. They are access, termination and paging functions. These functions have independent functional role and can be separated in different servers if network capacity demands. In this section when access management server is referenced implies an access function of the access management server. The AIL distributes signaling information to the appropriate servers depending on the type of signaling. Optionally, such distribution can be implemented at the AML.

[0147] Now referring to figure 9, the access management layer processes the registration request 900. The domain database 902 within the AML provides the local decision point to the AML components to make primary decisions. The access management server 904 checks with the domain database 902. If the mobile host 906 is already registered, mobile host's current location is updated. If the mobile host 906 is not active within this domain, the access management server sends REGISTER request to the LSF service layer component - mobility manager 908. A SIP message, REGISTER is shown for examples that access management server sends to the mobility manager 908. It includes MIN or "user at domain" location information that identifies cell information.

[0148] Although the activities performed by the mobility manager 908 will not be described in great detail, a brief outcome of this activity is described here. This is the first step in establishing an access session between the mobile host and the serving network. The mobility manager 908 receives the REGISTER message. This indicates that the subscriber needs to be authenticated for access and authorized for the requested services. The mobility manager performs this task with the help of other LSF service layer components such as AAA+, directory services, DHCP, and policy server. If the mobile host is active within the regional serving domain, the LSF service layer components provide the service functions. I.e., an authentication is done through the local AAA server, an IP address assignment through the DHCP that is suitable to the AML domain, and subscriber's default profile is updated at the AML domain database as well as at the regional domain.

[0149] Once the authentication and authorization process is complete, it is assumed that the RAN is authorized to provide access to the mobile host. Now referring to figure 10, first, the access management server 904 interacts with the RF management server 1000. The access management server 904 instructs the RF management server 1000 to assign a traffic channel. The RF management server 1000 interacts with the access interface layer components and facilitates the sending of appropriate air link messages to the mobile host. The RF management server 1000 notifies the access management server 904 once the mobile host 906 establishes the traffic channel. At this time, data link connectivity is achieved between the mobile host and AIL. Second step is to establish PPP connection between the layer 2 of the mobile host and the connection management server 1002.

[0150] The access management server 904 then starts to interact with the connection management server 1002. First, it establishes the co-relation between traffic channel and assigned IP address at the connection management server 1002. Now referring to figure 11, the access management server 1002 handshakes configure/response layer 2 PPP connection messages with the layer 2 of the mobile host through the assigned IP address at the connection management server 1002. At the mobile host 906, layer 2 establishes an IP address service point link with the layer 3 (IP layer). During this handshake, the mobile host 906 accepts the network assigned IP address or provides a desired permanent IP address instead. In case of the latter, the access management server 904 reconfigures the connection management with a new IP address and also updates the appropriate hierarchical databases.

[0151] At this point, an access session is established between the mobile host 906 and the session server 1200 at the serving network as illustrated in figure 12. The application layer at the mobile host 906 becomes IP capable and can access any IP addressable device. The air link at the layer 2 is in the active mode. This link remains active for a pre-determined time that is based on the MAC layer specification. With no activity on air link, active status of this link changes to standby mode, and later goes to the dormant mode and then the traffic channel gets released. However, the established access session at the access management service layer remains active. This access session remains

BNSDOCID: <EP_____1098490A2_I_>

active until association of the mobile host is removed or deleted at the access management layer. When any data activity happens, either from the mobile host or from the access network, the air link turns from dormant mode to the active mode.

Invocation of service session

[0152] Now turning to figure 13, once the mobile host 906 establishes point of attachment at the session server 1200 within the serving network, the mobile host 906 becomes capable to invoke any services. The mobile host 906 can access any IP addressable device. The serving network can help provide locally or globally available services. The serving network becomes smarter and configured to provide services to the user. The default parameters are configured at the local decision points at appropriate domain levels.

[0153] At this time the network is capable to provide basic services. However, the network is capable and flexible enough to provide more complex services. A brief discussion is provided here for reference and will be explored later.

[0154] The serving network provides user capabilities and network preferences to the user. The user capabilities were determined during access session establishment as a result of executing subscriber management services. The network preferences based on network capabilities are pushed to the mobile client 906. Such preferences may include a choice of invoking different type of call/session control services (voice, data, multi-media, etc.) or value added services (Intranet services, location-based services, etc.). More over, the serving network can provide a choice to the mobile host of using the serving network as an ISP provider, or for other possible options. Some of these options are illustrated on screens 1300 and 1302 in figure 13.

Establishment of transport session

[0155] Based on the type of service session invoked, the service session manager (please refer to discussion on service session manager) notifies the connection management function to establish a virtual packet channel path. The connection session manager is instantiated by the connection management function that establishes appropriate network resources to establish requested transport session. The connection management function isolates activities from the call/session control activities. For example, it hides the underlying network topology and supports the inter-working between network layers. Based on the quality of service requirement (which is discussed below), the connection management function facilitates establishment of a path ranging from no packet control to fully dedicated virtual packet channel path. It may use different techniques to achieve the required quality of service. These techniques may include use of MPLS, RTP/RTCP, RSVP as well as other schemes. The quality of service requirements may include the following: bandwidth reservation for a data path (possible use of RSVP); end-to-end latency guarantees through the optimized IP network (possible use of MPLS); network infrastructure selection such as IP or ATM backbone (Layer 1 & 2 selection); protocol selection such as MPLS, RTP/RTCP, RSVP (based on quality of service requirements); and acceptability of loss of data (possibly establish limits on acceptable vs. unacceptable loss based on type of transport session established, such as voice, audio, video, etc.)

Call/Session procedures

[0156] The call flow procedure described here uses several scenarios to outline involvement of access function. However, certain assumptions are identified in the following paragraphs.

[0157] The Mobile host should be IP capable. For example, once the mobile host is attached to a wireless access system, the mobile host can reach any IP addressable device, server or end-user directly and transparently through the network. Also, any external user or device can reach the mobile host transparently through the network.

[0158] The mobile host can seek network services for call/session establishment or dynamic change in resource allocation using standard application protocol such as SIP or RSVP.

[0159] The RAN is IP capable. Particularly, the service components within the RAN; AIL and AML are IP capable. The PPP link is established between the mobile host and connection management component of the AML. The router between the AIL and AML will arbitrate the signaling and traffic packets before forwarding to the pre-configured IP devices of the AML components. This arbitration can be done at the AIL or at the AML depending on the choice of implementation.

[0160] The functions of the AML components are distributed based on the required function. Such functions include access, termination, handoff (location tracking), paging, power control, RF management (resource control), configuration management, and connection management. Also, local domain database for local aspects is used. It provides subscriber dependant data and local policy decision parameters for system dependant data. Alternative to these local aspects, global aspect entities such as AAA+ server and Policy Decision Point (PDP) can be accessed from the core network respectively.

BNSDOCID: <EP_____1098490A2_I_>

[0161] The AML components require assuming responsibility for the end-user as a User Agent Client and User Agent Server in an ingress and egress direction respectively.

[0162] The AML component interfaces with the core network when necessary. The core network components provide either redirect server function or value added service function to the access function.

Call/session general overview

[0163] The AML service components and the session server are the main network components that play a significant role in call/session management. The AML components are the edge components through which a mobile host in an area accesses the core network for Intranet services or external network for third-party network services or publicly available Internet services.

[0164] Thus, the AML components provide the access function. The access function establishes the functionality and the context needed to grant and support the user in accessing NGWN - Wireless Internet services. The functionality of access management server component within the AML takes the role of user agent in the network domain. Please refer to discussion on each service component.

[0165] The session server provides the call/session service function. The session server provides services to the user agent in establishing functionality and context involved in the negotiations of parties, selection of functional protocol components, configuration and QoS to be associated to the execution of a service. These services are unlike the call model services that facilitate in establishing connection-less or connection oriented call/session. Thus, the session server receives a request from the user agent and satisfies the service need. Upon access initiation or registration, the access management server component of the AML takes the role of user agent on behalf of the mobile host and interacts with the session server in establishing the requested need or service. Upon establishment of an access, appropriate network configuration takes place to serve the mobile host for its default services and network capabilities. In the process, the session service manager is instantiated that interfaces with the mobile host that satisfy the service request such as dynamic change in QoS. Please refer to the section discussing the session server.

[0166] The architecture vision is such that service requests will be facilitated appropriately by the AML components. The service session manager and transport session manager is instantiated by the access management server during access session establishment. These components provide the interface point and satisfy the end users' need and requests.

[0167] Upon terminal registration (e.g. at power up), the mobile host gets control of the radio channel and engage with a specific serving RAN in an area. The mobile hosts send registration messages to the RAN that appears at the associated access management service components. For an example, in case of a CDMA technology, a network layer IS-95 origination message is received from the mobile host to the network access interface. The AIL sends this message to the associated AML using HDLC protocol or simply in IP packets using Ethernet. The signaling IP packets are received at the edge router between AIL and AML. This router arbitrates the type of message and distributes to the appropriate AML components such as access management server, power control server, or handoff server. It is assumed that the IP security is established between AIL and associated AML, and also between identified network layers. The signaling arbitrator is configured with the appropriate IP addresses of the AML components and core network components. Thus, access related messages will be forwarded to the access management server, handoff and mobility related messages will be forwarded to the handoff server, while power control related messages to the power control server, and so on. The data packets will be distributed to the connection management server.

Exemplary Functional Component Interaction Sequence Flow

[0168] Although the functions of related service components and their interactions are described earlier, figure 14 provides functional component interaction sequence flow. The following paragraphs describe a general overview for these sequences.

[0169] Sequence 1 is described as when the network layer (L3) of the mobile host sends the registration request (e. g. at the power up) to establish a point of presence at the serving network. The access function of the AML service layer receives this request.

[0170] Sequence 2 comes into play when the access function at the AML service layer communicates with the mobility manager at the LSF service layer. The mobility manager performs several functions for which it may communicates with other functional components at the LSF service layer and/or with NSF service layer in order to provide subscriber management services. In this process the mobility manager may communicate back to the mobile host through the AML service layer to authenticate the mobile host.

[0171] Sequence 3 gets traversed when registration is completed, the mobility manager facilitates to download information such as a subset of user specific default parameters and allowed service options to the AML domain database. Such information provides local decision point to expedite future service invocation procedures if necessary.

BNSDOCID: <EP_____1098490A2_I_>

[0172] The access function at the AML service layer communicates with the RF management server in sequence step 4. For simplicity, the RF management server is not shown in this figure. The RF management server performs procedure to assign traffic channel.

[0173] Sequence 5 designates informing the access function upon completion of traffic channel assignment.

[0174] The access function of the AML service layer communicates with the connection management server in sequence 6. It facilitates to establish relation between traffic channel and assigned IP address. Then, the access function negotiate with the mobile host at the layer 2 through the connection management server of the AML service layer to establish PPP connection and IP address selection. The mobile host may accept the network provided IP address or mobile host may provide its permanent IP address to use.

[0175] The mobile host communicates back to the access function of the AML service layer in sequence 7 indicating accepted IP address assignment. The access function facilitates the necessary changes relative to the selected IP address at the AML domain and/or at the LSF service layer database.

[0176] Upon establishing PPP link between the mobile host and the connection management server, the access function at the AML service layer communicates to the session server in sequence 8 to download necessary information to the mobile host.

[0177] The session server downloads necessary information to the mobile host in sequence 9. The information includes: end user's capabilities that derived as a result of providing subscriber management services during access session establishment, and network preferred preferences for which network is configured to provide optimum service. Also, the session server communicates with the connection management to provision default bandwidth and required quality of service requirement corresponding to the end user.

[0178] The sequence 10 indicates the service invocation by the mobile host. The sequence 10' (10 prime) indicates an service invocation (e.g. origination) form the network layer of the mobile host. In this case, with respect to SIP, the access function at the AML service layer provides the function similar to the user agent client (UAC). The sequence 10 indicates an service invocation from the application layer of the mobile host. In this case, with respect to SIP, the mobile host application layer provides the function similar to the UAC. Based on the end user invocation of specific use of service, the mobile host has multiple options: it can reach directly to the callee (destination end user, i.e., e.g. user agent server in SIP context); it can reach to the other domain network. In SIP context, it can reach to a user agent server proxy that can terminate to the appropriate user agent server; or it can reach to the serving network's provided appropriate protocol server. In SIP context, it can reach to the user agent client proxy. The user agent client proxy can facilitate the further action to provide necessary resources and forward service session establishment request to the callee.

[0179] If the user chooses to use network provided appropriate protocol servers, then the appropriate protocol server receives the service session invocation request in sequence 10A and 10'A. The protocol server communicates with the session server that arbitrates to the appropriate controlling entity. For an example, in SIP context, the user agent client proxy will communicate with the Redirect server. Likewise, in H.323 context, the H.323 gateway will communicate with the gatekeeper (GK). The other GW performs similar functionality provided by the user agent client proxy in SIP context or H.323 gateway in H.323 context. Such gateways may include PSTN gateway, and similar others.

[0180] Sequence 10B, 10' B is the response from the session server. The session server provides information that required to appropriately forward the service session request to the callee or to the destination.

[0181] Sequence 10C, 10' C indicates when the session server at the LSF service layer or the access function at the AML service layer communicates with the connection management server to allocate allowed bandwidth and provide selected quality of service for the transport session. Such allocation will be committed upon completion of the signaling negotiation between end parties.

[0182] Sequence 10D, 10'D is the forwarding request go out to the appropriate destination.

[0183] Sequence 11 designates when the forwarding request arrives at the user agent server proxy in SIP context, or at the H.323 gateway in H.323 context, then, such entities performs necessary functions to validate for admission control, identifying location of the end user and forwards request to the end user. Similarly, the other gateway will provide the same functions.

Protocol choices

[0184] The list of network preferred protocol preferences could be provided to the mobile host during access session establishment. The access management functions at the AML and the session server at the LSF network layer facilitate the end user with varieties of options based on the type of user's capability, subscribed options, and network preferred protocol preferences. Based on the choice of user invocation, appropriate protocol servers are accessed to establish service session. If the end user is not capable of selecting protocol options, the end user can access the access management functions. This is also a traditional way of handling request from the mobile host. The access management functions interact with the session server to determine the appropriate protocol function and facilitate the selected

BNSDOCID: <EP_____1098490A2_I_>

capability components that can establish the service session. The request is hand over to the appropriate server to establish service session.

[0185] This scheme provides the support of any protocol. For an example, the SIP (SIP RFC 2543) and H.225 (H. 225 - Call Signaling Protocols and Media Stream Packetization for Packet Based Multimedia Communications Systems) & H.245 (H.245 - Control Protocol for Multimedia Communication) protocol stack can be supported independently and transparently. Also, legacy protocols can be supported in the same fashion.

Wireless access scenarios

[0186] Two paths are illustrated in figure 15. The first facilitates control of the air 1500 and the virtual packet channel path 1502. The second facilitates signaling interactions 1504 with the core network to establish session and allocation of local resources. The two distinct channels through which traffic data flows are identified in the following paragraphs.

One through the air link and another through the virtual packet channel

[0187] The virtual packet channel 1502 can be established through all the routers along the data path using RSVP (following PATH - RESV signaling sequence between routers). Thus, the control of the virtual link and dynamic bandwidth changes can be obtained by using RSVP processed at each router along the data path. However, the control of the air link is not trivial. This is because of two reasons. First, the data transformation at the connection management 1506 does not distinguish data from signaling and thus, does not process the signaling protocol. The RSVP signaling is merely transported through the wireless access point to the end terminal. Thus, it becomes the end terminal's responsibility to interact with the access point to allocate or modify the bandwidth necessary for the air path. This leads to the second point where bandwidth adjustment requires a unique signaling handshake between the IP Mobile host 1508 and the AIL-AML interface 1510.

Control of session establishment and resource allocation

[0188] Within the wireless access point, the client agent for the end user performs several functions. Some of these functions include interactions with the core network 1512. The user agent (client 1514 or server 1516) performs the role of policy enforcement while the core network 1512 performs the role of policymaking decisions. Depending on the implementation choice, interactions related to the policy may be performed locally or at the core network 1512. It may be practical to distribute default parameters and the subscribers' allowed resource allocation at the time of registration to the local domain database. In this case the policy enforcement function that is a part of the user agent (access management server), performs decisions based on the local decision point (LDP) 1518.

[0189] IP capable end terminals 1520 can communicate with each other transparently. However, the wireless access point plays an important role in establishing the air link path. An intervention at the wireless access point can occur several times during the communication. These scenarios are identified in the following paragraphs.

Scenario 1

[0190] As shown in figure 16, the IP capable end terminals 1508, 1520 are in active state. Assume terminal A 1508 is attached to the wireless access side. Terminal B 1520 is somewhere else on the Internet. Terminal B 1520 sends an INVITE message directly to the terminal A 1508 using the currently used call ID to modify an active call/session with different quality of service parameters than what is included in the SDP. Terminal A 1508 needs to send a request 1600 to the access system to modify the established air link 1500.

Scenario 2

[0191] Figure 17 shows the case of a termination. When the distant client 1520 sends a message 1700, for example, an INVITE message, to the AML 1510, the message ends up at the user agent proxy server. The policy enforcement points and call admission control functions take place at the user agent proxy server. The user agent proxy server may need to access the subscriber related or the system level policy decision database. Such databases can be located locally or at some central location. The subscriber dependent database can be accessed through the local database 1518 (domain dB) for validity, profile check and current cell location if available or may be accessed through AAA server centrally located within the core network. Similarly, system level policy decisions such as allocation of subscriber requested bandwidth with respect to the availability can be checked by the proxy server by accessing local policy decision database or globally located database.

BNSDOCID: <EP_____1098490A2_I_>

Scenario 3

[0192] Figure 18 shows the call/session invocation request scenario. Though an IP mobile host 1508 is capable of establishing a call/session with another external device 1520 transparently without interaction of AML 1510, it is possible that in many cases the IP mobile host 1508 may request the AML 1510 to establish such a call/session. An example of such cases may include where a mobile host 1508 wants to establish a multicast call/session; it that case, it would request the AML 1510 to establish such a session. This is important mainly due to the bandwidth limitation of the air link 1500. The AML 1510 would facilitate the multicast of packets to as many sessions as needed. Another example is where trigger based services are incorporated that allow mobiles to invoke pre-established value added services offered by a local service provider or a local Intranet.

Scenario 4

[0193] Figure 19 shows the power up registration scenario. The power up is one case when the AML 1510 is accessed to establish an air link 1500 and establish access session. Once the air link 1500 is established, the mobile host 1508 can stay in active or dormant state. In any of these cases, the subscribers' profile is kept in a local database (domain dB) 1518. QoS policy and policy enforcement points are distributed in the access (user agent client) function for ingress and terminating user agent proxy for egress activities. Depending on the QoS requested, that include bandwidth requirements at the default level.

Scenario 5

[0194] Figure 20 shows the scenario where default parameters are used and no intervention is required. That means the mobile user 1508 can establish a session with an external user 1520 using default QoS parameters provisioned during access session establishment. In egress, the user agent proxy server will use default parameters to establish call/session with the user 1508 within the domain of AML 1510.

[0195] Figure 21 illustrates an example implementation of the architecture of the preferred embodiment. As shown, one access management layer 2100 can have one or more access interface layers 2102 and one local service function layer 2104 can have one or more access management layer 2100. In addition, local service function layer 2106 is also depicted with one or more access management layers 2108, which in turn have one or more access interface layers 2110. Additionally, the local service function layers 2104 and 2106 are shown to be connected to a network service function layer 2112 through either a LSF firewall 2114, the public Internet 2116 and a NSF firewall 2118, or through a private link 2120. The LSFs 2104, 2106 would use the private link 2120 if the NSF belonged to the same service provider and would use the firewalls 2114, 2118 if the NSF belonged to a different service provider.

[0196] Moreover, NSF 2122 is connected to NSF 2112 through a private link 2124, through a service level agreement link 2126 or through another NSF firewall 2128, the public Internet 2116 and the original NSF firewall 2118. Similarly to the LSF/NSF connections, the two NSFs 2112, 2122 would use the private link 2124 if the two NSFs belonged to the same service provider, the service level agreement link 2126 if the two NSFs had a service level agreement and the firewalls 2128, 2118 if the two NSFs belonged to two different service providers.

[0197] In addition, LSFs 2130, 2132, private link 2134, LSF firewall 2136, access management layers 2138, 2142, and access interface layers 2140, 2144 are depicted in the same format as the other components on the right side of figure 21 for simplicity purposes. However, the network could be arranged in countless ways and still withhold the relationships described above.

Conclusion

[0198] It is understood that several modifications, changes and substitutions are intended in the foregoing disclosure and in some instances some features of the invention will be employed without a corresponding use of other features. Accordingly, it is appropriate that the appended claims be construed broadly and in a manner consistent with the scope of the invention.

BNSDOCID: <EP_____1098490A2_I_>

Appendix A: Service layer functional components

This section elaborates some of the functional components that are distributed in network service layers. The definitions given here are of generic. However, relevant details to the call/session management services are described in the specification.

Policy management & Policy enforce server - The policy management server defines business and service concerns, and more precisely, policies for users and network devices. It distributes policies to the network devices to enforce the policies defined by the network administrator. It provides policy decisions to control network behavior provided to the user. The policy enforcers are respectively at the lower layer to the policy management at appropriate network devices. These devices communicate with the policy management server using COPS protocol. The policy relevant information can be distributed at the appropriate hierarchy network layer in order to expedite the real time critical decisions.

Authentication server - The authentication server is the core network component. The mobility manager facilitates the authentication process for the mobile host. The authentication server is reachable through the AAA+ server that provides the common protocol for Authentication, Authorization, and Accounting activities. The authentication function is provided based on the digital certificates/signatures.

Directory server - The directory server stores the user service profile and policy in a database. The directory server communicates with other network components such as policy management server using LDAP protocol. The directory server uses Directory Enabled Networking (DEN) scheme. The DEN scheme takes an advantage of information already stored in directories.

DHCP - In an IP centric NGWN – Wireless Internet, a mobile host must be initially assigned a specific IP address that is appropriate to the network domain to which the mobile host is attached. If the mobile host moves to a new network domain, a new IP address must be assigned. The Dynamic Host Configuration Protocol provides such mechanism through which an IP address is allocated to the attached mobile host. The mobility manager component of the LSF service layer facilitates this procedure.

DNS – NAI DNS - The Domain Name System is the software that allows name to

BNSDOCID: <EP_____1098490A2_I_>

number mapping. The name richweb is the 47.161.113.52 and vice versa. This is achieved through the DNS. The DNS is a hierarchy. There are small number of root domain name servers that are responsible for tracking the top-level domains and who is under them. The root domain servers between them know about all the people who have name servers that are authoritative for domains under the root. In the NGWN – Wireless Internet the DNS hierarchy is established based on the user's current location.

Mobility Manager - The mobility manager functional component is the part of the core network component. It facilitates to provide subscribers' management services during the access session establishment between the mobile host and the serving network. It also facilitates the inter-domain handoff activities.

Access Accounting server - The access accounting server is the core network component. The session server that facilitates to configure service session invocation, that also facilitates the instance for that service session at the accounting server to record the usage activities. The access accounting server is reachable through the AAA+ server that provides the common protocol for Authentication, Authorization, and Accounting activities.

AAA+ - The AAA+ server provides the common protocol access to the network clients to access Authentication, Authorization, and Accounting servers. Currently, the DIAMETER and RADIUS protocols are under evaluation for the AAA+ server access.

Network management - The network management functions at the different network layer hierarchy provide appropriate management functions. The management functions take care of business and service oriented concerns. Ideally these functions can be distributed to the core network for business decision (policy management) and service session related activities and at the AML for the network resources and transport session related activities. These functions include fault management, configuration management, accounting management performance management, and security management.

Call Server - The call server is the core network component. It takes the role of media gateway controller. It controls signaling gateway and media gateway components that interface with the PSTN.

Session server - Please refer to text above describing session server.

BNSDOCID: <EP_____1098490A2_I_>

Location tracking - The location tracking is the part of the access management layer component. It keeps track of the mobile host's location movement activities in the WAG domain. It facilitates the handoff activities between cells within the WAG domain. Also, it facilitates in inter-WAG domain handoff activities. The neighboring WAG domain information can be exchanged directly. It interacts with resource manager for the purpose of maintaining radio link and Care Of Address (COA) relationship. Also it interacts with the domain database server to update the end-user's location.

Power Control function - Power control function handles all power control related activities. It performs the necessary algorithm to manipulate special situations, which may occur due to interference or adjustment during the start of a call. It interacts with resource manager for the purpose of maintaining power level of the radio link.

Connection management server - The connection management server handles activities to establish virtual packet channel through the serving network. It gets instructions from the access management server. For each service session created, a transport session manager is also instantiated. The transport session keeps track of usage activities based on the instruction provided either per packet, per byte, time in active session, or flat time. It facilitates to establish point to point or point to multi-point transport session.

Access management server - Please refer to text above for access and termination-paging function.

RF management - The RF management server is the access management layer component. It facilitates the controlling function for the radio dependent activities. It interfaces with the access management layer components. Also, it interfaces with the access interface layer components.

BNSDOCID: <EP_____1098490A2_I_>

Appendix B: Core network functions

The LSF/NSF network layer consists of core functional service components required for telecommunication network. This section identifies the major core network functionality expected from the LSF/NSF network layer functional service components shown in Figure 2. Some of the core network functions are described in the following paragraphs.

Serving domain specific address assignment.

Policy decision based on subscriber's profile, assigned network preferences, and available network resources.

Network management control function.

Subscriber management services during access session establishment that at least include authentication and authorization.

Providing subscriber's capabilities and network preferences in serving end user.

Configuring appropriate application servers or facilitating functional service components based on the subscriber's default services or invoked services.

Usage data collection and accumulation of network resources and recording.

Handoff activities to support continuous mobility between multiple access points.

Claims

1. A method for a first user to communicate in an Internet Protocol (IP) centric distributed network with a plurality of service layers providing a plurality of functions associated with each of the service layers, the method comprising:

   accessing the network to establish a point of presence at an access management layer and a core portion of the network and to designate a default amount of bandwidth and a plurality of default setup parameters;
   invoking service through a session server on the network to establish an amount of network resources requested by the first user; and
   establishing a transport session to create and manage a connection from the first user to a destination address.

2. The method of claim 1 wherein the plurality of service layers includes a network service function layer.

3. The method of claim 1 wherein the plurality of service layers includes a local service function layer.

4. The method of claim 1 wherein the plurality of service layers includes an access service function layer.

5. The method of claim 3 wherein the local service function layer is independent of a specific access technology used for the first user to communicate to the network.

6. The method of claim 4 wherein the access service function layer accommodates a plurality of technologies used for the first user to communicate to the network.

7. The method of claim 1 wherein the invocating service through the session server includes providing a list of a

BNSDOCID: <EP_____1098490A2_I_>

plurality of functions available to the first user.

8. The method of claim 7 wherein the plurality of functions available to the first user are based on capabilities of the first user and a plurality of network preferences.

9. The method of claim 8 wherein the session server also provides addressing of any appropriate server to contact for each of the plurality of functions available to the first user.

10. The method of claim 7 wherein the session server contacts an accounting server through an Authorizing, Authentication and Accounting server and initiates an appropriate record of resources committed to the first user.

11. The method of claim 10 wherein the accounting server sends information to an accounting accumulator at the network service layer.

12. The method of claim 10 wherein the session server instructs a connection management server to record usage information according to resources used by the first user.

13. The method of claim 12 wherein the usage information includes at least one of the group consisting of: time used by first user, packets used by first user, flat rate for each access by first user or bytes used by first user.

14. The method of claim 2 wherein the network service layer includes a mobility manager that provides handoff services to the first user when the first user leaves the local service function layer for another local service function layer.

15. The method of claim 3 wherein the local service layer includes a mobility manager that provides handoff services to the first user when the first user leaves an access management layer for another access management layer.

16. The method of claim 3 wherein the access management layer includes a location tracking server that provides handoff services to the first user when the first user leaves a first cell in a first access interface layer for another cell in another access interface layer.

17. The method of claim 1 wherein a session server reserves any quality of service parameters and an amount of bandwidth requested by the first user.

18. The method of claim 1 wherein an access and termination function at an access management layer reserves any quality of service parameters and an amount of bandwidth requested by the first user.

19. The method of claim 1 further including sending communications from an application layer at the first user wherein an user agent client resides at the first user.

20. The method of claim 1 further including sending communications from a layer 3 at the first user wherein an user agent client resides at an access management layer of the access layer.

21. The method of claim 1 further including an user agent server associated for each of a plurality of access interface layer of the access layer.

22. The method of claim 1 further including an user agent server that acts as a gateway by converting incoming protocols of incoming communications to a protocol understood by the first user.

23. The method of claim 1 further including an user agent server that delivers incoming protocols of incoming communications to the first user when the incoming protocol is understood by the first user.

24. The method of claim 1 wherein the session server further provides admission control functions and address resolution to an user agent client and an user agent client proxy at a SIP protocol server.

25. The method of claim 1 wherein the session server further provides admission control functions and address resolution to a H.323 terminal and a H.323 gateway at a H.225 protocol server.

26. The method of claim 1 wherein the network includes a connection management server that can transport commu-

BNSDOCID: <EP_____1098490A2_I_>

nications on a plurality of backbone infrastructures.

27. The method of claim 1 wherein the network includes a connection management server that can transport communications on a point to point basis.

28. The method of claim 1 wherein the network includes a connection management server that can transport communications on a point to multi-point basis.

29. The method of claim 1 further including providing the requested amount of network resources by utilizing a connection management server that utilizes a plurality of protocols to deliver a requested quality of service for latency.

30. The method of claim 1 further including providing the requested amount of network resources by utilizing a connection management server that utilizes a plurality of protocols to deliver a requested bandwidth.

31. The method of claim 1 further including deciding policy parameters at a core network level.

32. The method of claim 31 further including enforcing policy parameters at an access management level.

33. The method of claim 1 wherein a plurality of access management layer components interact with a network layer of the first user to establish an access session.

34. The method of claim 1 wherein a plurality of access management layer components interact with a plurality of components to bring the mobile host on the traffic channel.

35. The method of claim 1 wherein a plurality of access management layer components interact through a connection management component to establish point to point protocol path that allows the first user to access any other IP capable device through a serving network.

36. The method of claim 1 wherein a plurality of network preferred call/session control services are handled through a plurality of access management components.

37. The method of claim 1 wherein handoff, power control, and paging functions related handshakes with the first user are controlled by a plurality of access management components.

38. The method of claim 1 wherein the first user interacts with a plurality of protocol servers and access management service layer components.

39. The method of claim 38 wherein the plurality of protocol servers and access management service layer components interact with a plurality of components at the local service function layer.

40. The method of claim 1 wherein a plurality of components at a local service function layer provide specific services to a plurality of access management components during establishment of an access session and service session with the first user.

41. The method of claim 1 wherein the accessing includes providing subscriber management and policy decision services for the first user.

42. The method of claim 1 wherein policy decision services are provided for the first user during user session invocation.

43. The method of claim 1 wherein Intranet services are provided to the first user by a local service function layer through specialized application servers.

44. The method of claim 1 wherein the first user interacts with a plurality of global network service components

45. The method of claim 1 wherein the accessing further includes a network service function layer providing services to a local service function layer.

46. The method of claim 1 further including providing subscriber management services during an access session

BNSDOCID: <EP_____1098490A2_I_>

establishment for the first user.

47. The method of claim 1 further including facilitating publicly available services.

48. The method of claim 1 further including facilitating direct home network accesses.

49. A communications network architecture for an Internet Protocol centric wireless network for a first user to communicate to a destination, the network comprising:

a plurality of network service function layers within the wireless network;
a first set of a plurality of local service function layers associated with one of the plurality of network service function layers within the wireless network;
a first set of a plurality of access service function layers associated with one of the plurality of local service function layers; and
a second set of a plurality of access service function layers associated with a second of the plurality of local service function layers.

50. The communications network of claim 49 wherein at least two of the plurality of network service function layers belong to a first wireless network service provider and are connected through a private link.

51. The communications network of claim 49 wherein at least two of the plurality of network service function layers belong to two different wireless network service providers and are connected through a private link governed by a service level agreement.

52. The communications network of claim 49 wherein at least two of the plurality of network service function layers belong to two different wireless network service providers and are connected through a public link.

53. The communications network of claim 49 wherein the network service function layer includes a mobility manager that manages a handoff when the first user leaves one of the plurality of access service function layers and enters another of the plurality of access service function layers.

54. The communications network of claim 49 wherein at least one of the plurality of network service function layers and at least one of the local service function layers reside in a single entity.

55. The communications network of claim 49 wherein the first set of the plurality of local service layers includes a session server

56. The communications network of claim 55 wherein the session server provides a list of a plurality of functions available to the first user.

57. The communications network of claim 56 wherein the plurality of functions available to the first user are based on capabilities of the first user and a plurality of network preferences.

58. The communications network of claim 56 wherein the session server provides addressing of any appropriate server to contact for each of the plurality of functions available to the first user.

59. The communications network of claim 56 wherein the session server contacts an accounting server through an Authorizing, Authentication and Accounting server and initiates a record of resources committed to the first user.

60. The communications network of claim 59 wherein the accounting server sends information to an accounting accumulator at one of the plurality of network service layers.

61. The communications network of claim 59 wherein the session server instructs a connection management server at the first set of a plurality of the local service layer to record usage information according to resources used by the first user.

62. The communications network of claim 61 wherein the usage information includes at least one of the group consisting of: time used by first user, packets used by first user flat rate for each access by the first user or bytes used

BNSDOCID: <EP_____1098490A2_I_>

by first user.

63. The communications network of claim 59 wherein each of the plurality of network service layers includes a mobility manager that provides handoff services to the first user when the first user leaves one of the first set of the plurality of local service function layers for another of the first set of the plurality of local service function layers.

64. The communications network of claim 59 wherein at least one of the plurality of the network service layers includes a mobility manager that provides handoff services to the first user when the first user leaves one of the first set of the plurality of access management layers for another one of the first set of the plurality of access management layers.

65. The communications network of claim 59 wherein the session server reserves any quality of service parameters and an amount of bandwidth requested by the first user.

66. The communications network of claim 59 wherein an access and a termination functions at one of the first set of the plurality of access management layers reserves any quality of service parameters and an amount of bandwidth requested by the first user.

67. The communications network of claim 49 further including an application layer that sends communications from the first user and an user agent client residing at the first user.

68. The communications network of claim 49 further including a layer 3 at the first user that sends communications to the network and an user agent client residing at one of the first set of the plurality of access service function layers.

69. The communications network of claim 49 further including an user agent server associated for each of a plurality of access interface layer at the first set of the plurality of access service function layers.

70. The communications network of claim 69 wherein the user agent server acts as a gateway by converting incoming protocols of incoming communications to a protocol understood by the first user.

71. The communications network of claim 69 wherein the user agent server delivers incoming protocols of incoming communications to the first user when the incoming protocol is understood by the first user.

72. The communications network of claim 59 wherein the session server further provides admission control functions and address resolution to an user agent client and an user agent client proxy at a SIP protocol server.

73. The communications network of claim 59 wherein the session server further provides admission control functions and address resolution to a H.323 terminal and a H.323 gateway at a H.323 protocol server.

74. The communications network of claim 59 further including a connection management server at a access management layer within one of the first set of access service function layers and wherein the connection management server can transport communications on a plurality of backbone infrastructures.

75. The communications network of claim 74 wherein the connection management server can transport communications on a point to point basis.

76. The communications network of claim 74 wherein the connection management server can transport communications on a point to multi-point basis.

77. The communications network of claim 74 wherein the connection management server provides a requested amount of network resources by utilizing a plurality of protocols to deliver a requested quality of service for latency.

78. The communications network of claim 74 wherein the connection management server provides a requested amount of network resources by utilizing a plurality of protocols to deliver a requested bandwidth.

79. The communications network of claim 49 further including a core network lever including the plurality of network service function layers and the first set of the plurality of local service function layers and wherein the core network layer decides policy parameters.

BNSDOCID: <EP_____1098490A2_I_>

80. The communications network of claim 49 further including an access management layer within the first set of access service function layers and wherein the access management layer enforces policy parameters.

81. A communications network architecture for an Internet Protocol centric wireless network for a first user to communicate to a destination, the architecture comprising:

a network service function layer within the wireless network, wherein the network service layer comprises a plurality of interconnected servers including:

a policy management server;
an authorization server;
a service accounting server;
an authentication, authorization and accounting server;
an unified directory within a directory server;
a security gateway; and
a mobility manager;

a local service function layer communicably linked with the network service function layer within the wireless network, wherein the local service function layer comprises a plurality of interconnected servers including:

an access accounting server;
an authentication, authorization and accounting server;
a security gateway;
a policy enforcement server;
a mobility manager;
a network management server; and
a wireless gateway;

an access management layer communicably linked with the local service function layer, wherein the access management layer comprises a plurality of interconnected servers including:

a location tracking server;
a connection management server;
a plurality of protocol servers;
a RF management server which includes power control, traffic control and channel assignment;
an access management server includes access, termination and paging;
a domain database server which provides a local decision point to expedite service invocation for the first user;
a policy enforcement server;
a network management server; and
a resource management server; and

an access interface layer communicably linked with the access management layer, wherein the access interface layer comprises a plurality of interconnected servers including:

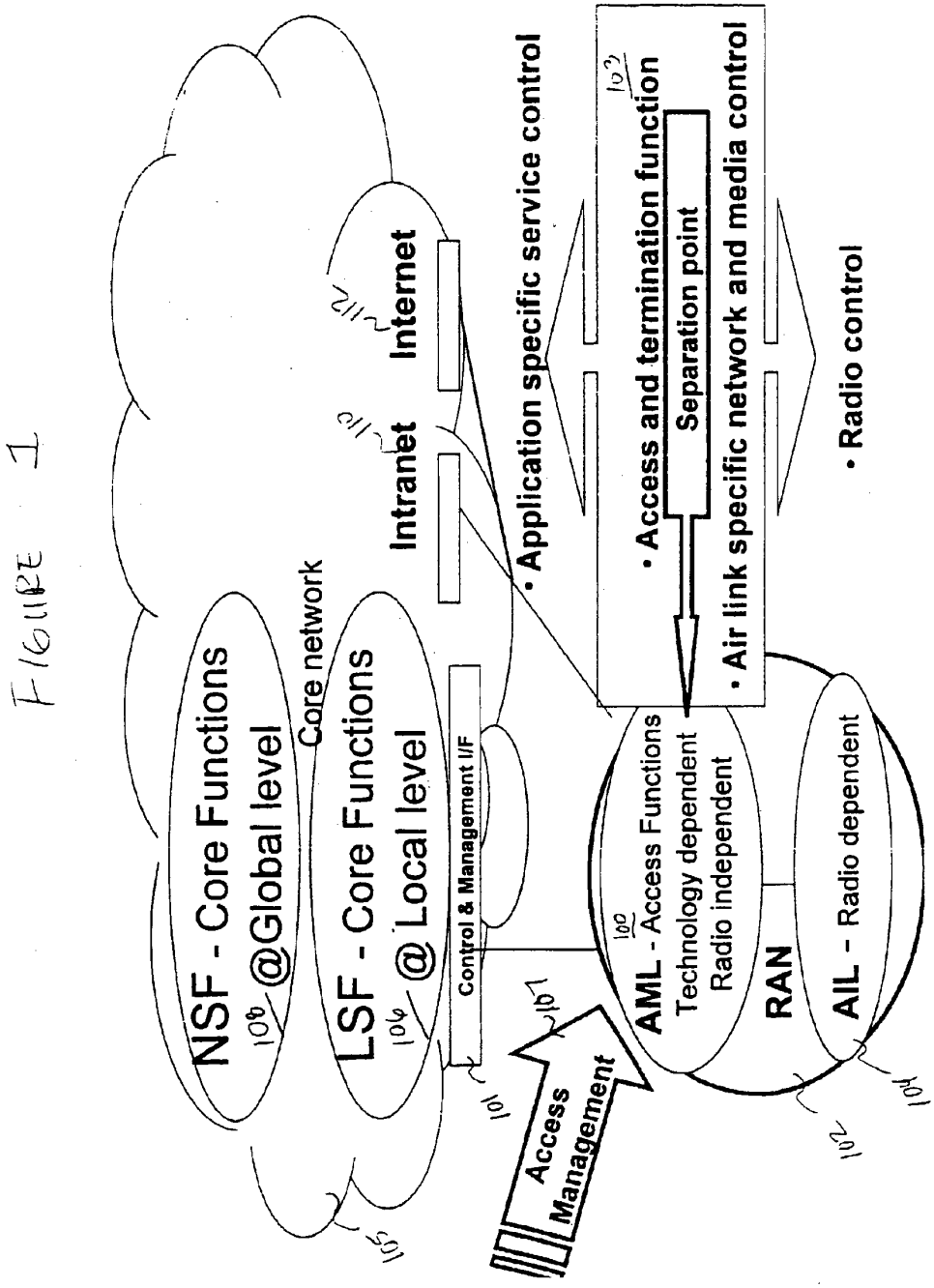
a channel management server;
a policy enforcement server;
an administration and maintenance server; and
a radio frequency server.

82. The communications network architecture of claim 81 wherein the access management layer provides policy enforcement.

83. The communications network architecture of claim 81 wherein the local service layer provides policy decision functions.

BNSDOCID: <EP_____1098490A2_I_>

FIGURE 1



BNSDOCID: <EP_____1098490A2_I_>

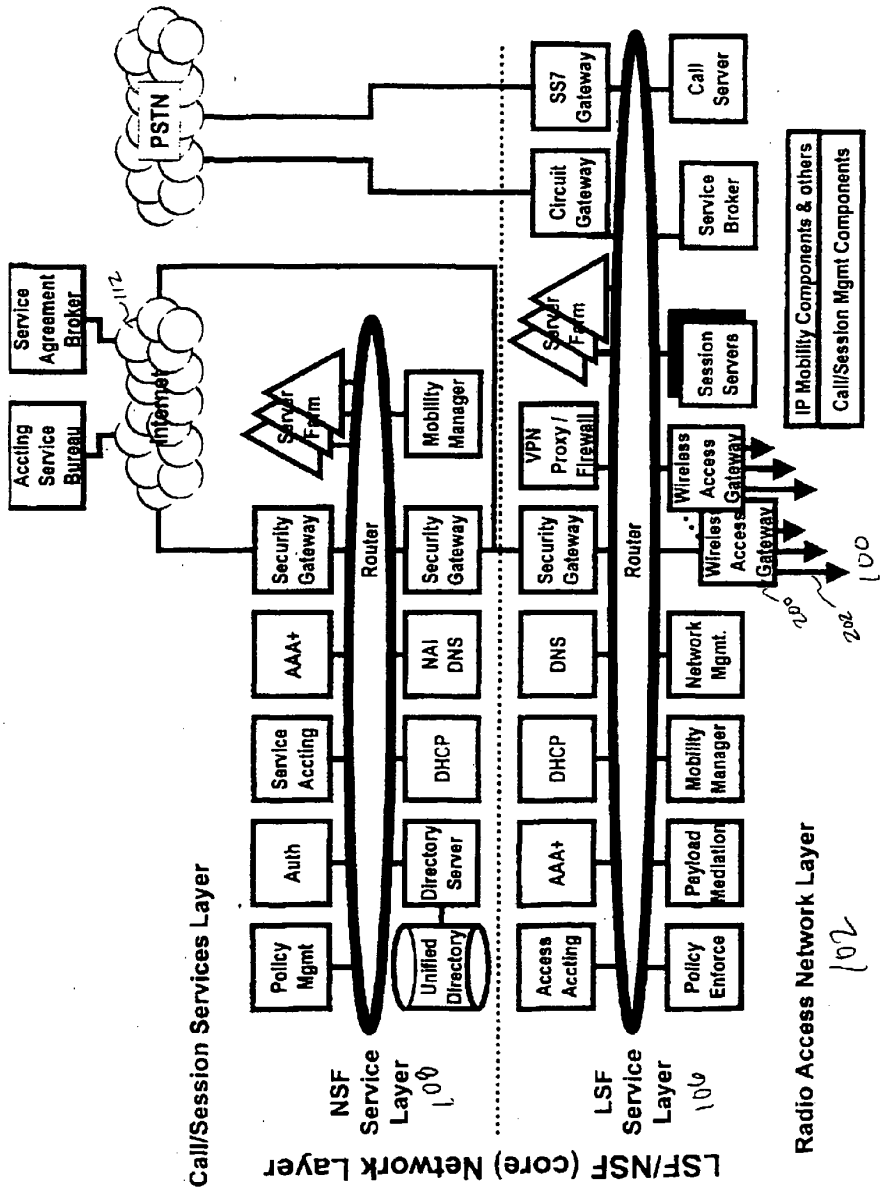


FIGURE 2

BNSDOCID: <EP_____1098490A2_I_>

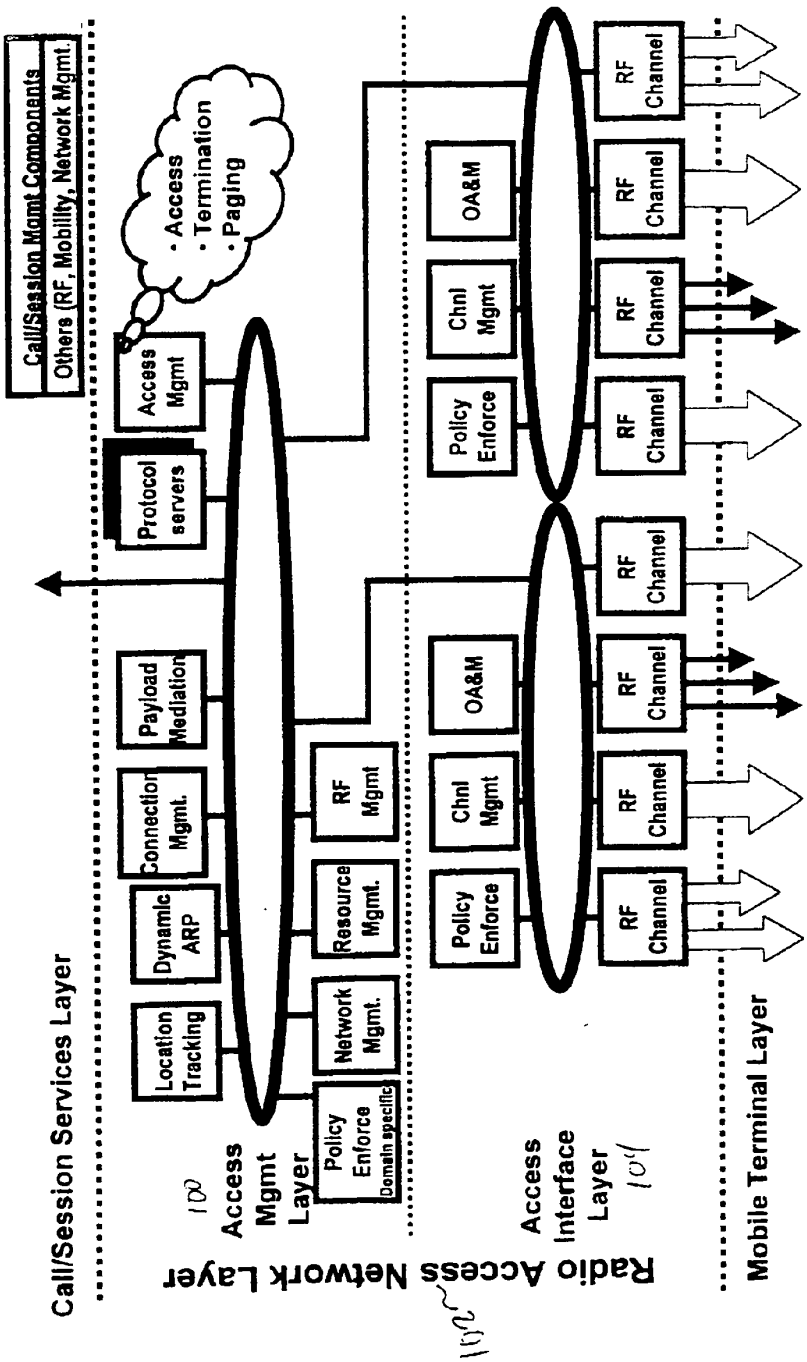


FIGURE 3

BNSDOCID: <EP_____1098490A2_I_>

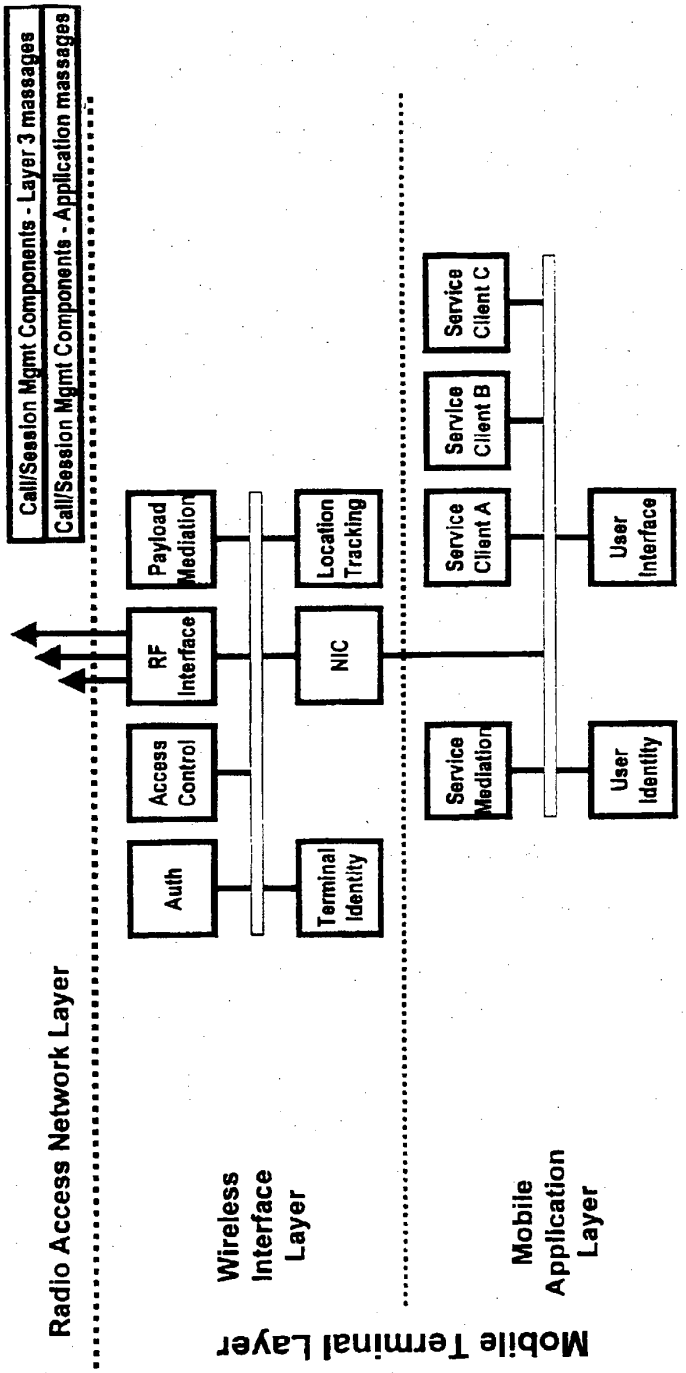


FIGURE 4

BNSDOCID: <EP_____1098490A2_I_>

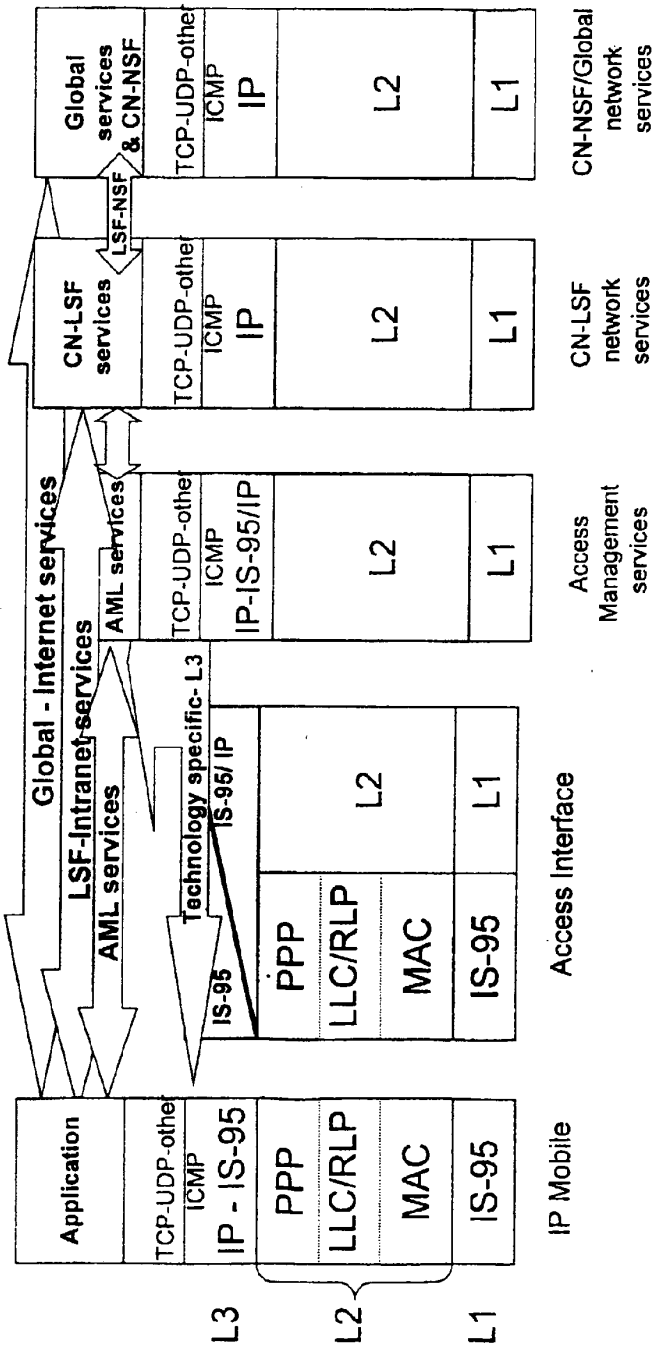


Figure 5

BNSDOCID: <EP_____1098490A2_I_>

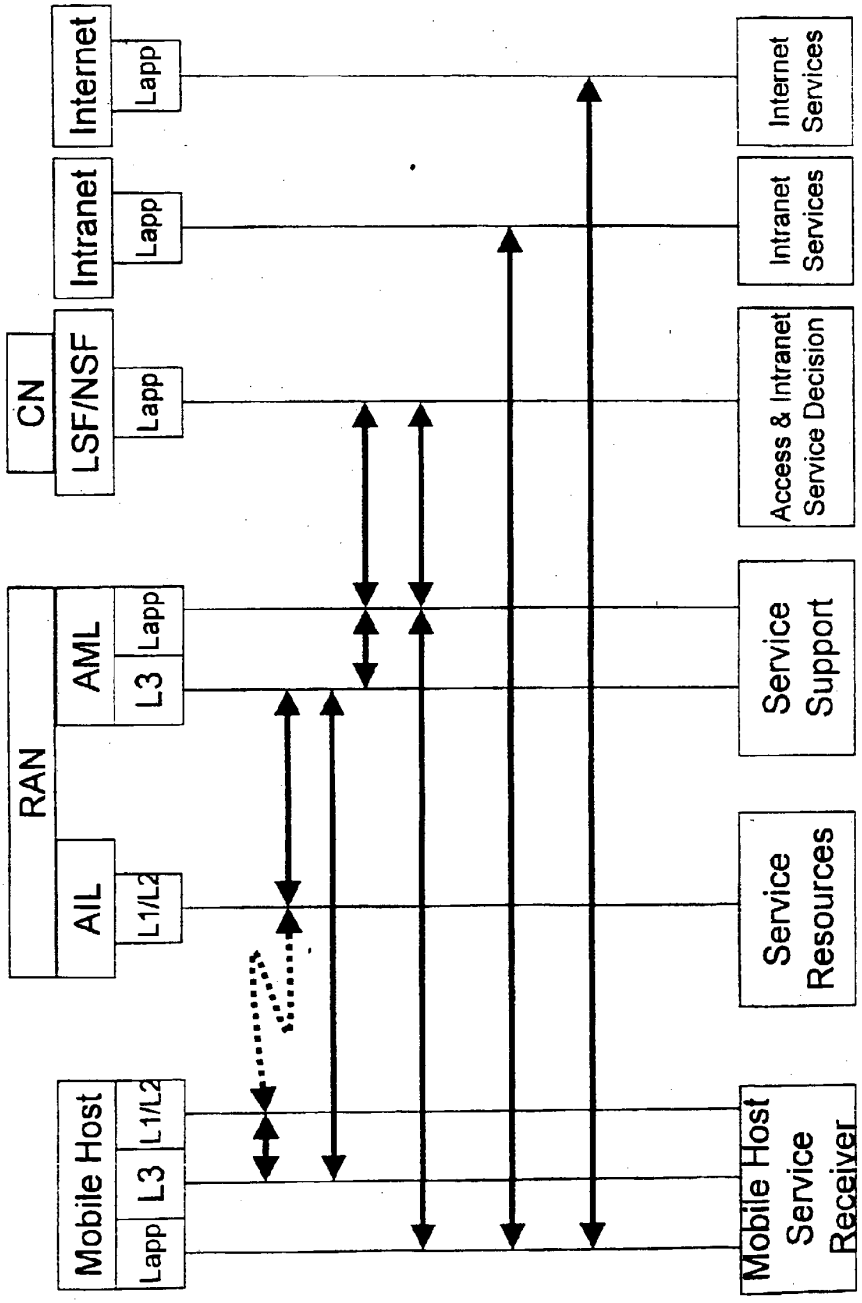


Figure 6

BNSDOCID: <EP_____1098490A2_I_>

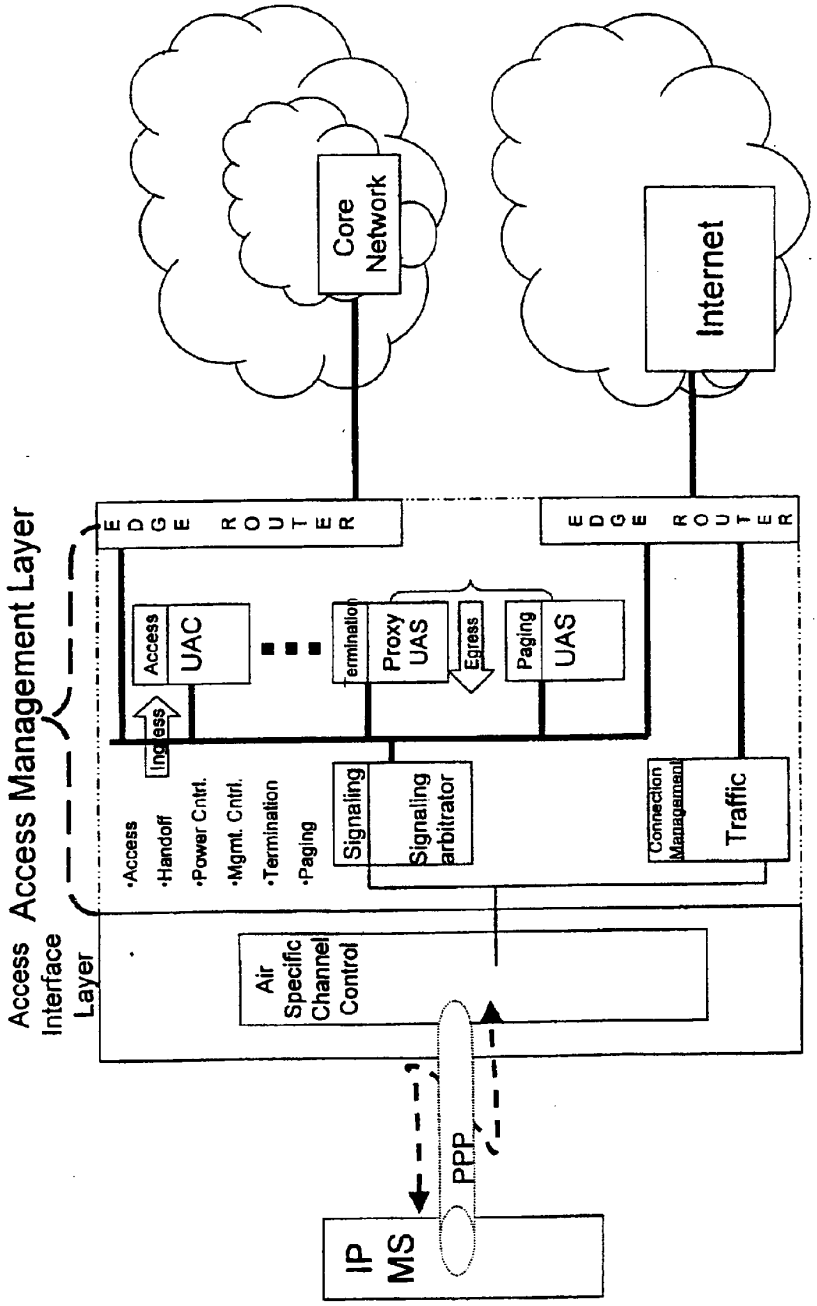


FIGURE 7

BNSDOCID: <EP_____1098490A2_I_>

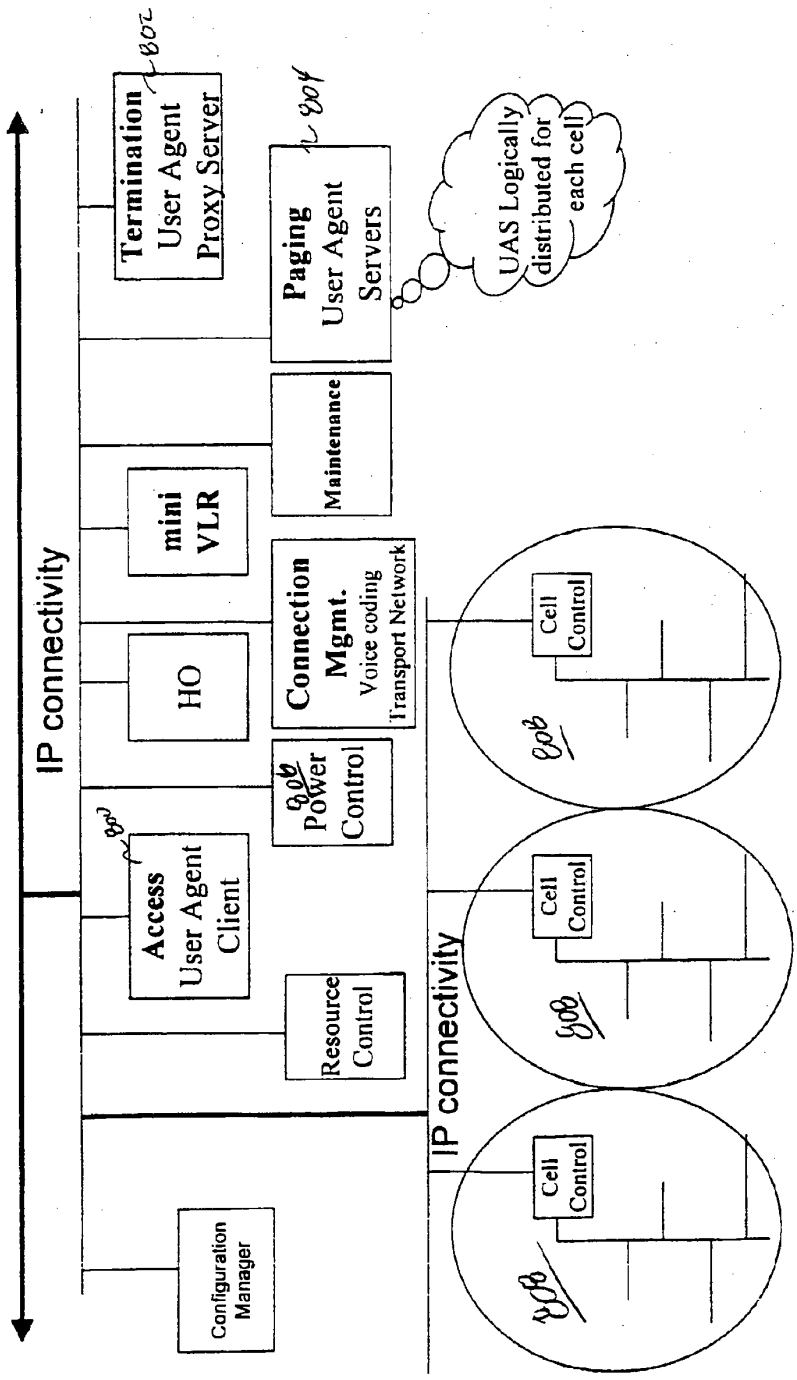


FIGURE 8

BNSDOCID: <EP_____1098490A2_I_>

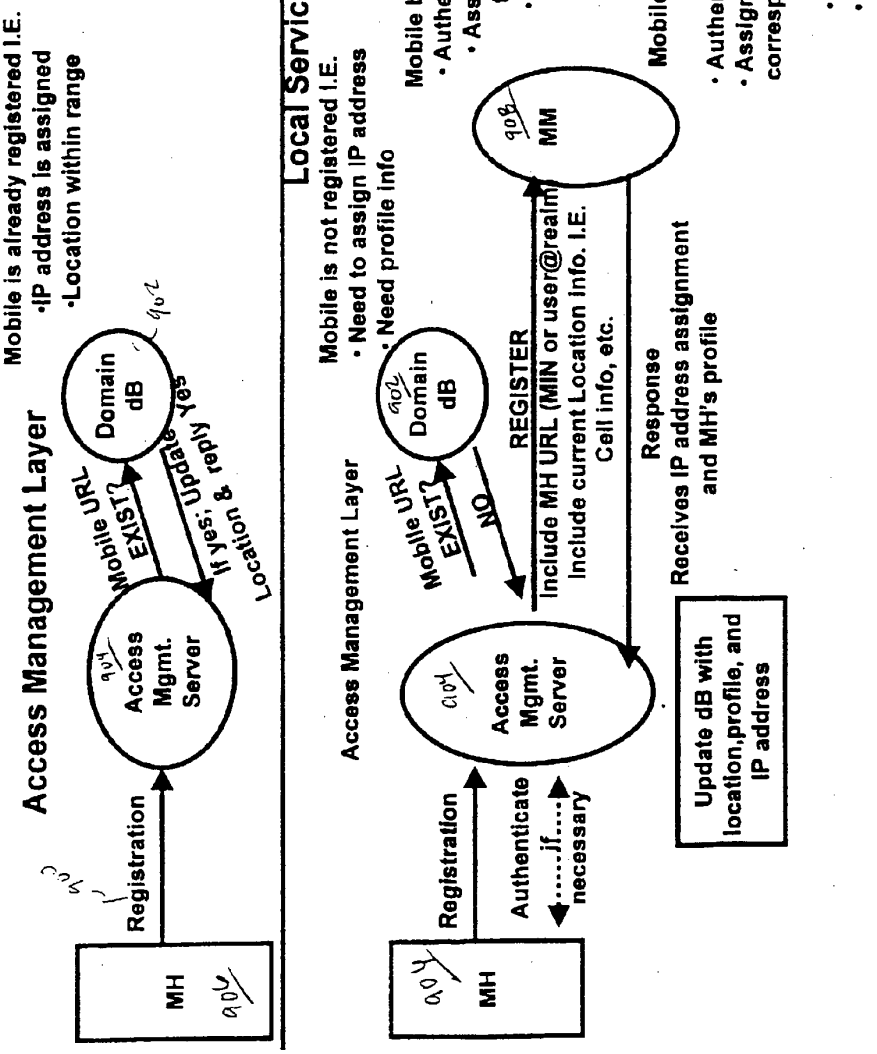


Figure 9

BNSDOCID: <EP_____1098490A2_I_>

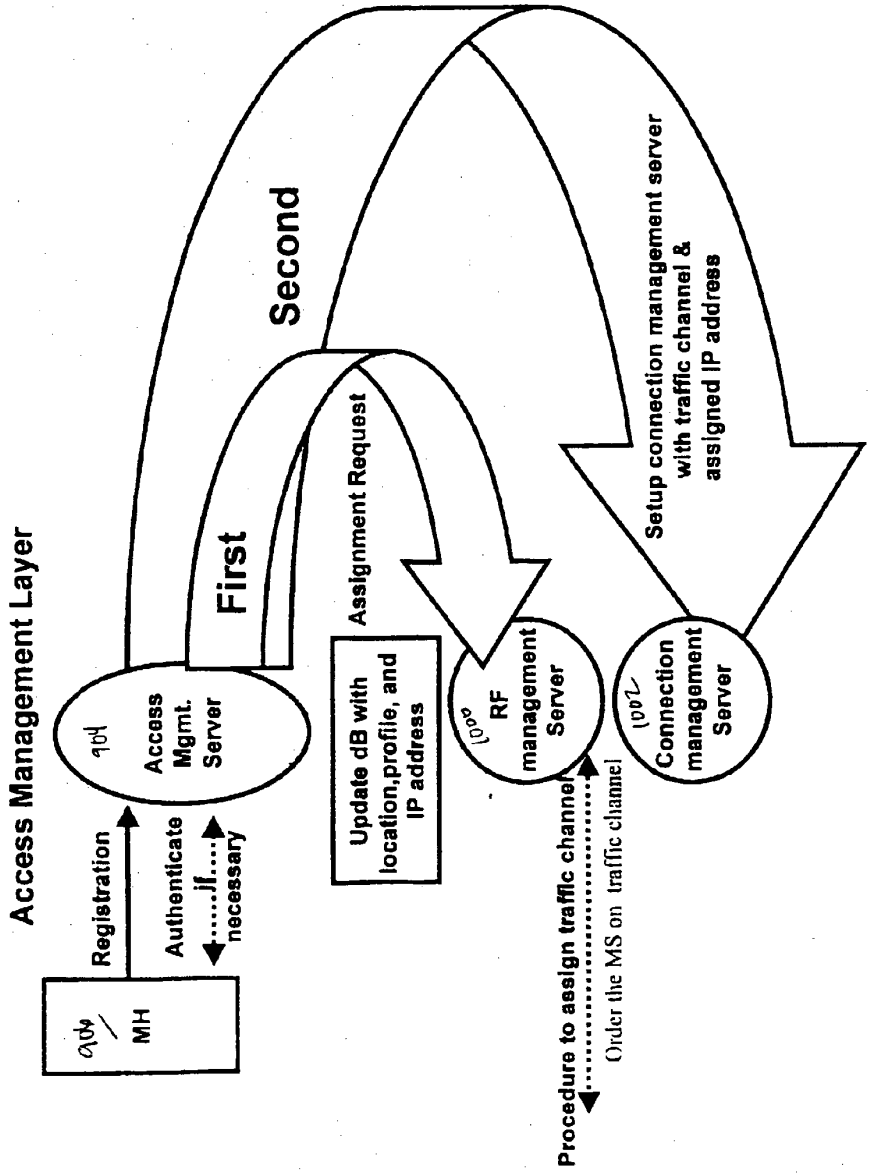


FIGURE 10

BNSDOCID: <EP_____1098490A2_I_>

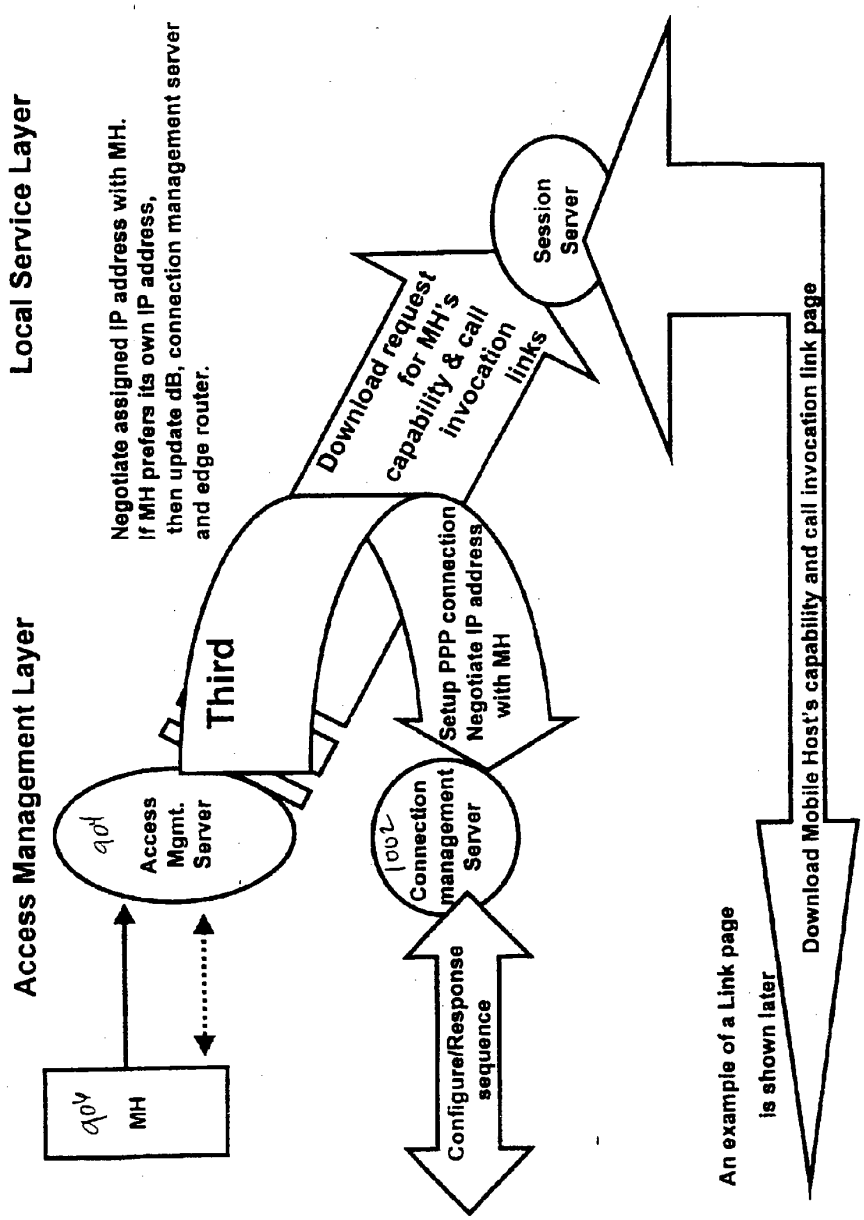


FIGURE 11

BNSDOCID: <EP_____1098490A2_I_>

Figure 12

BNSDOCID: <EP_____1098490A2_I_>

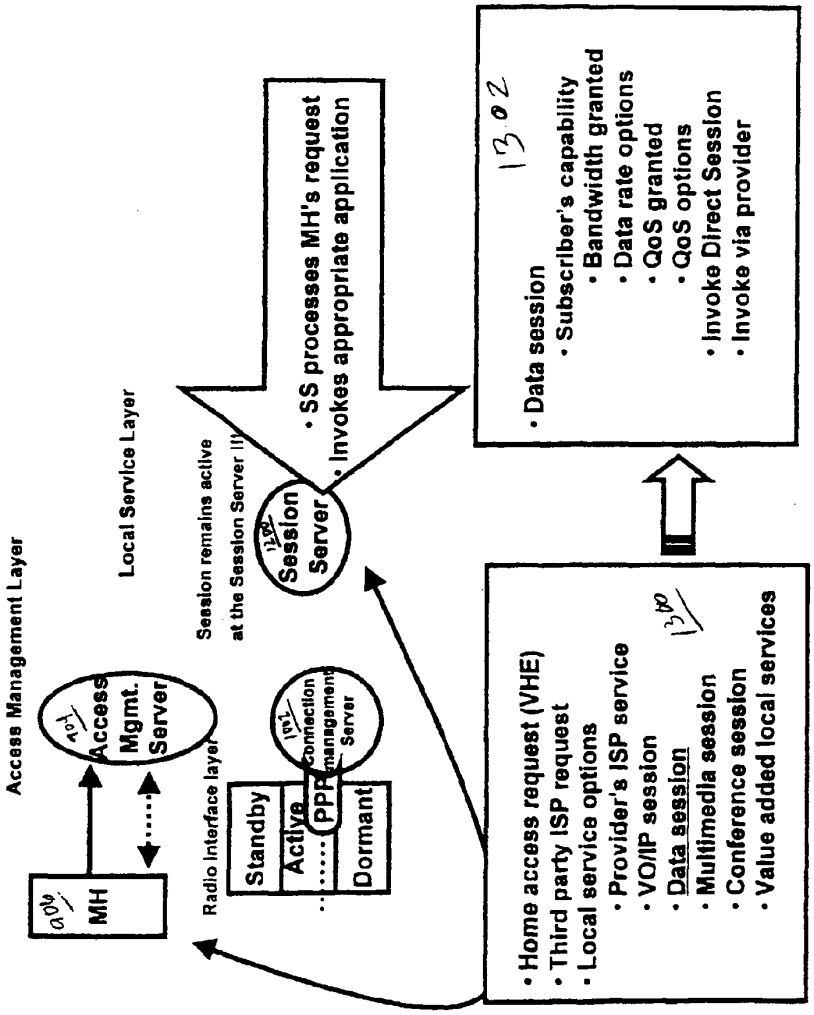


FIGURE 13

BNSDOCID: <EP_____1098490A2_I_>

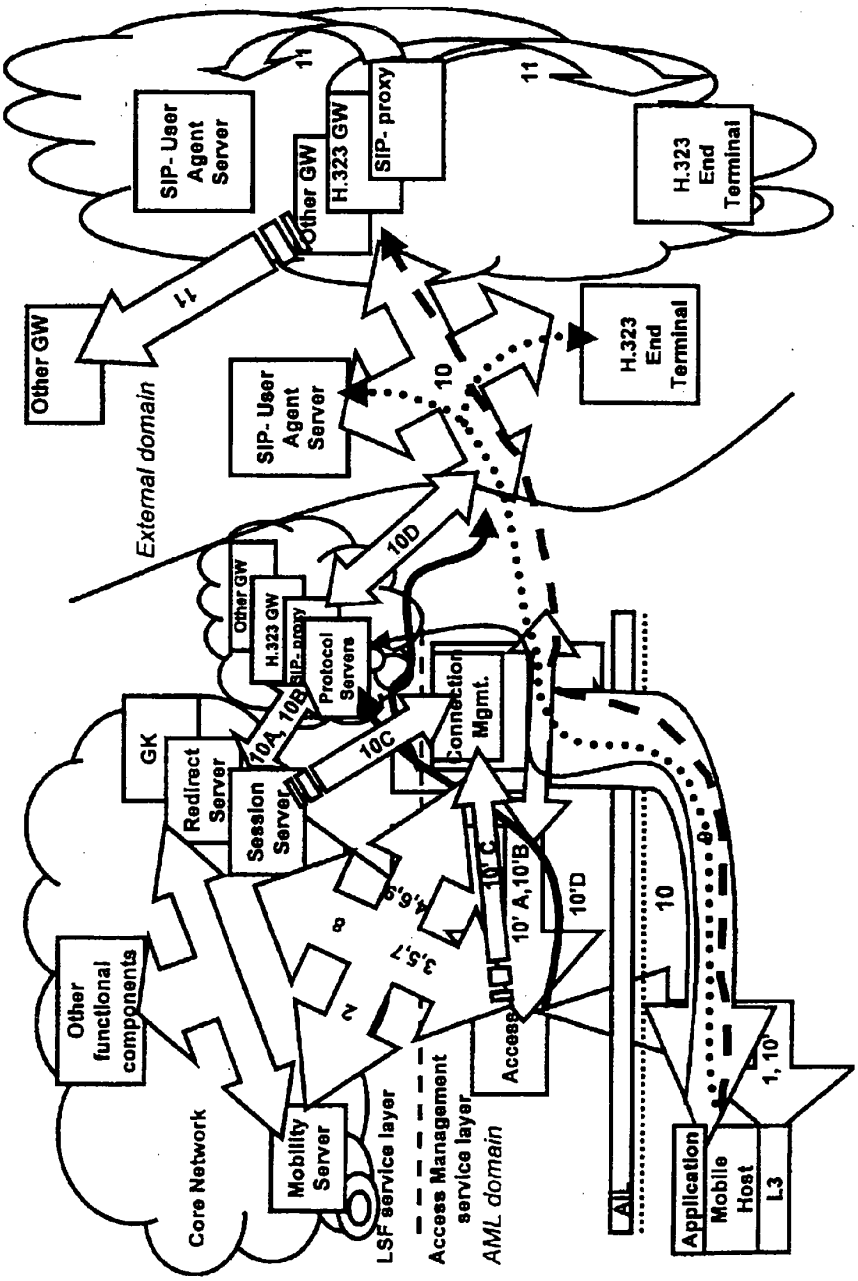


Figure 17

BNSDOCID: <EP_____1098490A2_I_>

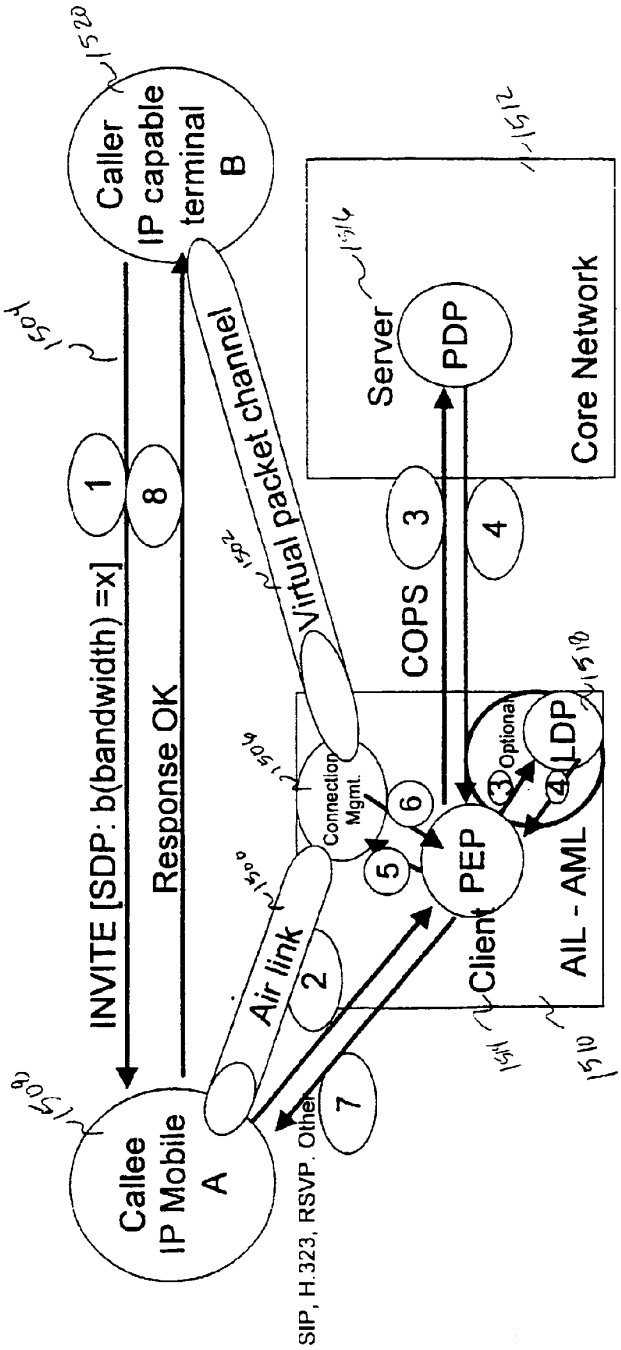


FIGURE 15

BNSDOCID: <EP_____1098490A2_I_>

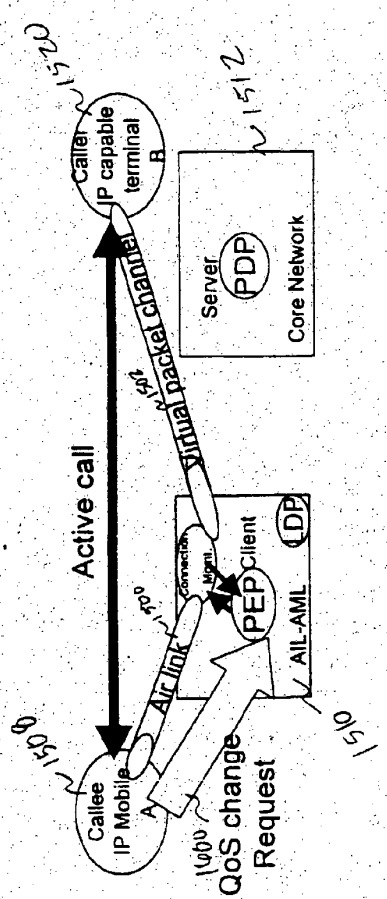


Figure 16

BNSDOCID: <EP_____1098490A2_I_>

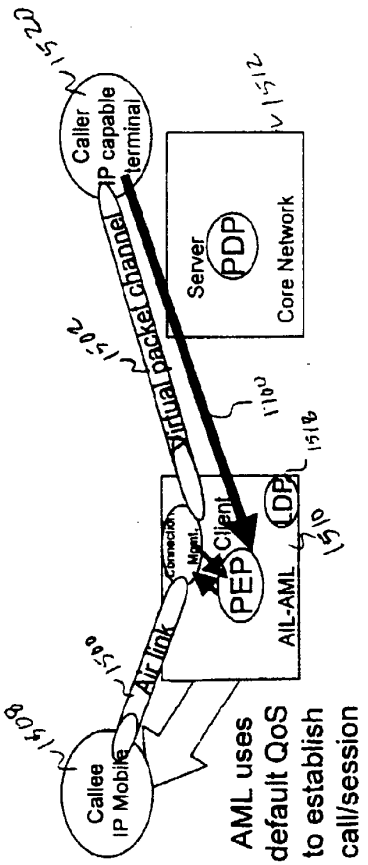


FIGURE 17

BNSDOCID: <EP_____1098490A2_I_>

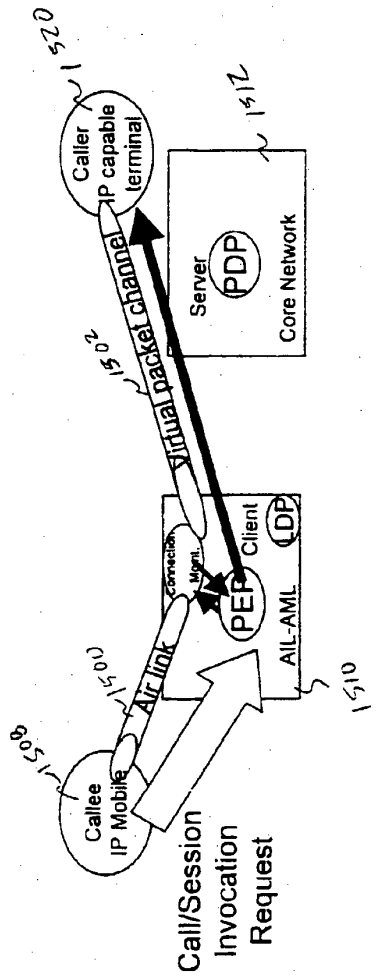


FIGURE 18

BNSDOCID: <EP_____1098490A2_I_>

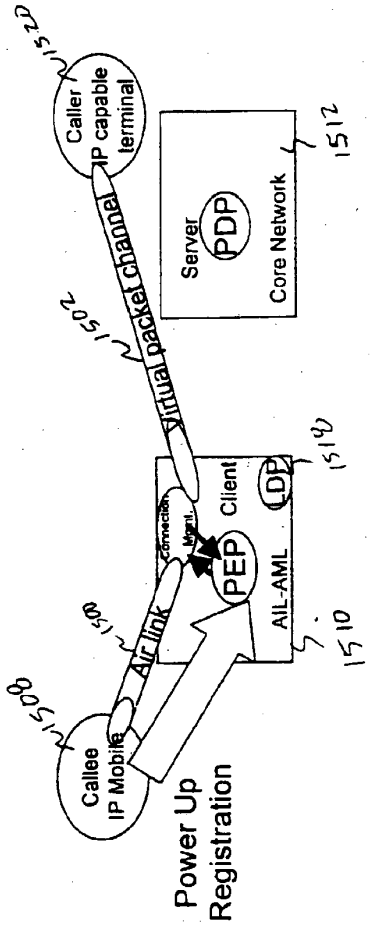
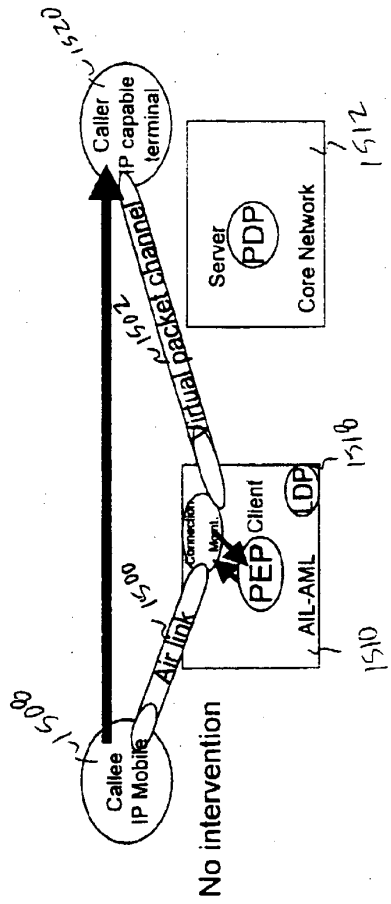


FIGURE 17

BNSDOCID: <EP_____1098490A2_I_>

FIGURE 20



BNSDOCID: <EP_____1098490A2_I_>

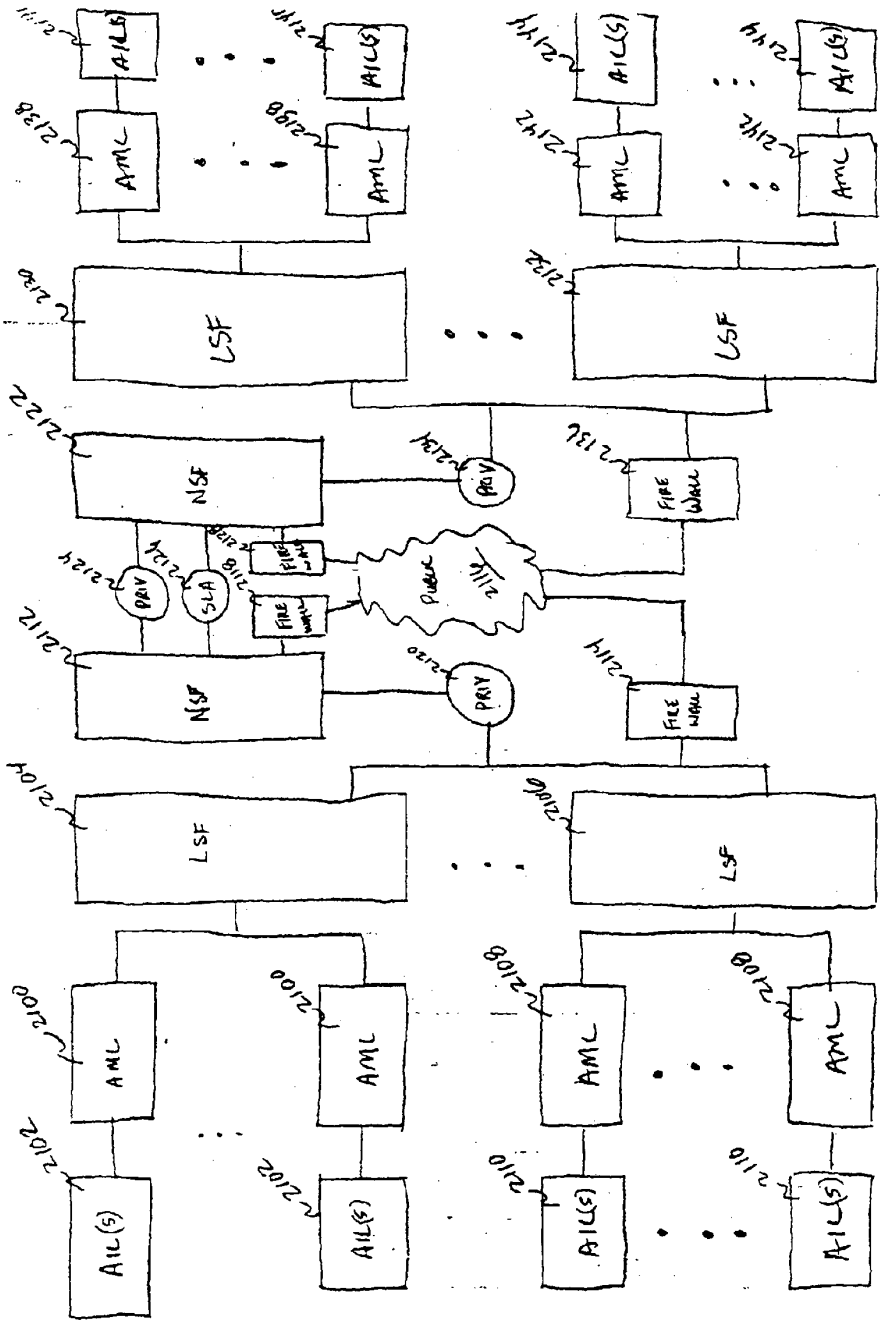


FIGURE 21

BNSDOCID: <EP_____1098490A2_I_>

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

(11) EP 1 098 490 A3

(12) **EUROPEAN PATENT APPLICATION**

(88) Date of publication A3:
27.08.2003 Bulletin 2003/35

(43) Date of publication A2:
09.05.2001 Bulletin 2001/19

(21) Application number: **00309735.9**

(22) Date of filing: **03.11.2000**

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

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

(30) Priority: **05.11.1999 US 434628**

(71) Applicant: **Nortel Networks Limited**
Montreal, Quebec H2Y 3Y4 (CA)

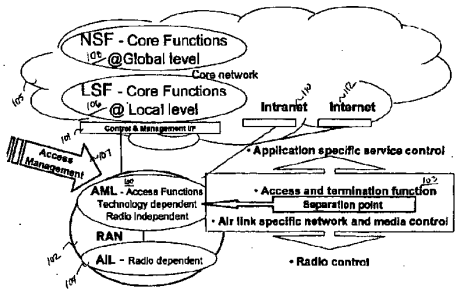
(72) Inventors:
- **Amin, Rajesh B.**
  Desoto, Texas 75115 (US)
- **Hanley, Donald V.**
  McKinney, Texas 75075 (US)
- **Morrow, Glenn C.**
  Plano, Texas 75075 (US)
- **Allahyar, John**
  Dallas, Texas 75252 (US)

(74) Representative: **Mackenzie, Andrew Bryan et al**
Sommerville & Rushton,
45 Grosvenor Road
St Albans, Herts. AL1 3AW (GB)

(54) **An architecture for an IP centric distributed network**

(57) A method and system to for a communications network architecture for an Internet Protocol centric wireless network for a first user to communicate to a destination, the architecture comprising: a network service function layer within the wireless network. The network service function layer can include: a policy management server; an authorization server; a service accounting server; an authentication, authorization and accounting server; an unified directory within a directory server; a security gateway; and a mobility manager. The architecture also includes a local service function layer associated with the network service function layer. The local service function layer can include: an access accounting server; an authentication, authorization and accounting server; a security gateway; a policy enforcement server; a mobility manager; a network management server; and a wireless gateway. The architecture also includes an access management layer associated with the local service function layer. The access management layer can include: a location tracking server; a connection management server; a protocol server; an access management server; a policy enforcement server; a network management server; and a resource management server. The architecture also includes an access interface layer associated with the access management layer. The access interface layer can include: a channel management server; a policy enforcement server; an administration and maintenance server; and a radio frequency server.

FIGURE 1



EP 1 098 490 A3

Printed by Jouve, 75001 PARIS (FR)

BNSDOCID: <EP_____1098490A3_I_>

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 00 30 9735

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	WO 99 48310 A (NOKIA TELECOMMUNICATIONS OY ;PUUSKARI MIKKO (FI)) 23 September 1999 (1999-09-23)	1-5, 7-14, 16-23, 26-34, 36-42, 44-50, 52-63, 65-71, 74-83	H04L29/06
Y	* page 1, line 17 - line 24 *	6,15,24, 25,35, 43,51, 64,72,73	
	* page 9, line 2 - line 5 *		
	* page 9, line 27 - page 10, line 23 *		
	* page 11, line 7 - line 30 *		
	* page 12, line 26 - line 29 *		
	* page 14, line 27 - line 29 *		
	* page 19, line 28 - line 35 *		
	* page 22, line 15 - line 20 *		
	* figure 1 *		
	---		TECHNICAL FIELDS SEARCHED (Int.Cl.7)
Y	EP 0 910 198 A (LUCENT TECHNOLOGIES INC) 21 April 1999 (1999-04-21)	6,15,24, 25,35, 43,51, 64,72,73	H04L
	* column 2, line 52 - column 3, line 5 *		
	* column 4, line 50 - line 58 *		
	* column 13, line 2 - line 16 *		
	* column 15, line 51 - column 16, line 7 *		
	* column 17, line 40 - line 50 *		
	* column 55, line 5 - line 9 *		

A	EP 0 903 905 A (TOKYO SHIBAURA ELECTRIC CO) 24 March 1999 (1999-03-24)	1-83	
	* the whole document *		

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
MUNICH	1 July 2003	HORN, R

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)

BNSDOCID: <EP_____1098490A3_I_>

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 00 30 9735

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.

01-07-2003

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9948310 A	23-09-1999	FI 980617 A	20-09-1999
		AU 2838999 A	11-10-1999
		EP 1064800 A1	03-01-2001
		WO 9948310 A1	23-09-1999
EP 0910198 A	21-04-1999	CA 2249817 A1	14-04-1999
		CA 2249830 A1	14-04-1999
		CA 2249831 A1	14-04-1999
		CA 2249836 A1	14-04-1999
		CA 2249837 A1	14-04-1999
		CA 2249838 A1	14-04-1999
		CA 2249839 A1	14-04-1999
		CA 2249862 A1	14-04-1999
		CA 2249863 A1	14-04-1999
		EP 0912026 A2	28-04-1999
		EP 0910198 A2	21-04-1999
		EP 0917320 A2	19-05-1999
		EP 0917318 A2	19-05-1999
		EP 0912027 A2	28-04-1999
		EP 0912012 A2	28-04-1999
		EP 0917328 A2	19-05-1999
		EP 0918417 A2	26-05-1999
		EP 0912017 A2	28-04-1999
		JP 11289353 A	19-10-1999
		JP 11252183 A	17-09-1999
		JP 11275154 A	08-10-1999
		JP 11275155 A	08-10-1999
		JP 2000022758 A	21-01-2000
		JP 11275156 A	08-10-1999
		JP 11275157 A	08-10-1999
		JP 11284666 A	15-10-1999
		JP 11331276 A	30-11-1999
		US 6577643 B1	10-06-2003
		US 6414950 B1	02-07-2002
		US 6421714 B1	16-07-2002
		US 6377982 B1	23-04-2002
		US 6400722 B1	04-06-2002
		US 2002089958 A1	11-07-2002
		US 6393482 B1	21-05-2002
EP 0903905 A	24-03-1999	JP 11163947 A	18-06-1999
		EP 0903905 A2	24-03-1999
		EP 0903906 A2	24-03-1999
		JP 11163946 A	18-06-1999
		US 6418128 B1	09-07-2002
		US 6272148 B1	07-08-2001

EPO FORM P0459

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

BNSDOCID: <EP_____1098490A3_I_>

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 00 30 9735

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.

01-07-2003

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0903905 A		US 2002186680 A1	12-12-2002

EPO FORM P0459

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

BNSDOCID: <EP_____1098490A3_I_>

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 November 2007 (15.11.2007)

PCT

(10) International Publication Number
WO 2007/129180 A2

(51) International Patent Classification:
H04B 7/005 (2006.01)

(21) International Application Number:
PCT/IB2007/001120

(22) International Filing Date: 30 April 2007 (30.04.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/797,943 5 May 2006 (05.05.2006) US

(71) Applicant *(for all designated States except US)*: **NOKIA CORPORATION** [FI/FI]; Keilalahdentie 4, FIN-02150 Espoo (FI).

(71) Applicant *(for LC only)*: **NOKIA INC.** [US/US]; 6000 Connection Drive, Irving, Texas 75039 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **KAIKKONEN, Jorma** [FI/FI]; Taskilantie 27 D 15, FIN-90580 Oulu (FI). **VIMPARI, Anna-Mari** [FI/FI]; Kummelintie 9, FIN-90520 Oulu (FI). **HINTZ-MADSEN, Mads** [DK/FI]; Luokkikuja 6, FIN-90310 Oulu (FI).

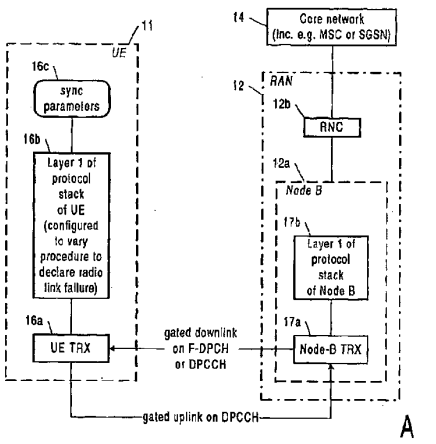
(74) Agents: **MAGUIRE, Francis, J.** et al.; Ware, Fressola, Van Der Sluys & Adolphson LLP, 755 Main Street, P.O. Box 224, Monroe, Connecticut 06468 (US).

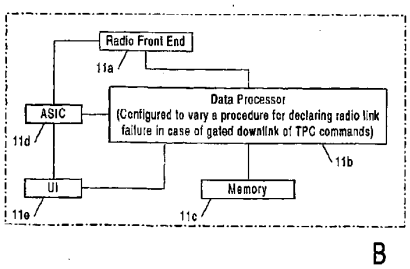
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, 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),

[Continued on next page]

(54) Title: ENHANCED UE OUT-OF-SYNC BEHAVIOR WITH GATED UPLINK DPCCH OR GATED DOWNLINK F-DPCH OR DPCCH TRANSMISSION





(57) Abstract: A method and corresponding equipment by which a wireless terminal communicatively coupled to a radio access network adapts to gating in respect to a downlink signal from a radio access network carrying power control commands (e.g. the F-DPCH of UTRAN with WCDMA), including gating by the radio access network of either just the power control commands or the channel itself, or gating of reception of the power control commands by the user equipment. The adaptation can include changing values of parameters used in determining when the wireless terminal declares a radio link failure, or instead only changing the procedures used to determine whether a parameter value has been achieved and thus only effectively changing the parameter values (or one or more of the parameters can be actually and effectively changed).

WO 2007/129180 A2

BNSDOCID: <WO____2007129180A2_I_>

European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, 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.

BNSDOCID: <WO_____2007129180A2_I_>

ENHANCED UE OUT-OF-SYNC BEHAVIOR WITH GATED UPLINK DPCCH OR GATED DOWNLINK F-DPCH OR DPCCH TRANSMISSION

CROSS REFERENCE TO RELATED APPLICATION

Reference is made to and priority claimed from U.S. provisional application Ser. No. 60/797,943 filed 5 May 2006.

BACKGROUND OF THE INVENTION

1. *Technical Field*

The present invention pertains to the field of wireless communications. More particularly, the present invention pertains to procedures to be followed by wireless terminals in case of gating of transmit power by the wireless terminals.

2. *Discussion of related art*

In some wireless communications systems, in particular UMTS (Universal Mobile Telecommunications System) using WCDMA (Wideband Code Division Multiple Access) for the air interface of its UTRAN (UMTS terrestrial radio access network), in order to save power a UE (user equipment) wireless communication terminal could turn its transmit power on and off, i.e. it could *gate* its transmit power according to a gating pattern (among other factors), i.e. according (at least in part) to a duty cycle having an on period and an off period. Using a UTRAN with WCDMA as an example, a UE sends data and/or control information (such as pilot bits) to a Node-B of the UTRAN, and the Node-B then estimates the UE uplink quality based on the control information, and commands the UE to change its transmit power accordingly. If a UE were to use transmit power gating, there would then be periods of time in which no control information would be transmitted, and correspondingly, there could be periods of time in which no power change commands would be issued by the Node-B, or periods of time in

BNSDOCID: <WO____2007129180A2_I_>

which if the Node-B were to issue power change commands, the commands would be based on unreliable quality information (signal to interference ratio measurements, for example) because of no control bits having been transmitted for the period of time in which the quality measurements are made (taking into account the time it takes for a transmission from the UE to reach the Node-B).

At present, there are procedures according to which a UE is to declare a radio link failure based on a predetermined threshold for minimum quality of the signal from the Node-B, and a predetermined value for a number of consecutive below threshold quality indications. These procedures and the predetermined threshold and number of below minimum quality indications assume continuous transmit power by the UE. But if a UE were to gate its uplink, then because the Node-B would in effect follow and gate its downlink (because of having no control information to estimate the uplink quality from when the UE is not transmitting), and because the UE uses the downlink as a basis for estimating the quality of the radio link, the UE could declare a radio link failure when in fact there would be no such failure. The apparent inability to "hear" the Node-B for a period of time would be due simply to the Node-B not transmitting during that period of time, not because of poor radio link quality.

What is needed, therefore, is a way to adapt the procedure for declaring a radio link failure, and also related procedures, in case of a UE gating its uplink.

UTRAN with WCDMA as the radio technology is a particular example of the need for a new procedure for declaring a radio link failure. First consider the need for gating by a UE. When no dedicated channels (DCHs)--and thus, no dedicated physical data channels (DPDCHs) (which carry payload as well as high-level signalling)--have been configured in the uplink

BNSDOCID: <WO____2007129180A2_I_>

(UL), all data is transmitted on the enhanced data channel (E-DCH), which is mapped to the enhanced dedicated physical data channel (E-DPDCH). Control signalling associated with E-DCH is transmitted on E-DPCCH. E-DPDCH and E-DPCCH are discontinuous, i.e. they are transmitted only when there is data to be transmitted and the transmission has been granted by the network. For an E-DCH transmission, a grant is needed: a non-scheduled grant for non-scheduled MAC-d (media access control-d) flows and a serving grant (and an allowed, active HARQ process) for scheduled transmissions.

The UL DPCCH carries control information generated at Layer-1 (i.e. the physical layer of the protocol stack). The layer-1 control information consists of e.g. known pilot bits for supporting channel estimation for coherent detection, for use in the Node-B determining transmit power control (TPC) commands to downlink (DL) on DPCH or on Fractional-DPCH (F-DPCH), feedback information (FBI), and an optional transport format combination indicator (TFCI).

UL DPCCH is continuously transmitted (even if there is no data to transmit for awhile), and there is one UL DPCCH for each radio link. Continuous transmission is acceptable with circuit-switched services, which typically send continuously. For bursty packet services, however, continuous DPCCH transmission is less desirable because it has substantial overhead.

The uplink capacity can be increased by decreasing the control overhead. One possibility for decreasing control overhead is UL DPCCH gating, i.e., not transmitting DPCCH all the time. A pattern could (at least in part) define the DPCCH transmission time periods and/or DPCCH may depend (also) on E-DCH and HS-DPCCH transmission times. (Other rules may in effect supercede the pattern so that from time to time the UE may uplink during what would ordinarily be an off-period/gap

BNSDOCID: <WO____2007129180A2_I_>

in the transmission, with the net result being irregular transmission, i.e. not strictly according to a pattern.) Gating can provide UE power saving and so longer battery life, depending on the duty cycle, i.e. the length of on period for DPCCH compared to the off period. Also, interference with other UEs could be reduced, and thus network capacity could be increased.

F-DPCH carries TPC command bits to a UE determined by the Node-B serving the UE, based on data and/or control information uplinked by the UE on DPCCH. F-DPCH is currently transmitted every time slot, independently of the data or control transmission activity by the UE, i.e. independent of whether the UE gates the DPCCH. However, in case of UL DPCCH gating by the UE so that an UL DPCCH time slot does not contain and data and/or control transmission by the UE (i.e. because the UE does not transmit during that UL DPCCH time slot on account of its gating), the Node-B cannot derive a sensible power control command corresponding to the time slot, to transmit on F-DPCH. Thus, if UL DPCCH is to be gated, F-DPCH and/or DL DPCCH could also be gated and/or discontinuously received. Discontinuous DL transmission decreases downlink interference and corresponding discontinuous reception by the UE improves UE battery consumption.

With respect to power control commands issued by the serving Node-B, a UE is considered out-of-sync (not synchronized) if the DL DPCCH quality or the quality of the TPC fields of the F-DPCH frame received from the serving HS-DSCH cell over the previous 160 ms period is worse than a threshold Q_{out} defined (implicitly) by tests in 3GPP TS 25.101. A UE is considered in-sync (synchronized) if the UE estimates the quality of the DL DPCCH or the TPC fields of the F-DPCH frame received from the serving HS-DSCH cell over the previous

BNSDOCID: <WO____2007129180A2_I_>

160 ms period to be better than a threshold Q_{in} also defined (implicitly) by tests in 3GPP TS 25.101.

According to 3GPP TS 25.101, if a UE estimates the DPCCH quality or the quality of the TPC fields of the F-DPCH frame received from the serving HS-DSCH cell over the last 160 ms period to be worse than the threshold Q_{out}, the UE is to turn its power off. On the other hand, if a UE estimates the DPCCH quality or the quality of the TPC fields of the F-DPCH frame received from the serving HS-DSCH cell over the last 160 ms period to be better than the threshold Q_{in}, the UE is to turn its power on. A UE is to determine that radio link failure has occurred if after some number N313 of consecutive out-of-syncs have been indicated (N313 being the label of a parameter whose value is the number), less than some number N315 of successive in-syncs are indicated before some number T313 of time periods expires (where the counting toward the number T313 is starting from when the N313 consecutive out-of-syncs are indicated).

DISCLOSURE OF INVENTION

The invention provides a method for use by a user equipment wireless communication terminal, comprising: determining on periods and off periods of a gated transmission in connection with receiving power control commands over a downlink channel of a radio access network; and varying a procedure used to determine when to declare a radio link failure based on the gated transmission by actually and/or effectively varying a quality measurement period used in the procedure or a parameter value used in the procedure. To actually vary a parameter, the value of the parameter would be changed. To only effectively vary a parameter, a procedure using the parameter is changed but the value of the parameter is not changed (so that the same parameter value then has a different effect).

BNSDOCID: <WO____2007129180A2_I_>

Corresponding equipment, including computer program products and application specific integrated circuits are also provided. In addition, wireless terminals are provided including such equipment and so operative according to methods provided by the invention. Also, a wireless communication system including elements communicatively coupled to such wireless terminals are also provided.

Brief Description of the Drawings

The above and other objects, features and advantages of the invention will become apparent from a consideration of the subsequent detailed description presented in connection with accompanying drawings, in which:

Figure 1A is a block diagram/ flow diagram of a UE and a Node-B communicatively coupled via a radio link including a gated uplink channel and a gated downlink channel, and showing parameters stored in the UE for use in (among other things) determining when to declare a radio link failure.

Figure 1B is a reduced block diagram (only portions relevant to the invention being shown) of the UE terminal or the Node B of Figure 1A.

Figure 2 is a block diagram showing a layer one (physical layer) of a protocol stack implemented in the UE receiving as inputs information indicating the gated downlink, and also the sync parameter values in case of no downlink gating, and providing changed sync parameters.

Figure 3 is a flow chart of the operation of a UE, according to the invention.

Figure 4 is a flow chart of the operation of a Node, B according to the invention.

BNSDOCID: <WO____2007129180A2_I_>

BEST MODE FOR CARRYING OUT THE INVENTION

The invention provides a method by which a UE, communicatively coupled to a Node-B of a UTRAN (UMTS radio access network) (or coupled to a corresponding entity of a radio access network on another cellular technology), adapts to gating (so as to perform what is sometimes called discontinuous transmission) of a downlink channel (F-DPCH or DPCCH) carrying power control commands from the Node-B. As explained above, such gating of the downlink can be the direct result of gating of the uplink by the UE, or can be at least associated with such gating, and the downlink gating is presumed known or knowable to the UE (as a result of monitoring/ measurements or other mechanism not the subject of the invention). As also explained above, the UE is required by standards to turn its power off in case of a number of consecutive out-of-sync indications, each corresponding to a determination that a quality metric for receiving control commands from the Node-B is below a threshold Q_{out}. Without adapting to such gating, the UE could turn its power off more than is desirable because of out-of-sync indications due simply to the Node-B not transmitting for a period of time--the off period of an on/off duty cycle. As indicated above, what is needed therefore, is a way to adapt the procedure for declaring a radio link failure, and also related procedures, in case of a UE gating its uplink.

In case of gating, different options exist for how the out-of-synch criterion could be determined. In general, according to the invention, to accommodate gating by the Node-B, the UE actually and/or effectively varies one or more parameter values used to determine when to declare a radio link failure based on the downlink gating. To actually vary a parameter, the value of the parameter is changed. To effectively vary a parameter, a procedure using the parameter

BNSDOCID: <WO____2007129180A2_I_>

is changed but the value of the parameter used in the procedure is not. For example, a procedure could require a number N of occurrences of an event in a time T. To actually vary N, the value of N would be changed, but not (necessarily) the value of T. (Alternatively, the value of T could be actually changed.) To effectively vary N, how T is measured could be changed. (This can also be viewed as effectively changing the value of T.) For example, the procedure could be changed so that off-period of a duty cycle does not count in measuring T.

Now in a first option for how the out-of-synch criterion could be determined, the Q_{out} and Q_{in} thresholds and the measurement window (the 160 ms time period) could be kept unchanged, and values for the parameters N313, T313 and N315, could be signaled to a UE to achieve the desired behavior for the downlink gated transmission. However, this has as a disadvantage lowered reliability of Q_{in} or Q_{out} due to a lower number of samples. In addition, the parameters are currently broadcast, and so they would need to be separately set for each user having a different gated transmission.

In a second option, the thresholds and parameters could be kept unchanged, but the measurement window could be increased (from 160 ms), or instead only effectively increased by counting only time increments when according to the gated transmission by the Node-B there is an actual downlink transmission. With both approaches--increasing the window or only changing how time is counted as contributing to the window--the measurement window could be set so that the number of evaluated samples (in terms of TPC commands) would be kept constant. This way the reliability of Q_{in} or Q_{out} could be improved.

In a third option, the option provided by the invention in at least some embodiments, the N313, T313 and N315

BNSDOCID: <WO____2007129180A2_I_>

parameter values would be broadcast by the network as before (and so known to all UEs served by the Node-B broadcasting the parameters). However, a UE would autonomously adjust one or more of the broadcast values for the N313, T313 and/or N315 parameters based on an on period and an off period of a gated transmission having an on/off duty cycle and associated with the transmission of the power control commands on the downlink channel of the radio access network, based on a predetermined methodology. In some other embodiments, the UE could adjust the values it used for the thresholds Q_{out} and Q_{in}.

In case of a UE changing the values it uses for one or more of the N313, T313 and N315 parameters, the methodology could, for example, increase the value of the T313 value and so lengthen the time before a radio link failure is declared (and perhaps prevent declaring a radio link failure because of allowing more time to receive an in-sync indication after N313 out-of-sync indications). For example, the T313 parameter would be increased by the percentage of time the Node-B is not transmitting compared to the total time. Alternatively, the methodology could increase the number N313 to require a greater number of out-of-sync indications, and again for example, in direct proportion to the off period of the duty cycle compared to the whole period of the duty cycle. (This alternative starts the T313 and N315 usage and thus has the greatest impact.) In still another alternative, the methodology could decrease the number N315 and so decrease the number of consecutive in-sync indications (before T313 units of time has expired) required to prevent a declaration of radio link failure (after N313 consecutive out-of-sync indications have been observed).

The invention also encompasses changing not just one of the N313, T313 and N315 parameters, but any combination of these parameters. Also, instead of changing a parameter value in direct proportion to the length of the off-period of the

BNSDOCID: <WO____2007129180A2_I_>

gated transmission (i.e. the off-period of the duty cycle of the UE transmitter), the parameter values could be changed in some other proportion, i.e. in a non-linear way.

As an alternative to changing the values of the N313, T313 and N315 parameters, the UE could change how it counts consecutive out-of-sync indications, and how it counts consecutive in-sync indications, and/or how it measures the time period corresponding to T313. The UE could, for example, only count as a consecutive out-of-sync indication an indication of out-of-sync occurring in a time when the Node-B gated transmission is in an on-period, i.e. when the Node-B is known by the UE to be transmitting. Similarly for the counting up to N315 in-sync indications, and similarly for measuring time after N313 consecutive out-of-sync indications (i.e. time would be measured only when the Node-B is known to be transmitting). Thus, the UE could only *effectively* change one or more of the N313, T313 and N315 parameter values, by changing how the UE determines whether a condition(s) corresponding to the one or more parameter values has occurred, e.g. changing the procedure used to monitor out-of-sync indications so as to count as a consecutive out-of-sync indication such an indication only if the out-of-sync indication occurs during the on period of the on/off duty cycle (and only if there has not been an in-sync indication anytime between the most recent previous out-of-sync indication occurring during an on period).

In order to vary (one or more of) the N313, T313 and N315 parameters (actually or just effectively), the UE must learn/ determine the on period and the off period of the on/off duty cycle used by the Node-B of the radio access network in gating the downlink channel conveying the power control commands. One way for the UE to determine the on and off periods of the duty cycle is by assuming that they are the same as the on and off periods of the duty cycle used by the UE in gating its

BNSDOCID: <WO____2007129180A2_I_>

uplink (on DPCCH), and so equating the downlink gated transmission by the Node-B to the uplink gated transmission of the UE. Another way is to monitor the downlink, observing the pattern of variation in received power on the gated downlink channel (for example, the F-DPCH in case of WCDMA and UTRAN), and equating the off period of the gated downlink pattern to the observed period of low received power, and equating the on period to the observed period of higher low received power. Another way is for the UE to receive via signaling from the Node-B information indicating the gated transmission used by the Node-B, and to determine from the signaling the on period and the off period of a duty cycle.

As mentioned, a UE could also change one or more of the values it uses for the thresholds Q_{out} and/or Q_{in}. This could be as an alternative to changing one or more of the N313, T313 and N315 parameters, or in addition. A UE could autonomously adjust the values it uses for the thresholds Q_{out} and/or Q_{in}, or it could select the values of the thresholds from a predefined set (in determining when out-of-sync or in-sync occurs and through out-of-sync / in-sync indications determining when a radio link failure is deemed to have occurred).

Instead of gating the downlink channel (and in particular, F-DPCH or DPCCH), the downlink channel could be continuously transmitted but discontinuously power controlled due to uplink gating, i.e. power control commands could be sent only in downlink time slots corresponding to uplink time slots when the UE is transmitting. Alternatively, the downlink channel (F-DPCH or DPCCH) could be continuously transmitted, but discontinuously received by the UE, in order to improve UE power consumption. Discontinuous power control potentially degrades performance during uplink transmission gaps and right after the gaps. Therefore methods could be applied similar to those described above and below (for use in case of a gated downlink channel) that treat downlink

BNSDOCID: <WO____2007129180A2_I_>

transmission during periods corresponding to an uplink transmission gap similarly to downlink off periods (of a gated downlink). Discontinuous reception is in effect the same as a gated downlink channel from the standpoint of F-DPCH usage in the UE and performance.

Referring now to Figure 1A, a UE 11 is shown communicatively coupled to a Node-B 12a of a UTRAN 12, via a radio link having an uplink and a downlink, where the downlink is gated according to a gated transmission, and the uplink is also gated (and as explained above, may cause the gating of the downlink). As illustrated, the UTRAN also includes a Radio Network Controller (RNC) 12b, for controlling the Node-B in at least some respects, and for coupling the Node-B to a Core Network 14 (and hence ultimately to other communication terminals, not shown). The UE is shown as including a UE transceiver (TRX) 16a rigged for radio communication with a corresponding Node-B TRX 17a. The UE is shown as also including a Protocol Stack Layer-1 16b that operates the UE TRX 16a, and the Node-B is shown as including a peer Protocol Stack Layer-1 17b. The UE is shown as also including a data store 16c for holding values of the various parameters and/ or thresholds used in different embodiments of the invention, called here the sync parameters.

Figure 1B shows some components of the UE 11 of Figure 1A from a different perspective. The UE is shown as including a suitable radio front end 11a (including a wireless transceiver, not shown) coupled to a data processor 11b that in turn is coupled to a (volatile and/or non-volatile) memory structure 11c. The data processor can be for example a microprocessor, i.e. a programmable digital electronic component that incorporates the functions of a central processing unit on a single semiconducting integrated circuit. The radio front end may include a digital signal processor (not shown), or the data processor 11b may provide digital

BNSDOCID: <WO____2007129180A2_I_>

signal processing in respect to signals transmitted or received by the wireless terminal. The memory structure 11c stores program code that is executable by the processor 11b, including program code that is provided to implement all or part of the invention. The UE 11, as shown, can also include one or more application specific integrated circuits 11d, for providing some or all of the functionality of the UE, as an alternative to providing the functionality via stored instructions executed by the processor. Finally, the UE 11, as shown, includes a user interface (UI) 11e (usually including, among other things, a display, a keypad, a microphone, and a speaker), coupled to the data processor and possibly also to one or more of the one or more ASICs. The UE TRX 16a of Figure 1A is a component of the radio front end 11a. The UE Protocol Stack Layer-1 16b of Figure 1A can be implemented so as to include one or more ASICs 11d, and/or program code stored in the memory structure 11c executable by the data processor 11b, and/or one or more components of the radio front end 11a.

Although not illustrated in the drawings, it will be appreciated that each Node-B 12a also includes a radio front end and a data processor and a memory structure and may include one or more ASICs coupled as shown in Figure 1B, and the RNC 12b also includes a data processor and a memory structure and possibly one or more ASICs.

In general, the various embodiments of the UE 11 can include, but are not limited to, cellular telephones, personal digital assistants (PDAs) having wireless communication capabilities, portable computers having wireless communication capabilities, image capture devices such as digital cameras having wireless communication capabilities, gaming devices having wireless communication capabilities, music storage and playback appliances having wireless communication capabilities, Internet appliances permitting wireless Internet

BNSDOCID: <WO____2007129180A2_I_>

access and browsing, as well as portable units or terminals that incorporate combinations of such functions.

Referring now also to Figures 2 and 3, in a first step 31, the UE determines that the downlink is gated, and then in a next step 32 adjusts values of one or more of the sync parameters it uses (actually or only effectively, as described above) compared to values used in case of no gating of the downlink. The term "sync parameter" is used here to indicate any one or more of the N and T parameters (N313, T313 and N315), and/ or any one or more of the thresholds (Q_{out} and Q_{in}). The adjustment is based on the downlink gated transmission. (As explained above, the adjustment may be based on, or may be proportional to, the off period of the on/off duty cycle of the gated transmission.) In Figure 2, the UE is shown (optionally) obtaining original values of the procedures and then storing the changed sync parameters (i.e. their values) in a data store of the UE for use for example in determining when to declare a radio link failure (or otherwise responding to out-of-sync or in-sync indications). As indicated in Figures 1 and 2, the functionality for changing the sync parameters can reside in the layer one (physical layer) implementation (in hardware or software) of the UE protocol stack.

Referring now to Figure 4, the Node-B is indicated there as operative according to a first step 41 in which the Node-B determines that the UE is gating its uplink. The Node-B can make such a determination by for example monitoring the power received on the uplink channel in case of a dedicated channel. In a next step 42, the Node-B gates its downlink to correspond to the uplink gating by the UE. For example, as explained above, the Node-B can simply respond to power change requests actually received (during an on period of the UE uplink gated transmission), and even turn off its receiver during the off period of the UE uplink.

BNSDOCID: <WO____2007129180A2_I_>

The functionality described above as provided by the invention can be implemented as software modules stored in a non-volatile memory of a device such as a mobile station, and executed as needed by the device (or more specifically, an operating system of the device) copying all or part of the software into executable RAM (random access memory). Alternatively, the logic provided by such software can also be provided by an ASIC (application specific integrated circuit). In case of a software implementation, the invention provided as a computer program product including a computer readable storage structure embodying computer program code--i.e. the software--thereon for execution by a computer processor.

It is to be understood that the above-described arrangements are only illustrative of the application of the principles of the present invention. Numerous modifications and alternative arrangements may be devised by those skilled in the art without departing from the scope of the present invention, and the appended claims are intended to cover such modifications and arrangements.

BNSDOCID: <WO____2007129180A2_I_>

What is claimed is:

1. A method for use by a user equipment wireless communication terminal, comprising:

determining on periods and off periods of a gated transmission in connection with receiving power control commands over a downlink channel of a radio access network; and

varying a procedure used to determine when to declare a radio link failure based on the gated transmission by actually and/or effectively varying a quality measurement period used in the procedure or one or more parameter values used in the procedure.

2. A method as in claim 1, wherein the gated transmission corresponds to a gating of transmission power or a gating of only the power control commands or a gating of reception of the power control commands by the UE.

3. A method as in claim 1, wherein the procedure is varied by changing how to measure a parameter value used by the procedure.

4. A method as in claim 3, wherein the change in the procedure is to count occurrences of events corresponding to the parameter value only if the events occur during one or another of the on periods of the gated transmission, instead of counting occurrences of such events regardless of when the events occur.

5. A method as in claim 3, wherein the change in the procedure is to count occurrences of events corresponding to the parameter for a period of time longer than in case of no gating.

6. A method as in claim 5, wherein the procedure used to measure when the parameter value is changed includes evaluating

BNSDOCID: <WO____2007129180A2_I_>

power change commands received during a time window, and wherein the change in the procedure is to evaluate power change commands over a longer time window.

7. A method as in claim 6, wherein the longer time window is longer than the time window in case of no gating by an amount such that the same number of power change commands are evaluated as in case of no gating.

8. A method as in claim 1, wherein the procedure uses one or more parameter values including a number N313 of consecutive out-of-sync indications, and/or a number N315 of successive in-sync indications, and/or a number T313 indicating a length of time, and/or a first threshold Q_{out} for minimum quality and/or a second threshold Q_{in} for minimum quality, and wherein the radio link to the radio access network is declared failed according to the procedure if N313 consecutive out-of-sync indications are determined and then a time interval of T313 units of time expires before N315 consecutive in-sync indications are determined, wherein an out-of-sync indication is determined whenever a quality metric for the downlink channel falls below the first threshold Q_{out} for minimum quality, and an in-sync indication is determined whenever the quality metric exceeds the second threshold Q_{in} for minimum quality.

9. A method as in claim 1, wherein the on periods and the off periods each correspond respectively to an on period and an off period of a duty cycle, and wherein at least one of the parameter values is changed from a broadcast or predetermined value by an amount that is based on the off period compared to a whole period of the on/off duty cycle.

10. A computer program product comprising a computer readable storage structure embodying computer program code thereon for execution by a computer processor, wherein said computer program

BNSDOCID: <WO____2007129180A2_I_>

code comprises instructions for performing a method according to any of claims 1-9.

11. An application specific integrated circuit provided so as to operate according to a method as in any of claims 1-9.

12. An apparatus for use by a user equipment wireless communication terminal, comprising:

means for determining on periods and off periods of a gated transmission in connection with receiving power control commands over a downlink channel of a radio access network; and

means for varying a procedure used to determine when to declare a radio link failure based on the gated transmission by actually and/or effectively varying a quality measurement period used in the procedure or a parameter value used in the procedure.

13. An apparatus as in claim 12, wherein the gated transmission corresponds to a gating of transmission power or a gating of only the power control commands or a gating of reception of the power control commands by the UE.

14. An apparatus as in claim 12, wherein the means for varying a procedure is configured to vary the procedure by changing how to measure a parameter value used by the procedure.

15. An apparatus for use by a user equipment wireless communication terminal, comprising:

a first component of a physical layer implementation of a protocol stack of a wireless terminal, for determining on periods and off periods of a gated transmission in connection with receiving power control commands over a downlink channel of a radio access network; and

BNSDOCID: <WO____2007129180A2_I_>

a second component of a physical layer implementation, for varying a procedure used to determine when to declare a radio link failure based on the gated transmission by actually and/or effectively varying a quality measurement period used in the procedure or a parameter value used in the procedure.

16. An apparatus as in claim 15, wherein the gated transmission corresponds to a gating of transmission power or a gating of only the power control commands or a gating of reception of the power control commands by the UE.

17. An apparatus as in claim 15, wherein the second component is configured to vary the procedure by changing how to measure a parameter value used by the procedure.

18. An apparatus as in claim 17, wherein the change in the procedure is to count occurrences of events corresponding to the parameter value only if the events occur during one or another of the on periods of the gated transmission, instead of counting occurrences of such events regardless of when the events occur.

19. An apparatus as in claim 17, wherein the change in the procedure is to count occurrences of events corresponding to the parameter for a period of time longer than in case of no gating.

20. An apparatus as in claim 19, wherein the procedure used to measure when the parameter value is changed includes evaluating power change commands received during a time window, and wherein the change in the procedure is to evaluate power change commands over a longer time window.

21. An apparatus as in claim 20, wherein the longer time window is longer than the time window in case of no gating by an amount such that the same number of power change commands are evaluated as in case of no gating.

BNSDOCID: <WO____2007129180A2_I_>

22. An apparatus as in claim 15, wherein the procedure uses one or more parameter values including a number N313 of consecutive out-of-sync indications, and/or a number N315 of successive in-sync indications, and/or a number T313 indicating a length of time, and/or a first threshold Q_{out} for minimum quality and/or a second threshold Q_{in} for minimum quality, and wherein the radio link to the radio access network is declared failed according to the procedure if N313 consecutive out-of-sync indications are determined and then a time interval of T313 units of time expires before N315 consecutive in-sync indications are determined, wherein an out-of-sync indication is determined whenever a quality metric for the downlink channel falls below the first threshold Q_{out} for minimum quality, and an in-sync indication is determined whenever the quality metric exceeds the second threshold Q_{in} for minimum quality.

23. An apparatus as in claim 15, wherein the on periods and the off periods each correspond respectively to an on period and an off period of a duty cycle, and wherein at least one of the parameter values is changed from a broadcast or predetermined value by an amount that is based on the off period compared to a whole period of the on/off duty cycle.

24. A user equipment wireless communication terminal, comprising:

an apparatus as in claim 12; and

a transceiver for communicatively coupling with the radio access network, and configured to transmit to the radio access network.

25. A user equipment wireless communication terminal, comprising:

a radio front end;

BNSDOCID: <WO____2007129180A2_I_>

a processor communicably coupled to the radio front end; and

a memory coupled to the processor for storing a set of instructions, executable by the processor, wherein the instructions comprise:

determining on periods and off periods of a gated transmission in connection with receiving power control commands over a downlink channel of a radio access network; and

varying a procedure used to determine when to declare a radio link failure based on the gated transmission by actually and/or effectively varying a quality measurement period used in the procedure or a parameter value used in the procedure.

26. A system comprising a user equipment wireless communication terminal as in claim 24 or claim 25 and a radio access network including a wireless terminal for communicably coupling to the user equipment wireless terminal by transmitting downlink signals to the user equipment wireless communication terminal and by receiving uplink signals from the user equipment wireless communication terminal.

27. A system as in claim 26, wherein the wireless terminal of the radio access network is configured to:

determine that the uplink signals are being transmitted according to a gated transmission; and

gate the downlink signals to correspond to the uplink gating.

BNSDOCID: <WO____2007129180A2_I_>

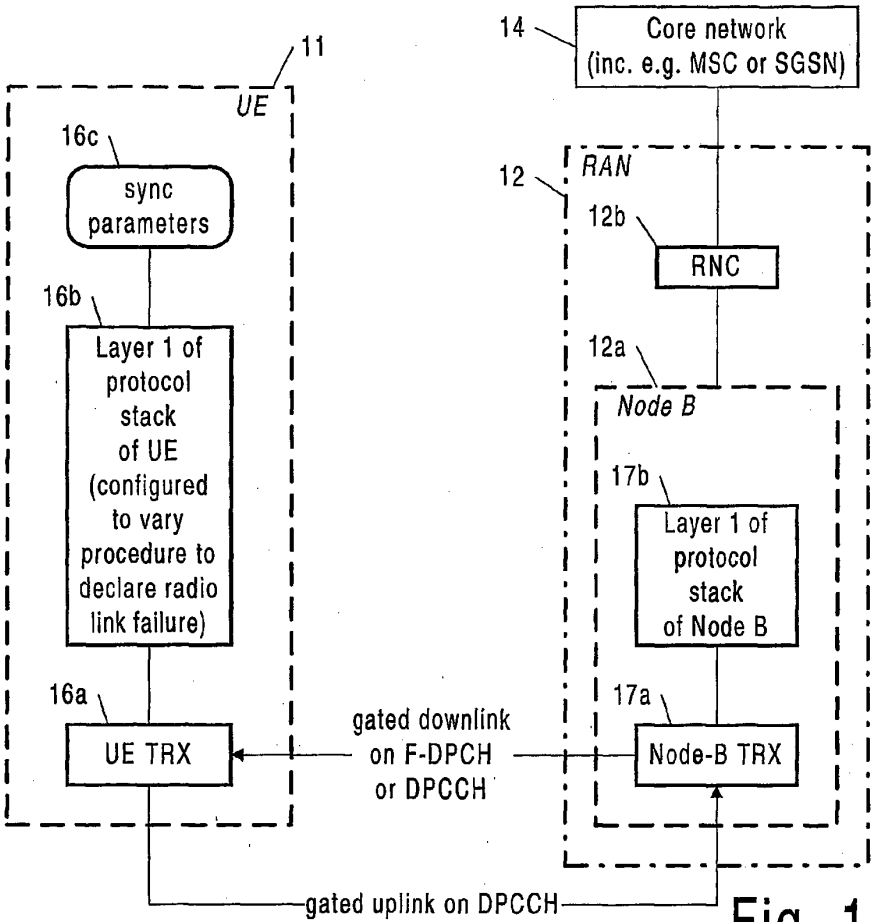


Fig. 1A

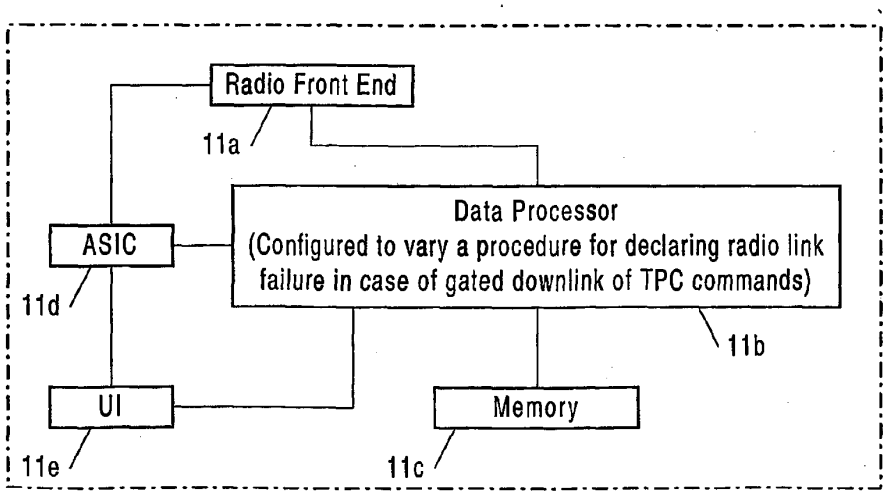


Fig. 1B

BNSDOCID: <WO_____2007129180A2_I_>

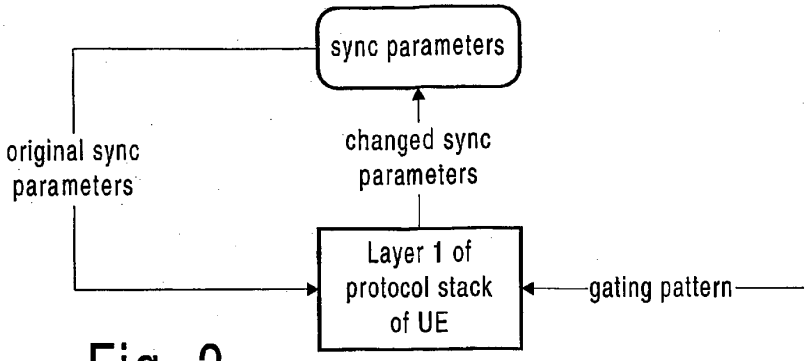


Fig. 2

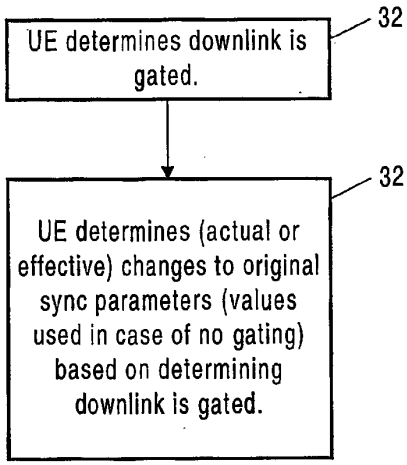


Fig. 3

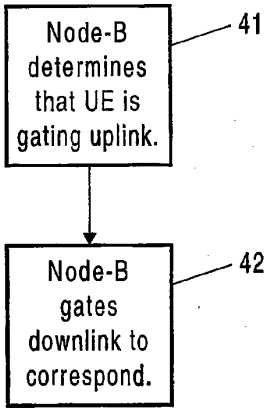


Fig. 4

BNSDOCID: <WO_____2007129180A2_I_>

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 November 2007 (15.11.2007)

PCT

(10) International Publication Number
WO 2007/129180 A3

(51) International Patent Classification:
H04B 7/005 (2006.01) *H04Q 7/32* (2006.01)

(21) International Application Number:
PCT/IB2007/001120

(22) International Filing Date: 30 April 2007 (30.04.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/797,943 5 May 2006 (05.05.2006) US

(71) Applicant *(for all designated States except US)*: **NOKIA CORPORATION** [FI/FI]; Keilalahdentie 4, FIN-02150 Espoo (FI).

(71) Applicant *(for LC only)*: **NOKIA INC.** [US/US]; 6000 Connection Drive, Irving, Texas 75039 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **KAIKKONEN, Jorma** [FI/FI]; Taskilantie 27 D 15, FIN-90580 Oulu (FI). **VIMPARI, Anna-Mari** [FI/FI]; Kummelintie 9, FIN-90520 Oulu (FI). **HINTZ-MADSEN, Mads** [DK/FI]; Luokkikuja 6, FIN-90310 Oulu (FI).

(74) Agents: **MAGUIRE, Francis, J.** et al.; Ware, Fressola, Van Der Sluys & Adolphson LLP, 755 Main Street, P.O. Box 224, Monroe, Connecticut 06468 (US).

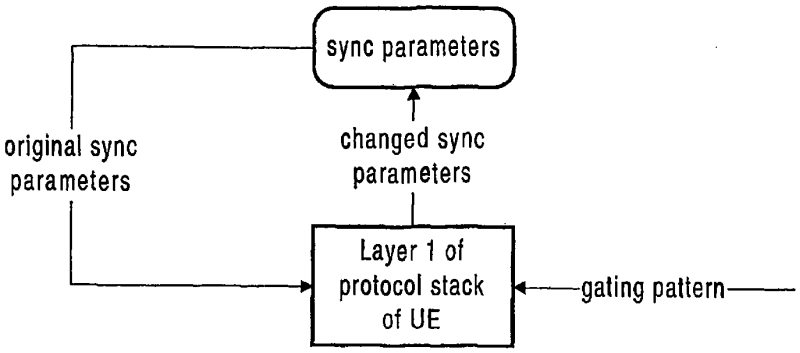
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, 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, HU, IE, IS, IT, LT, LU, LV, MC, MT, 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:
— *with international search report*

(88) Date of publication of the international search report:
28 February 2008

(54) Title: ENHANCED UE OUT-OF-SYNC BEHAVIOR WITH GATED UPLINK DPCCH OR GATED DOWNLINK F-DPCH OR DPCCH TRANSMISSION



(57) Abstract: A method and corresponding equipment by which a wireless terminal communicatively coupled to a radio access network adapts to gating in respect to a downlink signal from a radio access network carrying power control commands (e.g. the F-DPCH of UTRAN with WCDMA), including gating by the radio access network of either just the power control commands or the channel itself, or gating of reception of the power control commands by the user equipment. The adaptation can include changing values of parameters used in determining when the wireless terminal declares a radio link failure, or instead only changing the procedures used to determine whether a parameter value has been achieved and thus only effectively changing the parameter values (or one or more of the parameters can be actually and effectively changed).

WO 2007/129180 A3

BNSDOCID: <WO____2007129180A3_I_>

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB2007/001120

A. CLASSIFICATION OF SUBJECT MATTER

IPC: see extra sheet
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04B, H04L, H04Q

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

SE,DK,FI,NO classes as above

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

EPO-INTERNAL, WPI DATA, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	3GPP TS 25.331 V6.9.0 (2006-03), paragraph 8.5.4, 8.5.6	1-27
	--	
A	3GPP TS 25.101 V6.11.0 (2006-03), 3rd Generation Partnership Project: Technical Specification Group Radio Access Network: User Equipment(UE) radio transmission and reception (FDD) (Release 6), paragraph 6.4.4	1-27
	--	
A	3GPP TS 25.214 V6.8.0 (2006-03), 3rd Generation Partnership Project: Technical Specification Radio Access Network: Physical layer procedures (FDD) (Release 6), page 9-page 13	1-27
	--	

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
6 December 2007	10 -12- 2007
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Anders Ackeberg/ABW Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (April 2007)

BNSDOCID: <WO_____2007129180A3_I_>

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB2007/001120

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 1083678 A1 (LUCENT TECHNOLOGIES INC.), 14 March 2001 (14.03.2001), paragraphs [0013]-[0016]	1-27
	--	
A	US 20020112288 A1 (LUNDBY, S ET AL), 15 August 2002 (15.08.2002), paragraphs [0025]-[0028],[0035]-[0037],[0045], figures 3B-C, claims 1-9, abstract	1-27
	--	
A	US 6493541 B1 (GUNNARSSON, F ET AL), 10 December 2002 (10.12.2002), column 5, figure 8, abstract	1-27
	--	
A	US 20050281222 A1 (RANTA-AHO, K ET AL), 22 December 2005 (22.12.2005), paragraph [0017], abstract	1-27
	--	
A	3GPP TSG RAN2#47 Athens, Greece, 9-13 May, 2005. Change Request: "Faster L1 DCH synchronization". Paragraph 8.5.6	1-27
	--	

Form PCT/ISA/210 (continuation of second sheet) (April 2007)

BNSDOCID: <WO_____2007129180A3_I_>

International patent classification (IPC)
H04B 7/005 (2006.01)
H04Q 7/32 (2006.01)

Download your patent documents at www.prv.se
The cited patent documents can be downloaded at www.prv.se by following the links:

- In English/Searches and advisory services/Cited documents (service in English) or
- e-tjänster/anförda dokument (service in Swedish).

Use the application number as username.
The password is **YGPZDTUMYO**.

Paper copies can be ordered at a cost of 50 SEK per copy from PRV InterPat (telephone number 08-782 28 85).

Cited literature, if any, will be enclosed in paper form.

EP	1083678	A1	14/03/2001	CA	2316722	A	07/03/2001
				JP	2001103004	A	13/04/2001
				KR	20010050378	A	15/06/2001
				US	6571104	B	27/05/2003
US	20020112288	A1	15/08/2002	DE	10108635	A	19/09/2002
				JP	2002282238	A	02/10/2002
				US	6668403	B	30/12/2003
US	6493541	B1	10/12/2002	AU	6037800	A	22/01/2001
				TW	469708	B	21/12/2001
				WO	0103329	A	11/01/2001
US	20050281222	A1	22/12/2005	CA	2571423	A	05/01/2006
				EP	1759555	A	07/03/2007
				KR	20070030280	A	15/03/2007
				MX	PA06015030	A	08/02/2007
				WO	2006000876	A	05/01/2006

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

(11) EP 2 026 514 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
18.02.2009 Bulletin 2009/08

(51) Int Cl.:
H04L 12/56 *(2006.01)*

(21) Application number: **07425527.4**

(22) Date of filing: **14.08.2007**

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

(71) Applicants:
- **Nokia Siemens Networks S.p.A.**
  20126 Milano (IT)
- **Nokia Siemens Networks Oy**
  02610 Espoo (FI)

(72) Inventors:
- **Cavalli, Simona**
  21027 Ispra (VA) (IT)
- **Meago, Francesco**
  23100 Sondrio (IT)

(54) Resource management method for multi acces networks

(57) Every controller (RNC, BSC, E-NodeB, BS) of multi-RAT PLMN (UTRAN, GERAN, LTE, WiMAX) calculates for each controlled cell a MUB IE describing the availability of transport services in terms of maximum user bitrate that can currently be allowed to each transport service, separately for UL and DL, needed to plan usage of radio resources in the current and neighbouring cells, such as for handovers, cell reselections and new service setups. The MUB computation avails of:
-calculating an available capacity for a given service by taking a normalised capacity accessible to said service and by subtracting to it a normalized load of said service and of any other service that cannot be pre-empted by said service;
-calculating the MUBN for said service as the minimum between said available capacity and the maximum capacity MAXUB allowed to the single user for said service as a configuration setting;
-calculating a quantized representation MUB of the MUBN for said service as the nearest power of two raised at an integer n.

The MUB is included into management messages forwarded to the other controllers, either of the same or different technologies. Every controller checks the received MUB coming from the other controllers in order to decide on the most suited target cell, among the current and neighbouring cells, for resource management issues such as handover, cell reselection, and new service set-up (fig.6).

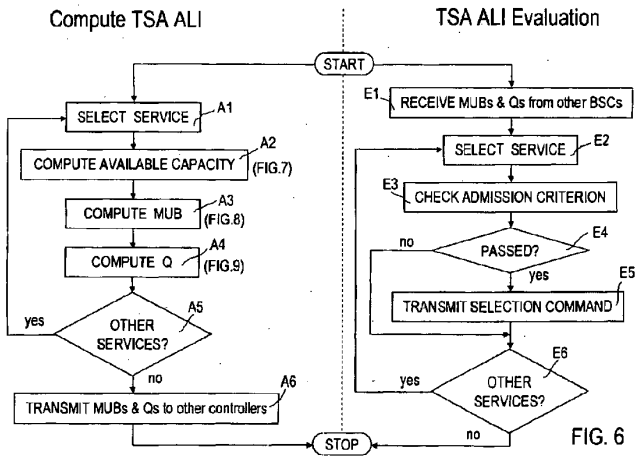


FIG. 6

Printed by Jouve, 75001 PARIS (FR)

EP 2 026 514 A1

BNSDOCID: <EP_____2026514A1_I_>

Description

FIELD OF THE INVENTION

[0001] The present invention relates to the so-called Ambient Networks (AN), and in particular to a resource management method for multi-access networks. (Used acronyms description and bibliographic references are given at the end of the description).

BACKGROUND ART

[0002] The communications industry has a truly historic opportunity over the coming years to connect the majority of the world using mobile, wireless broadband and fixed broadband systems. As a result, in 2015 we will live in a world, in which five billion people are connected, most of them 'always on' with a broadband connection. People can use the services they want anytime, anywhere with their preferred devices.

[0003] The Internet will be the dominant platform to connect these five billion people and their various devices with each other, and to provide access to a great variety of content and applications. Mobility will dominate in voice services with 70-90% of all traffic, depending on the market.

[0004] Broadband IP connections will be available practically anywhere in the world, across developed and growth markets. A combination of mobile, wireless and fixed systems will ensure global coverage, full mobility and adequate speed and capacity. In the growth markets mobile and wireless broadband will play a crucial role in broadband coverage.

[0005] In the converged telecom, Internet, media and IT landscape there will be a much larger variety of services providers and business models compared to today's telecom environment. Each provider will compete in a larger market than traditionally seen, creating both a huge opportunity and increased competition.

[0006] Taking into account said converged landscape, future internetworking will continue to signify "the interaction of heterogeneous networks", today including cellular, wireless and wire-line networks, public and private, belonging to users and operators. In this context the Ambient Networks project (see Ref. [1], [2], and [3] at the end) works for specifying a system capable to handle future internetworking by enabling dynamic composition of networks and establishment of inter-network agreements, coexistence of multiple access technologies, multi-operator and multi-hop functions, mobility and security support. The vision for multi-access operations is characterized by heterogeneous access technologies, radio or fixed, through which data may flow in series (multi-hop) or in parallel, alternatively or concurrently.

[0007] To enable multi-access operations, efficient resource management methods need to consider the diverse characteristics of the heterogeneous access technologies. This translates into the need to identify how the dissimilar access resources should be abstracted in order to provide the most suited building block for resource management operations, optimizing the trade-off between performance of the adopted resource management schemes, and cost of signalling and processing as contextualized in today's technologies. Started in January 2004 as part of the IST 6th Framework Programme of the European Union, the Ambient Networks project is developing a new networking environment providing thorough inter-working among today's networks, characterized by their diverse features and services. The objectives include enabling the emergence of new businesses, as well as stimulating continuous growth in the communication market.

[0008] Ambient Networks described in Ref.[3] realizes its objectives through the definition of a new network convergence layer, the "Ambient Control Space" (ACS), as a control stratum typically referred to as an overlay, where the envisaged Ambient Networks functionality is introduced. Open implementation options exist how this networking realm should be realized, while the main interfaces are under specification process.

[0009] **Fig.1** schematizes a typical Ambient Network (AN) scenario characterised by the ACS as a control plane, and an Ambient Connectivity (ACY) functionality. The ACS includes a number of functionalities capable of managing Multi-radio Access, Context information, mobility, security and even more. The ACS includes interfaces towards the higher layers of control functionality, such as user applications through the Ambient Service Interface (ASI), and also includes Ambient Resource Interfaces (ARI) towards the ACY, i.e. the lower layers of control functionality. ANs and their respective ACSs interact through the ANI. ASI, ARI and ANI are logical interfaces that may run over heterogeneous communication means and access technologies.

[0010] The issue of multi-access in the ACS described in Ref.[4] mainly refers to criteria how resource management may handle communication paths of diverse access technology both in series and in parallel, alternatively or concurrently. For solving this issue, it is of primary importance to identify suitable abstractions of the access resource through which the ACS can view and control the "Ambient Connectivity" layers, where technology-specific communication paths are accessible via the "Ambient Resource Interface" (ARI). **Fig.2** schematizes a process involving both ACS and Ambient connectivity in which technology-specific information needs to be abstracted up to a level and to a type that allows provisioning the envisaged multi-access operations in the ACS through respective algorithms. To this aim, "Abstracted (load) information" is defined as a more generic type of information, typically technology-independent, or quasi-technol-

BNSDOCID: <EP_____2026514A1_I_>

ogy-independent, obtained by transformation through algorithms (abstraction layer algorithms) from a technology specific information. The goal is therefore not only defining the most suitable abstractions, but also providing the related mechanisms and algorithms for the technology-specific Abstraction Layers, together with the related access selection and admission control algorithms for the ACS.

[0011] Cell Capacity/load abstractions have been suggested up to now within discussions around load balancing in 3GPP for achieving a timely specification enabling some coordination between RNCs and BSCs. Cell load is a measurement typically easy to retrieve from parameters like total transmitted power, interference, number of occupied timeslots, etc.

[0012] "Transport Service Availability" (TSA) abstraction, limitedly to the bearer service, is disclosed in Patent application EP-A1-1503606 of the same inventors, which describes: a common radio resource management method in a mobile radio communication network employing different radio access technologies that overlap over a geographic area subdivided into cells belonging to the domains of respective controllers which are connected to each other in overlapping or adjacent domains and to a core network by means of relevant interfaces, suitable to be carried out for each controlled cell by the respective controller through the steps of:

- starting from acquired information about QoS and throughput of all the active connections with the served mobile terminals (UE/MS), calculating traffic-related Information Elements, separately for uplink and downlink, needed to plan handovers and/or cell reselections; said traffic-related Information Elements including indications of the availability of bearer services in the cell in terms of maximum bitrate, either guaranteed or not guaranteed, that can currently be allowed to each bearer service, said bearer service being distinguished by traffic class due to the different QoS characteristics of the bearer services in terms of Eb/No, error rates, priorities, and delay;
- including said traffic-related Information Elements in management messages forwarded to the controllers of different cells to the one in turn considered, either of the same or different technologies;
- checking said traffic-related Information Elements coming from the other controllers (BSC, RNC) in order to decide either of issuing or preventing handovers and/or cell reselection commands towards a neighbouring cell.

OUTLINED TECHNICAL PROBLEM

[0013] The teaching of the aforementioned document EP-A1-1503606 was only directed to announce the Bearer Service Availability as an exemplary abstraction based on Transport Service, but none other than reference to generic tables it is said of how calculating the Bearer Service Availability, so it is not currently known how to produce Transport Service Availability information elements. Without an effective criterion of how calculating said TSA, the access network controllers originating the information cannot "forecast" the outcome of the resident admission control algorithms for the specific service to be admitted.

OBJECT AND SUMMARY OF THE INVENTION

[0014] The main object of the present invention is that to overcome the lack of a clear teaching in the prior art of how calculating a transport service availability information element.

[0015] The invention achieves said object by providing a radio resource management method in a mobile radio communication network employing different radio access technologies, e.g.: UTRAN, GERAN, LTE, WiMAX, that overlap over a geographic area subdivided into cells belonging to the domains of respective controllers (RNC, BSC, E-NodeB, BS), including the following steps carried out by every controller for each controlled cell:

a) calculating a transport service availability information element, called hereafter MUB, describing the availability of transport services in terms of maximum user bitrate that can currently be allowed to each transport service, separately for uplink and downlink, needed to plan usage of radio resources in the current and neighbouring cells, such as for handovers, cell reselections and new service setups; the computation at step a) including at least the following substeps executed for each implemented service characterised by service type and high/low priority:

a1) calculating an available capacity for a given service by taking a normalised capacity accessible to said service and by subtracting to it a normalized load of said service and of any other service that cannot be preempted by said service;

a2) calculating the MUBN for said service as the minimum between said available capacity and the maximum capacity MAXUB allowed to the single user for said service as a configuration setting;

a3) calculating a quantized representation MUB of the MUBN for said service for transmission over digital transmission means;

BNSDOCID: <EP_____2026514A1_I_>

b) including said MUB information elements calculated as above into management messages forwarded to the other controllers, either of the same or different technologies;
c) checking said MUB information elements coming from the other controllers (BSC, RNC, E-NodeB, BS) in order to decide on the most suited target cell, among the current and neighbouring cells, for resource management issues such as handover, cell reselection, and new service setup, as described in claim 1.

[0016] Details on the calculation and other aspects of the invention are described in the dependent claims.

[0017] A radio resource management method which avails of the precise teaching of how calculating TSA information according to the present invention, constitutes an effective improvement of the access selection and admission control algorithms in the control space of the Ambient Networks.

[0018] The smartness of the method has been tested by means of a comparative emulation applied to a GSM access network between TSA Abstraction Layer Information (ALI) calculated according to the method of the invention and 3GPP ALI based on Cell capacity/load. To the only aim of the emulation, some algorithms have been appositely developed also for calculating 3GPP (GSM) ALI and successively using it in evaluating some selection criteria of target cells for a given service.

[0019] Finally, a comparative algorithm between performances of two types of ALI has been developed for calculating the admission control error probability versus minimum cell load using 3GPP ALI instead of TSA ALI in emulating a GSM scenario characterized by a single target cell. The outcome of the comparative algorithm is the bunch of error curves reported in **fig.10** which clearly attests the superiority of TSA ALI calculated according to the method of the invention: typically, gains are higher for higher cell load, i.e. in the most critical situations.

BRIEF DESCRIPTION OF THE DRAWINGS

[0020] The invention and its advantages may be understood with reference to the following detailed description of an embodiment thereof taken in conjunction with the accompanying drawings given for purely non-limiting explanatory purposes and wherein:

- **fig.1** shows an Ambient Control Space and Connectivity diagram of the so-called Ambient Networks;
- **fig.2** schematized the mechanisms involved with the abstraction paradigm used at the ARI interface between ACS and Connectivity of fig.1;
- **fig.3** shows a known diagram of a Multi-RAT (GSM + 3G) PLMN as an exemplary scenario of Ambient Network;
- **fig.4** shows a very general diagram of the exchange of TSA Abstracted Load Information (ALI) calculated according to the method of the present invention, between a GSM controller and another Access Controller which performs TSA-based evaluation algorithms for traffic planning inside the network of fig.3;
- **fig.5** shows a very general diagram which differs from the previous one for the additional exchange of traditional 3GPP ALI based on capacity /load, so at the other Access Controller two evaluation algorithms for access selection can be compared to each other in order to calculate the evaluation error of the 3GPP ALI approach in respect of more correct evaluations performed by the algorithm which makes use of TSA ALI calculated according to the method of the invention;
- **fig.6** is the most general flow chart of GSM abstraction layer for computation of TSA ALI and concurrent execution of TSA ALI evaluation for admission control according to the method of the invention;
- **figures 7, 8, and 9** are flow charts relevant to corresponding steps of the flow chart of fig.6;
- **fig.10** shows a bunch of 3GPP ALI error curves versus minimum cell load (plotted for various services) in taking cell selection decisions comparatively based on both 3GPP ALI and TSA ALI, when the GSM scenario of fig.5 is emulated limitedly to a single target cell;
- **fig.11** shows an evolution of the Multi-RAT PLMN depicted in fig.3 as a future candidate to host the present invention;
- **fig.12** shows a diagram of inter E-Node B communication according to 3GPP Long Term Evolution (LTE) Access Network as another candidate to host the present invention;
- **fig.13** shows a similar diagram for a WiMAX Access Network as still another candidate to host the present invention.

DETAILED DESCRIPTION OF AN EMBODIMENT OF THE INVENTION

[0021] **Fig.3** shows a multi-RAT (Radio Access Technology) PLMN that will be soon completed in Europe. The new Universal Mobile Telecommunications System (UMTS) shares the existing GSM (Global System for Mobile communications) Core Network CN with the GPRS service. Relevant GSM RAN (Radio Access Network) in fig.3 is the so-called GERAN (GSM EDGE RAN), corresponding to the ultimate GSM RAN based on new EDGE (Enhanced Data rates for GSM Evolution) techniques that allow higher data rates in GSM, e.g. higher modulations. The Core Network CN is connected to one or more BSS (Base Station Subsystem) of the GSM, and to one or more RNS (Radio Network

BNSDOCID: <EP_____2026514A1_I_>

Subsystem) of an UTRAN (Universal Terrestrial Radio Access Network). The UMTS system of fig.3 is described in the TS 23.002 (CN) and TS 25.401 (UTRAN). Both the UTRAN and BSS are connected, on air, to a plurality of User Equipment UE/MS, each including a Mobile Equipment ME with a respective USIM card (UMTS Subscriber Identity Module). The present invention applies to UEs of single but preferably multistandard type: so that they are indicated as UE/MS (without limitation, often the only term UE is indicated). The UTRAN includes a plurality of Node B blocks each connected to a respective Radio Network Controller RNC by means of an Iub interface. A node B includes a Base Transceiver Station BTS connected to the UEs through an on-air Uu interface. The upper RNC is a Serving S-RNC connected to the Core Network CN by means of a first Iu(CS) interface for Circuits Switched and a second Iu(PS) interface for Packet Switched of the GPRS. It is also connected to an Operation and Maintenance Centre (OMC). The RNC placed below can be a Drift D-RNC and is connected to the upper S-RNC by means of an Iur interface. The UTRAN with the served UEs constitute a Radio Network Subsystem (RNS) disclosed in TS 23.110.

[0022] The GSM - BSS block includes a plurality of BTSs connected to a Base Station Controller BSC by means of an Abis Interface and to the UEs through an on-air Um interface. The BSC is interfaced to the Core Network CN by means of a Gb interface (packet switched) and is further connected to a Transcoder and Rate Adaptor Unit TRAU also connected to the Core Network CN through an A interface. It is also connected to an Operation and Maintenance Centre (OMC).

[0023] The CN network includes the following Network Elements: Switching Centre MSC / Visitor Location Register VLR, Gateway MSC GMSC, Interworking Function IWF / Transcoder TC, Camel Service Environment CSE, Equipment Identity Register EIR, Home Location Register HLR, Authentication Centre AuC, Serving GPRS Support Node SGSN, and Gateway GPRS Support Node GGSN. The following interfaces are visible inside the CN block: A, E, Gs, F, C, D, Gf, Gr, Gc, Gn, and Gi. The IWF block translates the Iu(CS) interface into the A interface towards MSC / VLR block. The TC element performs the transcoding function for speech compression/expansion concerning UTRAN (differently from GSM where this function is performed outside the CN network) also connected to the MSC block through the A interface. The GMSC is connected to the MSC / VLR through the E interface and to a Public Switched Telephone Network PSTN and an Integrated Services Digital Network ISDN. Blocks CSE, EIR, HLR, AUC are connected to the MSC / VLR through, in order, the Gs, F, C, and D interfaces, and to the SGSN node through the Gf and Gr interfaces. The SGSN block is interfaced at one side to the S-RNC inside UTRAN block by means of the Iu(PS) interface, and to the BSC inside the GSM-BSS block through the Gb interface. At the other side the SGSN node is interfaced to the GGSN node through the Gn interface. The last block is connected through the Gi interface to a packet data switching network of the IP (Internet Protocol) type and/or the X.25 type. The Core Network CN of fig.3 consists of an enhanced GSM Phase 2+, as described in TS 23.101, with a Circuit Switched CS part and a packet Switched part (GPRS). Another important Phase 2+ is the CAMEL (Customised Application for Mobile network Enhanced Logic) Application Part (CAP) used between the MSC and CSE for Intelligent Network (IN) applications. CAP is described in TS 29.078.

[0024] In operation, the MSC, so as the SGSN node, keep records of the individual locations of the mobiles and performs the safety and access control functions. More BSS and RNS blocks are connected to the CN Network, which is able to perform intrasystem handovers between adjacent RNSs or between adjacent BSSs, and intersystem handovers between a RNS and an adjacent BSS. UTRAN in respect of GSM further improves data service by making possible greater throughputs and the asymmetrical traffic typical of the Internet Protocol (IP). The network of fig.3, which only represents a minimal part of a world-wide network, shall allow the routing of a telephone call inside an International UMTS / GSM Service Area subdivided into National Service Areas. By way of the hierarchical structure of the network, each National Service Area is subdivided into the following nested domains of decreasing area: PLMN Service Area; MSC / SGSN Service Area; Location Area LA (CS-domain) uniquely defined by its LAI (Location Area Identity) code; Routing Area RA inside the SGSN Service Area as a partition of the CS Location Area; Cell Area where the UE is actually located in the radio coverage of a target Node B or BTS. Many known protocols described in the relevant standardization are deputed to govern the exchange of information at the various interfaces.

[0025] To the aim of the present invention the multi-RAT network of **fig.3** is a particular embodiment of the Ambient Network of **fig.1** whose controllers RNC and BSC are capable of handling TSA ALI calculated as will be described soon. More in particular, the functional blocks indicated in **figures 4** and **5** are mapped in the network of **fig.3.**

[0026] Referring also to **figures 11** to **13** for what concerns the SAE/LTE and WiMAX technologies, this figures being explained later in detail, we describe a method where different access technologies (including UTRAN, GERAN, LTE and WiMAX) totally or partially overlapping over a geographic area, or having respective neighbouring cells, are coordinated through their respective controllers (RNC, BSC, E-NodeB, BS, ...) for the sake of handovers, cell reselections and new service setups. The method is based on the calculation, exchange and evaluation of TSA information, including indication of the maximum user bitrate (MUB) and quantity (Q) that can currently be allowed to the single user for each service.

[0027] Now with reference to the **figures 6** to **9** a TSA ALI computation algorithm is described limitedly to the GSM case for the BSC, but this shouldn't constitute a bar for the skilled in the art in adapting the algorithm to the UTRAN or other RAT networks. Parallelly to the description of the TSA ALI computation algorithm a 3GPP ALI computation algorithm

BNSDOCID: <EP_____2026514A1_I_>

is described to the only aim of comparison between the twos and without dedicated figures.

[0028] We consider for GSM a number of transport service types including conversational circuit-switched services, Enhanced GPRS streaming services, non-real-time GPRS services and non-real-time Enhanced GPRS services. Also, we consider different service priorities for a portion of the described service types: in particular we consider as higher priority services the ones in handover, and as lower priority services any new service setup request.

[0029] We start describing the algorithm for computing the TSA information described in **fig.6 (leftmost part).** For each service (**fig.6,** steps A1 and A5), characterised by service type and service priority, we compute the available capacity (step A2), then we compute the MUB (step A3) and finally we compute the additional element Q (step A4) describing the quantity of available services at the bitrate indicated by MUB.

[0030] For computing the available capacity for a given service, we start by computing the accessible capacity to that service, which equals at first the total fixed cell capacity. However, when taking into account reserved capacities for different services, the accessible capacity for that service needs to exclude any capacity reserved to other services, for example resources reserved to circuit switched and/or packet switched services (**fig.7** step C1). In particular, reserved resources can be dynamically set in time according to policies, current resource usage and resource bookings.

[0031] Moreover, the accessible capacity is either all capacity accessible to the given service type for the highest service priority of that service, or a percentage of all capacity accessible to the given service type according to a respective load threshold set for lower service priorities (**fig.7** steps C2 and C3). When taking into account reserved capacities for different services, load thresholds for lower service priorities can be set on the reserved and shared capacities limiting the accessible capacity for those service priorities accordingly to a related portion.

[0032] Having computed the accessible capacity, its current occupation in terms of load needs to be considered. When there exist non-guaranteed resources given as a surplus resource to any service, the guaranteed load of any service needs to be computed as the current load in the portion required for providing a guaranteed Quality of Service, excluding any surplus resource currently allocated (**fig.7** step C4).

[0033] The available capacity for a given service is then computed (**fig.7** step C5) by taking the capacity accessible to the service and by subtracting to it the guaranteed load of that service and of any other service that cannot be pre-empted by that service. When taking into account reserved capacities for different services, the load of any other service that cannot be pre-empted by that service would be considered only in the portion of allocation into the capacity accessible to that service. Finally, when taking into account additional control signalling load, the available capacity for a given service would need not to include the capacity allocated for control signalling in the portion of allocation into the capacity accessible to that service.

[0034] The available capacity, together with the accessible capacity and the load of different services, can be computed in a number of ways, for example as a bitrate indication or a pure number. When computing it as a bitrate indication a normalisation criteria is required: for example for any service the capacity available can be computed first as a gross normalised bitrate as if the capacity available would be used by a reference service (e.g. voice), and only in a second step the capacity available can be expressed as net user bitrate through a conversion factor (**fig.7** step C6).

[0035] Once computed the available capacity for a given service, taking into account the maximum capacity MAXUB allowed to the single user for that service as a configuration setting, the algorithm needs to compute MUBN as the minimum between the available capacity and MAXUB (**fig.8** step M1). In particular, MAXUB can be dynamically set in time as a function of the available capacity. The algorithm then computes for the given service the TSA parameter MUB as a quantized representation of MUBN, for the sake of transmission over digital transmission means (**fig.8** step M2). This can be done in a number of ways, e.g. by taking the integer part of MUBN, or by taking the nearest power of two raised at an integer n.

[0036] Once computed MUB, and in particular MUBN, the algorithm computes QN describing the number of available services of bitrate MUBN as the ratio between the available capacity and MUBN (**fig.9** step Q1). Finally the algorithm computes for the given service the TSA parameter Q as a quantized representation of QN, for the sake of transmission over digital transmission means (**fig.9** step Q2). This can be done e.g. through thresholds on QN distinguishing a number of quantity levels.

[0037] When TSA is computed for each service of interest in terms of MUB and Q, this information is passed to other access controllers (**fig.6** step A6), which on need will use this information for performing access selection for a given service (**fig.6** step E1).

[0038] With regards to the access selection algorithms, **fig.6 (rightmost part)** describes the undertaken steps. First of all, a service is selected (**fig.6** step E2) for which an access selection decision needs to be taken, based e.g. on handover/cell reselection needs, new service requests and load management needs.

[0039] Regarding the access selection criterion (**fig.6** step E3) there exist two cases: the case where a single cell is evaluated as a potential target, and the case where two or more cells are compared as potential targets. In both cases the algorithms need to take the TSA information corresponding to that service. In the former case the algorithm needs then to check if the MUB information indicates the availability of the required bitrate for that service, in which case the cell is a suitable target cell. In the latter case instead the algorithm needs then to check if the MUB information indicates

BNSDOCID: <EP_____2026514A1_I_>

the availability of the required bitrate for that service in each cell, in which case the cells satisfying this requirement are suitable target cells, and if required finally check the Q information element of the different suitable target cells for selecting the cell with highest Q as the best target cell.

[0040] If a target cell could be selected (**fig.6** step E4), a selection command is transmitted (**fig.6** step E5), triggering e.g. handover/cell reselection requests of service setup requests towards the target cell. Concluding, the algorithm may be repeated for any additional service requiring access selection (**fig.6** step E6).

General assumptions

[0041]

- UUDL: in general, similar parameters and characteristics apply for uplink and downlink. For simplicity we refer e.g. to only DL for calculation and evaluation of the TSA, although similar work should be done for UL. Also, an aggregated figure could be obtained for UL and DL by combining the TSA for UL and DL.
- there exist resources reserved for different services (voice, GPRS) and priorities (voice handover), and/or vendor specific thresholds (e.g. new calls will be accepted only under 75% load). We assume for simplicity that for each service dedicated (reserved) resources are filled first, i.e. that the system can be configured as such.
- there exists a varying capacity occupied by signalling and other overheads (broadcast channels, coding, signalling for call setup, ...)
- there exist surplus resources, i.e. resources that are given to the user as a surplus, i.e. above the guaranteed bitrate, under favourable conditions. This exists only for RT services, as for NRT nothing is guaranteed. E.g. it considers the allocation of full-rate codecs or high-quality AMR codecs, that can be given under favourable load conditions, but which availability cannot be guaranteed.
- there exist different classes of terminals with different values for max throughput that can be provided to the user. Also, due to particular interference conditions, different terminals may adopt more or less favourable coding schemes. Still, we don't use these assumptions because the described realization of TSA is agnostic of the specific user exploiting the service.

DEFINITION OF ABSTRACTED RESOURCES

GSM Resource Status (RS)

[0042] The following characterization is defined in order to build the abstraction layers on something concrete. The information elements presented have the following requirements:

- They need to represent technology-specific resource abstractions.
- They need to significantly describe the status of the resources.
- They need to be obtainable, i.e. it must be possible to calculate them through specific modules.

[0043] We characterize GSM resource status (RS) as follows:

- C: a total fixed capacity, depending on the number of TRX/channels, in normalised kbit/s (normalised for a typical channel, e.g. voice under normal conditions - gross occupancy) [182.4 .. 8755.2 kbit/s]
- C(C), C(P): set of resources reserved to circuit (C) and packet (P) services [0 .. 8755.2 kbit/s]
- L: load parameter in normalised kbit/s indicating the gross total occupancy [0 .. 8755.2 kbit/s]
- L(RTC): load parameter in normalised kbit/s indicating the gross occupancy due to circuit RT services (voice) [0 .. 8755.2 kbit/s]
- L(RTP): load parameter in normalised kbit/s indicating the gross occupancy due to packet RT services (streaming)

BNSDOCID: <EP_____2026514A1_I_>

[0 .. 8755.2 kbit/s]

- L(NRT): load parameter in normalised kbit/s indicating the gross occupancy due to (packet) NRT services [0 .. 8755.2 kbit/s]

- L(S): load parameter in normalised kbit/s indicating the gross occupancy due to overheads including call signalling, L2 overheads and other overheads (BCCH, ... overhead not yet included in other parameters L(RTC), L(RTP), L (NRT)). [0 .. 8755.2 kbit/s]

- K(service): parameter indicating for every service the ratio between the net kbit/s of the user service (maximum for the best case, while possible) and the gross normalised kbit/s of the same service [k(service)].

    o k(conv) = 13 / 22.8 = 0.570

    o k(str) = 59.2 / 22.8 = 2.596

    o k(GPRS NRT) = 21.4 / 22.8 = 0.939

    o k(EGPRS NRT) = 59.2 / 22.8 = 2.596

- O(RTC): load parameter in normalised kbit/s indicating within L(RTC) the gross occupancy due to SURPLUS RT circuit services [0 .. 8755.2 kbit/s]. O(RTC)<L(RTC)

- O(RTP): load parameter in normalised kbit/s indicating within L(RTP) the gross occupancy due to SURPLUS RT packet services [0 .. 8755.2 kbit/s]. O(RTP)<L(RTP)

- S: load threshold above which the system does not accept requests for new guaranteed services (e.g. 0.75 (75%)).

[0044] 3GPP ALI (it is only used for the comparison with TSA ALI)
From 3GPP specifications, abstracted load information is characterized as follows:

- UL CCC: cell capacity class [1..100]
- DL CCC: cell capacity class [1..100]
- UL LV: load value [0..100] (linear, percentage of capacity)
- DL LV: load value [0..100]
- UL RTLV: RT load value [0..100] (linear, RT percentage of load value)
- DL RTLV: RT load value [0..100]
- UL NRTLI: NRT load indication [0..3] (low, medium, high, overload)
- DL NRTLI: NRT load indication [0..3]

TSA ALI (GSM)

[0045] We characterize abstracted load information in terms of "Transport Service Availability" (TSA), defined as follows:

- UL/DL information may be communicated separately or jointly.
- conversational TSA
- EGPRS streaming TSA
- GPRS NRT TSA
- EGPRS NRT TSA
- TSA includes: 1 bit for priority (high = 1, any = 0); 5 bits for max user bitrate according to a table, 1 bit for a quantity indicator (few / many).

ABSTRACTION LAYER ALGORITHMS

[0046] Abstraction layer algorithms are given for both 3GPP ALI and TSA ALI.
[0047] These algorithms are candidate for inclusion in the GLL Abstraction Layer, or in the abstraction layers below the ACS in general.

BNSDOCID: <EP_____2026514A1_I_>

Algorithms GSM RS → 3GPP ALI (it is only used for the comparison with TSA ALI) Assumption:
MPL = 0.95 (maximum planned load as a fraction of the maximum capacity).
Algorithms:
CCC = C / 182.4 (in this way CCC will go from 1 to 48, allowing other technologies to go further up)
LV = (L / (C x MPL)) x 100
L(RT) = L(RTC) + L(RTP)
RTLV = (L(RT) / L) x 100
NRTOCC = L(NRT) / (C - L(RT) - L(S))
NRTLI = 0 [NRTOCC < 0.3]; 1 [NRTOCC < 0.6]; 2 [NRTOCC < 0.9]; 3 [NRTOCC ≥0.9].
Algorithms GSM RS → TSA ALI (GSM) (is part of the invention)
Assumptions:
prio = priority
MAXUB(service, prio) = maximum capacity that the system can give to a single user as a configuration setting. It may be allowed to vary depending on load condition (e.g. the higher the load, the smaller MAXUB)
CATS(service, prio) = Considerable Amount of Transport Services: threshold on the number of transport services determining discrimination between availability in quantity "few" or "many" for the same transport service. E.g. CATS = 2.

Algorithms:

[0048] With reference to **fig. 6 (leftmost part)**, the TSA ALI computation algorithm starts with the execution of step A1 in which one out of n foreseen services is selected; in the successive step A2 the Available Capacity is calculated as will be illustrated in **fig.7.** The sequential steps A3 and A4 are devoted to computation of MUB (fig.**8**) and Q (fig.**9**) parameters: MUB is the maximum capacity that the system can give to a single user according to Cavail and configuration settings. MUB can be expressed as an integer: note that an integer value already represents a quantization of a real value. In real messaging, it would need to be coded in a more compact format, e.g. by using n, where 2 at the power of n would indicate the approximate maximum user bitrate. Quantity QN indicates the available number of described bearers or transport services, while Q is a quantized description of QN indicating e.g. whether few (0) or many (1) of the described bearers are available. In the next step A5 the computation is iterated to the other services. When all services are completed, the BSC transmits MUB and Q Information Elements (IE) to other controllers in step A6. Alternatively, the transmission might be executed inside the loop.

[0049] With reference to **fig.7,** for any service and prio the Available Capacity is calculated as indicated in steps C1 to C6 described hereafter for the various services:

```
*/for all services /*
GL(RTC) (Guaranteed L(RTC)) = L(RTC) - O(RTC)
GL(RTP) = L(RTP) - O(RTP)
GL(RT) = GL(RTC) + GL(RTP)
*/ conversational /*
if GL (RTP) < C(P)
Cavail(conv, any prio) = (C - C(P) - GL(RTC) - L(S)) x k(conv)
else Cavail(conv, any prio) = (C - GL(RT) - L(S)) x k(conv)
if GL(RT)/C > S ≥Cavail(conv, prio 0) = 0
*/ streaming /*
if GL(RTC) < C(C)
Cavail(str, any prio) = (C-C(C)-GL(RTP)-L(S)) x k(str)
else Cavail(str, any prio) = (C-GL(RT) - L(S)) x k(str)
if GL(RT)/C > S → Cavail(str, prio 0) = 0
*/ NRT /*
if GL(RTC) < C(C)
Cavail(NRT) = C-C(C) - GL(RTP)-L(NRT) - L(S)
else Cavail(NRT) = C-GL(RT) - L(NRT)-L(S)
Cavail(GPRS NRT, any prio) = Cavail(NRT) x k(GPRS NRT)
Cavail(EGPRS NRT, any prio) = Cavail(NRT) x k(EGPRS NRT).
    With reference to fig.8 and fig.9, for any service and prio,
if Cavail(service, prio) ≥MAXUB(service, prio) then {
MUBN(service, prio) = MUB(service, prio) = MAXUB(service, prio);
QN = Cavail(service, prio) / MAXUB(service, prio);
if QN > CATS(service, prio) then Q(service, prio) = 1 else Q(service, prio) = 0;}
else {
MUBN = Cavail(service, prio);
```


BNSDOCID: <EP_____2026514A1_I_>

```
MUB(service, prio) = int (MUBN);
QN(service, prio) = Q(service, prio) = 0;}
endif
```

ALI EVALUATION ALGORITHMS

[0050] Algorithms are given for both 3GPP ALI and TSA ALI.

[0051] These algorithms are candidate for inclusion in MRRM, or in access selection algorithms within the ACS in general.

3GPP ALI evaluation algorithm (it is only used for the comparison with TSA ALI). Input variables: service, 3GPP ALI info of candidate target cells

Note: the (100 - Cell_Load) x Cell_Capacity_Class gives the absolute free capacity in the cell. This is what needs to be compared in order to decide the best cell load-wise, in order to take into account different cell sizes.

Note: thresholds mechanisms are not included because we assume LV is relative to "the maximum planned load".

[0052] We do not make straight connection between CCC and kbit/s because it was not meant by the 3GPP solution to do so.

service: conversational RT, streaming RT, GPRS NRT, EGPRS NRT;

```
if there is only one candidate target cell
ranking = 0 (i.e. service cannot fit in)
if (service = RT and LV < 100) ranking = 1 (i.e. service can fit in)
if (service = NRT and NRTLI < 3) ranking = 1
if there are two candidate cells (1, 2) to be compared
ranking(1) = 0;
ranking(2) = 0;
freecapacity:
FC(1) = (100-LV(1)) x CCC(1);
FC(2) = (100-LV(2)) x CCC(2);
if (service = RT)
if FC(1) ≥FC(2) and FC(1) > 0 then
 ranking(1) = 1;
 else
 if FC(2) > 0 then ranking(2) = 1;
endif
endif
if (service = NRT)
if NRTLI(1) ≤NRTLI(2) and NRTLI(1) < 3 then
 ranking(1) = 1;
 else
 if NRTLI(2) < 3 then ranking(2) = 1;
endif
endif
```

TSA ALI evaluation algorithm (is part of the invention)

[0053] With reference to **fig. 6 (rightmost part)**, the TSA ALI Evaluation algorithm starts with the execution of step E1 in which MUBs and Qs IEs transmitted by other BSCs are received. The successive steps E2 to E6 is a loop to check for each service the access selection criterion and, if passed, transmit an access selection command for that service towards a target cell. In the following the TSA ALI Evaluation algorithm is better detailed. Input variables: service, prio, bitrate, TSA ALI info of candidate target cells

```
if there is only one candidate target cell
if MUB(service, prio) ≥bitrate then ranking = 1; else ranking = 0;
if there are two candidate cells (1, 2) to be compared:
ranking(1) = 0;
ranking(2) = 0;
if Quantity(1, service, prio) ≥Quantity(2, service, prio) and MUB(1, service, prio) ≥bitrate
then
ranking(1) = 1;
else
if MUB(2, service, prio) ≥bitrate then ranking(2) = 1;
```


BNSDOCID: <EP_____2026514A1_I_>

```
endif.
```

EVALUATING TSA vs. 3GPP ALI PERFORMANCES (calculates the curves of **fig.10**)

[0054] Now 3GPP and TSA approaches are compared within a scenario characterized by a single target cell, where a controller has to decide if a given service fits or not in the target cell based on the ALI.

[0055] The comparative evaluation algorithm provides estimation of the difference in admission control success rate implied by use of 3GPP ALI vs. TSA ALI. By performing the evaluation for different values of minimum cell load, we obtain curves. The method is rather fast, since each RS configuration is considered only once.

[0056] The comparative algorithm does not emulate variations in the RS that could allow measuring the effects of aged information on both 3GPP ALI and TSA ALI. However, results show that TSA performs better then capacity/load even when generation and evaluation of the abstractions are done simultaneously.

[0057] Variables and parameters considered in the evaluation includes: Service type; Resource status.

Service type

[0058] The following service types are considered:

1. Conversational, MUB =13 kbit/s (Max User Bitrate), prio = 1 (e.g. handover)
2. Conversational, MUB =13 kbit/s, prio = 0 (e.g. new service request)
3. EGPRS streaming, MUB = 59.2 kbit/s, prio = 1
4. EGPRS streaming, MUB = 59.2 kbit/s, prio = 0
5. GPRS NRT, MUB = 21.4 kbit/s
6. EGPRS NRT, MUB = 59.2 kbit/s

Resource Status (RS)

[0059] The RS Information elements: C, C(C), C(P), L, L(RTC), L(RTP), L(NRT), L(S), K(channel), O(RTC), O(RTP) and S have been already defined.

Setting GSM RS parameters and variable limits

[0060] In the following, we assign values to GSM RS parameters and variable limits. Parameters:

- TRX = 182.4 kbit/s
- C = 5 x TRX kbit/s
- C(C) = 2 x TRX kbit/s
- C(P) = 1 x TRX kbit/s
- K(channel):
    - o k(conv) = 13 / 22.8 = 0.570
    - o k(EGPRS str) = 59.2 / 22.8 = 2.596
    - o k(GPRS NRT) = 21.4 / 22.8 = 0.939
    - o k(EGPRS NRT) = 59.2 / 22.8 = 2.596
- S = 0.75
- Sigmin = 0.04
- Sigmax = 0.08
- Op = 0.5
- Step = 8 kbit/s
- StepSig = 0.01
- Lmin: 60% = 0.6*C = 1094.4 kbit/s (we emulate loaded situations only, therefore the overall load ≥Lmin)

Variable limits:

- L [C x Lmin .. C kbit/s]
- L(RTC) [0 .. (C - C(P)) kbit/s]
- L(RTP) [0 .. (C - C(C)) kbit/s]

BNSDOCID: <EP_____2026514A1_I_>

- L(NRT) [0 .. (C - C(C)) kbit/s]
- L(S) [Sigmin x L .. Sigmax x L kbit/s]
- O(RTC) [0 .. Op x L(RTC)]
- O(RTP) [0 .. Op x L(RTP)]

COMPARATIVE EVALUATION ALGORITHM

[0061] This algorithm goes through each configuration of interest for the RS and performs evaluation.

```
Count = 0;
Errcount(..) = 0;
Cc = C-C(P);
For L(RTC) = 0 to Cc step = Step
{Coc = Op x L(RTC);
Cp = min (C-C(C), C-L(RTC));
For O(RTC) = 0 to Coc step = Step
{For L(RTP) = 0 to Cp step = Step
  Cop=Op x L(RTP);
 {For O(RTP) = 0 to Cop step = Step
   {Lrt = L(RTC) + L(RTP);
     Cnrt= Cp - L(RTP);
     For L(NRT) = 0 to Cnrt step = Step
     {Lt = Lrt + L(NRT);
      For Sig = Sigmin to Sigmax step StepSig
      {L(S) = Lt x Sig;
        L = Lt + L(S);
        if L ≤C and Lmin < L
        {Count = Count + 1;
          For any service:
          {Errcount(service) = Errcount(service) + XOR (ALlevaluation(service,
3GPP ALI (RS)), ALlevaluation(service, TSA ALI (RS));}}}}}}}}.
```

[0062] The next **figures 11, 12,** and **13** report some future 3GPP and WiMAX network architectures candidate to host the present invention.

[0063] With reference to fig.**11**, 3GPP System Architecture Evolution (SAE) is a recent architectural development for the 3GPP system reported as a feasibility study in 3GPP TR 23.882 v1.9.0, "3GPP System Architecture Evolution: Report on Technical Options and Conclusions (Release 7)", March 2007.

[0064] SAE is composed by an Evolved Packet Core (EPC) that connects to several access networks, other core networks (including the legacy GPRS core network) and external elements. External elements include Policy and Charging Rules Function (PCRF, interface S7), Home Subscriber Server (HSS, interface S6), Operator IP Services or external Packed Data Networks (interface SGi). In particular, EPC connects to several access networks including Evolved RAN (also called LTE RAN, interface S1), trusted non-3GPP IP access including trusted fixed IP access (interface S2a), VVLAN access network. Within the EPC, the Mobility Management Entity (MME) and User Plane Entity (UPE) connect to the Evolved RAN (interface S1), the enhanced Packet Data Gateway (ePDG) connects to the VVLAV access network, while the inter Access System Anchor (IASA) connects to trusted non-3GPP IP access (interface S2a) and external Packet Data Networks (interface SGi). Regarding the elements within EPC, MME/UPE connects to IASA through interface S5a, IASA connects to ePDG through interface S2b. IASA is formed by the two additional elements 3GPP Anchor and SAE Anchor connected through S5b. EPC and GPRS Core networks may be interconnected in several ways (interfaces S3 and S4), for example through MME/UPE or through IASA. It should be noted that the presented SAE architecture is not the finalized architecture model for the evolved system, i.e. it does not contain all functions/interfaces required, and some functions/interfaces may be added, deleted or modified in the course of the key issue discussions within 3GPP.

[0065] With reference to fig.**12**, 3GPP Evolved RAN, or Long Term Evolution (LTE) RAN, or evolved UTRAN (E-UTRAN), is a recent architectural development for future 3GPP radio access networks, described in 3GPP TR25.813 v710. The LTE RAN is composed by Enhanced-NodeBs (E-NodeBs), directly interfacing to user terminals through antennas, connected to each other through interface X2, and connected to the EPC and in particular to an access Gateway through the interface S1 already described.

[0066] With reference to fig.13, the WiMAX Access Network is another access network being described in the IEEE 802.16 protocol suite and in documents originated by the WiMAX Forum. The WiMAX Access Network is composed by Base Stations (BS), directly interfacing to user terminals through antennas, possibly connected to each other through

respective interfaces, and connected to the Edge Router (also called Broadband Remote Access Server) through a respective interface. The WiMAX Access Network can connect to the 3GPP system via a Packet Data Gateway, ePDG or through an external Packet Data Network like the Internet.

[0067] In particular, TSA information along with its elements MUB and Q can be exchanged between entities such as E-NodeB, Access Gateway, MME/UPE, IASA, EPC, GPRS Core, BS, Edge Router and the controllers of any access network on the respective interfaces. For a GSM cell, TSA information can be exchanged between GERAN, GPRS Core and EPC, towards any relevant controller.

USED ACRONYMS

[0068]

3GPP	3rd Generation Partnership Program
ACS	Ambient Control Space
ALI	Abstracted Load Information
AMR	Adaptive Multi-Rate
AN	Ambient Network
ANI	Ambient Networks Interface
ARI	Ambient Resource Interface
ASI	Ambient Service Interface
BCCH	Broadcast Control CHannel
BS	Base Station
BSC	Base Station Controller
CS	Circuit Switched
DL	Downlink
E-NodeB	Enhanced NodeB
e-PDG	Packet Data Gateway
EGPRS	Enhanced GPRS
EPC	Evolved Packet Core
FC	Free Capacity
GERAN	GSM EDGE Radio Access Network
GLL	Generic Link Layer
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
HP	High Priority
HSS	Home Subscriber Server
HTTP	Hyper Text Transfer Protocol
IASA	Inter Access System Anchor
IE	information Element
IEEE	Institute of Electrical and Electronics Engineers
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IST	Information Society Technologies
LP	Low Priority
LTE	3GPP Long Term Evolution
MME	Mobility Management Entity
MPL	Maximum Planned Load
MRRM	Multi-Radio Resource Management
NRT	Non Real Time
NRTLI	Non Real Time Load Information
NSN	Nokia Siemens Networks
NW	Network
PCRF	Policy and Charging Rules Function
PS	Packet Switched
PSS	Packet-Switched Streaming service
QoS	Quality of Service
RA	Routing Area
RAN	Radio Access Network

BNSDOCID: <EP_____2026514A1_I_>

RAT	Radio Access Technology
RNC	Radio Network Controller
RRM	Radio Resource Management
RS	Resource Status
RT	Real Time
SAE	3GPP System Architecture Evolution
SGSN	Serving GPRS Support Node
TRX	Transceiver
TSA	Transport Service Availability
UE	User Equipment
UL	Uplink
UMTS	Universal Mobile Telecommunication System
UPE	User Plane Entity
UTRAN	Universal Terrestrial Radio Access Network
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network

REFERENCES

[0069]

[1] http//www.ambient.networks.org

[2] N. Niebert, A. Schieder, H. Abramowicz, G. Malmgren, J. Sachs, U. Horn, C. Prehofer, and H. Karl. Ambient Networks - An Architecture for Communication Networks Beyond 3G. IEEE Wireless Communications, 11(2):14-21, Apr. 2004.

[3] Deliverable D-1.5, "AN Framework Architecture", December 2005.

[4] P. Magnusson, F. Berggren, I. Karla, R. Litjens, F. Meago, H. Haitao, R. Veronesi, "Multi-radio resource management for communication networks beyond 3G,". IEEE 62nd VTC (2005).

Claims

1. Radio resource management method in a mobile radio communication network employing different radio access technologies (UTRAN, GERAN, LTE, WiMAX) that overlap over a geographic area subdivided into cells belonging to the domains of respective controllers (RNC, BSC, E-NodeB, BS), including the following steps carried out by every controller for each controlled cell:

   d) calculating a transport service availability information element, called hereafter MUB, describing the availability of transport services in terms of maximum user bitrate that can currently be allowed to each transport service, separately for uplink and downlink, needed to plan usage of radio resources in the current and neighbouring cells, such as for handovers, cell reselections and new service setups;
   e) including said MUB information elements into management messages forwarded to the other controllers, either of the same or different technologies;
   f) checking said MUB information elements coming from the other controllers (BSC, RNC, E-NodeB, BS) in order to decide on the most suited target cell, among the current and neighbouring cells, for resource management issues such as handover, cell reselection, and new service setup;

   characterised in that said calculating step a) includes in its turn the following steps executed for each implemented service **characterised by** service type and high/low priority:

   a1) calculating an available capacity for a given service by taking a normalised capacity accessible to said service and by subtracting to it a normalized load of said service and of any other service that cannot be pre-empted by said service;
   a2) calculating a MUBN parameter for said service as the minimum between said available capacity and the maximum capacity MAXUB allowed to the single user for said service as a configuration setting;

BNSDOCID: <EP_____2026514A1_I_>

a3) calculating a quantized representation MUB of the MUBN for said service for transmission over digital transmission means.

2. The method of claim 1, **characterized in that** said calculating step a) further includes for said service the steps of:

a4) calculating a parameter QN associated to MUB for said service and describing the number of available services of bitrate MUBN as the ratio between the available capacity and MUBN;
a5) calculating a parameter Q associated to MUB for said service as a quantized representation of QN for transmission over digital transmission means.

3. The method of claim 1, **characterized in that** in said step a1) the accessible capacity is either:

- all capacity accessible to the given service type for the highest service priority of said service or
- a percentage of all capacity accessible to the given service type according to a respective load threshold set for lower service priorities.

4. The method of claim 1, **characterized in that** said step a1) further includes the steps of:

- calculating the capacity accessible to said service by taking the total fixed cell capacity and by subtracting to it any capacity reserved to other services;
- considering the load of any other service that cannot be pre-empted by said service only in the portion of allocation into the capacity accessible to said service.

5. The method of claim 1, **characterized in that** said step a1) further includes subtracting the capacity allocated for control signalling in the portion of allocation into the capacity accessible to said service.

6. The method of claim 1, **characterized in that** said step a1) further includes considering the load of said service and of any other service that cannot be pre-empted by said service only in the portion required for providing a guaranteed Quality of Service, excluding any surplus resources currently given to said services.

7. The method of claim 1, **characterized in that** in said step a1) further includes using a conversion factor for translating normalised values of available capacity in net user bitrate indications of the same available capacity.

8. The method of claim 1, **characterized in that** in said step a2) further includes dynamically set in time the MAXUB as a function of the available capacity for the same service.

9. The method of claim 4, **characterized in that** further includes dynamically set in time said reserved capacities according to policies, current resource usage, resource bookings.

10. The method of claim 3 and 4, **characterized in that** further includes setting load thresholds on the reserved capacities for limiting access to the same capacities to a related portion, limiting in that the capacity accessible for lower service priorities.

11. The method of any claim from 1 to 10, **characterized in that** said MUB concerns conversational circuit-switched services.

12. The method of any claim from 1 to 10, **characterized in that** said MUB concerns Enhanced GPRS streaming services.

13. The method of any claim from 1 to 10, **characterized in that** said MUB concerns non-real-time GPRS services.

14. The method of any claim from 1 to 10, **characterized in that** said MUB concerns non-real-time Enhanced GPRS services.

15. The method of any claim from 1 to 10, **characterized in that** said MUB concerns low priority services.

16. The method of any claim from 1 to 10, **characterized in that** said MUB concerns high priority services.

BNSDOCID: <EP_____2026514A1_I_>

17. The method of claim 1, **characterized in that** when a cell is evaluated as a potential target for a given service, said checking step c) includes in its turn the following steps:

c1) selecting for said cell the MUB information corresponding to said service;
c2) checking if the MUB information indicates the availability of the required bitrate for said service, in which case the cell is a suitable target cell.

18. The method of claim 2, **characterized in that** when two or more cells are compared as a potential target cells for a given service, said checking step c) includes in its turn the following steps:

c1) selecting for said cells the MUB information corresponding to said service;
c2) checking if the MUB information indicates the availability of the required bitrate for said service, in which case the cells satisfying this requirement are suitable target cells;
c3) checking the Q information element associated to said MUB information of different suitable target cells and selecting the cell with highest Q as the best target cell.

BNSDOCID: <EP_____2026514A1_I_>

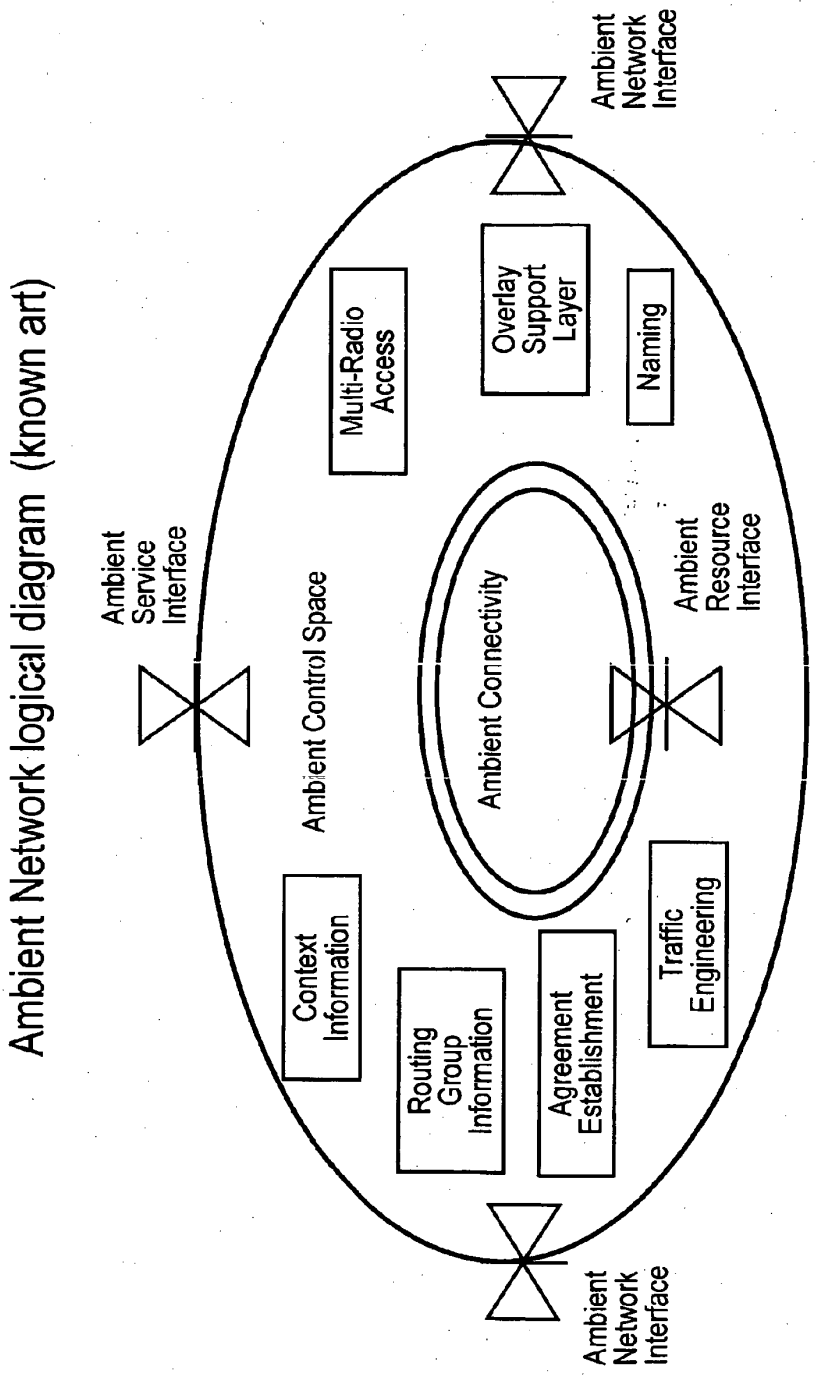


FIG. 1

BNSDOCID: <EP_____2026514A1_I_>

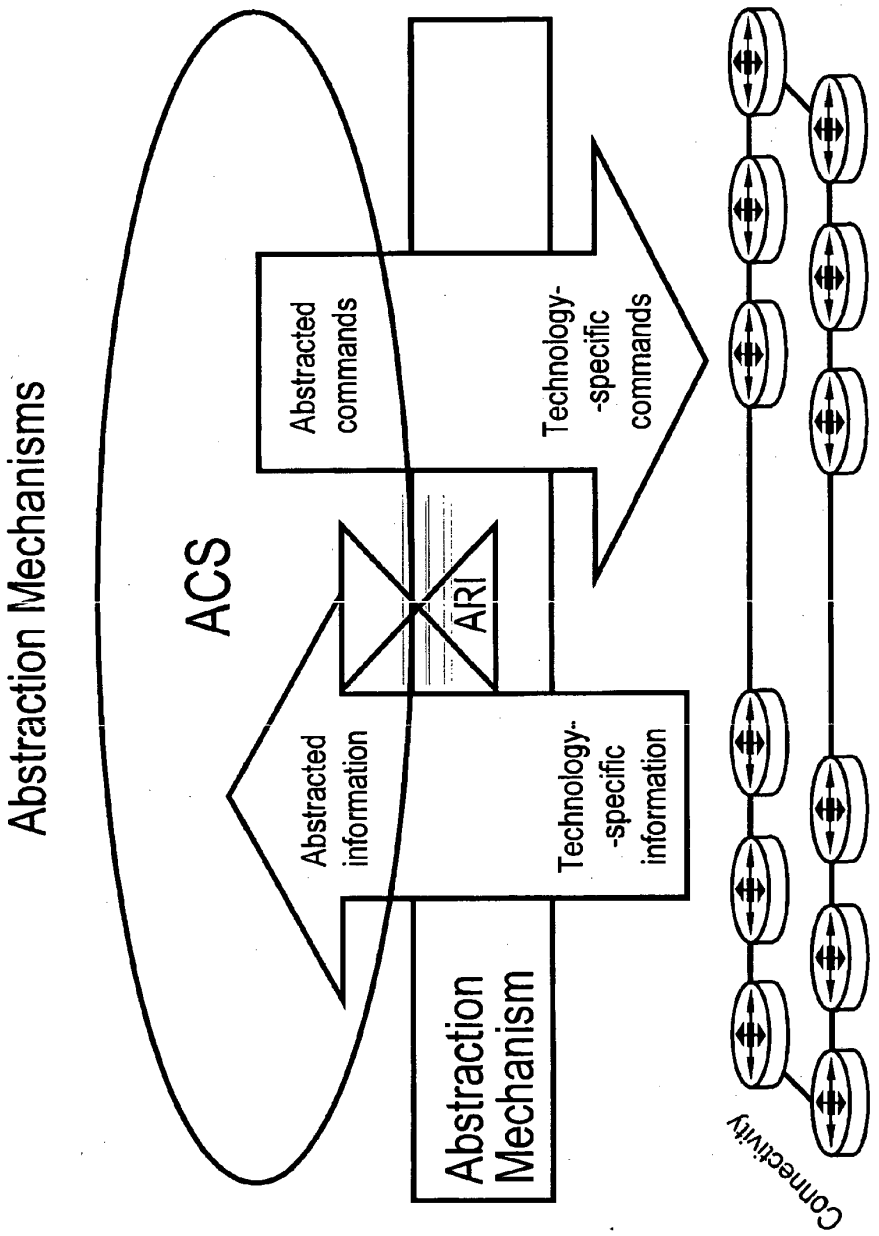


FIG. 2

BNSDOCID: <EP_____2026514A1_I_>

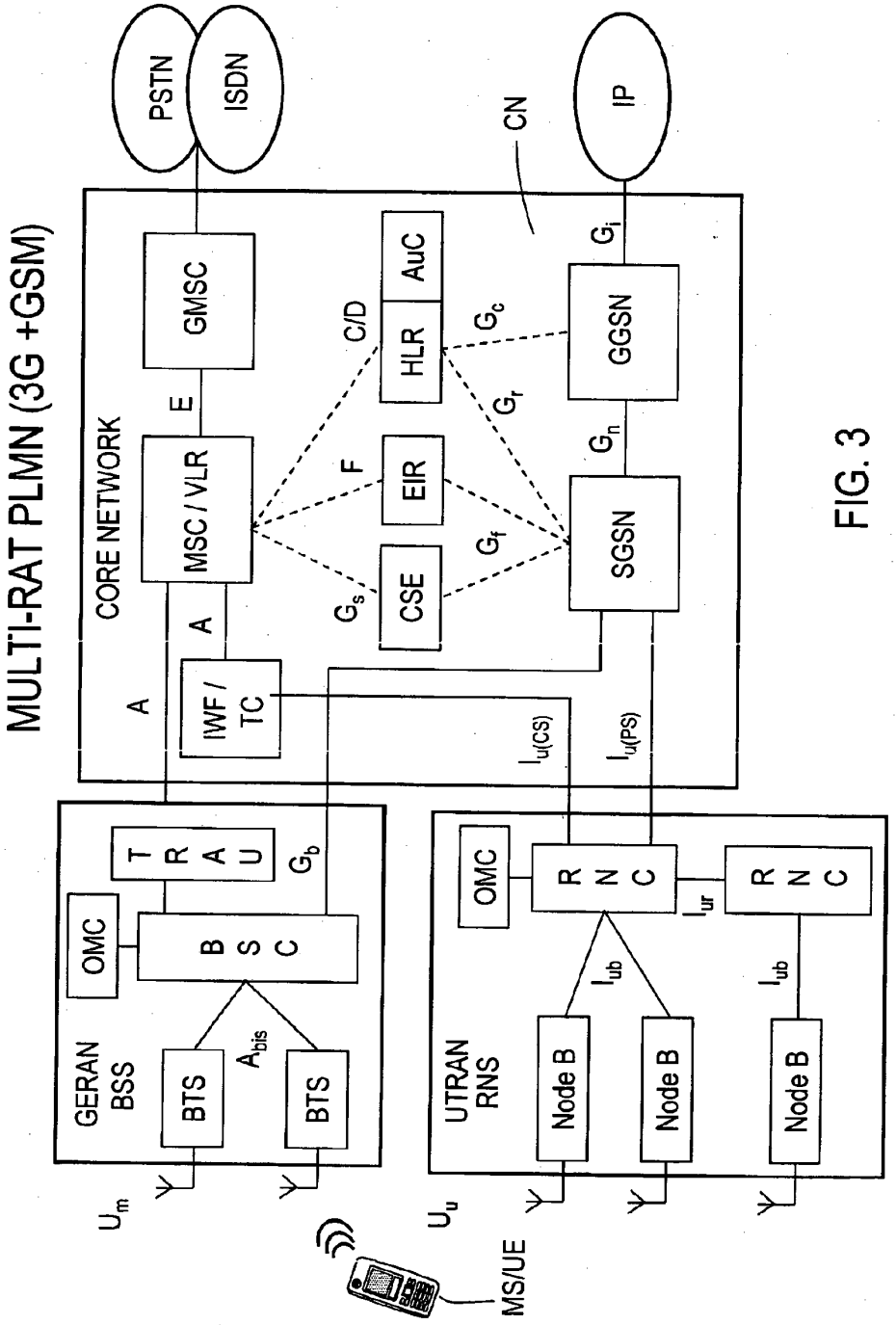


FIG. 3

BNSDOCID: <EP_____2026514A1_I_>

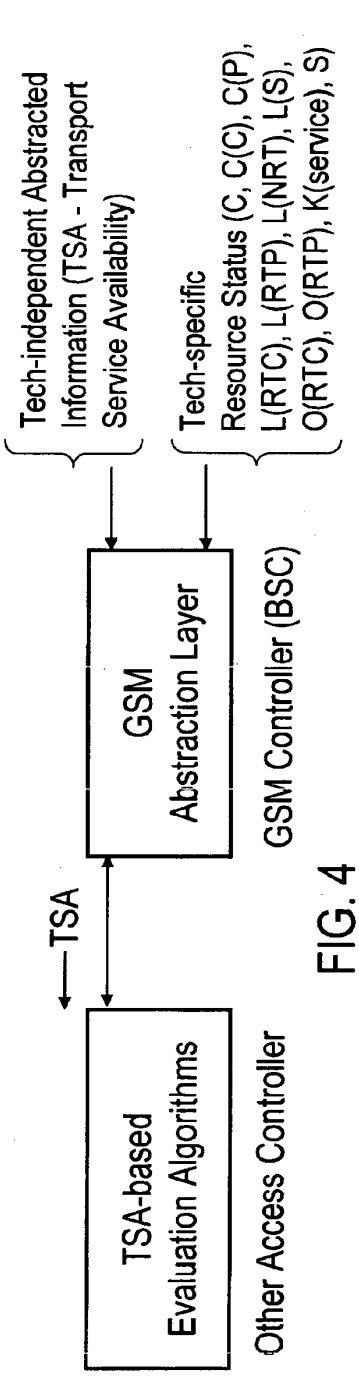


FIG. 4

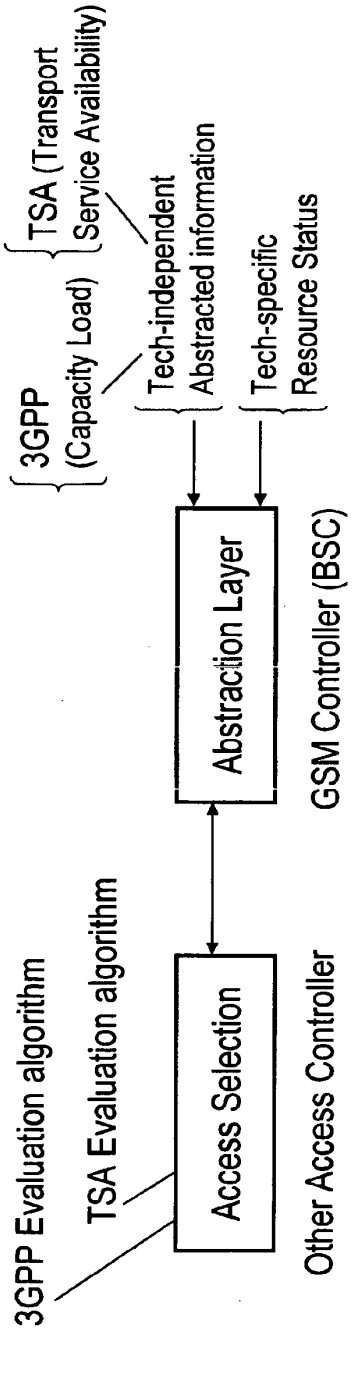


FIG. 5

BNSDOCID: <EP_____2026514A1_I_>

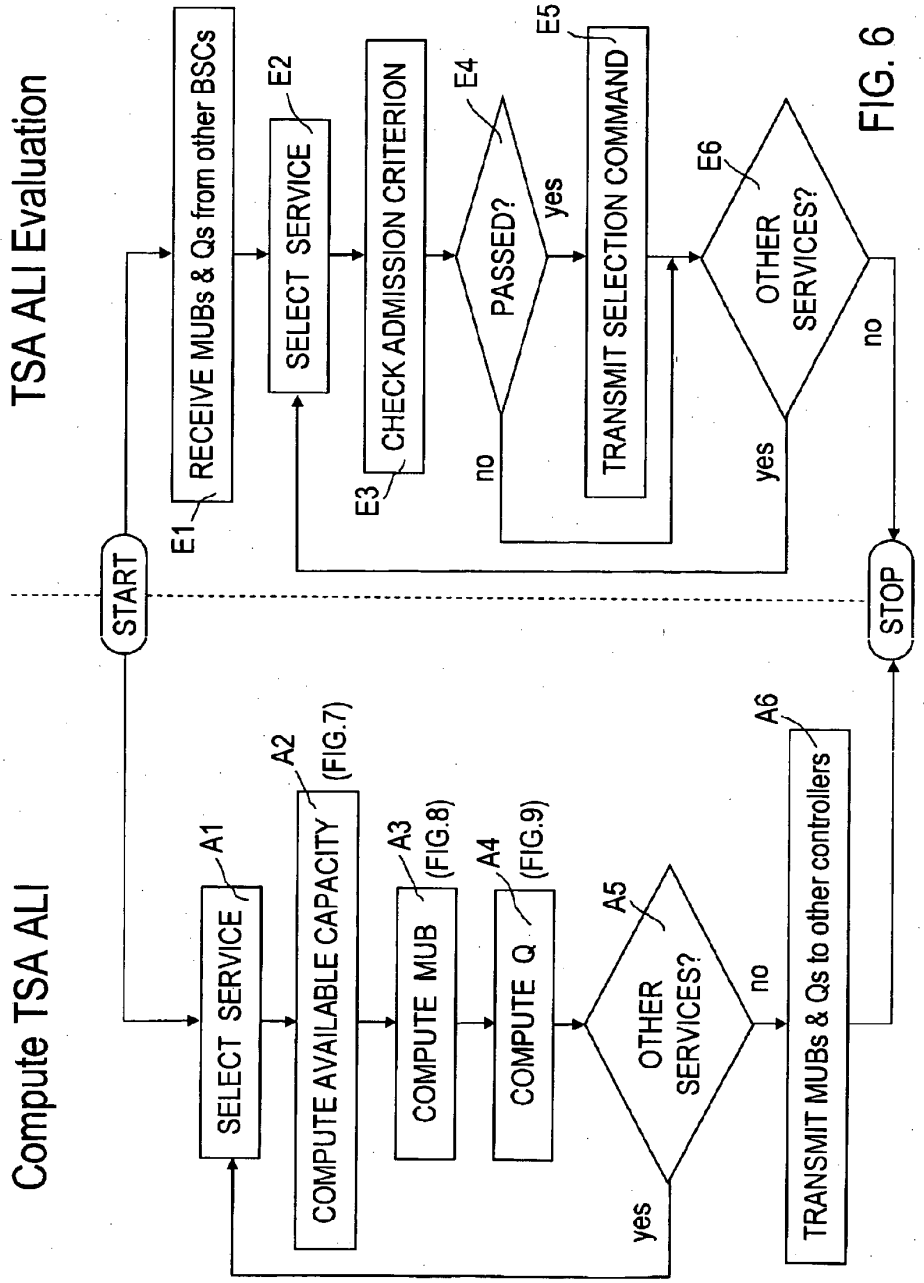


FIG. 6

BNSDOCID: <EP_____2026514A1_I_>

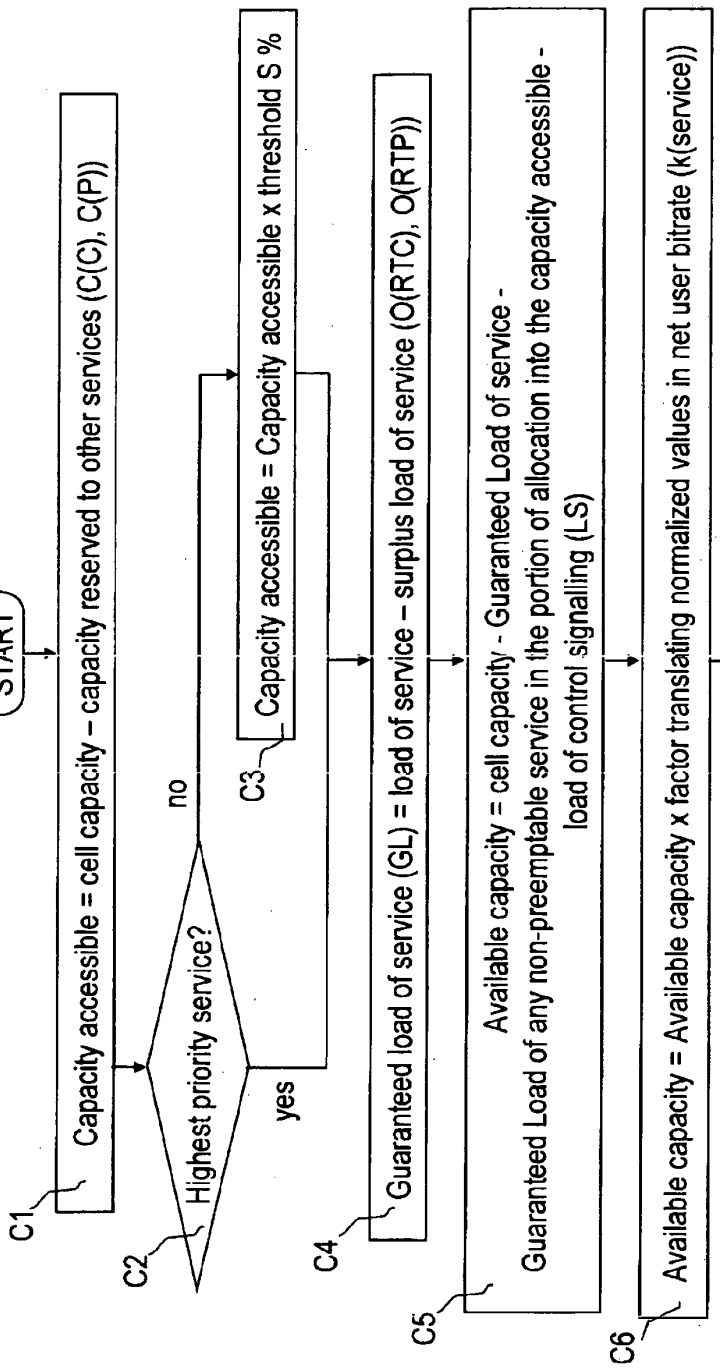


FIG. 7

BNSDOCID: <EP_____2026514A1_I_>

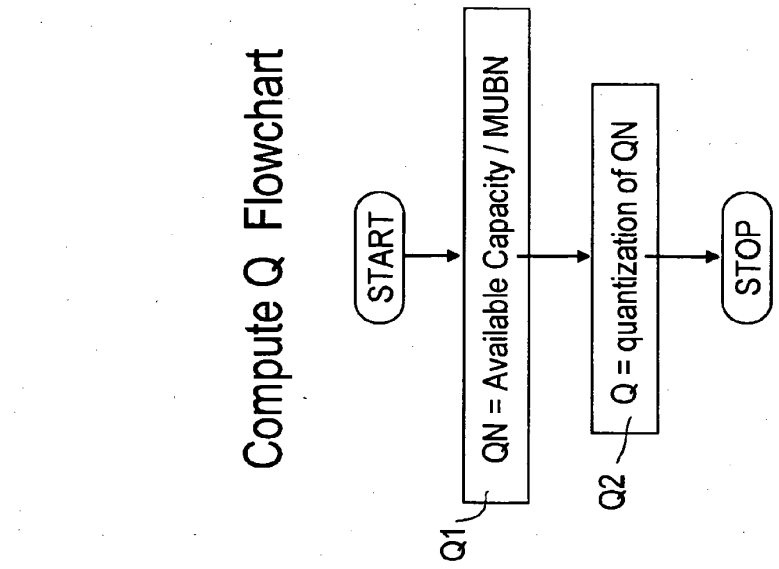


FIG. 9

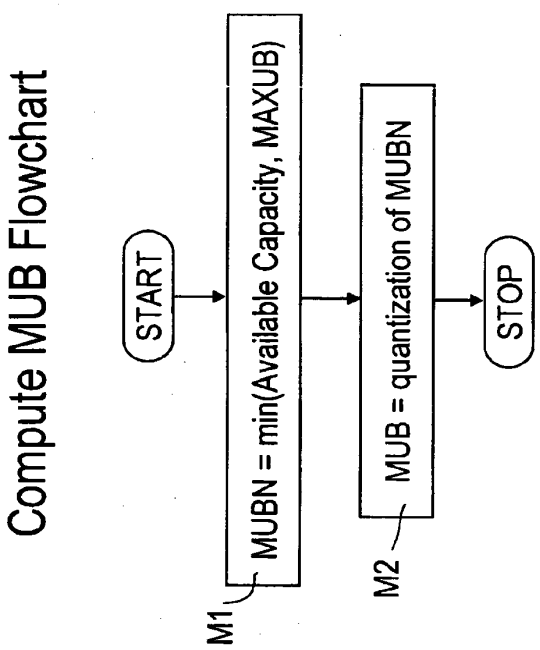


FIG. 8

BNSDOCID: <EP_____2026514A1_I_>

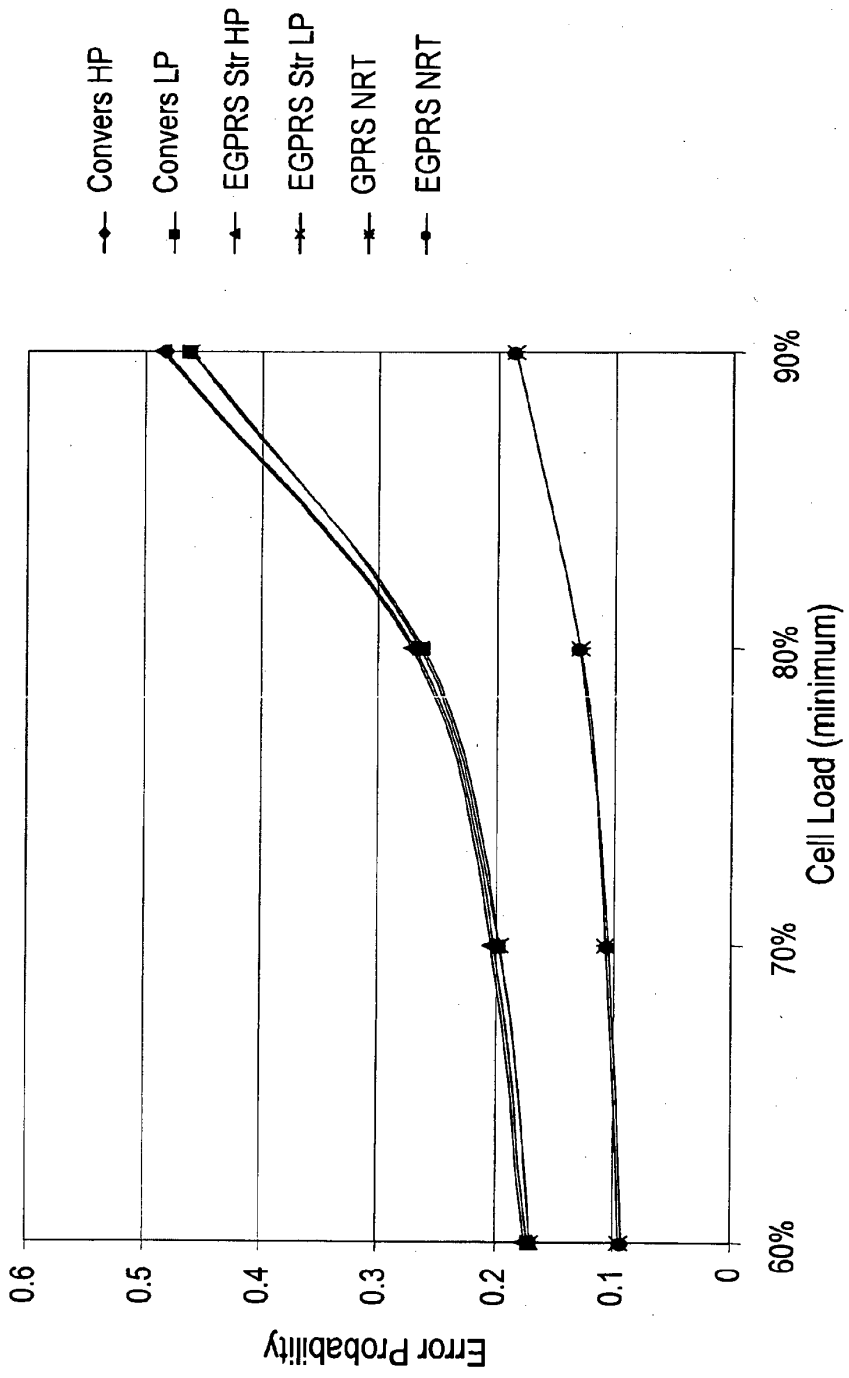


FIG. 10

BNSDOCID: <EP_____2026514A1_I_>

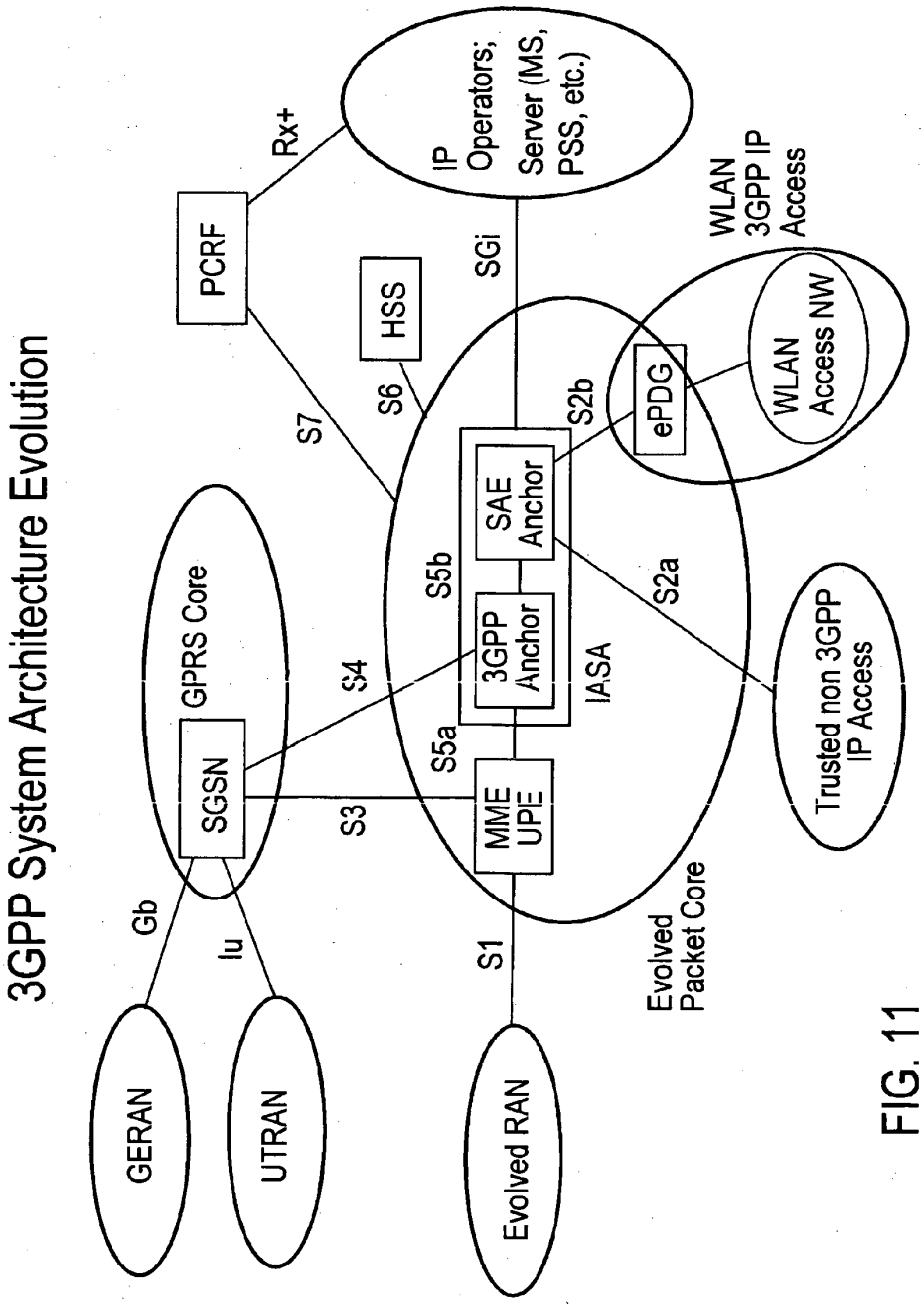


FIG. 11

BNSDOCID: <EP_____2026514A1_I_>

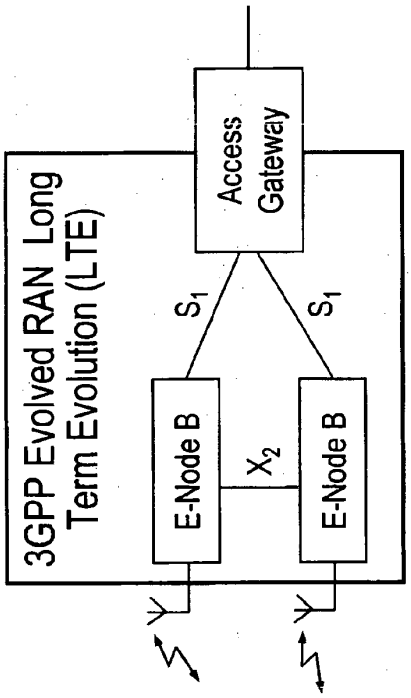


FIG. 12

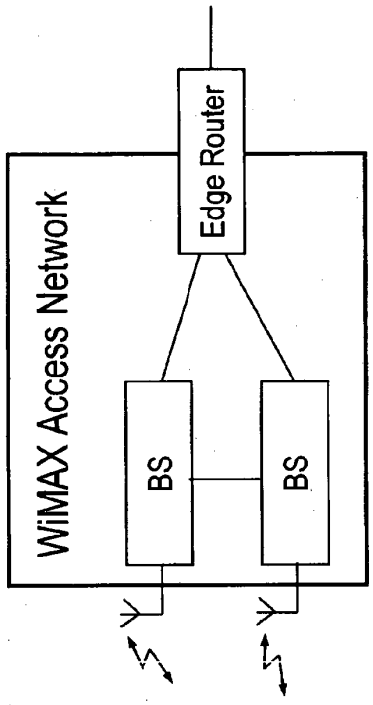


FIG. 13

BNSDOCID: <EP_____2026514A1_I_>

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 07 42 5527

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
Y	EP 1 503 606 A (SIEMENS MOBILE COMM SPA [IT]) 2 February 2005 (2005-02-02) * abstract; claims 1-21 * -----	1-18	INV. H04L12/56
Y	US 6 804 222 B1 (LIN WEI [US] ET AL) 12 October 2004 (2004-10-12) * abstract * * column 12, line 41 - column 13, line 11 * -----	1-18	
A	US 2003/117951 A1 (WIEBE MARVIN JAKE [CA] ET AL) 26 June 2003 (2003-06-26) * abstract * -----	1-18	
A	EP 1 420 604 A (SIEMENS MOBILE COMM SPA [IT] SIEMENS SPA ITALIANA [IT]) 19 May 2004 (2004-05-19) * abstract * * claims 1-10 * -----	1-18	
			TECHNICAL FIELDS SEARCHED (IPC) H04L

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	13 February 2008	Wolf, William

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)

BNSDOCID: <EP_____2026514A1_I_>

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 07 42 5527

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.

13-02-2008

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1503606 A	02-02-2005	CN 1582054 A	16-02-2005
		US 2005026616 A1	03-02-2005
US 6804222 B1	12-10-2004	US 2005041670 A1	24-02-2005
US 2003117951 A1	26-06-2003	EP 1330060 A2	23-07-2003
		JP 2003229902 A	15-08-2003
EP 1420604 A	19-05-2004	AT 341170 T	15-10-2006
		DE 60215026 T2	16-05-2007
		EP 1657862 A1	17-05-2006

EPO FORM P0459

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

BNSDOCID: <EP_____2026514A1_I_>

REFERENCES CITED IN THE DESCRIPTION

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

Patent documents cited in the description

- EP 1503606 A1 **[0012] [0013]**

Non-patent literature cited in the description

- **N. NIEBERT ; A. SCHIEDER ; H. ABRAMOWICZ ; G. MALMGREN ; J. SACHS ; U. HORN ; C. PREHOFER ; H. KARL. AMBIENT NETWORKS.** An Architecture for Communication Networks Beyond 3G. *IEEE Wireless Communications,* April 2004, vol. 11 (2), 14-21 **[0069]**
- *Deliverable D-1.5, "AN Framework Architecture,* December 2005 **[0069]**
- **P. MAGNUSSON ; F. BERGGREN ; I. KARLA ; R. LITJENS ; F. MEAGO ; H. HAITAO ; R. VERONESI.** Multi-radio resource management for communication networks beyond 3G. *IEEE 62nd VTC,* 2005 **[0069]**

BNSDOCID: <EP_____2026514A1_I_>

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

(11) EP 1 942 698 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
09.07.2008 Bulletin 2008/28

(51) Int Cl.:
H04Q 7/38 (2006.01)

(21) Application number: **08250053.9**

(22) Date of filing: **07.01.2008**

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

(30) Priority: **07.01.2007 US 879318 P**
22.06.2007 US 821598
22.06.2007 US 821597

(71) Applicant: **Apple Inc.**
Cupertino, CA 95014 (US)

(72) Inventors:
- **Gautier, Patrice**
  San Francisco, CA 94121 (US)
- **Shimizu, Debbie**
  San Jose, CA 95126 (US)
- **Anderson, Alexandrea**
  Clovis, CA 93611 (US)
- **Cue, Eddy**
  Los Altos, CA 94024 (US)
- **Gromek, Monika**
  Oakland, CA 94607 (US)
- **Kondrk, Robert, H.**
  San Francisco, CA 94107 (US)

(74) Representative: **Alton, Andrew**
Urquhart-Dykes & Lord LLP
Tower North Central
Merrion Way
Leeds LS2 8PA (GB)

(54) Method and system for mobile device activation

(57) Methods, systems and graphical user interfaces that facilitate activation of mobile devices, such as communication devices or multi-function devices, via computers are disclosed. According to one embodiment, activation of a mobile device with respect to a wireless service provider can be performed by users through use of a computer (e.g., personal computer) that communicate with a remotely located activation server. According to another embodiment, graphical user interfaces can be presented to users so as to enable end users to easily activate mobile devices.

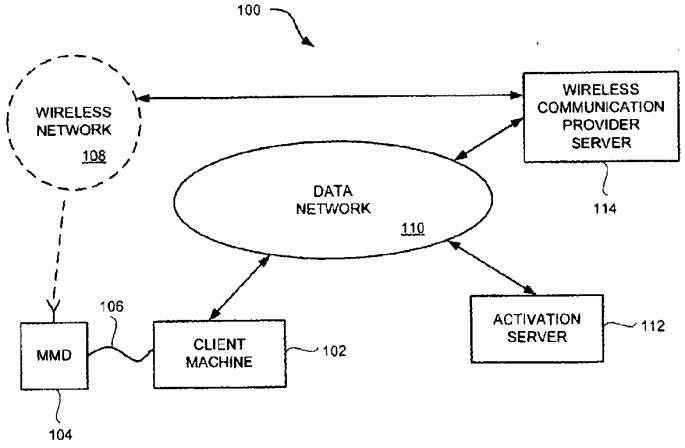


FIG. 1

Printed by Jouve, 75001 PARIS (FR)

EP 1 942 698 A1

BNSDOCID: <EP_____1942698A1_I_>

Description

BACKGROUND OF THE INVENTION

Field of the Invention

[0001] The present invention relates to mobile electronic devices and, more particularly, to activation of mobile electronic devices having wireless communication capabilities.

Description of the Related Art

[0002] Mobile phones are often used by individuals on a personal basis. When a mobile phone is newly acquired, the wireless network infrastructure (e.g., cellular phone network) of the appropriate wireless carrier or service provider needs to be setup to work with the mobile phone. Mobile phone setup is principally done at retail establishments that sell mobile phones and wireless service plans. Alternatively, mobile phones can be configured at a manufacturing or distribution site or at a service center. Unfortunately, however, mobile phone setup is time consuming and restrictive to consumers. Additionally, once a mobile phone and service plan have been setup for a consumer, the wireless network needs to be informed of the mobile phone and the mobile phone thereafter needs to register with the wireless network whenever being used. Registration requires a location update request be sent from the mobile phone to the wireless network. In the case of initial phone setup, since location update is triggered on power-up, typically the person configuring the mobile phone would be required to power-off and then power-on the mobile phone to render it active on the wireless network. There is thus a need to avoid the various inconveniences and inefficiencies of conventional mobile phone setup.

SUMMARY OF THE INVENTION

[0003] The invention pertains to methods, systems and graphical user interfaces that facilitate setup or activation of mobile devices, such as communication devices or multi-function devices, via computers. According to one embodiment, activation of a mobile device with respect to a wireless service provider can be performed by users through use of a computer (e.g., personal computer) that communicate with a remotely located activation server. According to another embodiment, graphical user interfaces can be presented to users so as to enable end users to easily activate mobile devices.

[0004] The invention can be implemented in numerous ways, including as a method, system, device, apparatus, graphical user interface, or computer readable medium. Several embodiments of the invention are discussed below.

[0005] As a computer-implemented method for activating wireless network service for an electronic device through use of a host device, where the electronic device is associated with a customer for wireless network service provided by a wireless network service provider, one embodiment can, for example, include at least the acts of: receiving device information from the electronic device when the electronic device is attached to the host device; acquiring customer information pertaining to the customer; receiving a service plan selection from the customer; receiving billing information for payment of the service plan; and initiating activation of a wireless service account for use of the electronic device with the wireless network service provided by the wireless network service provider. The wireless service account being activated can be based on the customer information, the service plan and the billing information.

[0006] As a computer-implemented method for activating an electronic device for wireless network service through use of a host device, where the electronic device is associated with a customer for wireless network service provided by a wireless network service provider, one embodiment can, for example, include at least the acts of: receiving device information from the electronic device while the electronic device is attached to the host device; acquiring customer information pertaining to the customer; offering the user one or more service plans; receiving a user selection of one of the service plans; and receiving billing information for payment of the selected service plan.

[0007] As a computer-implemented method for activating an electronic device for wireless network service from a host device, where the electronic device is associated with a customer for wireless network service provided by a wireless network service provider, one embodiment can, for example, include at least the acts of: receiving device information from the electronic device when the electronic device is attached to the host device; determining whether the electronic device has already been activated based on the device information; and automatically initiating activation of the electronic device when it is determined that the electronic device has not already been activated.

[0008] As a graphical user interface to assist an end user in activating an account for an electronic device having wireless communication capabilities, where the account is with respect to a wireless service provider providing wireless network service, one embodiment of the invention can, for example, include at least a plurality of displayable pages that are presented on a display device associated with a host computer. The displayable pages can, for example, include: an end user status page to facilitate selection of a type of activation; a service plan selection page to facilitate selection of a service plan for the wireless network service; a media account page for a media account associated with an online media store so that a user can create a new media account or login to an existing media account; an end user information entry page to facilitate entry of end user information; a billing information page to facilitate entry of billing infor-

mation for one or both the user media account and a wireless account; a terms and conditions page regarding legal agreements with the online media store and with the wireless service provider; and/or an activation page to inform the end user of activation information.

[0009] As a computer-implemented method for activating an electronic device for wireless network service, where the electronic device is associated with a customer of a wireless service provider associated with the wireless network service, one embodiment can, for example, include at least the acts of: informing an activation server of an electronic device having wireless communication device that is to be activated for wireless network service; displaying a customer status page to facilitate selection of a type of activation; specifying to the activation server a type of activation desired by the customer; displaying a service plan selection page to facilitate selection of a service plan for the wireless network service; informing the activation server of a selected service plan; displaying a customer account page to facilitate login to or creation of a user media account with an online media store; providing account information for the user media account for the customer; displaying a customer information entry page; providing customer information to the activation server; displaying a billing information page to facilitate entry of billing information for one or both the user media account and a wireless account; informing the activation server of the billing information; displaying a terms and conditions page regarding legal agreements with the online media store and with the wireless service provider; informing the activation server of acceptance of the legal agreements; displaying an information review page; informing the activation server of approval of the information provided on the information review page; displaying an activation completion page; and displaying a device preference page to assist the customer with setting one or more preferences or options to be applied to the operation of the electronic device.

[0010] As a computer readable medium including at least computer executable program code tangibly embodied therein for activating wireless network service for an electronic device through use of a client computing device, the electronic device being associated with a customer for wireless network service provided by a wireless network service provider, one embodiment can, for example, include at least: computer program code for receiving device information from the electronic device when the electronic device is attached to the host device; computer program code for acquiring customer information pertaining to the customer; computer program code for receiving a service plan selection from the customer; computer program code for receiving billing information for payment of the service plan; and computer program code for initiating activation of a wireless service account for use of the electronic device with the wireless network service provided by the wireless network service provider.

[0011] As a computer readable medium including at least computer executable program code tangibly embodied therein for activating an electronic device for wireless network service through use of a host device, the electronic device being associated with a customer for wireless network service provided by a wireless network service provider, one embodiment can, for example, include at least: computer program code for receiving device information from the electronic device while the electronic device is attached to the host device; computer program code for acquiring customer information pertaining to the customer; computer program code for offering the user one or more service plans; computer program code for receiving a user selection of one of the service plans; and computer program code for receiving billing information for payment of the selected service plan.

[0012] Other aspects and advantages of the invention will become apparent from the following detailed description taken in conjunction with the accompanying drawings which illustrate, by way of example, the principles of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

[0013] The invention will be readily understood by the following detailed description in conjunction with the accompanying drawings, wherein like reference numerals designate like structural elements, and in which:

[0014] FIG. 1 is a block diagram of an activation system according to one embodiment of the invention.

[0015] FIG. 2A is a flow diagram of a system activation process according to one embodiment of the invention.

[0016] FIG. 2B is a flow diagram of a setup process according to one embodiment of the invention.

[0017] FIG. 3 is a flow diagram of a device operational process according to one embodiment of the invention.

[0018] FIG. 4 is a flow diagram of a device operation process according to another embodiment of the invention.

[0019] FIG. 5 is a system state diagram according to one embodiment of the invention.

[0020] FIGs. 6A-6C are flow diagrams of a network service setup process according to one embodiment of the invention.

[0021] FIG. 6D is a flow diagram of an alternative portion of the network service setup process according to one embodiment of the invention.

[0022] FIG. 7 is a flow diagram of a network service setup process according to one embodiment of the invention.

[0023] FIGs. 8A-8C are flow diagrams of an activation process according to one embodiment of the invention.

[0024] FIG. 9 is a flow diagram of an activation process according to another embodiment of the invention.

[0025] FIG. 10 is a flow diagram of an activation process according to another embodiment of the invention.

[0026] FIG. 11 is a flow diagram of an activation process according to another embodiment of the invention.

[0027] FIGs. 12A-12C are flow diagrams of a mobile

BNSDOCID: <EP_____1942698A1_I_>

device provisioning process according to one embodiment of the invention.

[0028] FIG. 13 is a screen shot of an exemplary initial registration page according to one embodiment of the invention.

[0029] FIG. 14 is a screen shot of an exemplary customer status page according to one embodiment of the invention.

[0030] FIG. 15 is a screen shot of an exemplary screen shot of a mobile number transfer page.

[0031] FIG. 16 is a screen shot of an exemplary screen shot of a landline number transfer page.

[0032] FIG. 17A and 17B are screen shots of an exemplary service plan selection page according to one embodiment of the invention.

[0033] FIG. 18 is a screen shot of an exemplary customer account page according to one embodiment of the invention.

[0034] FIG. 19 is a screen shot of a customer information entry page according to one embodiment of the invention.

[0035] FIG. 20 illustrates an exemplary billing information page according to one embodiment of the invention.

[0036] FIG. 21A is an exemplary screen shot of a first terms and conditions page according to one embodiment of the invention.

[0037] FIG. 21B is an exemplary screen shot of a second terms and conditions page according to one embodiment of the invention.

[0038] FIG. 22 is a screen shot of an exemplary review information page according to one embodiment of the invention.

[0039] FIG. 23 is an exemplary screen shot of a setup completion page according to one embodiment of the invention.

[0040] FIG. 24A is an exemplary screen shot of a setup completion page according to another embodiment of the invention.

[0041] FIG. 24B is an exemplary screen shot of a setup completion page according to still another embodiment of the invention.

[0042] FIG. 25 is an exemplary screen shot of a device preference page according to one embodiment of the invention.

[0043] FIG. 26 is a screen shot of an exemplary customer status page according to one embodiment of the invention.

[0044] FIG. 27 is a screen shot of an exemplary account information page according to one embodiment of the invention.

[0045] FIG. 28 is a screen shot of an exemplary customer status page according to one embodiment of the invention.

[0046] FIG. 29 is a screen shot of an exemplary account information page according to one embodiment of the invention.

[0047] FIG. 30 is a screen shot of an exemplary account type selection page according to one embodiment of the invention.

[0048] FIG. 31 is a screen shot of an exemplary customer status page according to one embodiment of the invention.

[0049] FIG. 32 is a screen shot of an exemplary account type selection page according to one embodiment of the invention.

[0050] FIG. 33 is a screen shot of an exemplary prepayment requirement page.

[0051] FIG. 34 is a block diagram of a mobile multi-function device according to one embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

[0052] The invention pertains to methods, systems and graphical user interfaces that facilitate setup or activation of mobile devices, such as communication devices or multi-function devices, via computers. According to one embodiment, activation of a mobile device with respect to a wireless service provider can be performed by users through use of a computer (e.g., personal computer) that communicate with a remotely located activation server. According to another embodiment, graphical user interfaces can be presented to users so as to enable end users to easily activate mobile devices.

[0053] Embodiments of the invention are discussed below with reference to FIGs. 1 - 34. However, those skilled in the art will readily appreciate that the detailed description given herein with respect to these figures is for explanatory purposes as the invention extends beyond these limited embodiments.

[0054] FIG. 1 is a block diagram of an activation system 100 according to one embodiment of the invention. The activation system 100 includes a client machine 102. The client machine 102 is, for example, a computing device, such as a personal computer. The client machine 102 can also be referred to as a host device. A mobile multi-function device 104 can be connected (e.g., temporarily connected) to the client machine 102. In one implementation, the mobile multi-function device 104 can be connected to the client machine 102 over a cable 106. As an example, the cable 106 can pertain to a peripheral bus (e.g., USB) connection. In another implementation, the mobile multi-function device 104 can connect to the client machine 102 over a wireless connection. The mobile multi-function device 104 operates to support a plurality of different functions. For example, the mobile multi-function device 104 can operate as a media playback device, such as an MP3 player, video player, game player, etc. In addition, the mobile multi-function device 104 can support wireless voice communications through a wireless network 108. The wireless voice communications through the wireless network 108 can enable a user of the mobile multi-function device to communicate with users of other mobile multi-function devices or other communication devices. Similarly, the mobile multi-function device 104 can support wireless data exchange (e.g.,

SMS messages) through the wireless network 108. Although FIG. 1 illustrates one client machine 102 and one mobile multi-function device 104, it should be noted that the activation system 100 can have multiple client machines 102 and multiple mobile multi-function devices 104. In addition, one or more of the mobile multi-function devices can connect to one or more client machines. In one implementation, the wireless network 108 can represent a cellular telephone network. In another implementation, the wireless network 108 can represent a local or regional wireless network (e.g., WiFi, WiMax). In still another implementation, the wireless network 108 can represent multiple wireless networks.

[0055] The activation system 100 also illustrates a data network 110. The data network is, for example, a local area network, a wide area network, or a global network, such as the Internet. The client machine 102 can couple to the data network 110. In addition, the activation system 100 includes an activation server 112 and a wireless communication provider server 114. In order to activate the mobile multi-function device 104, the mobile multi-function device 104 interacts with the activation server 112. To do so, the mobile multi-function device 104 communicates with the client machine 102 and the client machine 102 in turn communicates with the activation server 112 through the data network 110. In this regard, the activation server 112 can coordinate and control activation of the mobile multi-function device 104. In addition, the activation server 112 can communicate with the wireless communication provider server 114 so that an appropriate account to be utilized by the mobile multi-function device 104 can be established by the wireless communication provider that is operating on the wireless network 108.

[0056] FIG. 2A is a flow diagram of a system activation process 200 according to one embodiment of the invention. The system activation process 200 concerns activation of a mobile multi-function device (MMD). The system activation process 200 begins with a mobile multi-function device being obtained 202. For example, a user can obtain 202 a mobile multi-function device at a retail location or by mail order. In this embodiment, when the mobile multi-function device is obtained 202, it is not activated for use with any wireless network. As a result, the mobile multi-function device needs to go through an activation process in order to operate. In this regard, after the mobile multi-function device is obtained 202, a service plan and a payment arrangement need to be setup 204. After the service plan and payment arrangement have been successfully setup 204, the mobile multi-function device can be enabled 206. In addition, the mobile multi-function device can be registered with a network, namely, a wireless network. Here, the registration 208 with the network is performed to permit the mobile multi-function device to be utilized on the network.

[0057] Following successful enabling 206 and registration 208, the mobile multi-function device can operate 210 with or without utilization of the network. In this regard, since the mobile multi-function device supports multiple functions, the mobile multi-function device can be utilized in a non-network manner, such as playing local games, displaying local data, playing music from local storage, viewing local pictures, viewing locally stored electronic mail, etc. However, if the user of the mobile multi-function device desires to utilize the network (e.g., make or receive voice calls or electronic messages), network access is permitted in accordance with the service plan that has been setup 204, provided that the registration 208 was successful and provided that the network is available.

[0058] Once the mobile multi-function device is enabled 206 some or all of the functions or operations supported by the mobile multi-function device can be utilized. In one embodiment, once enabled 206, the mobile multi-function device can be utilized for all non-network functions or operations available from the mobile multi-function device, with network functions or operations becoming available following registration at block 208. In another embodiment, functions or operations of the mobile multi-function device can be prevented or restricted until completion of initial (i.e., first time) registration at block 208 at which point all functions or operations available from the mobile multi-function device can be utilized. In still another embodiment, certain, non-network functions or operations of the mobile multi-function device can be available even prior to the mobile multi-function device being enabled 206.

[0059] FIG. 2B is a flow diagram of a setup process 250 according to one embodiment of the invention. The setup process 250 operates to setup a service plan and/or payment arrangement with respect to one or more service providers. The setup process 250 is, for example, suitable for use as the setup 204 of a service plan and payment arrangement illustrated in FIG. 2A.

[0060] The setup process 250 retrieves 252 device information. Typically, the device information is retrieved 252 from the device itself. For example, the device can be referred to as a mobile multi-function device. Customer information can also be acquired 254, such as from the customer. The customer information can be acquired 254 so that the service provider can receive information regarding the customer that seeks to activate the mobile multi-function device. A service plan for the device is also set 256. The customer can be offered one or more service plans depending upon various different criteria, including customer's location, customer's credit history, customer's current service provider, etc. A service plan as used herein can also be referred to as a rate plan. Once a service plan to be utilized with the customer has been set 256, a billing account can be setup 258. The building account serves to facilitate billing the customer for the services provided by the service plan. Typically, the customer is billed monthly for the service plan. The setup 258 of the billing account acquires all the necessary information for billing the customer. As one example, the billing account can utilize a credit card whereby the cus-

BNSDOCID: <EP_____1942698A1_I_>

tomer is billed monthly via the credit card for the service plan. Subsequently, the customer account can be activated 260. In this regard, the setup process 250 can communicate with a computing device (e.g., activation server 112) associated with a service provider to activate a customer account so that the customer can utilize the mobile multi-function device with the at least one service provider in accordance with the service plan. The service provider is, for example, a wireless (communications) service provider. Additionally, an account with another service provider, such as an online media store, can be established. Following the block 260, the setup process 250 ends and subsequent processing can continue at block 206 of the system activation process 200 illustrated in FIG. 2A.

[0061] FIG. 3 is a flow diagram of a device operational process 300 according to one embodiment of the invention. The device operational process 300 is, for example, processing associated with a mobile multi-function device, such as the mobile multi-function device 104 illustrated in FIG. 1.

[0062] The device operational process 300 can begin when the mobile multi-function device is powered on. Hence, a decision 302 determines whether the mobile multi-function device has been powered on. When the mobile multi-function device has not been powered on, the device operational process 300 is not performed. On the other hand, when the decision 302 determines that the mobile multi-function device has been powered on, a decision 304 can determine whether the mobile multi-function device has been enabled. Here, it is assumed that the mobile multi-function device performing the device operational process 300 may or may not have been enabled to operate. Hence, when the decision 304 determines that the mobile multi-function device has not been enabled, the mobile multi-function device is eligible to operate 306 in a limited use mode. As an example, in the limited use mode, the mobile multi-function device can permit emergency communications (e.g., emergency telephone calls). However, the limited use mode may prevent other operations of the mobile multi-function device. For example, if the mobile multi-function device provides media playback or network browsing, then when in the limited use mode, media playback and/or network browsing can be prevented (or limited). In one implementation, while in the limited use mode, the mobile multi-function device can prevent all other operational uses except emergency communications.

[0063] On the other hand, when the decision 304 determines that the mobile multi-function device is enabled, the mobile multi-function device can operate in a full use mode. Following the blocks 306 and 308, a decision 312 can determine whether the mobile multi-function device is to be powered off. When the decision 312 determines that the mobile multi-function device should not be powered off, the mobile multi-function device continues to operate in the previously established operational mode (e.g., limited use mode or full use mode). On the other hand, when the decision 312 determines that the mobile multi-function device should be powered off, the mobile multi-functional device is powered down 314. Following the block 314, the device operational process 300 can end.

[0064] FIG. 4 is a flow diagram of a device operation process 400 according to another embodiment of the invention. The device operational process 400 is, for example, processing associated with a mobile multi-function device, such as the mobile multi-function device 104 illustrated in FIG. 1.

[0065] The device operational process 400 begins with a decision 402. The decision 402 determines whether the mobile multi-function device has been powered on. When the decision 402 determines that the mobile multi-function device has not been powered on, the device operational process 402 awaits power on of the mobile multi-function device. Once the decision 402 determines that the mobile multi-function device has been powered on, the device operational process 400 is effectively invoked. Once the decision 402 determines that the mobile multi-function device has been powered on, a decision 404 determines whether the mobile multi-function device has been enabled.

[0066] When the decision 404 determines that the mobile multi-function device has not yet been enabled, the device operational process 400 places 406 the mobile multi-function device in an emergency mode. In the emergency mode, the mobile multi-function device is permitted to make emergency calls only. Next, a decision 408 determines whether the mobile multi-function device is to be powered off. When the decision 408 determines that the mobile multi-function device is not to be powered off, the device operational process 400 returns to repeat the decision 404 to again evaluate whether the mobile multi-function device has been enabled. In an alternative embodiment, when the decision 408 determines that the mobile multi-function device is not to be powered off, the device operation process 400 can remain in the emergency mode and simply repeat the decision 404 until powered off.

[0067] Alternatively, when the decision 404 determines that the mobile multi-function device has been enabled, the mobile multi-function device is placed 410 in an active mode. Registration with a wireless network can also be requested 412. In one embodiment, a location update request can be used to request 412 registration with the wireless network. A decision 414 determines whether the registration with the wireless network has been successful. When the decision 414 determines that the registration has been successful, the device operational process 400 permits 416 the mobile multi-function device to perform network and/or non-network operations. Next, a decision 418 determines whether the mobile multi-function device is to be powered off. When the decision 418 determines that the mobile multi-function device has not been powered off, the device operational process 400 returns to repeat the block 416 so that the

mobile multi-function device can continue to perform 416 network and/or non-network operations.

[0068] On the other hand, when the decision 414 determines that registration with the wireless network has not been successful, then the user of the multi-function device can be notified 422 that the network is unavailable. In one implementation, the notification 422 can be displayed on a display screen for one or both of the multi-function device or a client device connected thereto. Further, the mobile multi-function device can be operated to permit 424 non-network operations. A decision 426 can then determine whether the mobile multi-function device is to be powered off. When the decision 426 determines that the mobile multi-function device is not to be powered off, the device operational process 400 returns to repeat the block 424 so that non-network operations can continue to be performed 424.

[0069] When any of the decisions 408, 418 or 426 determine that the mobile multi-function device is to be powered off, the mobile multi-function device can be powered down 420. After the mobile multi-function device has been powered down, the device operational process 400 ends.

[0070] FIG. 5 is a system state diagram 500 according to one embodiment of the invention. The system state diagram 500 illustrates a plurality of states associated with system activation of a mobile multi-function device (MMD) according to one embodiment. At state 502, a mobile multi-function device is obtained. At state 504, following the state 502, the mobile multi-function device is powered-on. Next, at state 506, the mobile multi-function device is connected to a computer, (e.g., personal computer). Thereafter, at state 508, one or more accounts can be arranged. These accounts can pertain to an account with an online media store and/or an account with a wireless service provider. Next, at state 510, a service plan can be selected. Typically, the service plans are associated with a wireless service provider that is providing wireless network access for the mobile multi-function device. In addition, payment can be arranged at state 512. It should also be noted that states 510 and/or 512 could be part of the state 508.

[0071] Following state 512, at state 514, the mobile multi-function device can be enabled. Once enabled, the mobile multi-function device is able to be fully utilized. Subsequently, the mobile multi-function device can be registered with a network (e.g., wireless network) at state 516. The registration with the network enables the mobile multi-function device to send and receive calls with respect to the network. Optionally, it should be noted that following the state 504, in the event that the mobile multi-function device was previously enabled, the mobile multi-function device can transition directly to state 516. In any case, once the mobile multi-function device has been registered with the network at state 516, the mobile multi-function device can be utilized with the network at state 518. Following the state 518, the mobile multi-function device can be powered off at state 520. Also, following the state 514, the mobile multi-function device can be disconnected from the computer at state 522 or the mobile multi-function device can be powered off at state 524.

[0072] In an alternative embodiment, at state 514, the mobile multi-function device can be enabled for only certain functions or operations. In this manner, the mobile multi-function device can have its available functions or operations controlled such that available functions or operations can be available (and others restricted) at (i) pre-enablement, (ii) post-enablement, and (iii) post-registration.

[0073] As such, activation can include one or more of account activation, device activation (i.e., enablement), and network activation (i.e., network setup). In one embodiment, the states 508, 510 and 512 can be considered account activation, and the state 514 can be considered device activation. Following state 512 or state 514 and prior to 516, the network can be setup (i.e., network activation) to support the account for the mobile multi-function device being activated.

[0074] FIGs. 6A-6C are flow diagrams of a network service setup process 600 according to one embodiment of the invention. For example, with reference to FIG. 1, the network service setup process 600 is processing performed when the mobile multi-function device 104 is connected to the client machine 102 illustrated in FIG. 1 so that interaction with the activation server 112 can be performed to setup service for the mobile multi-function device 104.

[0075] The network service setup process 600 can begin with a decision 602 that determines whether the mobile multi-function device is attached to the client machine (e.g., personal computer). When the decision 602 determines that the mobile multi-function device is not attached, then the network service setup process 600 is not performed. On the other hand, when the decision 602 determines that the mobile multi-function device is attached, the network service setup process 600 can be performed. In one embodiment, the network setup process 600 can be automatically initiated where the mobile multi-function device is attached to the client machine.

[0076] When the network setup process 600 is performed, mobile multi-function device (MMD) information is received 604 from the mobile multi-function device. Next, a decision 605 determines whether a user activation request has been received. When the decision 605 determines that a user activation request has not been received, the network service setup process 600 can await a user activation request. A user can request activation of the mobile multi-function device. In one example, the user can specify whether the activation of the mobile multi-function device is to be associated with a new account or an existing account. On the other hand, when the decision 605 determines that a user activation request has been received, a decision 606 can then determine whether the mobile multi-function device is to be subject to an existing account. The decision 606 can be based on the user activation request which can indicate

BNSDOCID: <EP_____1942698A1_I_>

whether the activation of the mobile multi-function device is to be associated with a new account or an existing account. When the decision 606 determines that the mobile multi-function device is not subject to an existing account, account setup information is requested 608. The account setup information is information used to setup a new account. The account setup information can, for example, be provided by user. A decision 610 then determines whether the account setup information has been received. When the decision 610 determines that the account setup information has not yet been received, the network service setup process 600 awaits such information. Once the decision 610 determines that the account setup information has been received, a user account can be setup 612. The user account can pertains to a user account with a wireless service provider, an online media store, and/or some other account. The user account contains information concerning the user and often includes personal information and financial information.

[0077] On the other hand, when the decision 606 determines that an existing account is associated with the mobile multi-function device, authentication information can be requested 614. A decision 616 can then determine whether the authentication information has been received. When the decision 616 determines that the authentication information has not yet been received, the network service setup process 600 can await such information. Alternatively, when the decision 616 determines that the authentication information has been received, a decision 618 can determine whether the user is authenticated for access to the existing account. When the decision 618 determines that the user has not been authenticated, an error indication 620 can be provided. Following the block 620, the network service setup process 600 can end with network setup not being completed.

[0078] Following the block 612 or following the decision 618 when the user has been properly authenticated, the user can be offered 622 one or more service plans. In one embodiment, the one or more service plans being offered 622 can depending on a credit evaluation (e.g., credit score) for the user. For example, a user having poor credit can be only offered service plans that require prepayment. A decision 624 then determines whether a plan has been selected but the user. When the decision 624 determines that a plan has not yet been selected, the network service setup process 600 awaits such a selection. Once the decision 624 determines that a plan has been selected, a decision 628 determines whether a new account is being processed. When the decision 628 determines that a new account is being processed, setup of a billing account can be requested 630. However, when the decision 628 determines that an existing account is being processed, the block 630 can be bypassed. The request 630 can include payment information, such as payment information provided by the user. In one embodiment, the network setup process 600 already received or has access to the payment information to be used for the account. As one example, the account setup information can include the billing account information. In another embodiment, the network setup process 600 can request and receive the payment information prior to the request 630. When the decision 628 determines that payment information has not yet been received, the network service setup process 600 can await receipt of the payment information. Once the decision 628 determines that the payment information has been received, setup of a billing account can be requested 630.

[0079] Thereafter, activation of the account for the user can be requested 631. A decision 632 can then determine whether activation confirmation and phone number for the account being established have been received. When the activation confirmation and phone number have not been received, the network service setup process 600 can await such information. Alternatively, when the decision 632 determines that the activation confirmation and phone number have been received, the user can be informed 634 of successful account setup and the appropriate phone number.

[0080] Following the block 634, the mobile multi-function device is enabled 636.

In one implementation, the client machine 102 can write certain information into data storage on the mobile multi-function device 104 to inform the mobile multi-function device 104 that the device is now enabled. The mobile multi-function device can then self-determine whether the device is enabled by reading the stored information. Following the block 636 the mobile multi-function device can be disconnected from the client machine.

[0081] In any case, following the block 636, a decision 638 determines whether network setup has been completed. When the decision 638 determines that network setup has been completed, the user can be notified 640 that network setup has completed. The notification can alert the user to perform an action with respect to the mobile multi-function device so that the mobile multi-function device can register with the network and thereafter be utilized thereon. As an example, the notification can be provided to the user by displaying an indication or by sending an electronic message (e.g., email or text message) to the associated client machine. For example, the user can be instructed by the notification to power cycle the mobile multi-function device or connect the mobile multi-function device to the client machine. Following the block 640, the network service setup process 600 ends.

[0082] On the other hand, when the decision 638 determines that the network setup is not complete, the network service setup process 600 can perform other processing 642 unassociated with the network setup. For example, the other processing 642 can pertain to the synchronization of data between the client machine 102 and the mobile multi-function device 104. The other processing 642 can also pertain to media playback at the mobile multi-function device, setting of preferences at the mobile multi-function device or at the client machine, etc. Following the block 642, a decision 644 can deter-

mine whether completion of the network setup for the mobile multi-function device should be re-checked. In one embodiment, the completion of the network setup can be re-checked periodically (e.g., every 2 minutes). Typically, if the network setup has not properly completed after a number of attempts or period of time, the network service setup process 600 could end and inform the use that the network service was not able to be setup. In any case, when the decision 644 determines that the network setup should be re-checked, the network service setup process 600 can repeat the decision 638 and subsequent blocks to again determine whether network setup has completed. Alternatively, when the decision 644 determines that the network setup should not be re-checked, the network service setup process 600 can repeat the block 642 so that other processing can optionally be performed.

[0083] FIG. 6D is a flow diagram of an alternative portion of the network service setup process 600 according to one embodiment of the invention. In particular, the blocks 646-660 illustrated in FIG. 6D represent an alternative embodiment for the portion of the network service setup process 600 illustrated in FIG. 6C, namely, blocks 636-644. Following the block 634, the mobile multi-function device is enabled 646. In one implementation, the client machine 102 can write certain information into data storage on the mobile multi-function device 104 to inform the mobile multi-function device 104 that the device is now enabled. The mobile multi-function device can then self-determine whether the device is enabled by reading the stored information. In any case, following the block 646, a decision 648 determines whether network setup has been completed. When the decision 648 determines that network setup has been completed, the mobile multi-function device can be instructed 650 to register with the network. The mobile multi-function device can be instructed 650 to register with the network by causing a location update to be issued from the mobile multi-function device. In one implementation, the client machine 102 can send a command to the mobile multi-function device 104 to initiate the location update. In another implementation, the client machine 102 can cause the mobile multi-function device 104 to reset its radio transmitter/receiver (i.e., a portion of its hardware) so as to trigger a location update.

[0084] On the other hand, when the decision 648 determines that the network setup is not complete, a decision 652 determines whether the mobile multi-function device has been disconnected from the client machine. When the decision 652 determines that the mobile multi-function device has not been disconnected, the network service setup process 600 can perform other processing 654 unassociated with the network setup. For example, the other processing 654 can pertain to the synchronization of data between the client machine 102 and the mobile multi-function device 104. The other processing can also pertain to media playback at the mobile multi-function device, setting of preferences at the mobile multi-function device or at the client machine, etc. Following the block 654, the network service setup process 600 returns to repeat the decision 648 to again determine whether network setup has completed.

[0085] Alternatively, when the decision 652 determines that the mobile multi-function device has been disconnected from the client machine, a decision 656 determines whether network setup has completed. When the decision 656 determines that network setup has not completed, other processing 658 can be performed until the network setup has completed. Alternatively, when the decision 656 determines that network setup has completed, the user can be notified 660 that network setup has completed. The notification can alert the user to perform an action with respect to the mobile multi-function device so that the mobile multi-function device can register with the network and thereafter be utilized thereon. As an example, the notification can be provided to the user by displaying an indication or by sending an electronic message (e.g., email or text message) to the user. The electronic message can, for example, be sent to the mobile multi-function device or the associated client machine. For example, the user can be instructed by the notification to power cycle the mobile multi-function device or connect the mobile multi-function device to the client machine. Following the blocks 650 and 660, the network service setup process 600 ends.

[0086] In one embodiment, the mobile multi-function device can store information that can be used to determine whether the mobile multi-function device is enabled. For example, the mobile multi-function device can stored an identifier (e.g., activation identifier) that is provided by a client machine once the mobile multi-function device is to be enabled. In one embodiment, the identifier is stored in a secured manner, such as through use of encryption, digital certificate or other cryptographic technique. The identifier can include or be based on a Subscriber Identity Module (SIM) that is included in the mobile multi-function device while activated. In one implementation, a SIM value, such as a SIM card identifier (e.g., ICCID), read from the SIM card itself within the mobile multi-function device is compared to the identifier stored in a data store (e.g., Flash memory) within the mobile multi-function device. If the identifier matches the read SIM value, then the mobile multi-function device has previously been enabled. As such, the mobile multi-function device can self-determine whether it has been enabled. This enablement verification can, for example, prevent different SIM cards from being used with a mobile multi-function device that has been previously activated while using a different SIM card. An alternative to a SIM is a Universal Subscriber Identity Module (USIM). SIM cards are used with GSM type wireless networks. Other types of networks, such as CMDA, can use other identifiers. Often the identifiers in other networks are not removable from the multi-function device by users. In such cases, the identifier is stored within the device itself such that the identifier is not removable from the device. In such

BNSDOCID: <EP_____1942698A1_I_>

cases, the mobile multi-function device can simply store a flag that indicates whether or not the mobile multi-function device is enabled.

[0087] FIG. 7 is a flow diagram of a network service setup process 700 according to one embodiment of the invention. The network service setup process 700 is, for example, processing performed when activating a Mobile Multi-function Device (MMD). For example, the network service setup process 700 can be associated with processing performed when the mobile multi-function device 104 is connected to the client machine 102 illustrated in FIG. 1 so that interaction with the activation server 112 can be performed via the client machine 102 to setup service for the mobile multi-function device 104.

[0088] The network service setup process 700 can begin with a decision 702 that determines whether the mobile multi-function device is attached to the client machine (e.g., personal computer). When the decision 702 determines that the mobile multi-function device is not attached, the network service setup process 700 is not performed. On the other hand, when the decision 702 determines that the mobile multi-function device is attached, the network service setup process 700 can be performed. Once the decision 702 determines that the mobile multi-function device is attached, Mobile Multi-function Device (MMD) information can be read 704 from the multi-function device. In one embodiment, the MMD information can be encrypted so as to prevent unauthorized access. For additional details on preventing unauthorized access to device information, such as the MMD information, see, for example, U.S. Patent Application No. 11/767,447, filed June 22, 2007, and entitled "DEVICE ACTIVATION AND ACCESS," which is hereby incorporated by reference herein. After the MMD information has been read 704, a decision 706 determines whether the mobile multi-function device has already been activated. When the decision 706 determines that the mobile multi-function device has already been activated, then other processing 708 can be performed In other words, in one embodiment, the mobile multi-function device can perform various other processing 708 supported by the device given that the device has been activated. In this regard, the mobile multi-function device can utilize network service. Following the block 708, since the mobile multi-function device has already been activated, the network service setup process 700 can end.

[0089] When the decision 706 determines that the mobile multi-function device has not already been activated, a decision 710 determines that a user activation request has been received. When the decision 710 determines that a user activation request has not been received, the network service setup process 700 awaits a user activation request. Alternatively, when the decision 710 determines that a user activation request has been received, a decision 712 determines whether the user is a new customer. When the decision 712 determines that the user is a new customer, a decision 714 determines whether the customer desires an individual plan or a family plan. When the decision 714 determines that the customer desires an individual plan, processing proceeds to FIGs. 8A-8C where an activation process for an individual plan is described. On the other hand, when the decision 714 determines that the customer desires a family plan, processing proceeds to FIG. 9 where an activation process for a family plan is described.

[0090] On the other hand, when the decision 712 determines that the user is not a new customer, but is instead an existing customer, then a decision 716 determines whether the mobile multi-function device is a new device being substituted for a previously activated device. When the decision 716 determines that the mobile multi-function device is a new device, then processing proceeds to FIG. 10 where an activation process for an existing account is described. Alternatively, when the decision 716 determines that the mobile multi-function device is not new, a decision 718 can determine whether a new line is to be added to an existing account. When the decision 718 determines that a new line is to be added to an existing account, then processing proceeds to FIG. 11 where an activation process for a new line is described. Alternatively, when the decision 718 determines that a new line is not to be provided, then activation can be deemed 720 unavailable. Following the block 720, the network service setup process 700 can end.

[0091] FIGs. 8A-8C are flow diagrams of an activation process 800 according to one embodiment of the invention. The activation process 800 corresponds to activation of a mobile multi-function device with respect to an individual user plan.

[0092] The activation process 800 can begin with a decision 802 that determines whether a phone number is to be transferred. A phone number that can be transferred can be associated with another service provider. Typically, the phone number eligible to be transferred is from another wireless service provider.

However, more generally, the phone number eligible to be transferred can correspond to either a wireless account or a land line account. In any case, when the decision 802 determines that a phone number is to be transferred, an existing phone number and account information for another service provider are provided 804. Typically, the customer will interact with a graphical user interface to provide the information regarding the existing phone number and account information.

[0093] Following the block 804 as well as directly following the decision 802 when a phone number is not to be transferred, customer information can be requested 806. The customer information can include name, address, date of birth, security question(s), e-mail address, account identifier, etc. The customer information can be utilized for one or more accounts that are to be established with one or more service providers. A decision 808 determines whether the customer information has been received. When the decision 808 determines that the customer information has not been received, the activation

EPO FORM 1503 03.82 (P04C01)

process 800 can await the customer information.

[0094] After the decision 808 determines that the customer information has been received, a decision 810 can determine whether the location of the customer is supported. Here, the service provider typically only supports specific geographical locations. Hence, the customer location can be examined to determine whether it is within a geographical location supported by the system. Hence, when the decision 810 determines that the customer location is not supported by the system of the service provider, the customer can be informed 812 that activation is unavailable. Following the block 812, the activation process 800 can end without activating the mobile multi-function device.

[0095] On the other hand, when the decision 810 determines that the customer location is supported by the system of the service provider, one or more service plans to be offered to the customer can be determined 814. Next, the one or more service plans are offered 816 to the customer. A decision 818 then determines whether the customer has selected one of the service plans. When the decision 818 determines that a service plan has not yet been selected, the activation process 800 can await a plan selection. Alternatively, when the decision 818 determines that a service plan has been selected, billing information can be requested 820. The billing information can be utilized by one or more service providers. A decision 822 determines whether the billing information has been received. When the decision 822 determines that the requested billing information has not been received, the activation process 800 can await the billing information. Once the decision 822 determines that the billing information has been received, account information approval is requested 824. The account information approval can pertain to approval of the customer for the account to be activated. In one example, the account information would be presented to the customer for review and approval. A decision 826 determines whether the account information has been approved. When the decision 826 determines that the account information has not yet been approved, the activation process 800 can await such approval.

[0096] Once the decision 826 determines that the account information has been approved, the activation process 800 requests 828 approval of one or more service agreements. In one example, the one or more service agreements would be presented to the customer for review and acceptance. A decision 830 then determines whether the one or more service agreements had been approved. When the decision 830 determines that the one or more service agreements have not been approved, then the activation process 800 can await such approval. Once the decision 830 determines that the one or more service agreements have been approved, setup of a billing account can be requested 832. A remote server associated with a service provider can receive and process the request to setup a billing account for the customer. The setup of the billing account can utilize the customer information and/or the billing information that has been previously obtained by the activation process 800. Billing accounts can be setup in this manner for one or more service providers.

[0097] Additionally, the activation process 800 can request activation of an account. In other words, the activation being requested 834 can correspond to an account activation process. The account activation can be perform by a remote server, e.g., activation server, associated with a service provider. Following the request 834 for activation of an account, a decision 836 can determines whether the account has been activated. When the decision 836 determines that the account has not yet been activated, a decision 838 can determine whether the account activation has failed. When the decision 838 determines that the account activation has not failed, the activation process 800 can return to repeat the decision 836. Alternatively, when the decision 838 determines that the account information has failed, the customer can be informed 840 of unsuccessful activation. Following the block 840, the activation process 800 ends.

[0098] On the other hand, when the decision 836 determines that the account associated with the customer has been activated, the customer can be informed 842 of the successful activation. Thereafter, the mobile multi-function device can be activated 844. The activation 844 of the mobile multi-function device can, for example, be processing described above with reference to FIGs. 6C or 6D.

[0099] FIG. 9 is a flow diagram of an activation process 900 according to another embodiment of the invention. The activation process 900 is, for example, processing associated with activating a mobile multi-function device for use on a family plan.

[0100] The activation process 900 can begin with a decision 902 that determines whether the mobile multi-function device is to be activated as a family plan. When the decision 902 determines that the mobile multi-function device is not to be activated as a family plan then the mobile multi-function device can alternatively be activated 904 on an individual plan basis. When the decision 902 determines that the mobile multi-function device is to be activated as a family plan, an activation process 906 can be carried out for a family plan. The activation process for a family plan is generally similar to the processing illustrated in FIGs. 8A-8C; however, the account being established is a family account not an individual account and also the service plans normally differ because they pertain to family plans. Following the blocks 904 and 906, the activation process 900 for a family plan is complete.

[0101] FIG. 10 is a flow diagram of an activation process 1000 according to another embodiment of the invention. The activation process 1000 is, for example, processing associated with activation of a new mobile multi-function device by an existing customer of the service provider.

[0102] The activation process 1000 can request 1002

BNSDOCID: <EP_____1942698A1_I_>

current account information. Typically, the current account information would be requested 1002 from a customer attempting to activate a mobile multi-function device. A decision 1004 then determines whether the current account information has been received. In one embodiment, the current account information is received from the customer through interaction with a graphical user interface. The current account information is requested so that the customer's current account can be identified. When the decision 1004 determines that the current account information has not been received, the activation process 1000 can await the current account information.

[0103] Once the decision 1004 determines that the current account information has been received, a decision 1006 determines whether the user is authenticated. The authentication of the customer (user) can be achieved in a variety of different ways, including use of a user name, password, and/or a security question, etc. Hence, authenticating the user typically requires user data entry. When the decision 1006 determines that the customer (user) is authorized with respect to the current account, a subscriber status for the current account can be checked 1008. A decision 1010 can then determine whether the account for the subscriber is active. When the decision 1010 determines that the account for the subscriber is active, then processing associated with blocks 814-844 are the activation process 800 illustrated in FIG. 8A-8C can be performed 1012 to activate an account (new or update to existing account) and also activate the mobile multi-function device. On the other hand, when the decision 1006 determines that the user is not authenticated or when the decision 1010 determines that the account is not active, an error indication can be presented 1014. As an example, the error indication can be presented 1014 by a graphical user interface that informs the customer that activation is not available. Following the block 1012 or the block 1014, the activation process 1000 can end.

[0104] FIG. 11 is a flow diagram of an activation process 1100 according to another embodiment of the invention. The activation process 1100 is concerned with adding an additional line to an existing account with a network service provider.

[0105] The activation process 1000 can request 1102 current account information. Typically, the current account information would be requested 1102 from a customer attempting to activate a mobile multi-function device. A decision 1104 determines whether the current account information associated with the customer has been received. In one embodiment, the current account information is received from the customer through interaction with a graphical user interface.

When the decision 1104 determines that the current account information has not been received, the activation process 1100 can await the current account information. Alternatively, when the decision 1104 determines that the current account information has been received, a decision 1106 can determine whether the customer (user) is authorized to access the client account (or its information). When the decision 1106 determines that the customer (user) is authenticated and able to access the account, a subscriber status for the account is checked 1108. A decision 1110 can then determine whether the account associated with the subscriber (customer) is active. When the decision 1110 determines that the account associated with the subscriber is inactive (i.e., not active), an error indication can be presented 1112. In the event that the account associated with the subscriber is inactive, the error indication being presented 1112 can inform the customer that they are unable to add a new line to an existing account because the account is inactive.

[0106] On the other hand, when the decision 1110 determines that the account associated with the subscriber is active, the activation process 1100 can determine 1114 whether an additional line is available to the subscriber. In one embodiment, a subscriber can be allocated up to a determined of number lines for which they may activate. The number of lines available to the subscriber can be determined based on the subscriber's credit history, service plan, anticipated or actual use, etc. When the decision 1116 determines that an additional line is not available to the subscriber, then the subscriber can be informed 1118 that the additional line is not available. In one implementation, such as illustrated in FIG. 11, when an additional line can still be available if the subscriber provides a deposit (e.g., security deposit), the subscriber can be so informed 1118. Alternatively, when the decision 1116 determines that the additional line is available, the activation process 1100 can perform various previously described operations to activate the mobile multi-function device at block 1120. In one embodiment, the activation operations are associated with blocks 802, 804 and 810-844 of the activation process 800 illustrated in FIGs. 8A-8C. Following the blocks 1112, 1118 and 1120, the activation process 1100 can end.

[0107] Another aspect of the invention pertains to online provisioning methods and graphical user interfaces therefore. The provisioning methods enable an end user to activate a mobile communication device (e.g., mobile phone). In one embodiment, an end user can connect a mobile communication device to a computing device, such as a personal computer, and then perform an online activation process with a wireless service provider. The invention can provide automation and flexibility to activation of wireless communication devices.

[0108] FIGs. 12A-12C are flow diagrams of a mobile device provisioning process 1200 according to one embodiment of the invention. The mobile device provisioning process 1200 is, for example, performed by a server, such as the activation server 112 of the activation system 100 illustrated in FIG. 1.

[0109] The mobile device provisioning process 1200 can begin with a decision 1202. The decision 1202 can determine whether a new mobile device needs to be provisioned (or activated). The new mobile device, for ex-

ample, can refer to a mobile device that requires provisioning in order to utilize a wireless network for voice (and/or data) communications. The new mobile device can, for example, be recognized by a client machine, such as the client machine 102 illustrated in FIG. 1, when the mobile device connects with the client machine. The client machine can then in turn interact with the activation server to present suitable graphical user interfaces that assist the user of the mobile device in provisioning (or activating) the mobile device. Hence, when the decision 1202 determines that a new mobile device is not present, then the mobile device provisioning process 1200 awaits the presence of a new mobile device. In other words, until a new mobile device is present, the mobile device provisioning process 1200 simply waits to recognize a new mobile device. On the other hand, once the decision 1202 determines that a new mobile device has been recognized, an initial registration page is displayed 1204. The initial registration page can provide initial information to a user regarding registration of a mobile device.

[0110] FIG. 13 is a screen shot of an exemplary initial registration page 1300 according to one embodiment of the invention. The initial registration page 1300 illustrated in FIG. 13 provides initial registration information regarding a device entitled "Debbie's iPhone" which in this example pertains to a mobile phone. In one embodiment, the mobile phone is a multi-function device. After the initial registration page is displayed 1204, a decision 1206 can determine whether a user continues with the mobile device provisioning process 1200. When the decision 1206 determines that the user has not yet elected to continue, the mobile device provisioning process 1200 can await such a request. Alternatively, the user could instead request to cancel the mobile device provisioning process 1200, in which case the mobile device provisioning process 1200 could end.

[0111] On the other hand, when the decision 1206 determines that the user has requested to continue with the mobile device provisioning process 1200, a customer status page can be displayed 1208. In general, the customer status page can allow a customer (user) to specify whether or not they are an existing customer to the wireless network provider, in this example, AT&T Wireless. Additionally, the customer status page may enable the customer to specify whether they are activating on an individual plan or a group plan, or whether they wish to keep their current phone number (i.e., transferring the phone number) or create a new phone number.

[0112] FIG. 14 is a screen shot of an exemplary customer status page 1400 according to one embodiment of the invention. The customer status page 1400 allows a new wireless network service customer to activate a new phone on an individual plan. Here, the customer may or may not desire to transfer their current mobile phone number. Further, the customer status page 1400 can allow an existing wireless network service customer to either keep their current phone number or create a new phone number for the particular mobile device being provisioned.

[0113] After the customer status page is displayed 1208, a decision 1210 determines whether the customer is a new customer. As an example, this determination can be made following submission of the customer status page 1400 which enables the user to indicate whether or not they are an existing customer.

[0114] Although not illustrated in FIGs. 12A-12C, the mobile device provisioning process 1200 can further display a number transfer page. The number transfer page can assist a user in transferring an existing number from another service provider to be used with the particular mobile device being provisioned.

[0115] FIG. 15 is a screen shot of an exemplary screen shot of a mobile number transfer page 1500. The mobile number transfer page 1500 includes a data entry region 1502 that enables a user to provide existing account information in the case where an existing mobile number is to be transferred. FIG. 16 is a screen shot of an exemplary screen shot of a landline number transfer page 1600. The landline number transfer page 1600 includes a data entry region 1602 that enables a user to provide existing account information in the case where an existing landline number is to be transferred.

[0116] When the decision 1210 determines that the user is a new customer, a service plan selection page can be displayed 1212. In general, the service plan selection page provides one or more available service plans to the customer. A customer can then select one of the available service plans.

[0117] FIG. 17A and 17B are screen shots of an exemplary service plan selection page 1700 according to one embodiment of the invention. The service plan selection page 1000 allows the customer to select from one of six service plans 1702-1712, each of which can offer a different package of services at different rates. A first three of the service plans are illustrated in FIG. 17A, and a second three of the service plans are illustrated in FIG. 17B.

[0118] Following the display 1212 of the service plan selection page, a decision 1214 can determine whether a service plan has been selected. When the decision 1214 determines that a service plan has not yet been selected, the mobile device provisioning process 1200 can await such a selection. On the other hand, once the decision 1214 determines that a service plan has been selected, as well as following the decision 1210 when the customer is not a new customer, a customer account page can be displayed 1216. The customer account page can allow an existing customer to login to their account. The account is, for example, associated with an on-line media store, such as the iTunes® media store.

[0119] FIG. 18 is a screen shot of an exemplary customer account page 1100 according to one embodiment of the invention. The customer account page 1100 includes a sign-in section 1802 that allows an existing account holder to sign-in, with an identifier (e.g., Apple ID) and password.

BNSDOCID: <EP_____1942698A1_I_>

[0120] After the customer account page has been displayed 1216, a decision 1218 can determine whether the customer is an existing account holder. When the decision 1218 determines that the customer has an existing account, the customer can login 1220 to the account. Alternatively, when the decision 1218 determines that the customer does not have an existing account, or following the block 1220 after a successful login to an account, a customer information entry page is displayed 1222. The customer information entry page can facilitate a user in entering customer information that is to be utilized by either the wireless network service provider or the media asset provider (e.g., on-line media store). For a customer with an existing account, the customer information can be pre-entered and/or the certain subsequent portions of the remaining processing for the mobile device provisioning process 1200 could be simplified or eliminated. For a customer without an existing account with the on-line media store, the customer information entry page can also allow the customer to create a new account with the on-line media store.

[0121] FIG. 19 is a screen shot of a customer information entry page 1900 according to one embodiment of the invention. The customer information entry page 1900 allows entry of basic customer information to be utilized in creating one or more accounts. The customer information can, for example, include information pertaining to the customer, such as e-mail address, password, security question and answer, and date of birth.

[0122] Once the customer has entered the requested customer information, the mobile device provisioning process 1200 can continue. A decision 1224 determines whether customer information has been received. When the decision 1224 determines that the customer information has been received, such as by completion of the customer information entry page, a billing information page can be displayed 1226. The billing information page enables a customer to provide billing information to be utilized to pay for the service plan that was previously selected by the customer. The billing information can also be used by another service provider, such as an online media store. It should be noted that sharing of customer information and/or billing information between two or more service providers provides an efficient and user friendly system is provided.

[0123] FIG. 20 illustrates an exemplary billing information page 2000 according to one embodiment of the invention. The billing information page 2000 provides a means for the customer to enter various billing information, such as name, billing address, phone number, social security number, credit card number, security code, and expiration date. The billing information can be used by one or more service providers, in this example, AT&T Wireless as the wireless service provider and iTunes® media store as an online media service provider.

[0124] After the billing information page is displayed 1226, a decision 1228 determines whether billing information has been received. When the decision 1228 determines that billing information has not been received, then the mobile device provisioning process 1200 awaits such billing information. On the other hand, when the decision 1228 determines that billing information has been received, a terms and condition page can be displayed 1230. The terms and conditions page can provide the customer with the terms and conditions of the one or more legal agreements that are being established with the customer.

[0125] FIG. 21A is an exemplary screen shot of a first terms and conditions page 2100 according to one embodiment of the invention. In this example, the customer is required to read and agree to a software license/usage agreement 2102 with respect to Apple Computer, Inc. for use of the iTunes® media store. FIG. 21B is an exemplary screen shot of a second terms and conditions page 2150 according to one embodiment of the invention. In this example, the customer is required to read and agree to a wireless service agreement 2502 with a wireless service provider. The terms and conditions pages 2100 and 2150 require that the user accept the respective terms and conditions of these agreements in order to continue.

[0126] Following the display 1230 of the terms and conditions page, a decision 1232 determines whether the customer has accepted the various terms and conditions. When the decision 1232 determines that the customer has not accepted the terms and conditions, then the mobile device provisioning process 1200 awaits such acceptance. Once the decision 1232 determines that the customer has accepted the various terms and conditions, a review information page can be displayed 1234. The review information page allows a user to finally review the information regarding the service plan (i.e., wireless network service) being established for the mobile device for the customer information, and the associated billing information.

[0127] FIG. 22 is a screen shot of an exemplary review information page 2200 according to one embodiment of the invention. The review information page 2200 summarizes the billing and plan information concerning the mobile device being activated. For example, as shown in FIG. 22, the review information page 2200 can specify the billing amount and the manner in which the customer is to be billed, a service plan and a brief description thereof, additional fees and explanation of additional costs.

[0128] After the review information page has been displayed, a decision 1236 can determine whether the mobile device provisioning process 1200 should continue. When the decision 1236 determines that the customer has decided to continue the mobile device provisioning process 1200, one or more setup completion pages can be displayed 1238. The one or more setup completion pages can inform the customer that the setup (or activation) of their mobile device is processing and/or has successfully completed. The setup completion page may also provide a phone number for the mobile device to the customer or indicate that the existing phone number is being transferred. The setup completion page may also

permit the customer to provide a name for the mobile device.

[0129] FIG. 23 is an exemplary screen shot of a setup completion page 2300 according to one embodiment of the invention. The setup completion page 2300 informs the customer that activation of the mobile device is being processed. FIG. 24A is an exemplary screen shot of a setup completion page 2400 according to another embodiment of the invention. The setup completion page 2400 provides the customer with a phone number 2402. FIG. 24B is an exemplary screen shot of a setup completion page 2450 according to still another embodiment of the invention. The setup completion page 2450 informs the customer that transfer of the existing phone number is ongoing. In one embodiment, the setup completion page 2400 and the setup completion page 2450 are alternative pages that are chosen dependent on whether a new phone number is being assigned or whether an existing phone number is being transferred.

[0130] After the setup completion page has been displayed 1238, a decision 1240 determines whether the customer desires to continue on with the mobile device provisioning process 1200. When the decision 1240 determines that the customer has not yet decided to continue, the mobile device provisioning process 1200 awaits the request to continue. Once the decision 1240 determines that the customer has requested to continue, a device preference page is displayed 1242. The device preference page can, for example, be provided by a media management application. In this regard, the media management application can assist the customer with the setting of one or more preferences concerning the mobile device that has just been provisioned (or activated). Alternatively, the customer can choose not to continue to the device preference page and instead end the mobile device provisioning process 1200. In any case, following the block 1242 (or alternatively following the block 1238), the mobile device provisioning process 1200 can end as the provisioning of the mobile device has been initiated and perhaps completed. Following the mobile device provisioning process 1200, the mobile device can thereafter be controlled or managed by the media management application. To the extent that the customer has set one or more preferences concerning the mobile device, the media management application can thereafter operate in accordance with the one or more preferences when interacting with or on behalf of the mobile device.

[0131] FIG. 25 is an exemplary screen shot of a device preference page 2500 according to one embodiment of the invention. The device preference page 2500 includes a source region 2501 and a preference information region 2502. A visual selector 2503 indicates selection of a device referred to as "Debbie's iPhone". For this selected device, the preference information area 2502 displays information 2506 regarding preferences associated with the particular device. In this specific example, a summary tab 2504 is active so that a summary preference window is displayed in the preference information area 2502. The summary preference window includes information describing the particular device, such as name, size, software version and serial number. The summary preference window also provides version information 2508 indicating whether or not an updated version of any software components might be available. Further, the summary preference window includes an options section 2510 that allows a customer to select one or more predetermined options regarding the mobile device. Device preferences can be set by a user for a plurality of different types of media. The device preferences can also be set differently for different types of media. The device preference page 2500 includes other tabs for distinct media types, including music, movies, TV shows, podcasts, photos, personal and games. These device preferences can be synchronization preferences used when synchronizing the media device with the client machine. For additional information on synchronization and synchronization preferences see (i) U.S. Provisional Patent Application No. 60/879,319, filed January 7, 2007, and entitled "MULTI-DEVICE DATA SYNCHRONIZATION OR BACKUP VIA A HOST DEVICE," which is hereby incorporated herein by reference; and (ii) U.S. Patent Application No. 11/679,082, filed February 26, 2007, and entitled "DATA SYNCHRONIZATION WITH HOST DEVICE IN ACCORDANCE WITH SYNCHRONIZATION PREFERENCES," which is hereby incorporated herein by reference.

[0132] As noted above, the provisioning method can also be used by existing customers. For example, an existing customer may get a new wireless communication device (e.g., mobile phone, multi-function device, etc.) that they want to use in place of their current wireless communication device. In one embodiment, the service plan (or rate plan) offered to the end user can have a predetermined minimum term (e.g., 2 years) or cancellation penalty duration. In one implementation, the user's new service plan will reset such minimum period(s) regardless of whether the user has already exceed the minimum period(s) for the user's existing plan.

[0133] FIG. 26 is a screen shot of an exemplary customer status page 2600 according to one embodiment of the invention. The customer status page 2600 allows a new wireless network service customer to activate a new mobile phone (i.e., mobile device) on pre-existing account in place of an existing mobile phone, whereby the phone number for the new mobile phone is the same as the phone number previously used for the existing mobile phone. Since the customer is an existing customer, an account information page can also be displayed. The account information page can permit the user to enter account information concerning their account with the wireless service provider. The account information serves to identify the pre-existing account of the user. As such, an activation server can locate the user account and associate the new mobile phone with the pre-existing account. FIG. 27 is a screen shot of an exemplary ac-

BNSDOCID: <EP_____1942698A1_I_>

count information page 2700 according to one embodiment of the invention. The account information page 2700 includes an account information entry area 2702 allows a user to enter account information.

[0134] An existing customer can also use the computer-assisted provisioning process to add an additional line to an existing account. FIG. 28 is a screen shot of an exemplary customer status page 2800 according to one embodiment of the invention. The customer status page 2800 allows an existing wireless network service customer to activate a new mobile phone on pre-existing account. Since the customer is an existing customer, an account information page can also be displayed. The account information page can permit the user to enter account information concerning their account with the wireless service provider. The account information serves to identify the pre-existing account of the user. As such, an activation server can locate the user account and associate the new mobile phone with the pre-existing account. FIG. 29 is a screen shot of an exemplary account information page 2900 according to one embodiment of the invention. The account information page 2900 includes an account information entry area 2902 allows a user to enter account information. Still further, in this scenario the pre-existing account is assumed to be an individual account. Hence, in one embodiment, an account type selection page can be displayed. FIG. 30 is a screen shot of an exemplary account type selection page 3000 according to one embodiment of the invention. The account type selection page 3000 allows the customer to choose to activate the new mobile phone on an individual plan or to instead convert to a family plan. Typically, with a family plan, the various mobile phones within the group can share service time (e.g., share plan minutes).

[0135] A new customer can also use the computer-assisted provisioning process to activate multiple mobile devices. FIG. 31 is a screen shot of an exemplary customer status page 3100 according to one embodiment of the invention. The customer status page 3100 allows a new customer for wireless network service to activate one mobile phone or multiple mobile phones. In one embodiment, when two or more mobile phones are to be activated an account type selection page can be displayed to enable the customer to choose between individual plans or family plans. FIG. 32 is a screen shot of an exemplary account type selection page 3200 according to one embodiment of the invention. The account type selection page 3200 allows the customer to choose to activate each of the multiple new mobile phones on individual plans or to instead activate all of the multiple new mobile phones on a family plan. Typically, with a family plan, the various mobile phones within the group can share service time (e.g., share plan minutes). In this example, the conversion to a family plan requires calling customer support; however, in other embodiments such can be part of the computer-assisted provisioning.

[0136] Mobile device provisioning can also enable remote provisioning of multiple wireless communication devices. For example, wireless service providers often refer to multiple devices on a primary account as a "family plan". Activation of multiple devices for such a primary account can require additional operations. In one embodiment, a first mobile device is connected to the host computer, such as using a USB connection, and then for the subsequent one or more mobile device to be also activated for the primary account can be identified to the provisioning server by having an end-user manually enter an identifier that is provided with another mobile device. For example, the identifier can be provided on or within a package containing the another mobile device. Hence, in would be possible for an end-user to activate a mobile device without it being present.

[0137] In one embodiment, the activation process uses two identifiers, IMEI and ICCID, when activating a mobile device. However, neither of these identifiers have built-in error correct or validation. Hence, manual entry of these identifiers by end-users could lead to failed or improper activation. One embodiment to enhance activation in such situations is to provide end-users with a computed identifier that uniquely maps to the needed IMEI and ICCID identifiers. The computed identifier can be more compact (i.e., less digits) and thus easier for manual entry. Moreover, the computed identifier can include error correction to guard against improper entry of the computed identifier.

[0138] Mobile device provisioning can also restrict payment options to those consumers that have low credit scores. For example, a wireless service provider may not desire to activate a wireless service plan to those customers that have poor credit. Hence, in one embodiment, the wireless service provider can offer different payment options to different customers dependent on at least credit information (e.g., credit score). For example, customers with poor credit can be required to pay a deposit or to pre-pay for such service.

[0139] In some cases, a new customer can be limited to service plans that require prepayment. In one embodiment, the provisioning process can decide whether prepayment is required based on the credit history of the customer. The credit history can, for example, result from a credit report on the customer. FIG. 33 is a screen shot of an exemplary prepayment requirement page 3300. The exemplary prepayment requirement page 3300 can present the customer with one or more option on activating wireless service. The exemplary prepayment requirement page 3300 allows the customer to (i) provide a pre-approval credit check code and continue activation, (ii) agree to a prepaid plan (e.g., with advance monthly payment via credit or debit card) and continue activation, or (iii) restart/cancel the activation process.

[0140] As noted above, the provisioning method can also be used by existing customers. For example, an existing customer may get a new wireless communication device (e.g., mobile phone, multi-function device, etc.) that they want to use it in place of their current wireless communication device. In one embodiment, the

service plan offered to the end user can have a predetermined minimum term (e.g., 2 years) or cancellation penalty duration. In one implementation, the user's new service plan will reset such minimum period regardless of whether the user has already exceed the minimum period for the user's existing plan.

[0141] FIG. 34 is a block diagram of a mobile multi-function device 3400 according to one embodiment of the invention. The mobile multi-function device 3400 can include the circuitry of the mobile multi-function device 104 illustrated in FIG. 1 and/or can perform the operations described with reference to FIGs. 3 and 4. The mobile multi-function device 3400 includes hardware and software components to provide at least two functions, namely, a media playback function and a wireless voice communications function. When providing media playback, the mobile multi-function device 3400 can operate as a media player capable of playing (including displaying) media items. The media items can, for example, pertain to audio items (e.g., audio files or songs), videos (e.g., movies) or images (e.g., photos). When providing wireless voice communications, the mobile multi-function device 3400 can operate a mobile telephone (e.g., cellular phone).

[0142] The mobile multi-function device 3400 includes a processor 3402 that pertains to a microprocessor or controller for controlling the overall operation of the mobile multi-function device 3400. The mobile multi-function device 3400 stores media data pertaining to media items in a file system 3404 and a cache 3406. In one embodiment, the file system 3404 is implemented by a storage disk or a plurality of disks. In another embodiment, the file system 3404 is implemented by EEPROM or Flash type memory. The file system 3404 typically provides high capacity storage capability for the mobile multi-function device 3400. However, since the access time to the file system 3404 is relatively slow, the mobile multi-function device 3400 can also include a cache 3406. The cache 3406 is, for example, Random-Access Memory (RAM) provided by semiconductor memory. The relative access time to the cache 3406 is substantially shorter than for the file system 3404. However, the cache 3406 does not have the large storage capacity of the file system 3404. Further, the file system 3404, when active, consumes more power than does the cache 3406. The power consumption is often a concern when the mobile multi-function device 3400 is a portable mobile multi-function device that is powered by a battery 3424. The mobile multi-function device 3400 also includes a RAM 3420 and a Read-Only Memory (ROM) 3422. The ROM 3422 can store programs, utilities or processes to be executed in a non-volatile manner. The ROM 3422 can be implemented by an EEPROM or Flash type memory so as to provide writable non-volatile data storage. The RAM 3420 provides volatile data storage, such as for the cache 3406.

[0143] In one embodiment, to support wireless voice communications, the mobile multi-function device 3400 includes a transceiver 3426 and a SIM card 3428. The transceiver 3426 supports wireless communication with a wireless network (such as a wireless cellular network). The SIM card 3428 includes an identifier (e.g., SIM identifier) can be used by the mobile multi-function device 3400 to gain access and utilize the wireless network. In other embodiments, a SIM card 3428 is not utilized.

[0144] The mobile multi-function device 3400 also includes a user input device 3408 that allows a user of the mobile multi-function device 3400 to interact with the mobile multi-function device 3400. For example, the user input device 3408 can take a variety of forms, such as a button, keypad, dial, etc. Still further, the mobile multi-function device 3400 includes a display 3410 (screen display) that can be controlled by the processor 3402 to display information to the user. A data bus 3411 can facilitate data transfer between at least the file system 3404, the cache 3406, the processor 3402, and the CODEC 3412.

[0145] In one embodiment, the mobile multi-function device 3400 serves to store a plurality of media items (e.g., songs) in the file system 3404. When a user desires to have the mobile multi-function device play a particular media item, a list of available media items is displayed on the display 3410. Then, using the user input device 3408, a user can select one of the available media items. The processor 3402, upon receiving a selection of a particular media item, supplies the media data (e.g., audio file) for the particular media item to a coder/decoder (CODEC) 3412. The CODEC 3412 then produces analog output signals for a speaker 3414. The speaker 3414 can be a speaker internal to the mobile multi-function device 3400 or external to the mobile multi-function device 3400. For example, headphones or earphones that connect to the mobile multi-function device 3400 would be considered an external speaker.

[0146] The mobile multi-function device 3400 also includes a bus interface 3416 that couples to a data link 3418. The data link 3418 allows the mobile multi-function device 3400 to couple to a host device (e.g., host computer or power source). The data link 3418 can also provide power to the mobile multi-function device 3400.

[0147] The various aspects, embodiments, implementations or features of the invention can be used separately or in any combination.

[0148] The invention can be implemented by software, hardware or a combination of hardware and software. The invention can also be embodied as computer readable code on a computer readable medium. The computer readable medium is any data storage device that can store data which can thereafter be read by a computing device (e.g., computer system). Examples of the computer readable medium include read-only memory, random-access memory, CD-ROMs, DVDs, magnetic tape, optical data storage devices, and carrier waves. The computer readable medium can also be distributed over network-coupled computer systems so that the computer readable code is stored and executed in a distributed

BNSDOCID: <EP_____1942698A1_I_>

fashion.

[0149] The advantages of the invention are numerous. Different aspects, embodiments or implementations may, but need not, yield one or more of the following advantages. One advantage of the invention is that mobile devices can be setup or activated to operate on wireless networks by end users. Another advantage of the invention is that setup or activation can be substantially automated and controlled by a computer-implemented system to facilitate setup or activation with a service provider (e.g., wireless service provider). Another advantage of the invention is that graphical user interfaces can be presented to users so as to enable end users to easily activate mobile devices. Still another advantage of the invention is that more than one account for different service providers can be concurrently arranged in an efficient and user friendly manner. Yet still another advantage of the invention is that mobile devices can be largely disabled until properly activated with a service provider.

[0150] The many features and advantages of the present invention are apparent from the written description. Further, since numerous modifications and changes will readily occur to those skilled in the art, the invention should not be limited to the exact construction and operation as illustrated and described. Hence, all suitable modifications and equivalents may be resorted to as falling within the scope of the invention.

Claims

1. A computer-implemented method for activating wireless network service for an electronic device through use of a host device, the electronic device being associated with a customer for wireless network service provided by a wireless network service provider, said method comprising:

   receiving device information from the electronic device when the electronic device is attached to the host device;
   acquiring customer information pertaining to the customer;
   receiving a service plan selection from the customer;
   receiving billing information for payment of the service plan; and
   initiating activation of a wireless service account for use of the electronic device with the wireless network service provided by the wireless network service provider, wherein the wireless service account being activated is based on the customer information, the service plan and the billing information.

2. A computer-implemented method as recited 1, wherein said method further comprises:

   enabling, following said activating, the electronic device for usage of at least one operation that was previously restricted prior to said enabling.

3. A computer-implemented method as recited 1, wherein said method further comprises:

   obtaining a credit indication for the customer; and
   determining one or more service plans that are made available to the customer based at least in part on the credit indication for the customer,

   wherein the service plan selection is one of the one or more service plans.

4. A computer-implemented method as recited in claim 1, wherein said method further comprises:

   requiring formation of a media account with the online media store when the customer does not already have a media account with the online media store.

5. A computer-implemented method as recited in claim 1, wherein said method further comprises:

   thereafter initiating activation of the wireless network service for the electronic device associated with the customer.

6. A computer-implemented method as recited in claim 1, wherein said method further comprises:

   presenting account information for approval; and
   receiving approval from the customer for the account information.

7. A computer-implemented method as recited in claim 1, wherein said method further comprises:

   presenting at least one service agreement for approval; and
   receiving approval of the at least one service agreement.

8. A computer-implemented method as recited in any of claims 1-7, wherein the host device is a personal computer, and wherein said method is performed by an application program operating on the personal computer.

9. A computer-implemented method as recited in claim 8, wherein the application program is a media management application.

10. A computer-implemented method for activating an

BNSDOCID: <EP_____1942698A1_I_>

electronic device for wireless network service through use of a host device, the electronic device being associated with a customer for wireless network service provided by a wireless network service provider, said method comprising:

receiving device information from the electronic device while the electronic device is attached to the host device;
acquiring customer information pertaining to the customer;
offering the user one or more service plans;
receiving a user selection of one of the service plans; and
receiving billing information for payment of the selected service plan.

11. A computer-implemented method as recited in claim 10, wherein said method further comprises:

offering the user a plurality of payment options; and
receiving a user selection of one of the payment options.

12. A computer-implemented method as recited in claim 10, wherein said method further comprises:

initiating activation of an account for the customer whereby the electronic device is provided with access to wireless network service in accordance with the selected service plan.

13. A computer-implemented method as recited in claim 10, wherein said method further comprises:

activating the electronic device for use with the wireless network service in accordance with the selected service plan.

14. A computer-implemented method as recited in claim 10, wherein said activating comprises:

enabling the electronic device; and
initiating setup of the wireless network service to permit usage by the electronic device.

15. A computer-implemented method as recited in claim 10, wherein the user is an end user and wherein the user selections are made by the user by a computer program operating on the host device.

16. A computer-implemented method as recited in claim 10, wherein said method is performed by an activation server that is operatively connected to the host device via a network.

17. A computer-implemented method as recited in claim 10, wherein said method is performed by the host device.

18. A computer-implemented method as recited in claim 10, wherein said method further comprises:

establishing wireless service account for the user, the wireless service account pertaining to the selected service plan and being paid for in accordance with the billing information.

19. A computer-implemented method as recited in claim 18, wherein said method further comprises:

thereafter activating the wireless network service for the electronic device associated with the user.

20. A computer-implemented method as recited in claim 10, wherein the electronic device is a multi-function device.

21. A computer-implemented method as recited in claim 10, wherein the electronic device comprises a mobile phone.

22. A computer-implemented method as recited in claim 10-21, wherein said method further comprises:

determining whether the user has a media account with an online media store.

23. A computer-implemented method as recited in claim 22, wherein said method further comprises:

requiring formation of a media account with the online media store when said determining determines that the user does not have a media account with the online media store.

24. A computer-implemented method as recited in claim 23, wherein said method further comprises:

establishing wireless service account for the user, the wireless service account pertaining to the selected service plan and being paid for in accordance with the billing information.

25. A computer-implemented method as recited in claim 24, wherein said method further comprises:

thereafter activating the wireless network service for the electronic device associated with the user.

26. A computer-implemented method as recited in claim 25, wherein said offering of one or more payment options is dependent on the credit worthiness of the

BNSDOCID: <EP_____1942698A1_I_>

user.

27. A computer-implemented method for activating an electronic device for wireless network service from a host device, the electronic device being associated with a customer for wireless network service provided by a wireless network service provider, said method comprising:

receiving device information from the electronic device when the electronic device is attached to the host device;
determining whether the electronic device has already been activated based on the device information; and
automatically initiating activation of the electronic device when said determining determines that the electronic device has not already been activated.

28. A computer-implemented method as recited in claim 27, wherein the host device is a personal computer, and wherein said method is performed by an application program operating on the personal computer.

29. A computer-implemented method as recited in claim 28, wherein the electronic device is a multi-function device, and wherein one function of the multi-function device is a wireless phone function, and another function of the multi-function device is a media playback function.

30. A computer-implemented method as recited in claim 29, wherein the application program is a media management application.

31. A computer readable medium including at least computer executable program code tangibly embodied therein for activating wireless network service for an electronic device through use of a client computing device, the electronic device being associated with a customer for wireless network service provided by a wireless network service provider, said computer readable medium comprising:

computer program code for receiving device information from the electronic device;
computer program code for acquiring customer information pertaining to the customer;
computer program code for receiving a service plan selection from the customer;
computer program code for receiving billing information for payment of the service plan; and
computer program code for initiating activation of a wireless service account for use of the electronic device with the wireless network service provided by the wireless network service provider.

32. A computer readable medium as recited in claim 31, wherein said computer readable medium further comprises:

computer program code for detecting connection of the electronic device to the host device; and

wherein said computer program code for receiving device information receives, the device information from the electronic device without user interaction once the electronic device is connected to the host device.

33. A computer readable medium including at least computer executable program code tangibly embodied therein for activating an electronic device for wireless network service through use of a host device, the electronic device being associated with a customer for wireless network service provided by a wireless network service provider, said computer readable medium comprising:

computer program code for receiving device information from the electronic device while the electronic device is attached to the host device;
computer program code for acquiring customer information pertaining to the customer;
computer program code for offering the user one or more service plans;
computer program code for receiving a user selection of one of the service plans; and

computer program code for receiving billing information for payment of the selected service plan.

34. A computer readable medium as recited in claim 33, wherein said computer readable medium further comprises:

computer program code for offering the user a plurality of payment options; and
computer program code for receiving a user selection of one of the payment options.

35. A computer readable medium as recited in claim 33, wherein said computer readable medium further comprises:

computer program code for initiating activation of an account for the customer whereby the electronic device is provided with access to wireless network service in accordance with the selected service plan.

36. A computer readable medium as recited in claim 33, wherein said computer readable medium further comprises:

computer program code for activating the electronic device for use with the wireless network service in accordance with the selected service plan.

37. A computer readable medium as recited in claim 33, wherein said computer program code for activating comprises:

computer program code for enabling the electronic device; and
computer program code for initiating setup of the wireless network service to permit usage by the electronic device.

38. A computer readable medium as recited in claim 33, wherein the user is an end user and wherein the user selections are made by the user by a computer program operating on the host device.

39. A computer readable medium as recited in claim 33, wherein said computer readable medium further comprises:

computer program code for establishing wireless service account for the user, the wireless service account pertaining to the selected service plan and being paid for in accordance with the billing information.

40. A computer readable medium as recited in claim 39, wherein said computer readable medium further comprises:

computer program code for thereafter activating the wireless network service for the electronic device associated with the user.

41. A computer-implemented method as recited in claim 33, wherein the electronic device is a multi-function device.

42. A computer-implemented method as recited in claim 33, wherein the electronic device comprises a mobile phone.

43. A computer-implemented computer readable medium as recited in any of claims 23-42, wherein said computer readable medium further comprises:

computer program code for determining whether the user has a media account with an online media store.

44. A computer readable medium as recited in claim 43, wherein said computer readable medium further comprises:

computer program code for requiring formation of a media account with the online media store when said determining determines that the user does not have a media account with the online media store.

45. A computer readable medium as recited in claim 44, wherein said computer readable medium further comprises:

computer program code for establishing wireless service account for the user, the wireless service account pertaining to the selected service plan and being paid for in accordance with the billing information.

46. A computer readable medium as recited in claim 45, wherein said computer readable medium further comprises:

computer program code for activating the wireless network service for the electronic device associated with the user.

47. A computer readable medium as recited in claim 46, wherein said computer program code for offering of one or more payment options is dependent on the credit worthiness of the user.

48. A graphical user interface to assist an end user in activating an account for an electronic device having wireless communication capabilities, the account being with respect to a wireless service provider providing wireless network service, said graphical user interface comprising:

a plurality of display screens that are presented on a display device associated with a host computer, said display screens includes at least:

an end user status page to facilitate selection of a type of activation;
a service plan selection page to facilitate selection of a service plan for the wireless network service;
a media account page for a media account associated with an online media store so that a user can create a new media account or login to an existing media account;
an end user information entry page to facilitate entry of end user information;
a billing information page to facilitate entry of billing information for one or both the user media account and a wireless account;
a terms and conditions page regarding legal agreements with the online media store and with the wireless service provider; and
an activation page to inform the end user of

BNSDOCID: <EP_____1942698A1_I_>

activation information.

49. A graphical user interface as recited in claim 48, wherein said display screens further comprises:

a final review and submit page to initiate activation of the account for the electronic device with respect to the wireless service provider.

50. A graphical user interface as recited in claim 48, wherein the final review and submit page can further initiate creation of the new media account for the user not having the existing media account.

51. A graphical user interface as recited in claim 48, wherein said plurality of display screens further comprises:

a device preference page to assist the end user with setting one or more preferences or options to be applied to the operation of the electronic device.

52. A graphical user interface as recited in claim 48, wherein the end user status page enables a user to select from a plurality of types of activation.

53. A graphical user interface as recited in claim 52, wherein the types of activation include an individual plan and a family plan.

54. A graphical user interface as recited in claim 52, wherein the types of activation include a new individual plan, an existing individual plan, a new family plan, and an existing family plan.

55. A graphical user interface as recited in claim 48, wherein the electronic device is a multi-function device, and wherein the multi-function device supports at least wireless voice communication and media playback.

56. A graphical user interface as recited in claim 48, wherein said plurality of display screens further comprises:

a media account page for identifying a media account for the end user.

57. A graphical user interface as recited in claim 48, wherein the type of activation pertains to individual plan activation or family plan activation.

58. A graphical user interface as recited in claim 48, wherein one of the types of activation pertains to use of an existing phone number or a new phone number.

59. A graphical user interface as recited in claim 48, wherein said service plan selection page presents information on a plurality of service plans and their costs and enables the end user to select from the service plans.

60. A graphical user interface as recited in claim 48, wherein the billing information provided via said billing information page includes information pertaining to name and billing address for the end user and credit card number.

61. A graphical user interface as recited in claim 48, wherein the activation completion page informs the end user of a phone number associated with the electronic device being activated.

62. A graphical user interface as recited in claim 48, wherein said plurality of display screens further comprises:

a device preference page to assist the customer with setting one or more preferences or options to be applied to the operation of the electronic device.

63. A graphical user interface as recited in claim 48, wherein said graphical user interface comprises:

a transfer number page for identifying a phone number and an existing account, wherein the phone number to be transferred is to be used with the account being activated and associated with the electronic device.

64. A graphical user interface as recited in claim 48, wherein said graphical user interface is presented on a display device associated with a computing device, and wherein the electronic device is electrically coupled to the computing device.

65. A graphical user interface as recited in claim 64, wherein the electronic device is a multi-function device, and wherein one function of the multi-function device is a wireless phone function, and another function of the multi-function device is a media playback function.

66. A graphical user interface as recited in claim 65, wherein the application program is a media management application.

67. A computer-implemented method for activating an electronic device for wireless network service, the electronic device being associated with a customer of a wireless service provider associated with the wireless network service, said method comprising:

informing an activation server of an electronic

device having wireless communication device that is to be activated for wireless network service;
displaying a customer status page to facilitate selection of a type of activation;
specifying to the activation server a type of activation desired by the customer;
displaying a service plan selection page to facilitate selection of a service plan for the wireless network service;
informing the activation server of a selected service plan;
displaying a customer account page to facilitate login to or creation of a user media account with an online media store;
providing account information for the user media account for the customer;
displaying a customer information entry page;
providing customer information to the activation server;
displaying a billing information page to facilitate entry of billing information for one or both the user media account and a wireless account;
informing the activation server of the billing information;
displaying a terms and conditions page regarding legal agreements with the online media store and with the wireless service provider;
informing the activation server of acceptance of the legal agreements;
displaying an information review page;
informing the activation server of approval of the information provided on the information review page;
displaying an activation completion page; and
displaying a device preference page to assist the customer with setting one or more preferences or options to be applied to the operation of the electronic device.

68. A method as recited in claim 67, wherein said displaying by said method is on a display device associated with a client computing device having the electronic device operatively coupled thereto.

BNSDOCID: <EP_____1942698A1_I_>

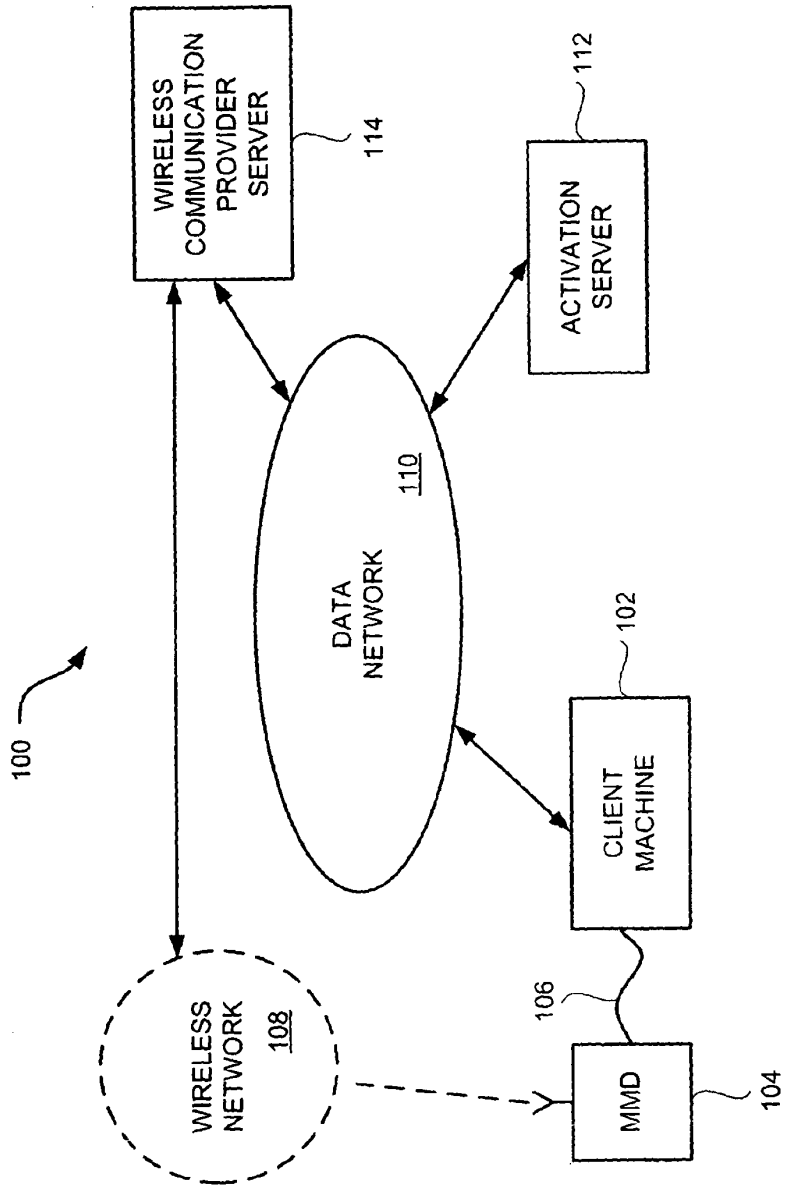


FIG. 1

EPNSDOCID: <EP 1942698A1 | >

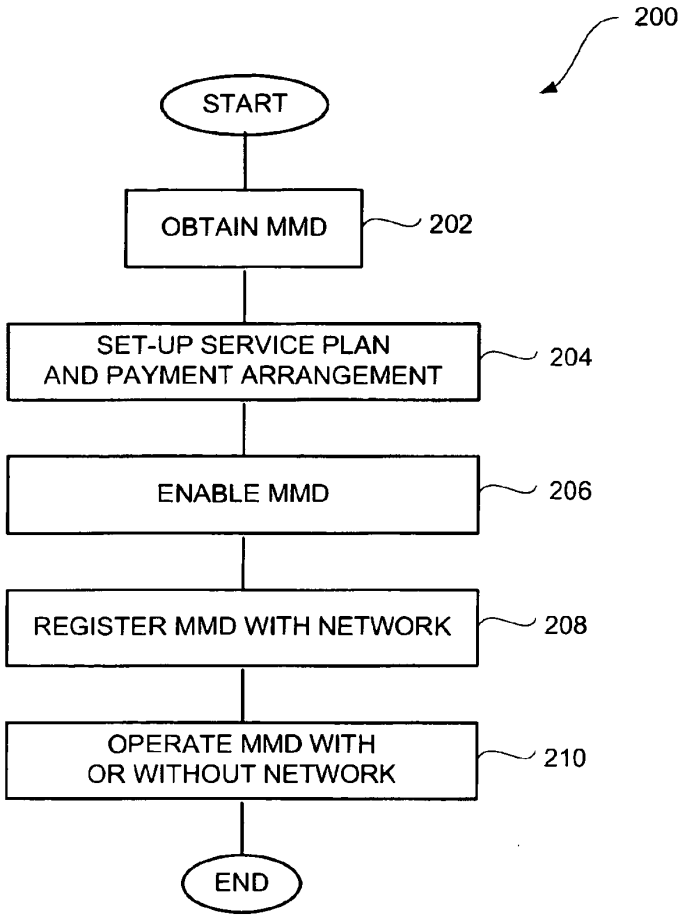


FIG. 2A

BNSDOCID: <EP_____1942698A1_I_>

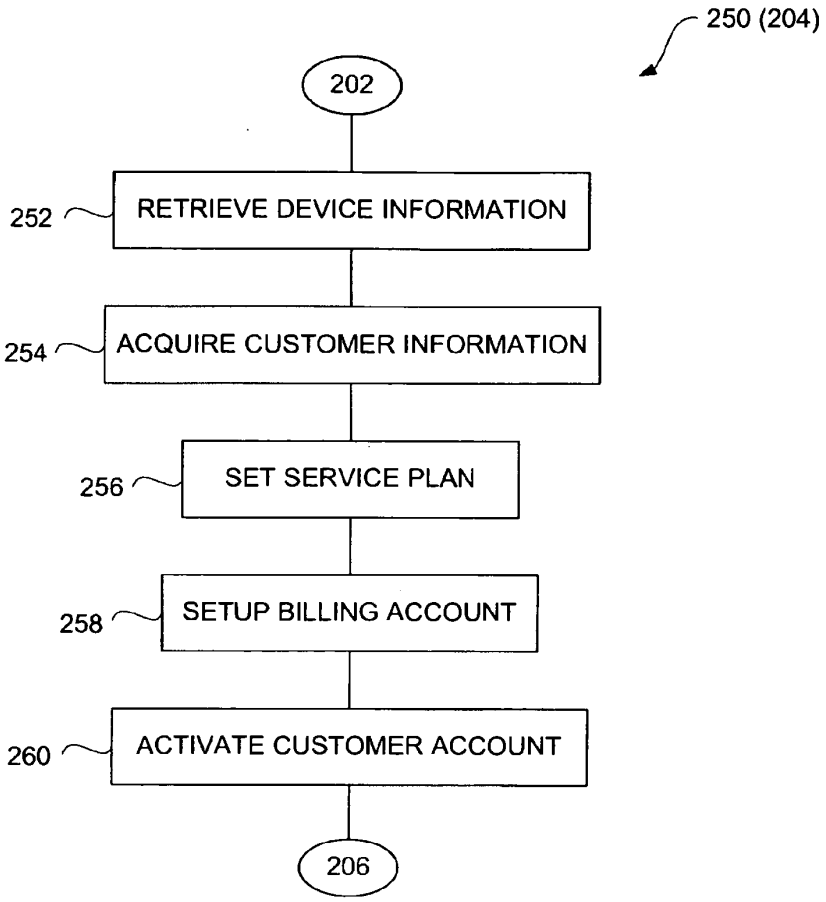


FIG. 2B

EPNSDOCID: <EP 1942698A1 | >

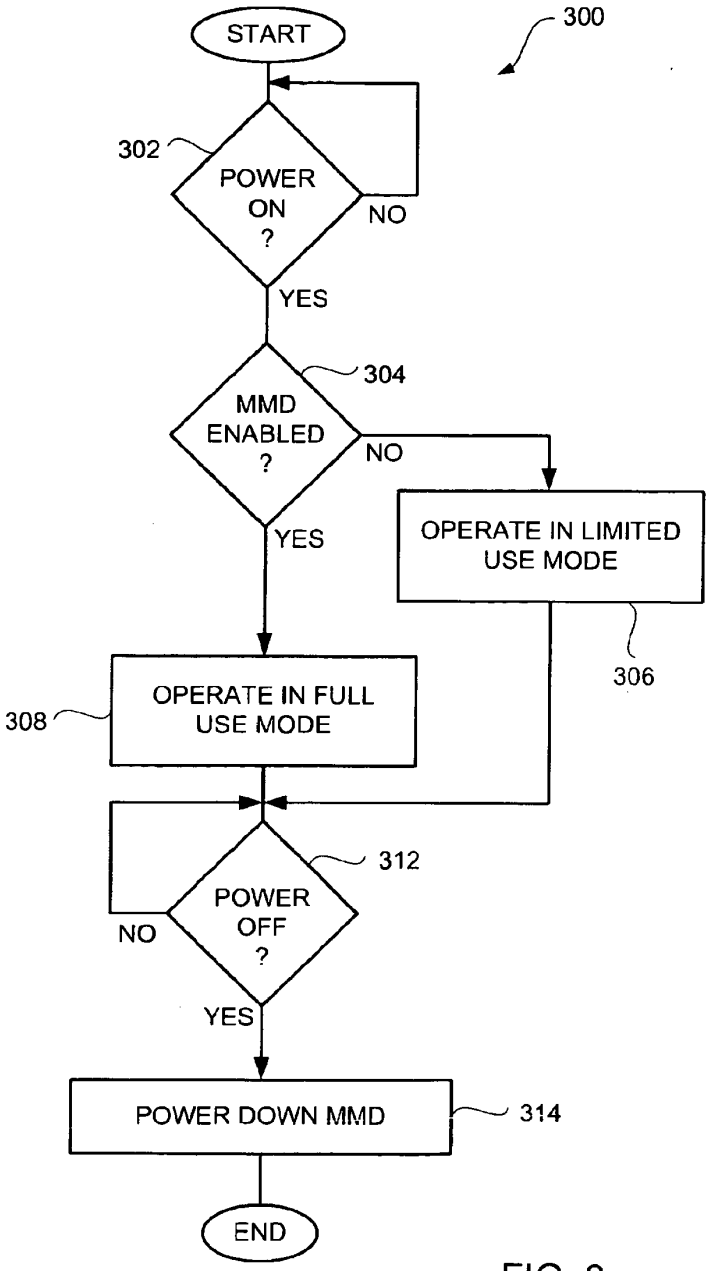


FIG. 3

BNSDOCID: <EP_____1942698A1_I_>

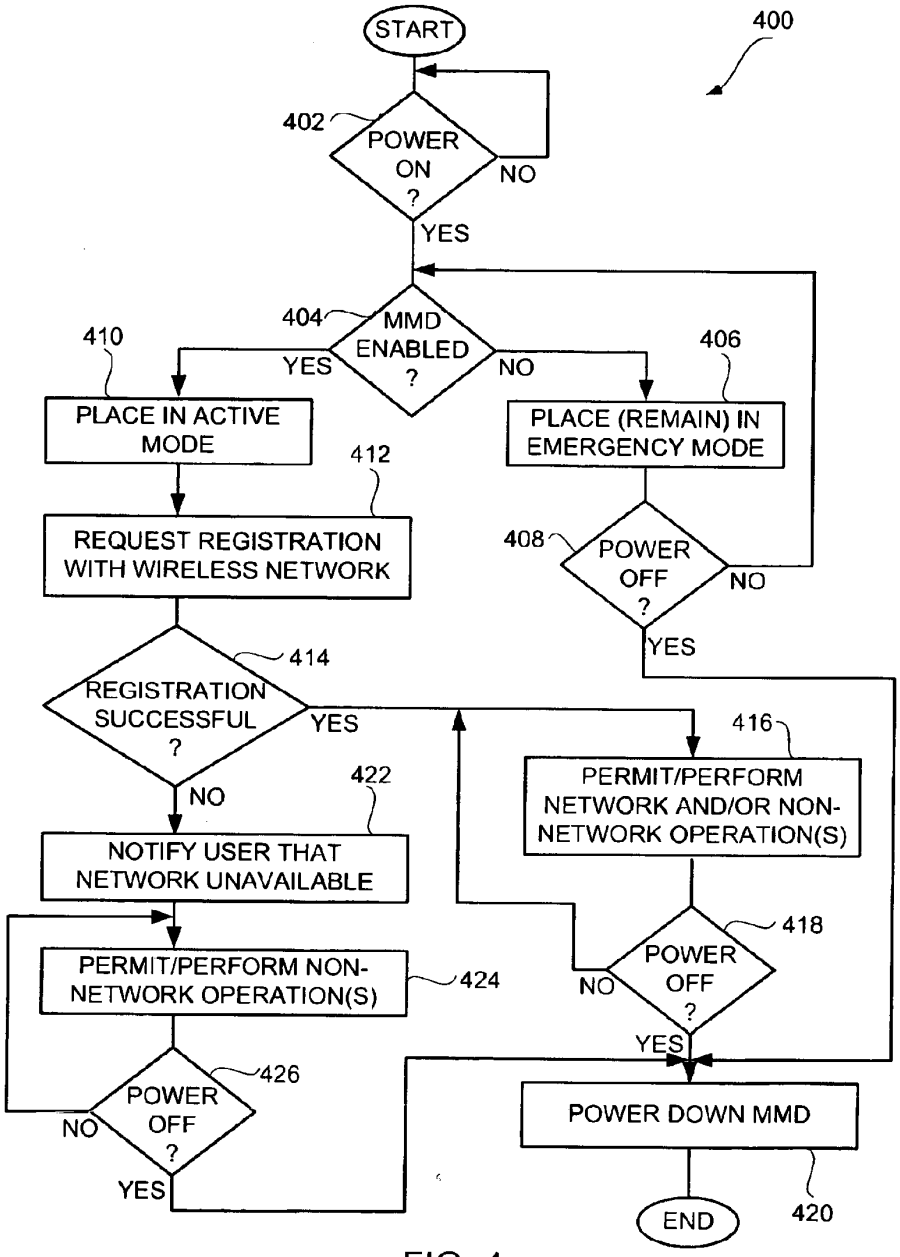


FIG. 4

BNSDOCID: <EP_____1942698A1_I_>

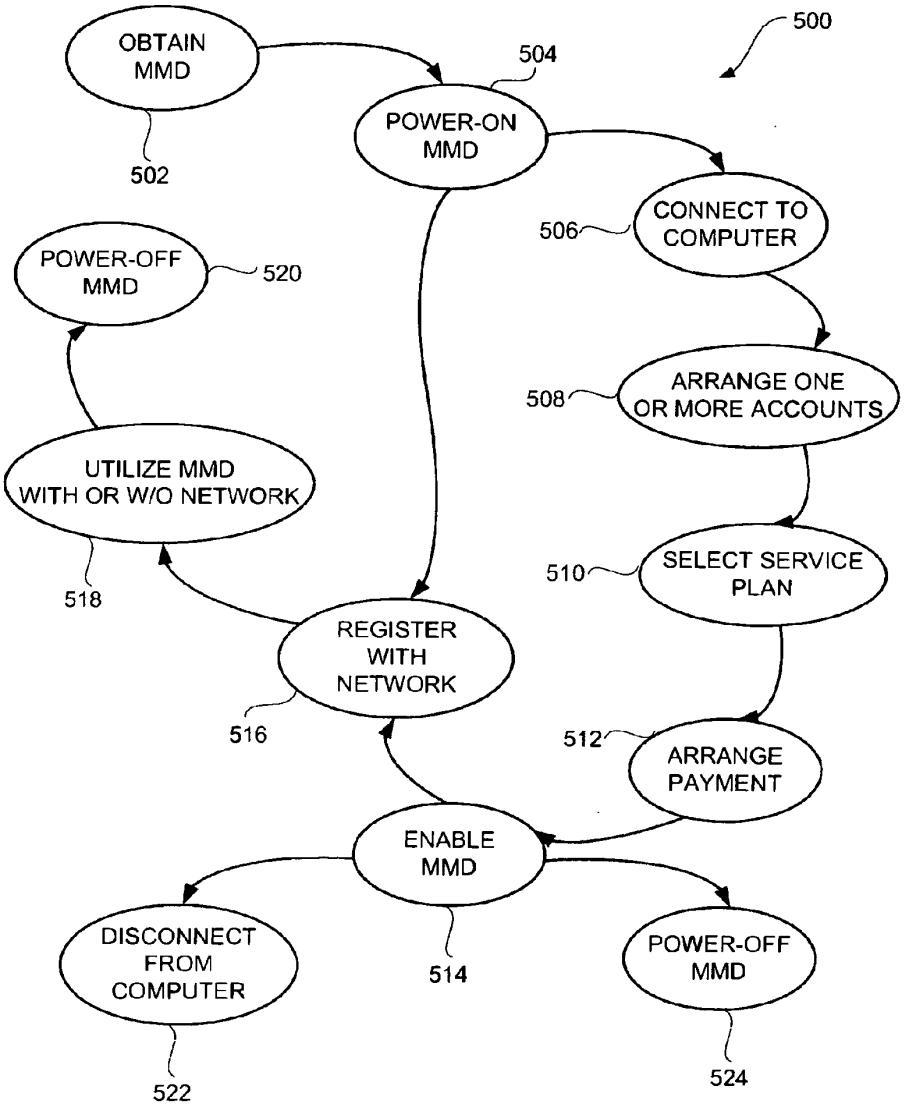


FIG. 5

BNSDOCID: <EP_____1942698A1_I_>

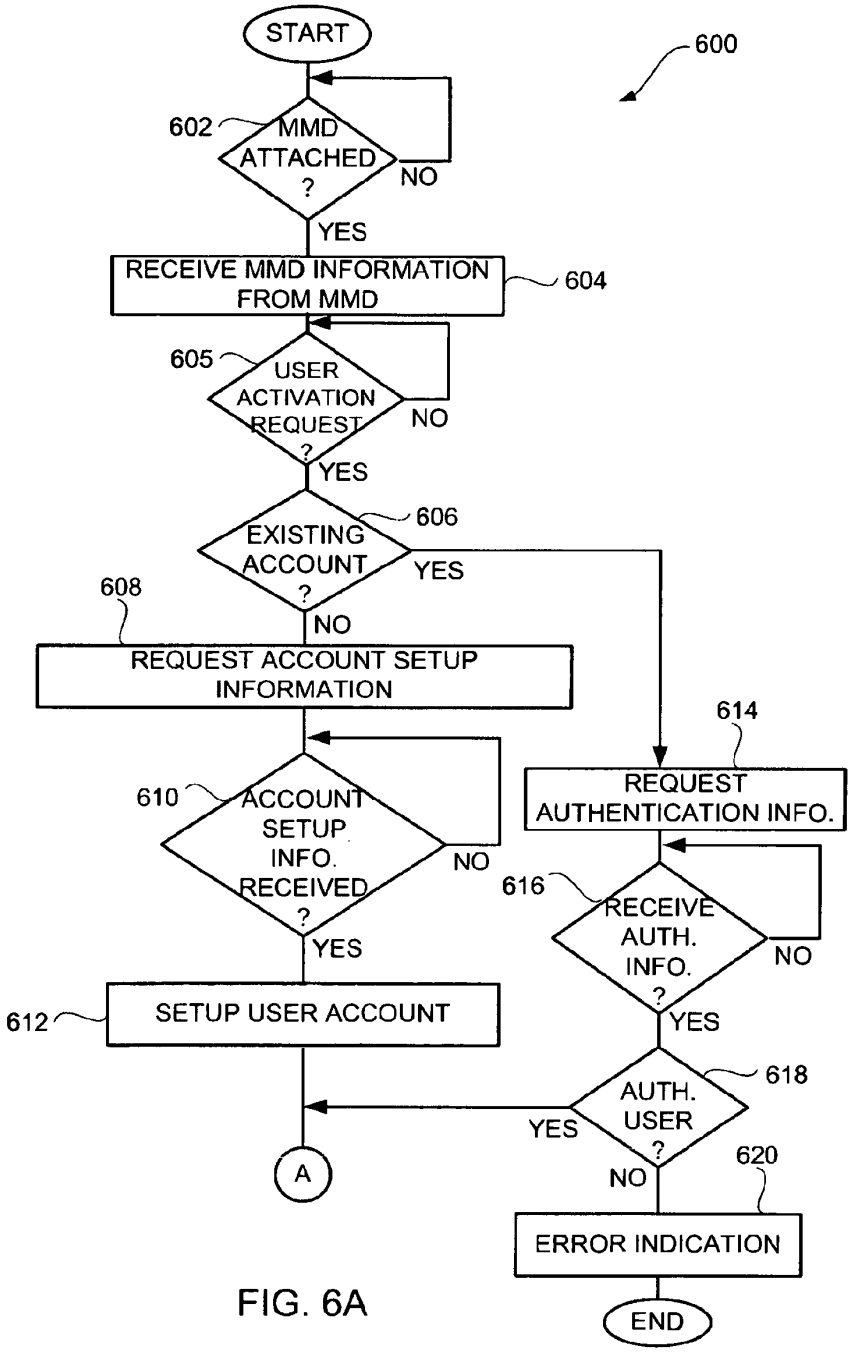


FIG. 6A

EPNSDOCID: <EP 1942698A1 | >

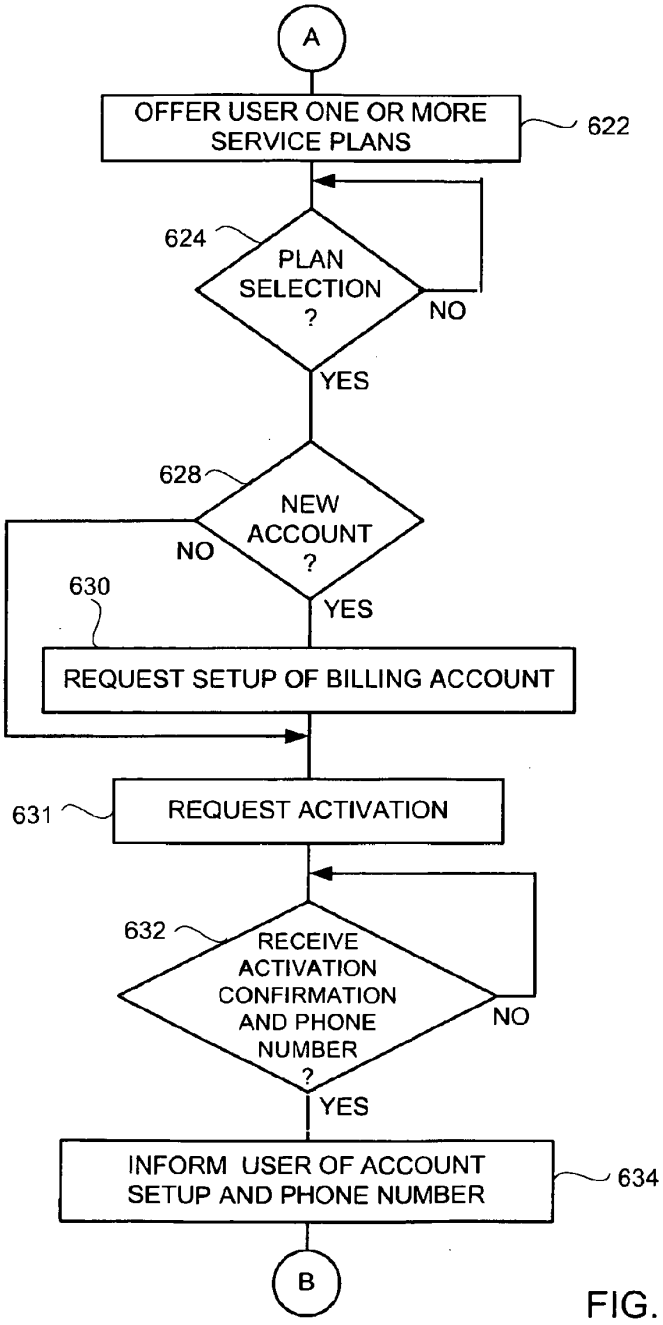


FIG. 6B

BNSDOCID: <EP_____1942698A1_I_>

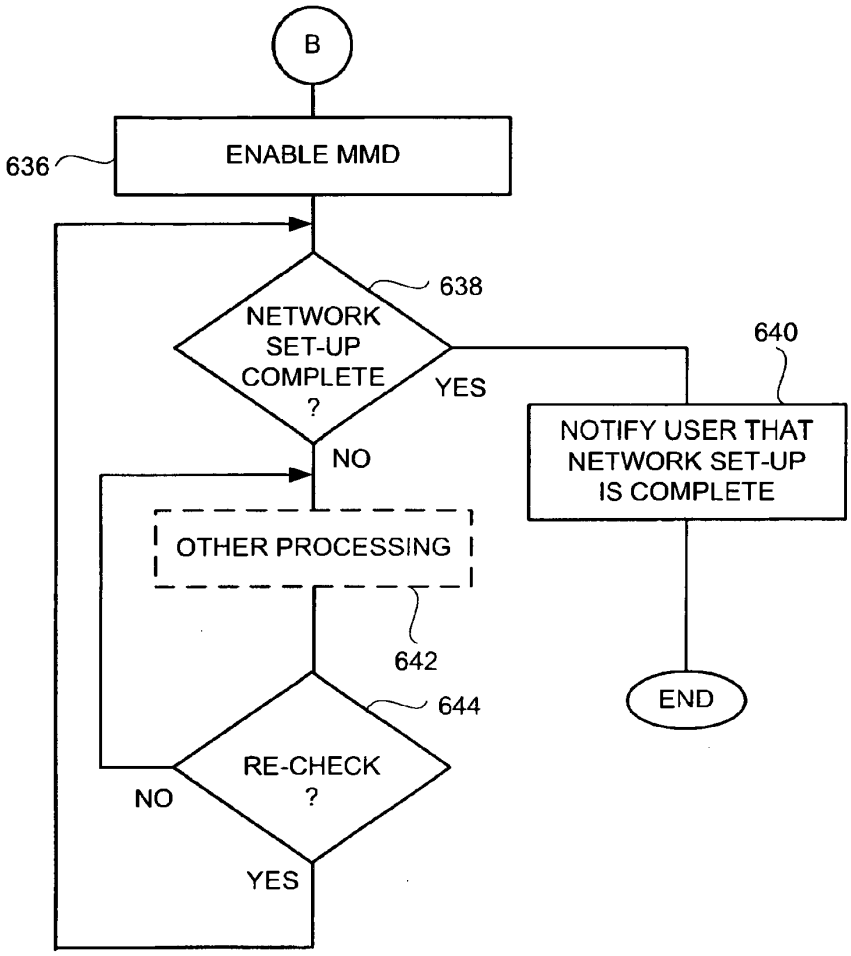


FIG. 6C

BNSDOCID: <EP_____1942698A1_I_>

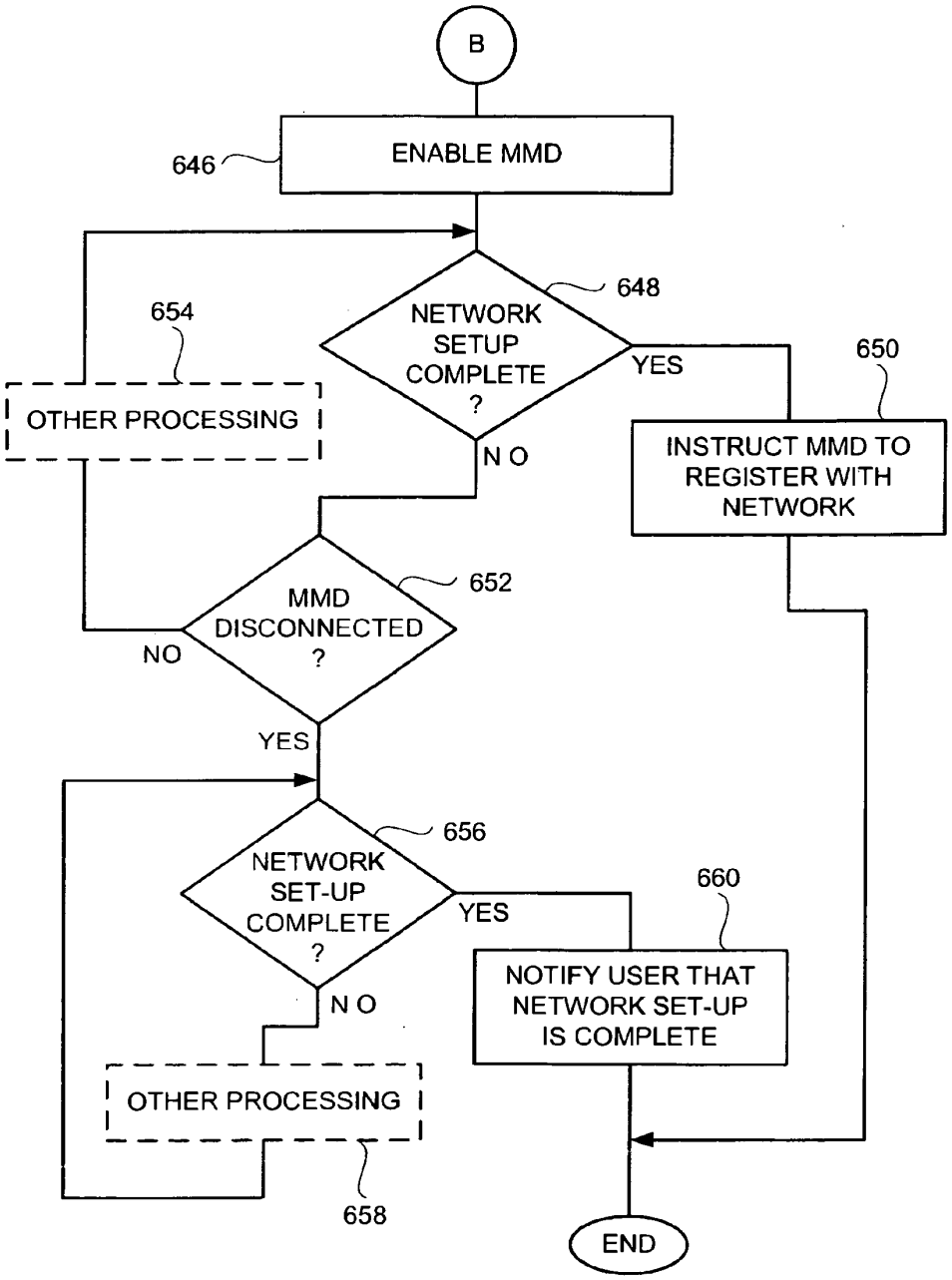


FIG. 6D

BNSDOCID: <EP_____1942698A1_I_>

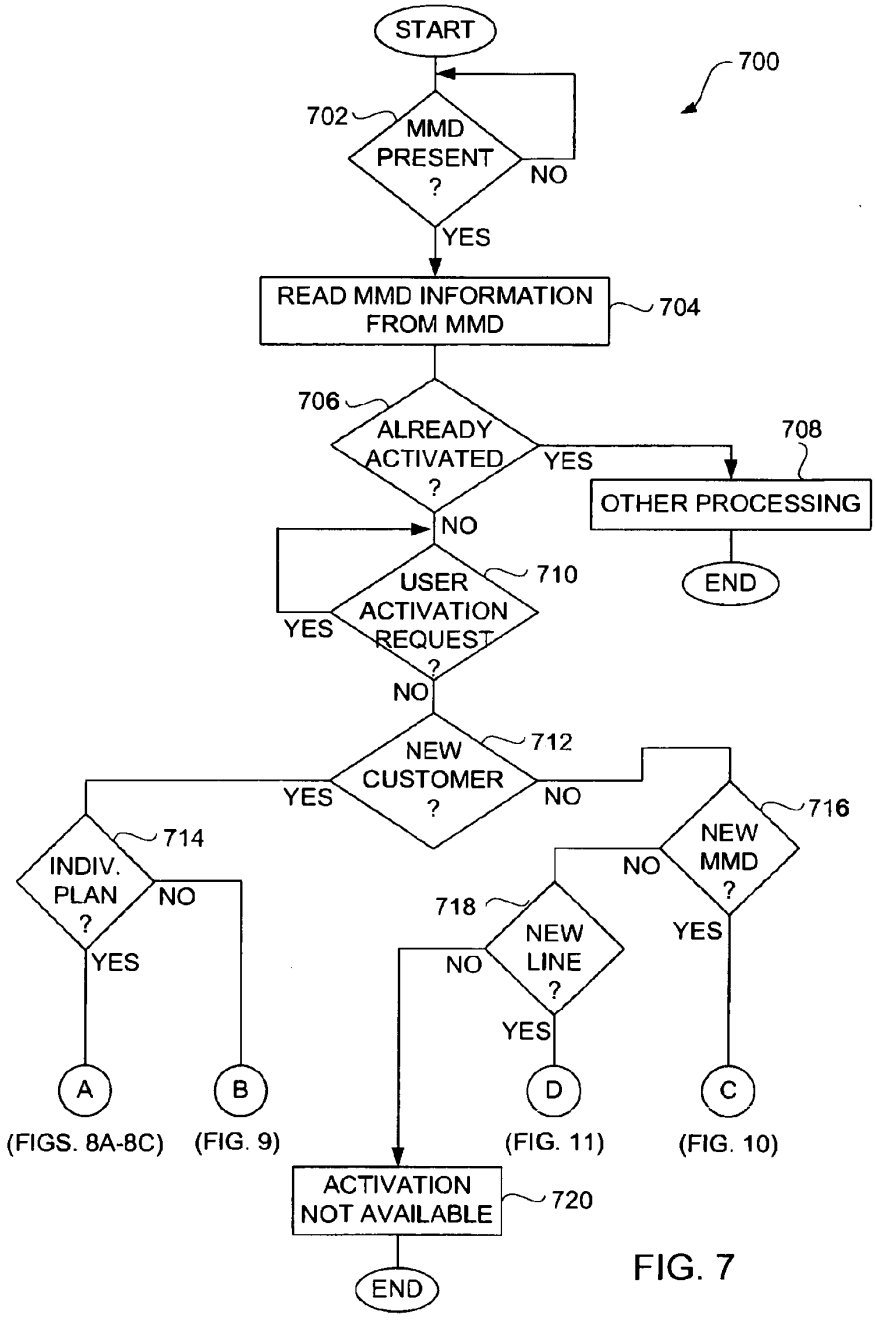

START
700
702
MMD PRESENT ?
NO
YES
READ MMD INFORMATION FROM MMD
704
706
ALREADY ACTIVATED ?
YES
708
OTHER PROCESSING
END
NO
USER ACTIVATION REQUEST ?
710
YES
NO
NEW CUSTOMER ?
712
YES
NO
INDIV. PLAN ?
714
NO
YES
NEW MMD ?
716
NO
YES
718
NEW LINE ?
NO
YES
A
B
D
C
(FIGS. 8A-8C)
(FIG. 9)
(FIG. 11)
(FIG. 10)
ACTIVATION NOT AVAILABLE
720
END

FIG. 7

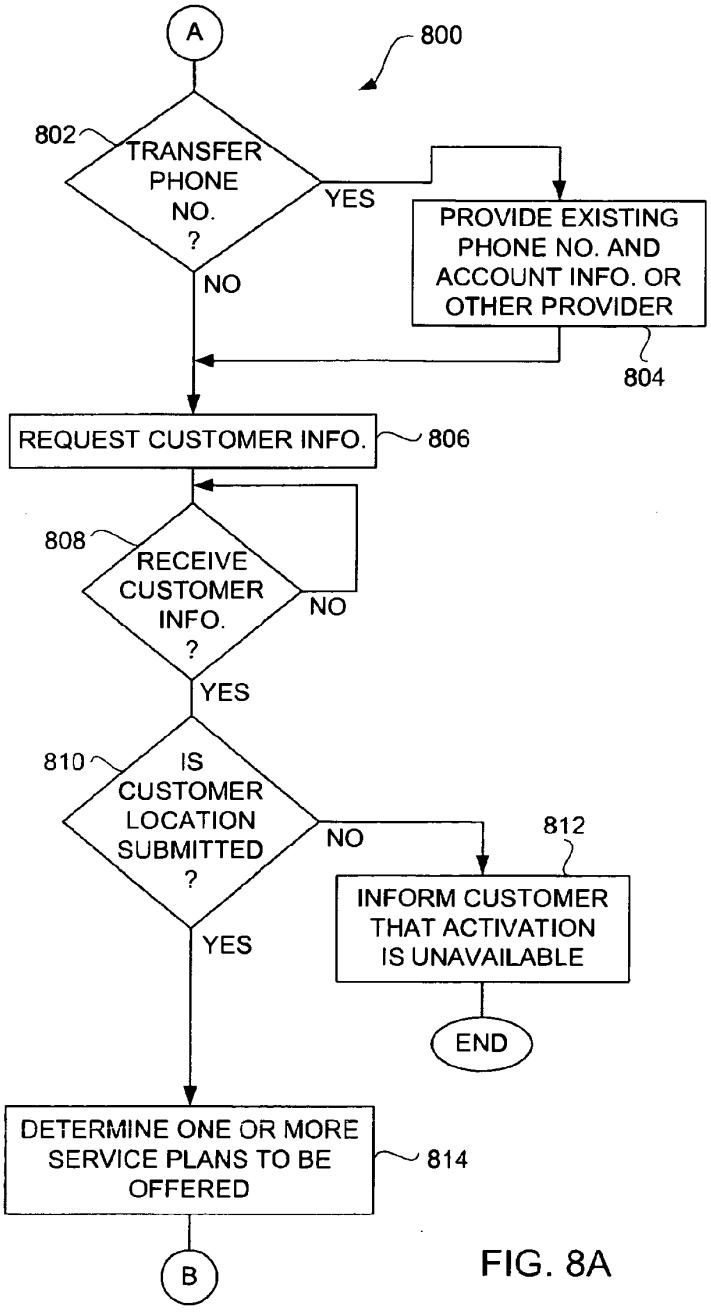


FIG. 8A

BNSDOCID: <EP_____1942698A1_I_>

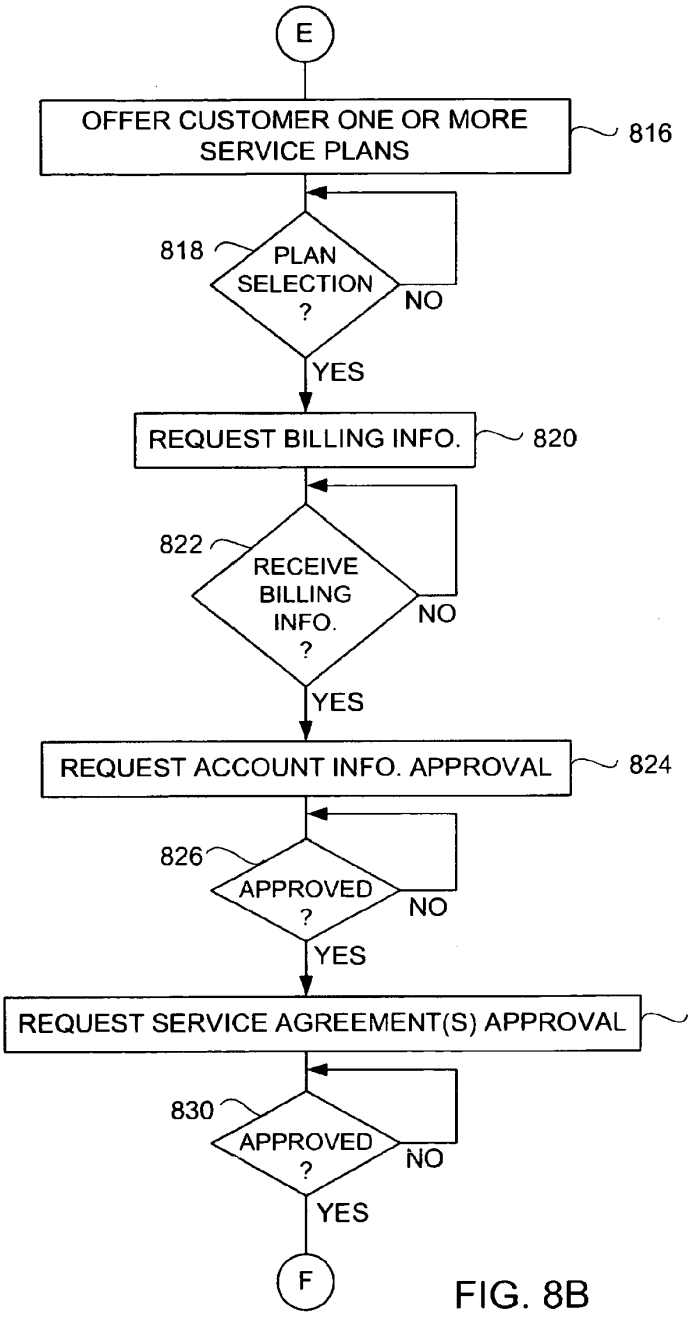


FIG. 8B

BNSDOCID: <EP 1942698A1 >

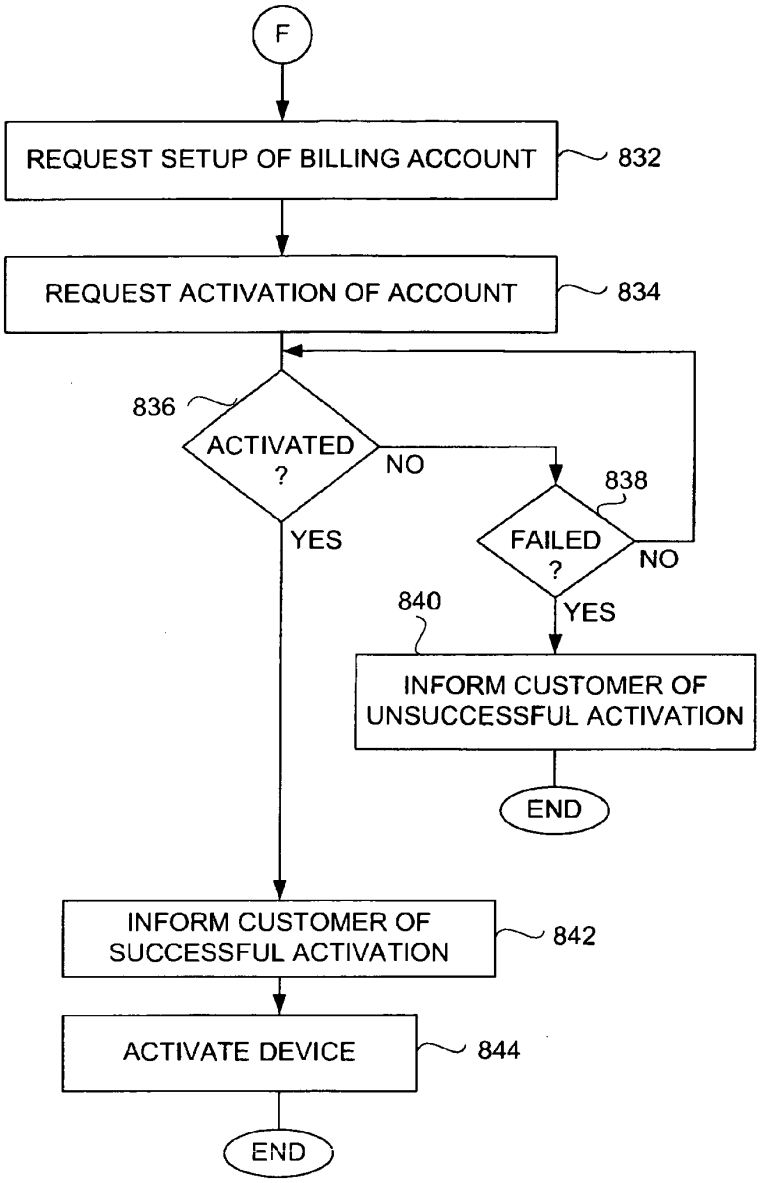


FIG. 8C

BNSDOCID: <EP_____1942698A1_I_>

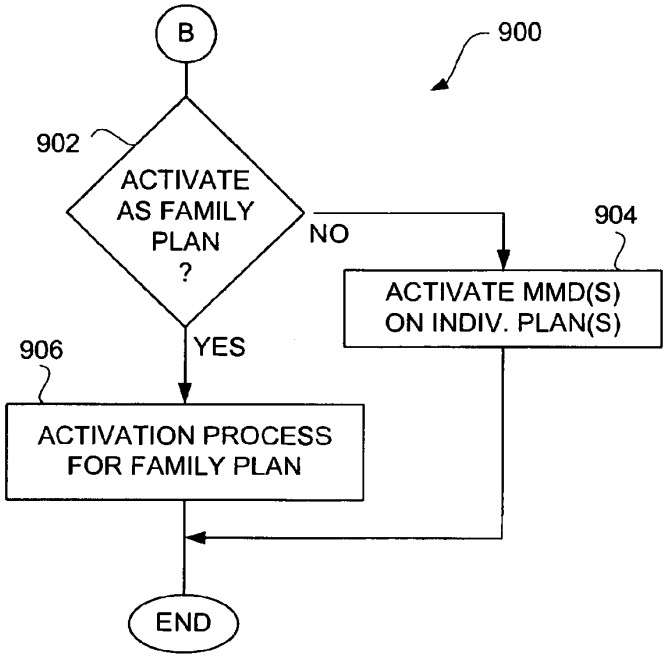


FIG. 9

EPNSDOCID: <EP 1942698A1 | >

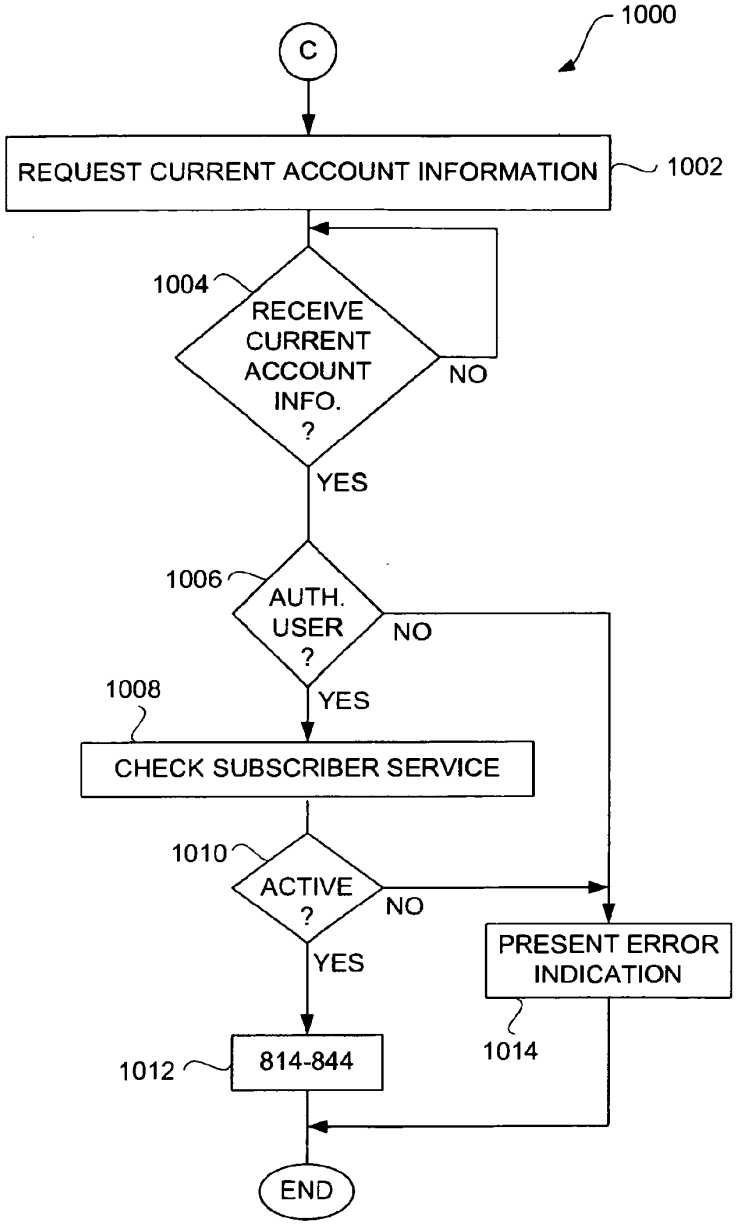


FIG. 10

BNSDOCID: <EP_____1942698A1_I_>

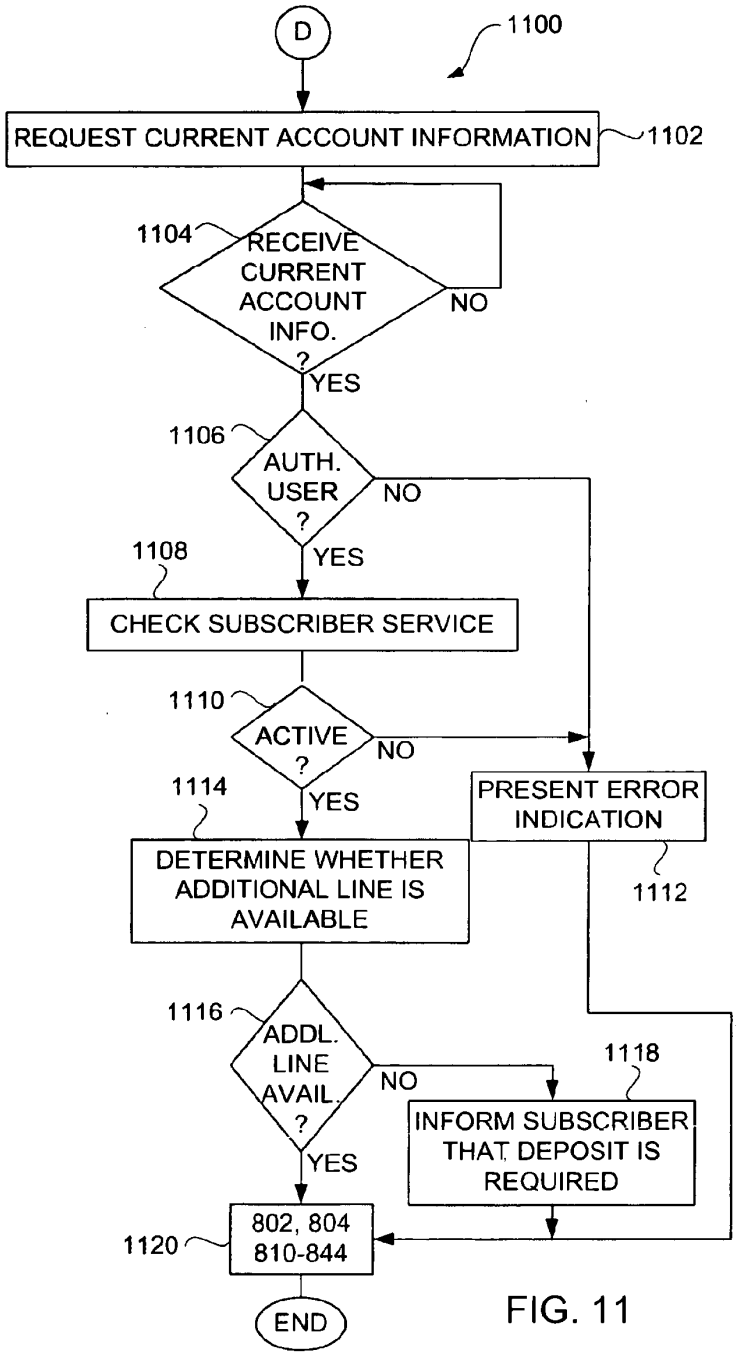

D
1100
REQUEST CURRENT ACCOUNT INFORMATION
1102
1104
RECEIVE CURRENT ACCOUNT INFO. ?
NO
YES
1106
AUTH. USER ?
NO
YES
1108
CHECK SUBSCRIBER SERVICE
1110
ACTIVE ?
NO
YES
1114
PRESENT ERROR INDICATION
1112
DETERMINE WHETHER ADDITIONAL LINE IS AVAILABLE
1116
ADDL. LINE AVAIL. ?
NO
YES
1118
INFORM SUBSCRIBER THAT DEPOSIT IS REQUIRED
1120
802, 804 810-844
END

FIG. 11

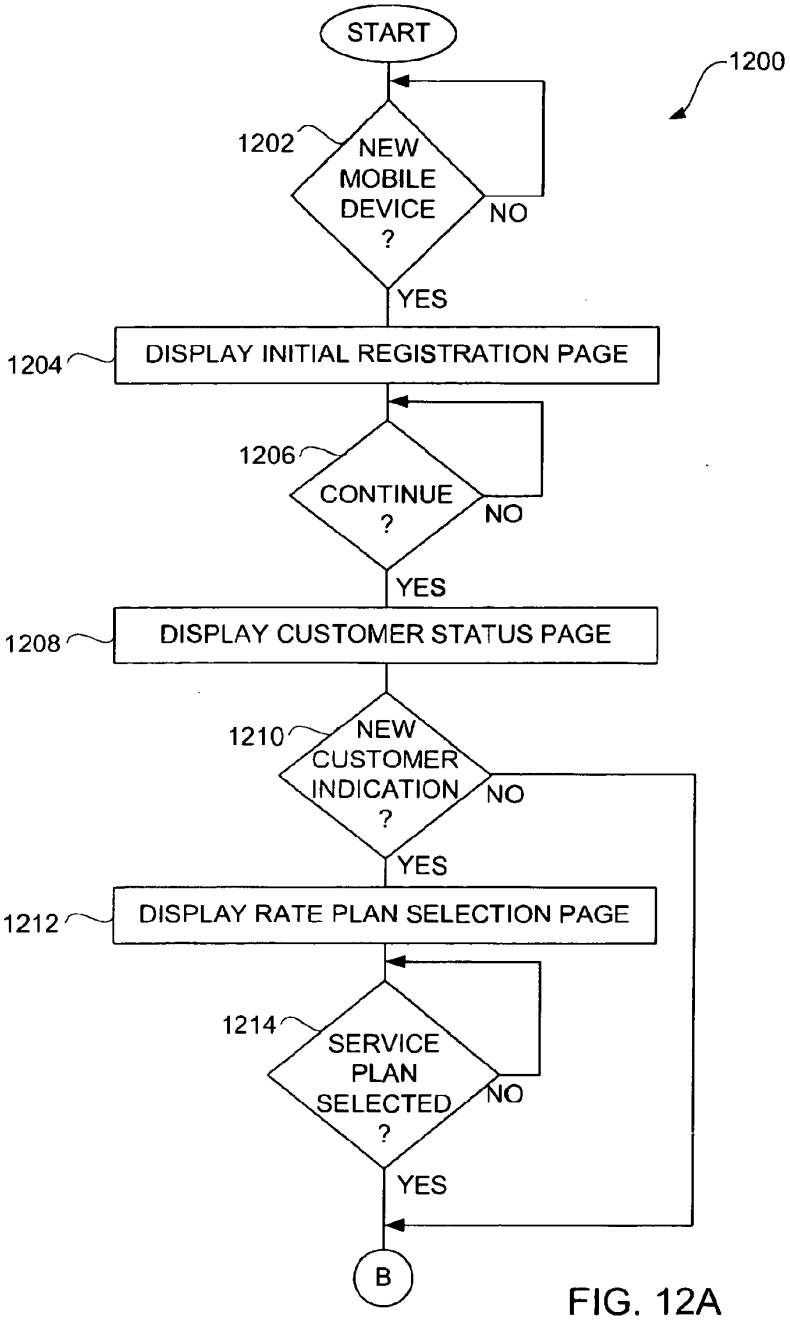


FIG. 12A

BNSDOCID: <EP_____194269BA1_I_>

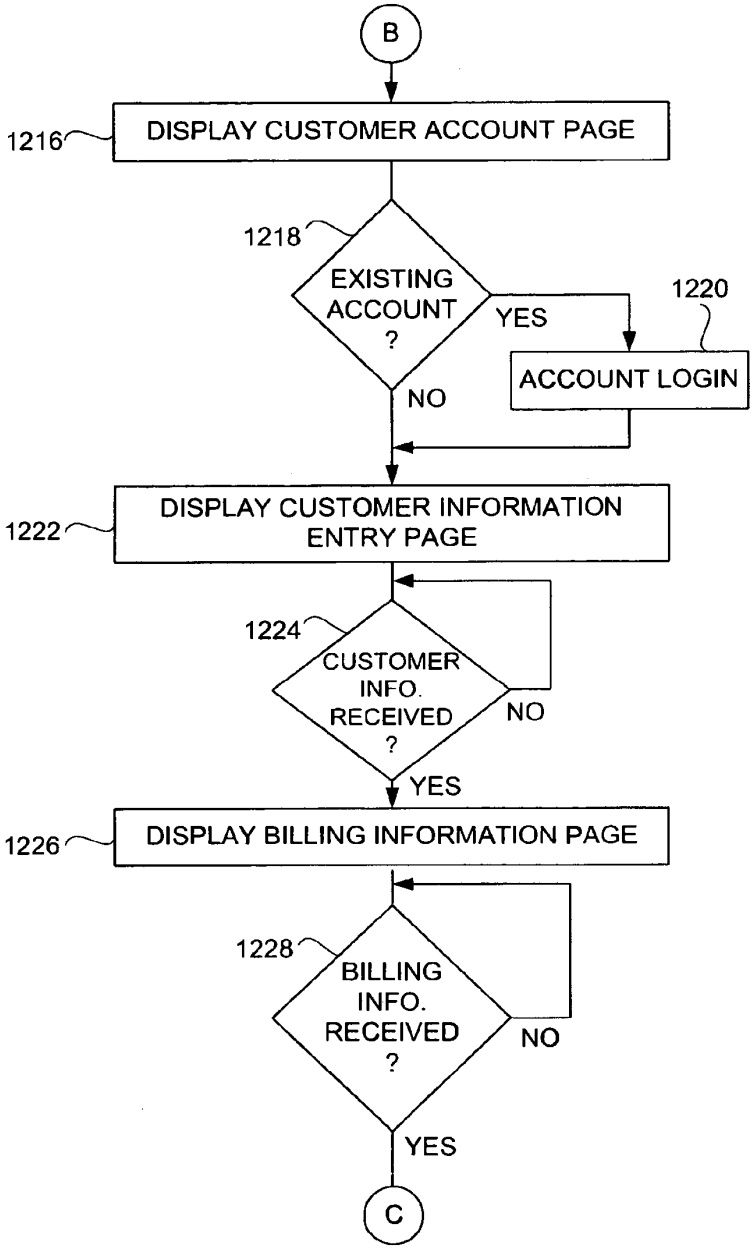

B
1216
DISPLAY CUSTOMER ACCOUNT PAGE
1218
EXISTING ACCOUNT ?
YES
1220
ACCOUNT LOGIN
NO
1222
DISPLAY CUSTOMER INFORMATION ENTRY PAGE
1224
CUSTOMER INFO. RECEIVED ?
NO
YES
1226
DISPLAY BILLING INFORMATION PAGE
1228
BILLING INFO. RECEIVED ?
NO
YES
C

FIG. 12B

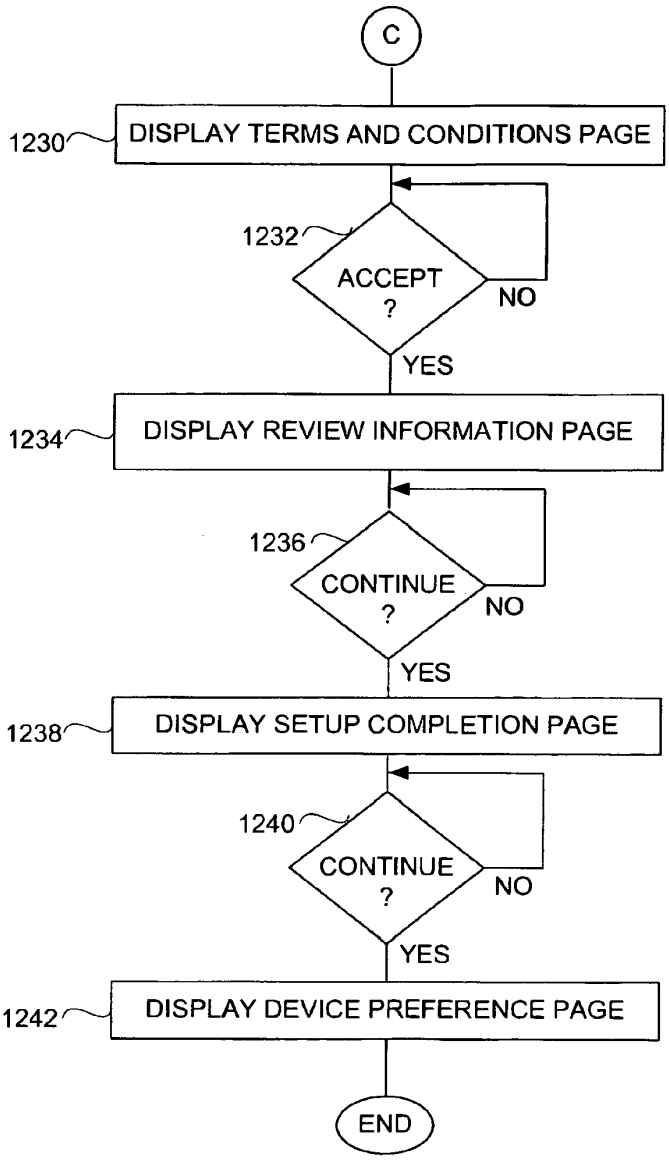


FIG. 12C

BNSDOCID: <EP_____1942698A1_I_>

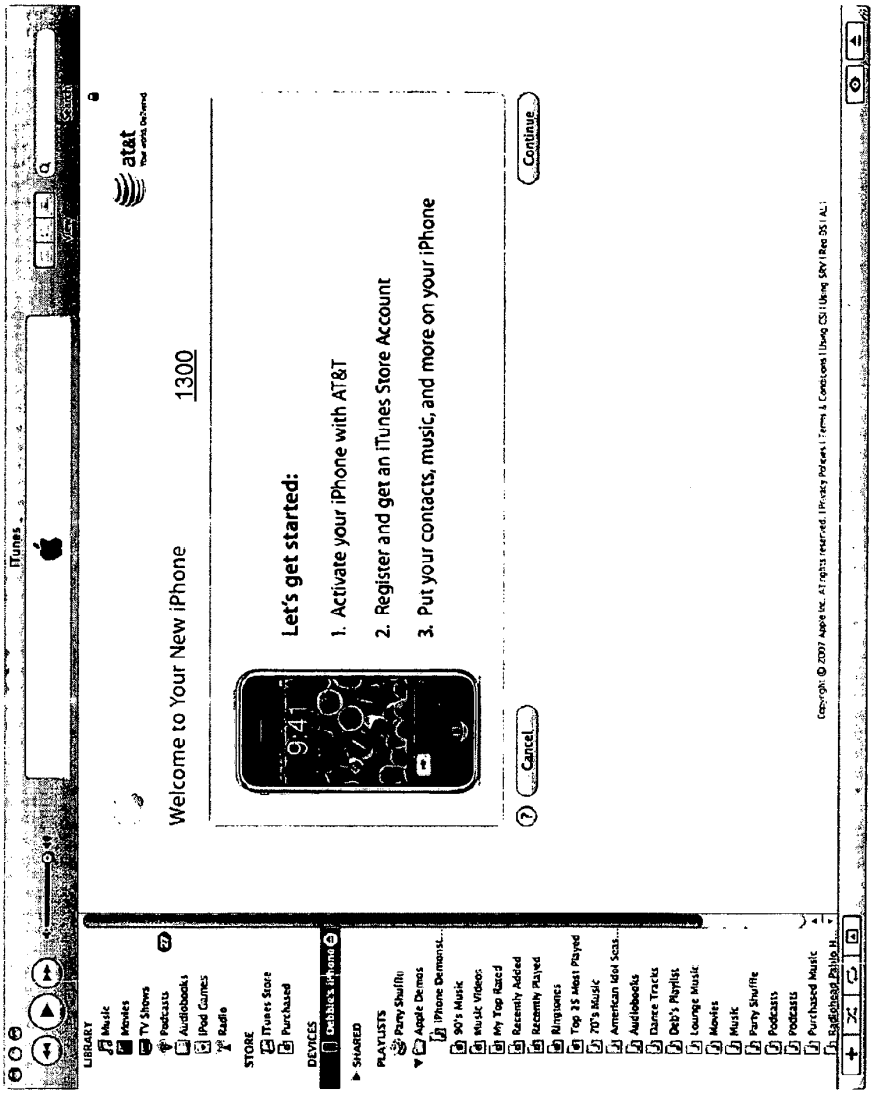


FIG. 13

BNSDOCID: <EP 1942698A1 | >

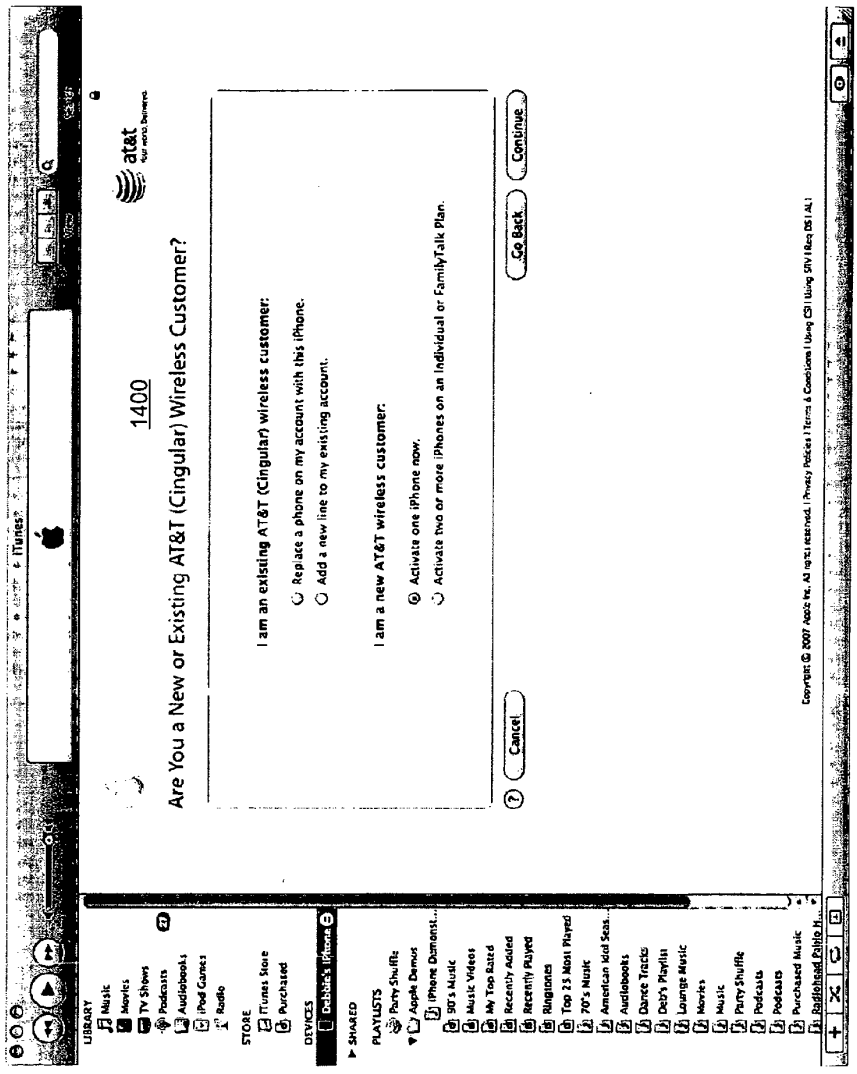


FIG. 14

BNSDOCID: <EP_____1942698A1_I_>

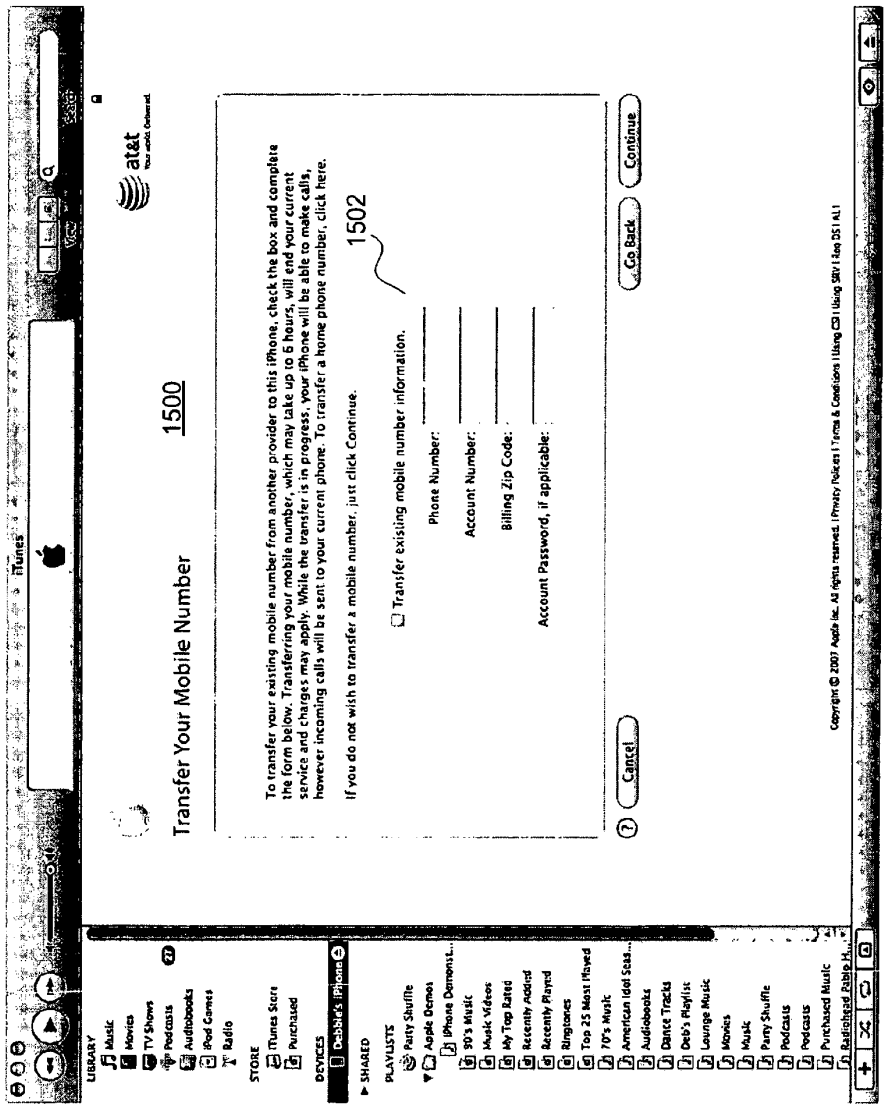

iTunes
LIBRARY
Music
Movies
TV Shows
Podcasts
Audiobooks
iPod Games
Radio
STORE
iTunes Store
Purchased
DEVICES
Debbie's iPhone
SHARED
PLAYLISTS
Party Shuffle
Apple Demos
iPhone Demonst...
90's Music
Music Videos
My Top Rated
Recently Added
Recently Played
Ringtones
Top 25 Most Played
70's Music
American Idol Seas...
Audiobooks
Dance Tracks
Deb's Playlist
Lounge Music
Movies
Music
Party Shuffle
Podcasts
Podcasts
Purchased Music
Radiohead Table M...
at&t
Transfer Your Mobile Number
1500
To transfer your existing mobile number from another provider to this iPhone, check the box and complete the form below. Transferring your mobile number, which may take up to 6 hours, will end your current service and charges may apply. While the transfer is in progress, your iPhone will be able to make calls, however incoming calls will be sent to your current phone. To transfer a home phone number, click here.
If you do not wish to transfer a mobile number, just click Continue.
1502
Transfer existing mobile number information.
Phone Number:
Account Number:
Billing Zip Code:
Account Password, if applicable:
Cancel
Go Back
Continue
Copyright © 2007 Apple Inc. All rights reserved. | Privacy Policy | Terms & Conditions | Using GSM | Using CDMA | Using EDGE | AU

FIG. 15

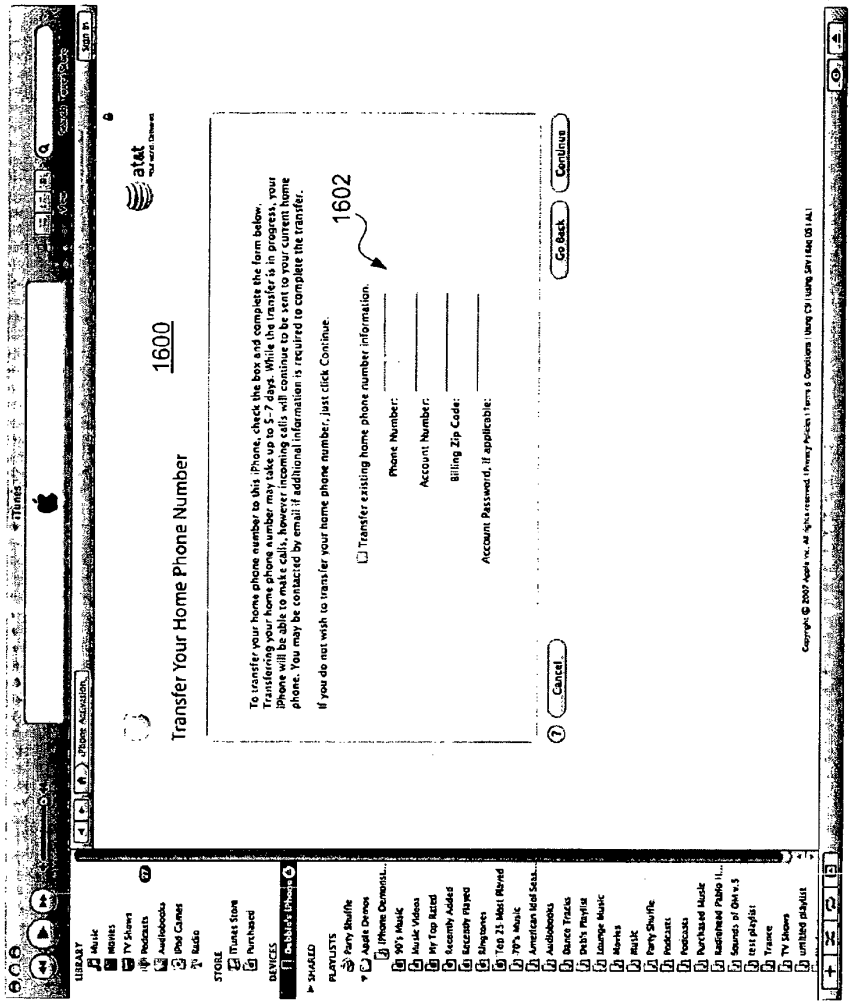


FIG. 16

BNSDOCID: <EP_____1942698A1_I_>

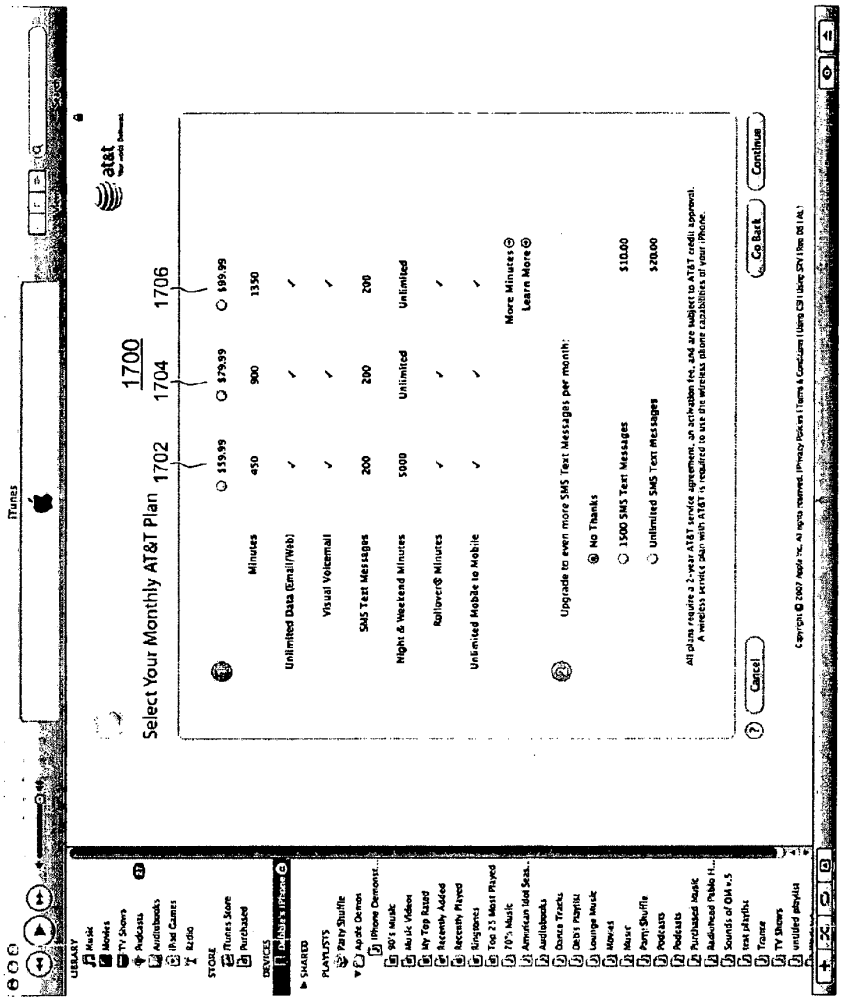


FIG. 17A

BNSDOCID: <EP_____1942698A1_I_>

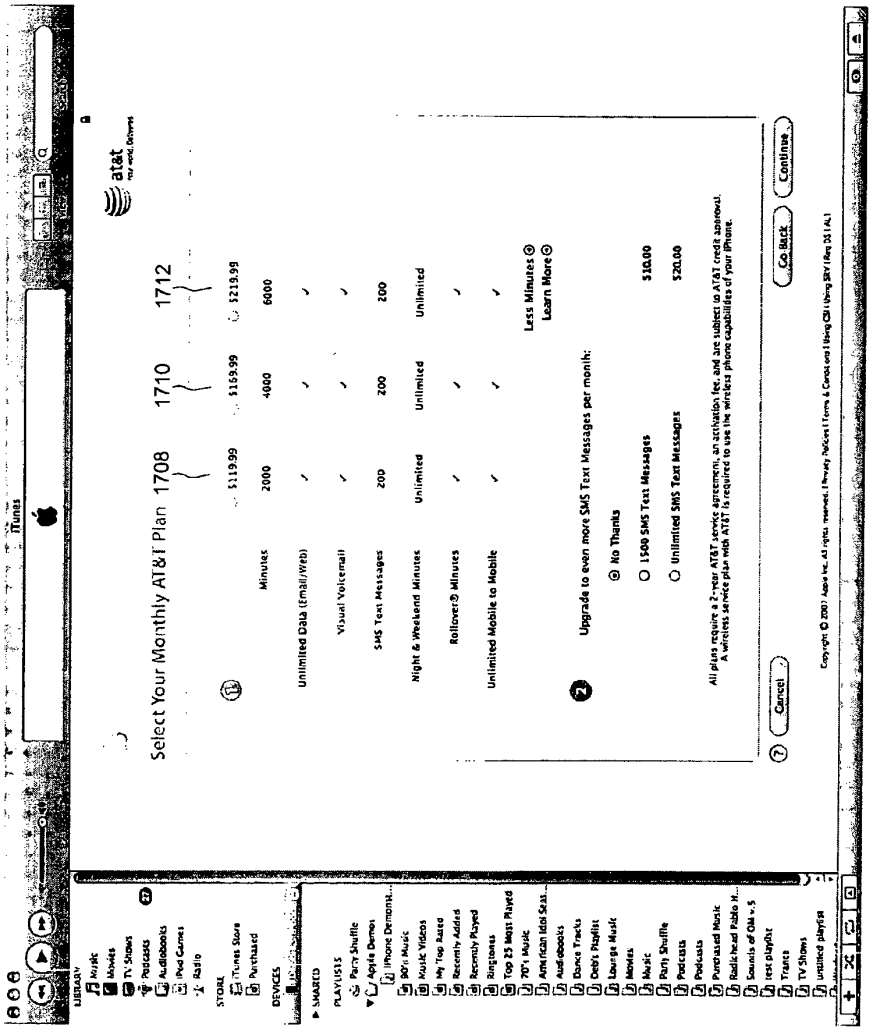


FIG. 17B

BNSDOCID: <EP_____1942698A1_I_>

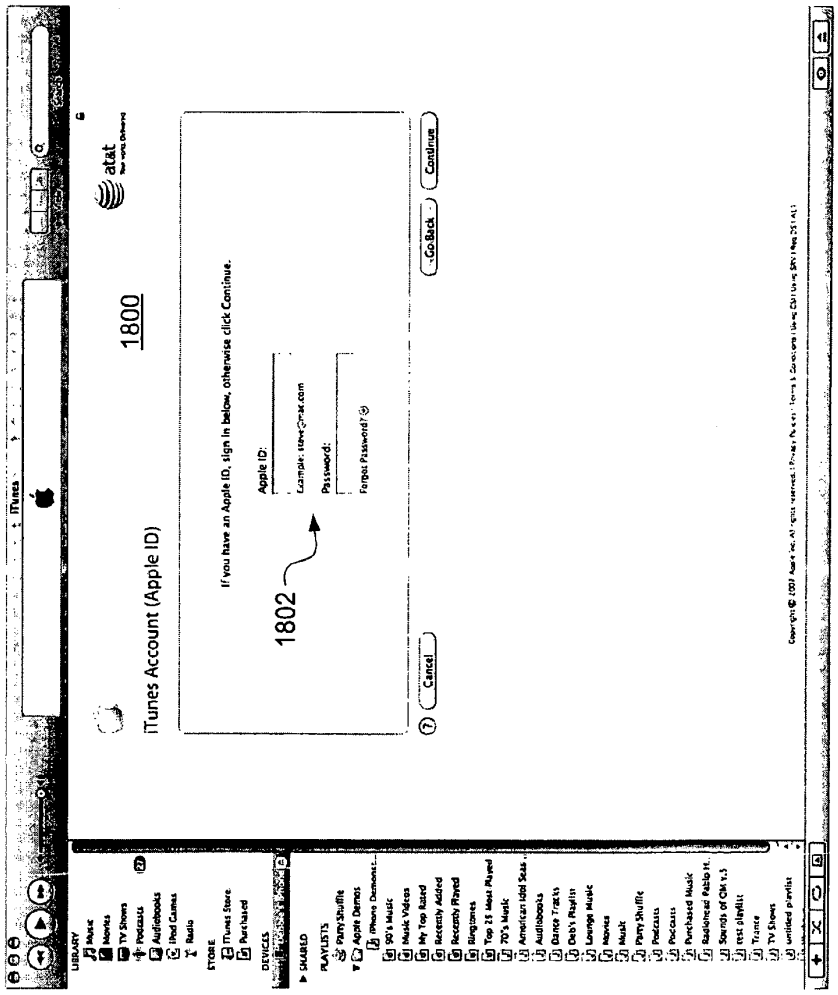


FIG. 18

BNSDOCID: <EP 1942698A1 >

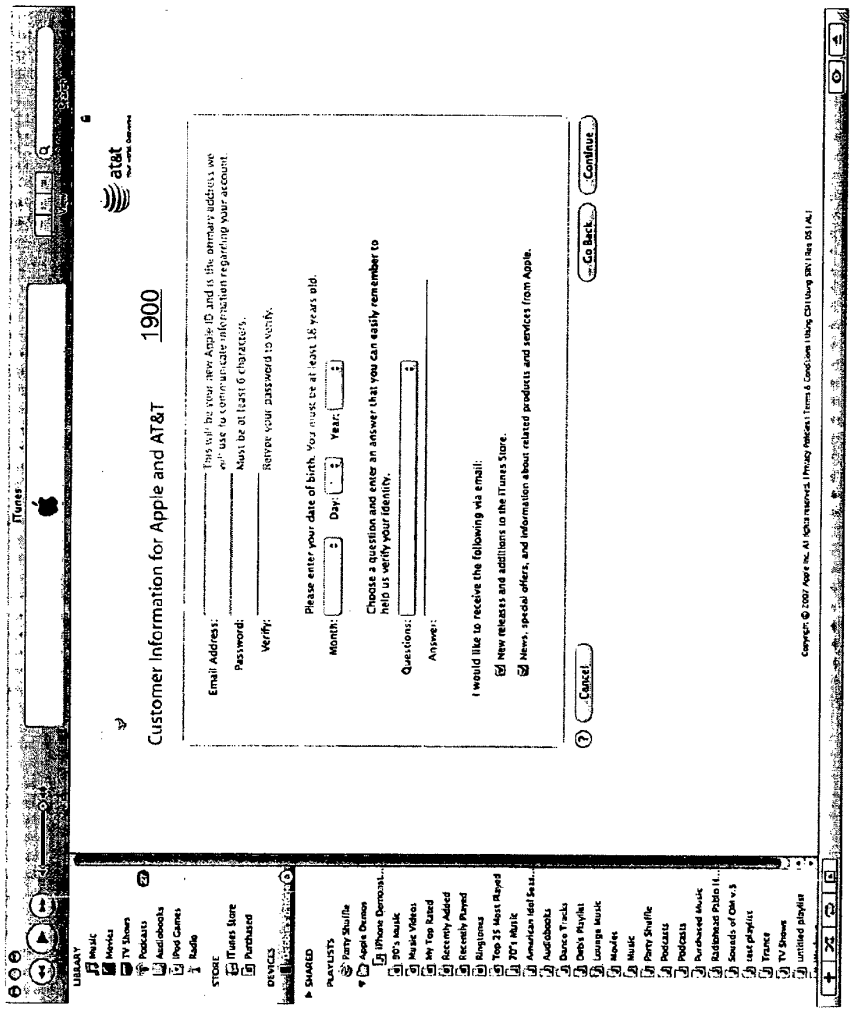


FIG. 19

BNSDOCID: <EP_____1942698A1_I_>

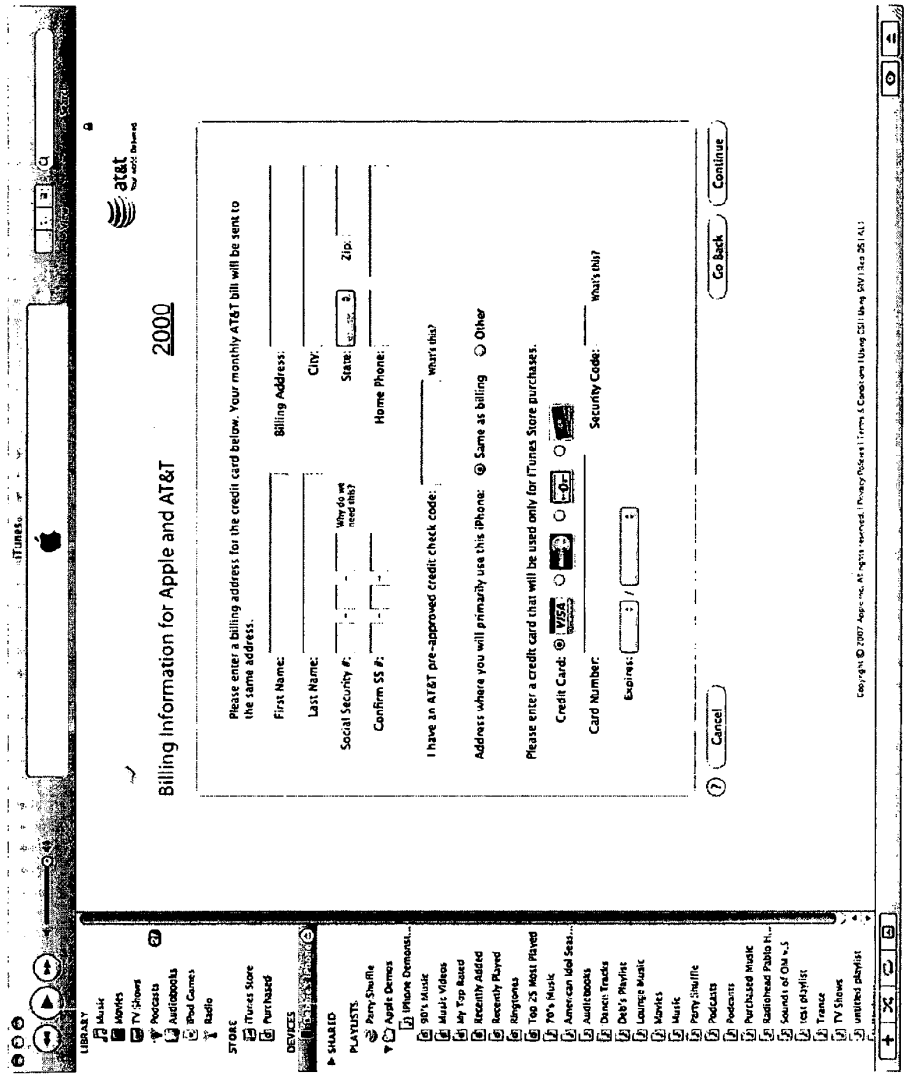

Billing Information for Apple and AT&T
2000
Please enter a billing address for the credit card below. Your monthly AT&T bill will be sent to the same address.
First Name:
Billing Address:
Last Name:
City:
Social Security #:
Why do we need this?
State:
Zip:
Confirm SS #:
Home Phone:
I have an AT&T pre-approved credit check code:
What's this?
Address where you will primarily use this iPhone: Same as billing Other
Please enter a credit card that will be used only for iTunes Store purchases.
Credit Card:
Card Number:
Security Code:
What's this?
Expires:
Cancel
Go Back
Continue

FIG. 20

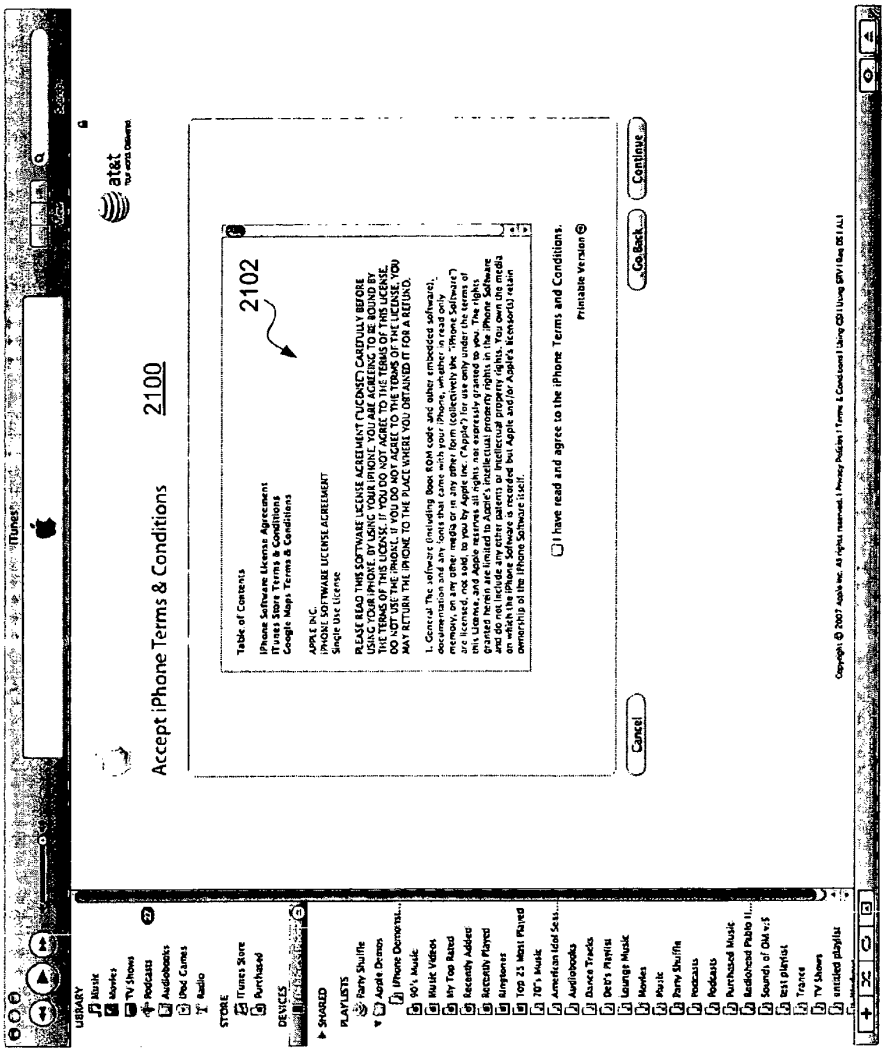


FIG. 21A

BNSDOCID: <EP_____1942698A1_I_>

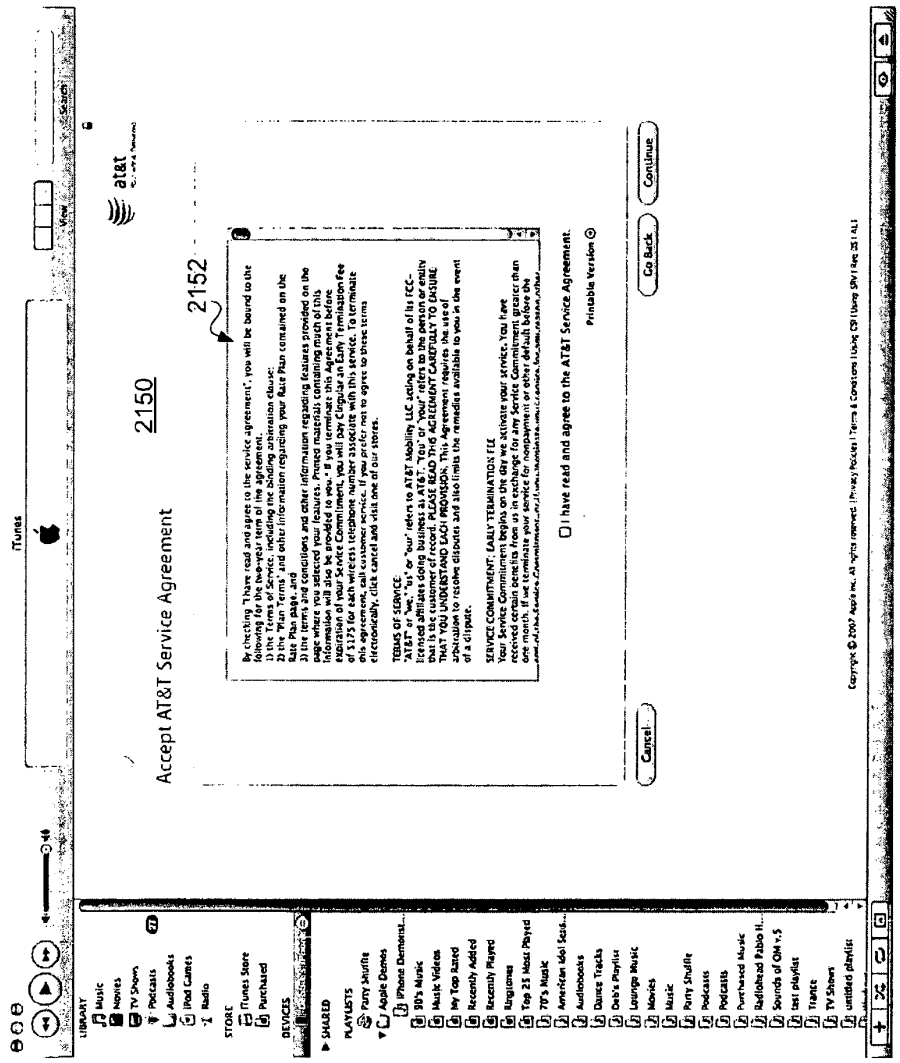


FIG. 21B

BNSDOCID: <EP_____1942698A1_I_>

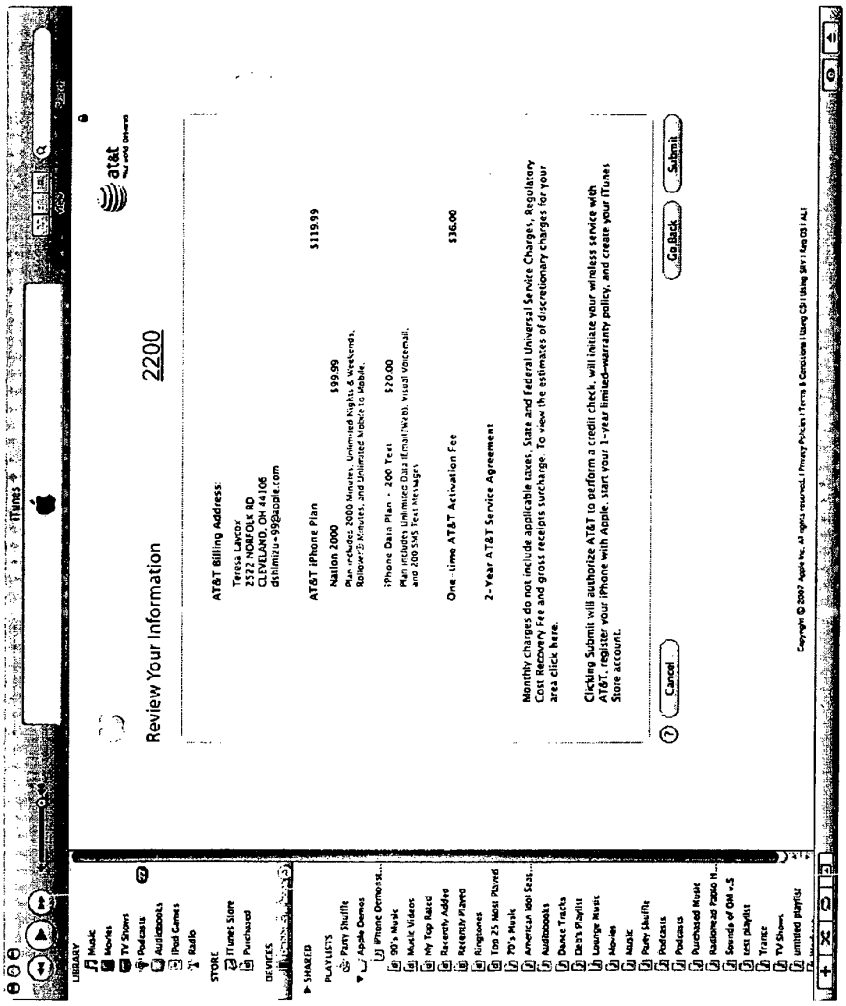


FIG. 22

BNSDOCID: <EP_____1942698A1_I_>

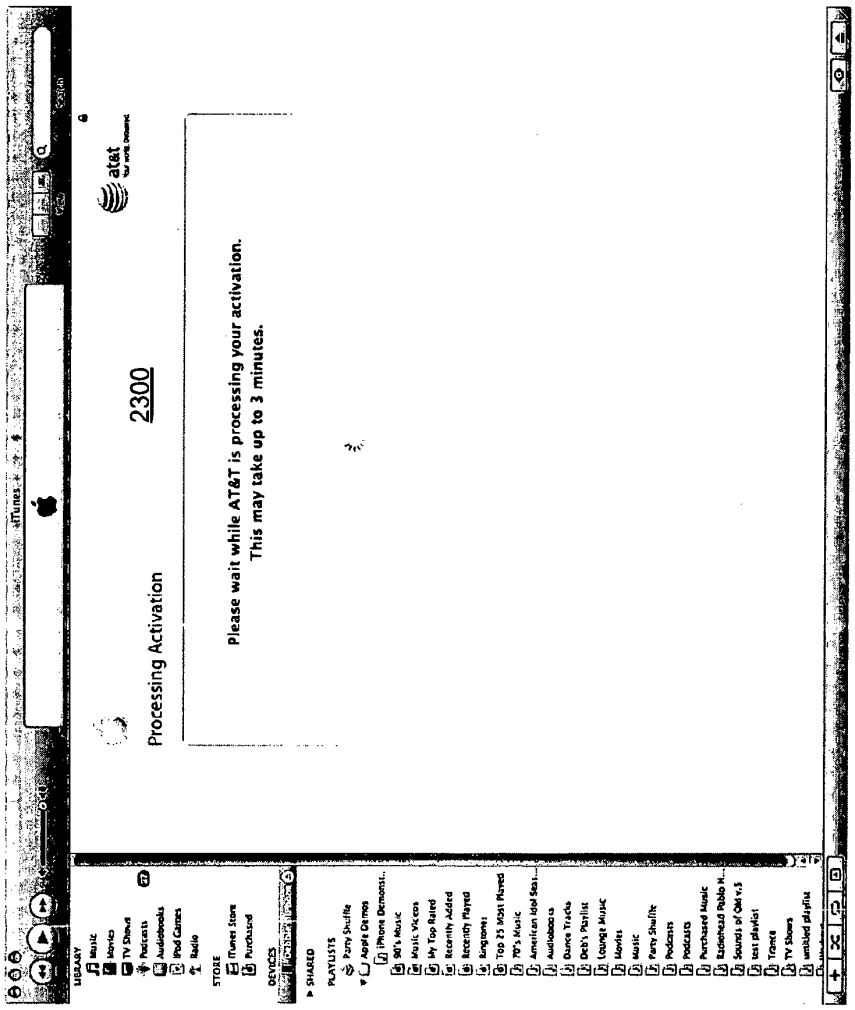


FIG. 23

BNSDOCID: <EP_____1942698A1_I_>

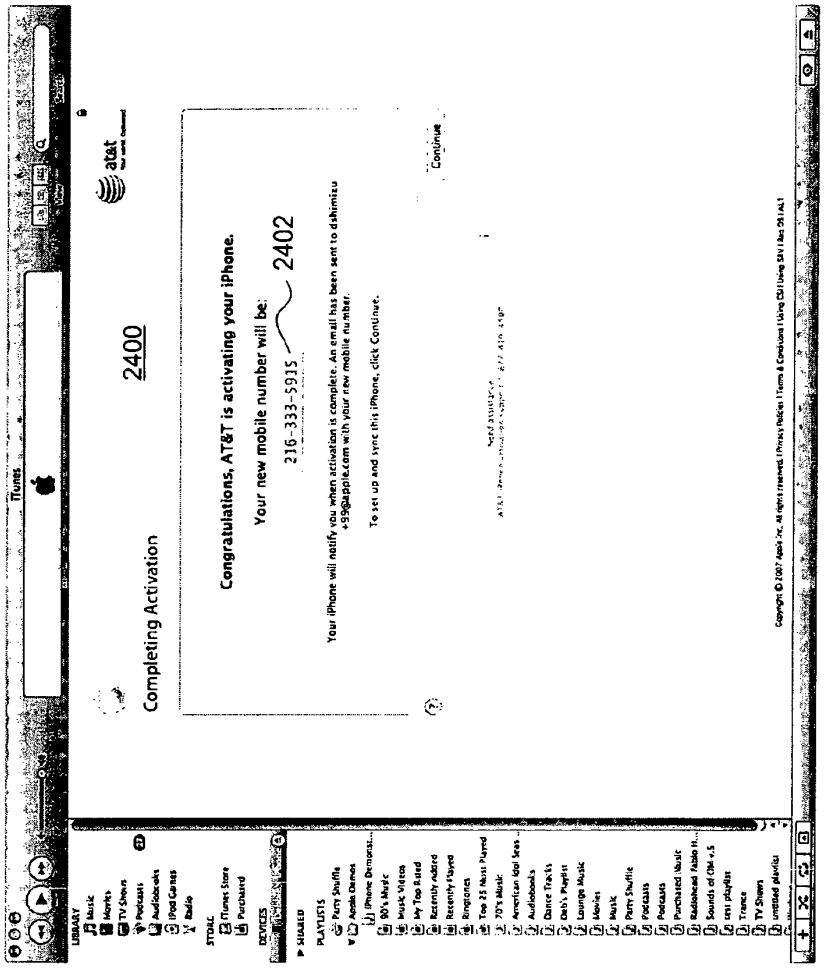


FIG. 24A

BNSDOCID: <EP_____1942698A1_I_>

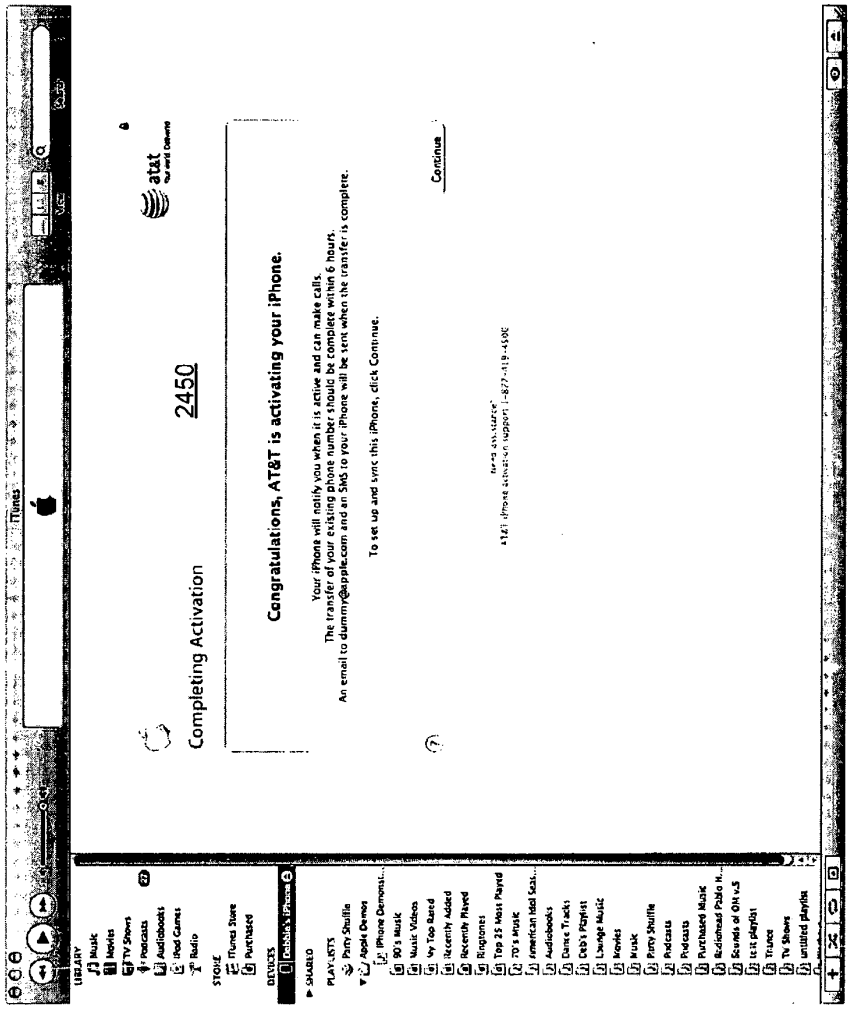

iTunes
LIBRARY
Music
Movies
TV Shows
Podcasts
Audiobooks
iPod Games
Radio
STORE
iTunes Store
Purchased
DEVICES
Debbie's iPhone
SHARED
PLAYLISTS
Party Shuffle
Apple Demos
iPhone Demonst...
90's Music
Music Videos
My Top Rated
Recently Added
Recently Played
Ringtones
Top 25 Most Played
70's Music
American Idol Seas...
Audiobooks
Dance Tracks
Deb's Playlist
Lounge Music
Movies
Music
Party Shuffle
Podcasts
Podcasts
Purchased Music
Radiohead Pablo H...
Sounds of Old v.5
test playlist
Trance
TV Shows
untitled playlist
Completing Activation
2450
Congratulations, AT&T is activating your iPhone.
Your iPhone will notify you when it is active and can make calls.
The transfer of your existing phone number should be complete within 6 hours.
An email to dummy@apple.com and an SMS to your iPhone will be sent when the transfer is complete.
To set up and sync this iPhone, click Continue.
Continue

FIG. 24B

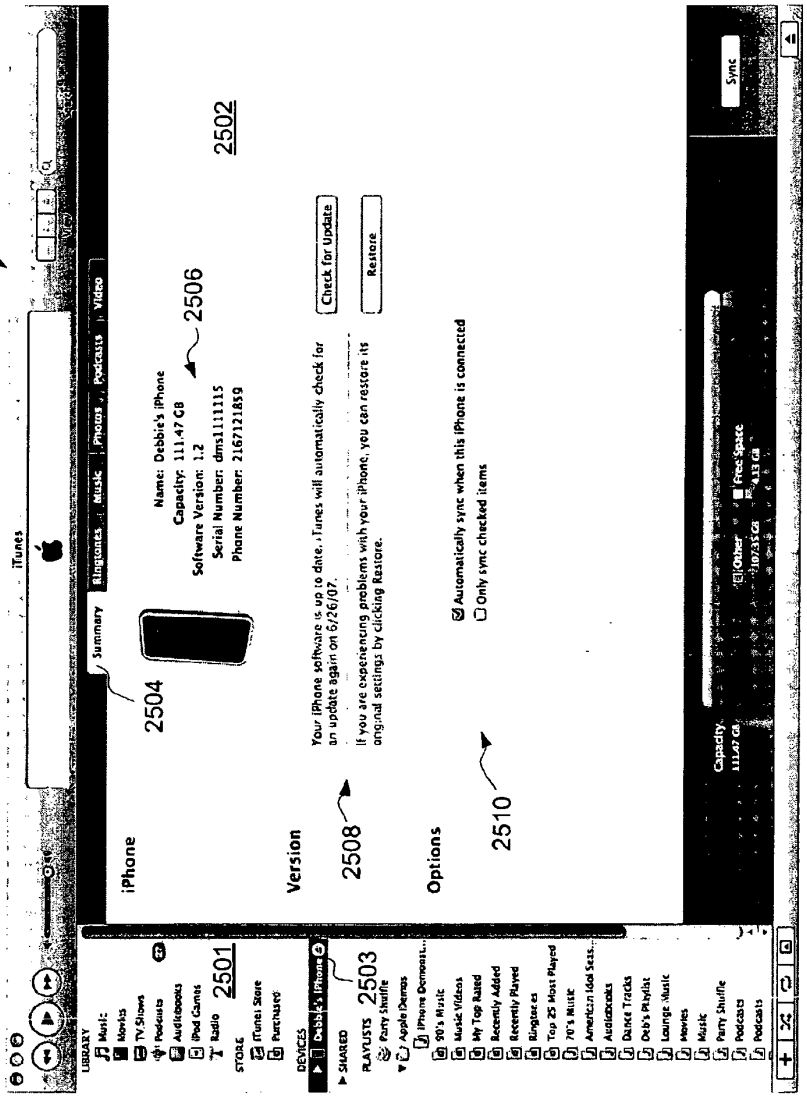


FIG. 25

BNSDOCID: <EP_____1942698A1_I_>

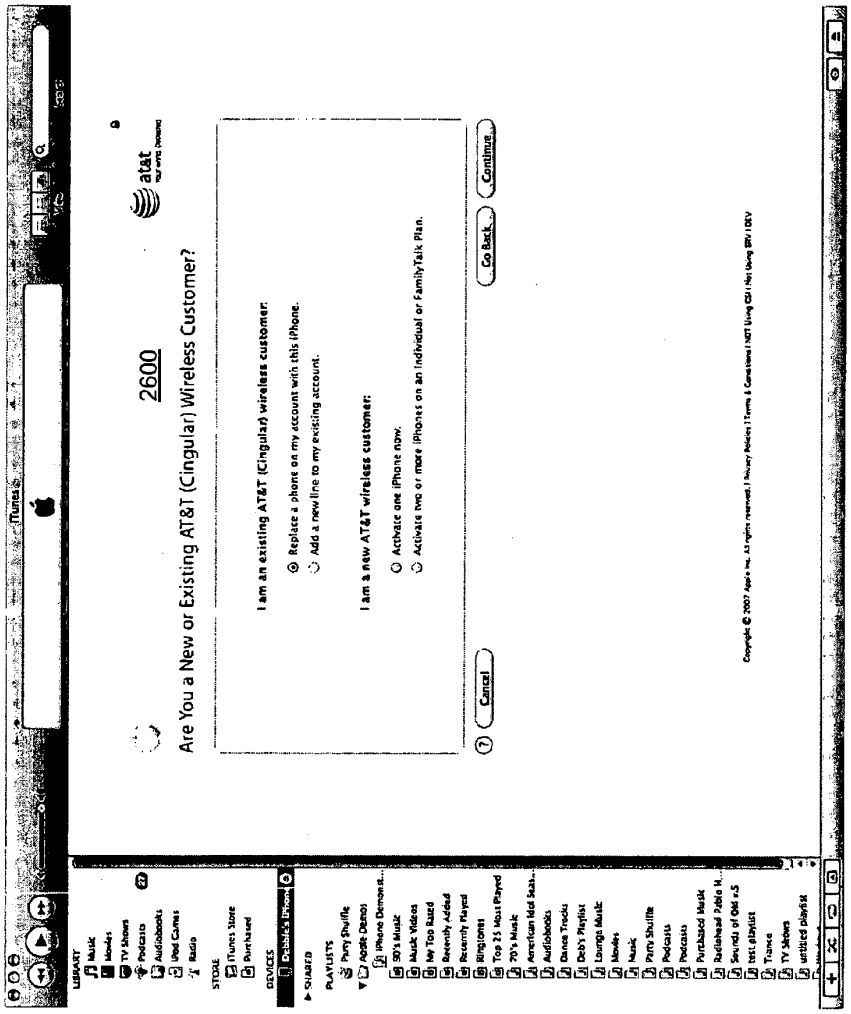

iTunes
LIBRARY
Music
Movies
TV Shows
Podcasts
Audiobooks
iPod Games
Radio
STORE
iTunes Store
Purchased
DEVICES
SHARED
PLAYLISTS
Party Shuffle
Apple Demos
90's Music
Music Videos
My Top Rated
Recently Added
Recently Played
Ringtones
Top 25 Most Played
70's Music
Audiobooks
Dance Tracks
Deb's Playlist
Lounge Music
Movies
Music
Party Shuffle
Podcasts
Purchased Music
Sounds of 60s v.5
test playlist
Trance
TV Shows
2600
at&t
Are You a New or Existing AT&T (Cingular) Wireless Customer?
I am an existing AT&T (Cingular) wireless customer:
Replace a phone on my account with this iPhone.
Add a new line to my existing account.
I am a new AT&T wireless customer:
Activate one iPhone now.
Activate two or more iPhones on an individual or FamilyTalk Plan.
Cancel
Go Back
Continue

FIG. 26

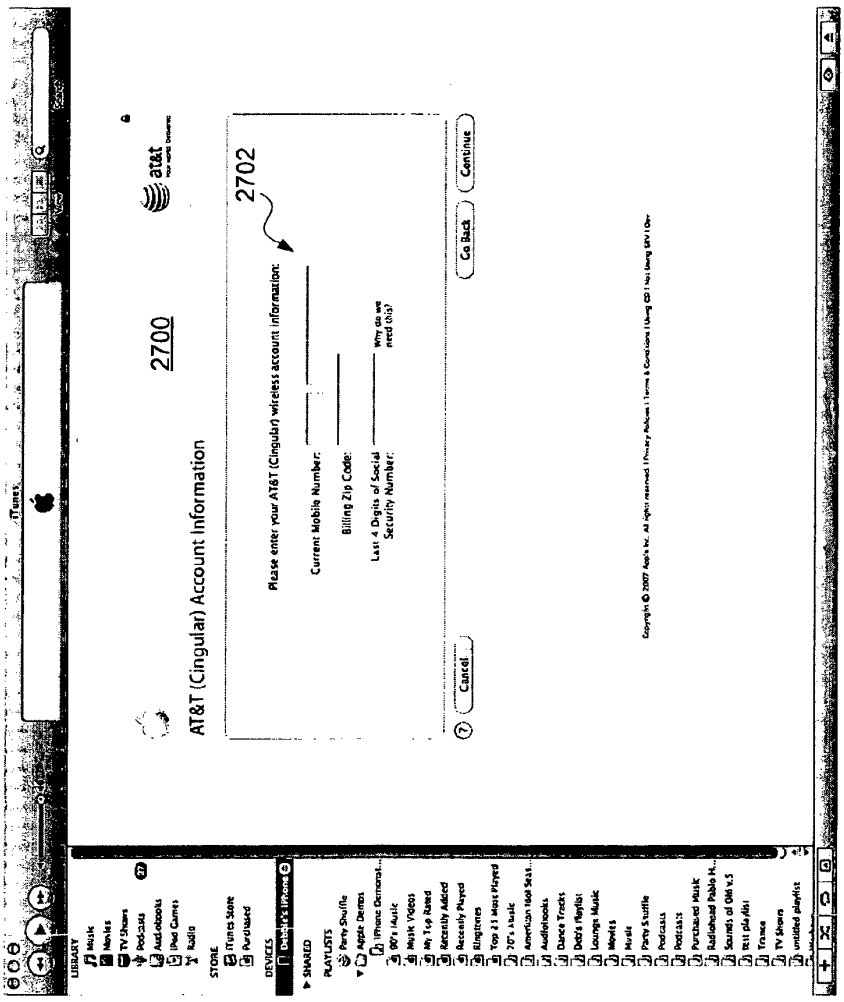


FIG. 27

BNSDOCID: <EP_____1942698A1_I_>

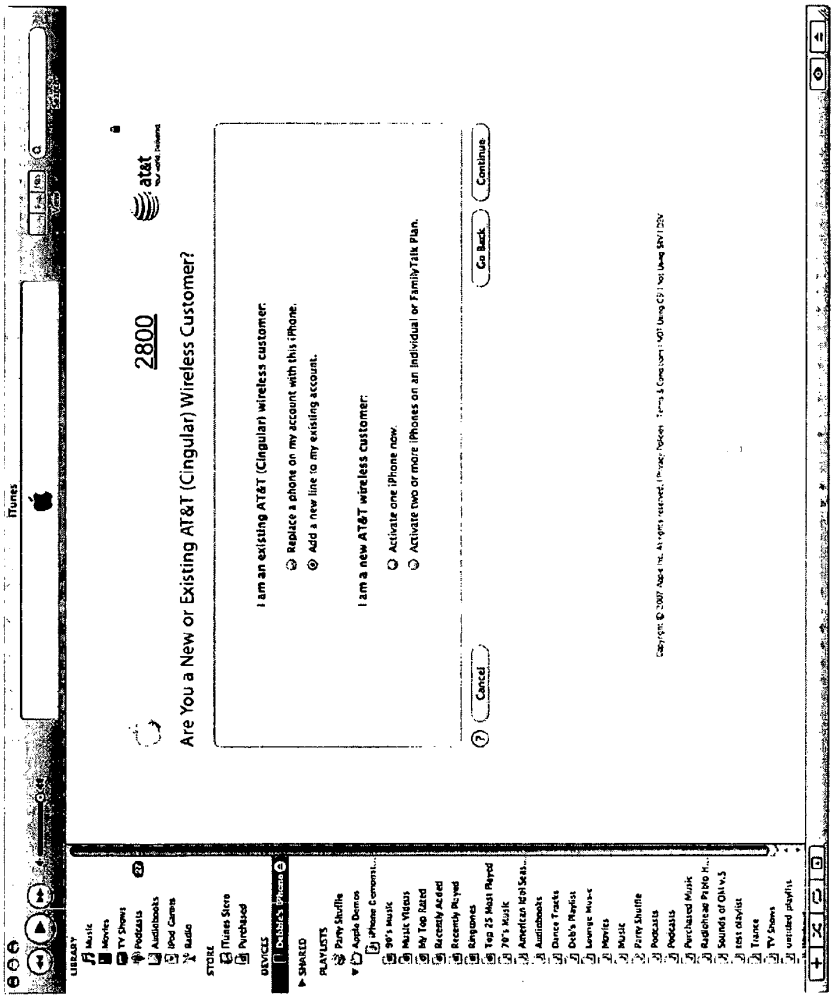

iTunes
2800
Are You a New or Existing AT&T (Cingular) Wireless Customer?
I am an existing AT&T (Cingular) wireless customer:
Replace a phone on my account with this iPhone.
Add a new line to my existing account.
I am a new AT&T wireless customer:
Activate one iPhone now.
Activate two or more iPhones on an individual or FamilyTalk Plan.
Cancel
Go Back
Continue

FIG. 28

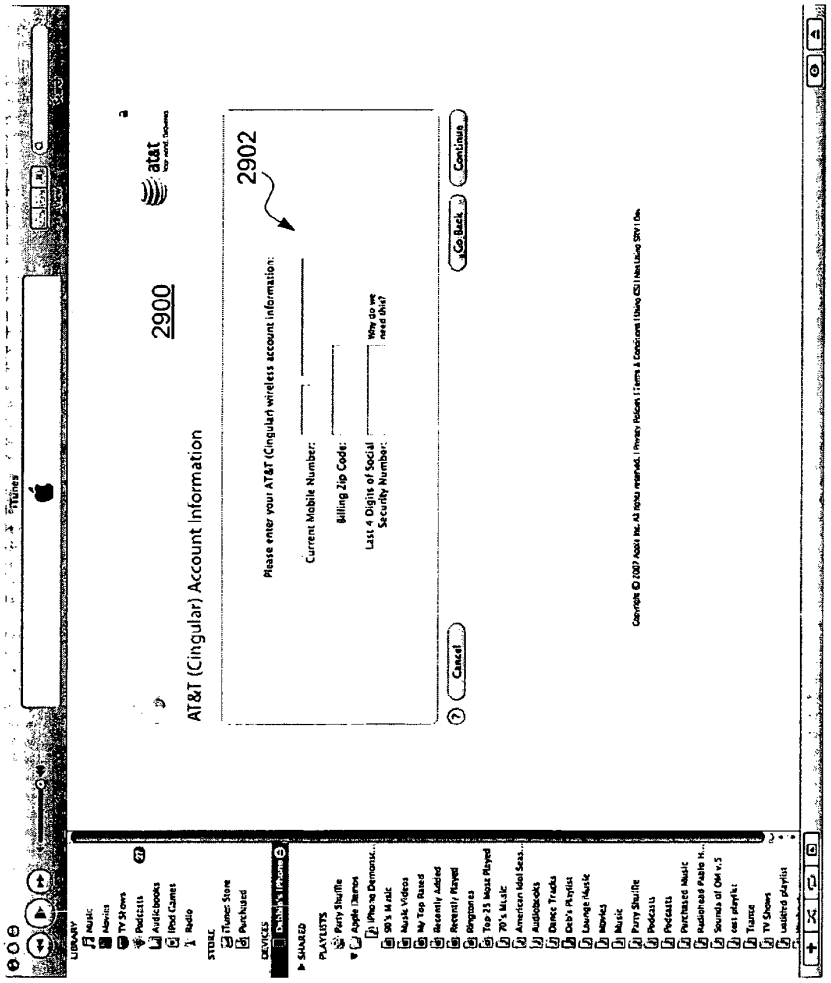


FIG. 29

BNSDOCID: <EP_____1942698A1_I_>

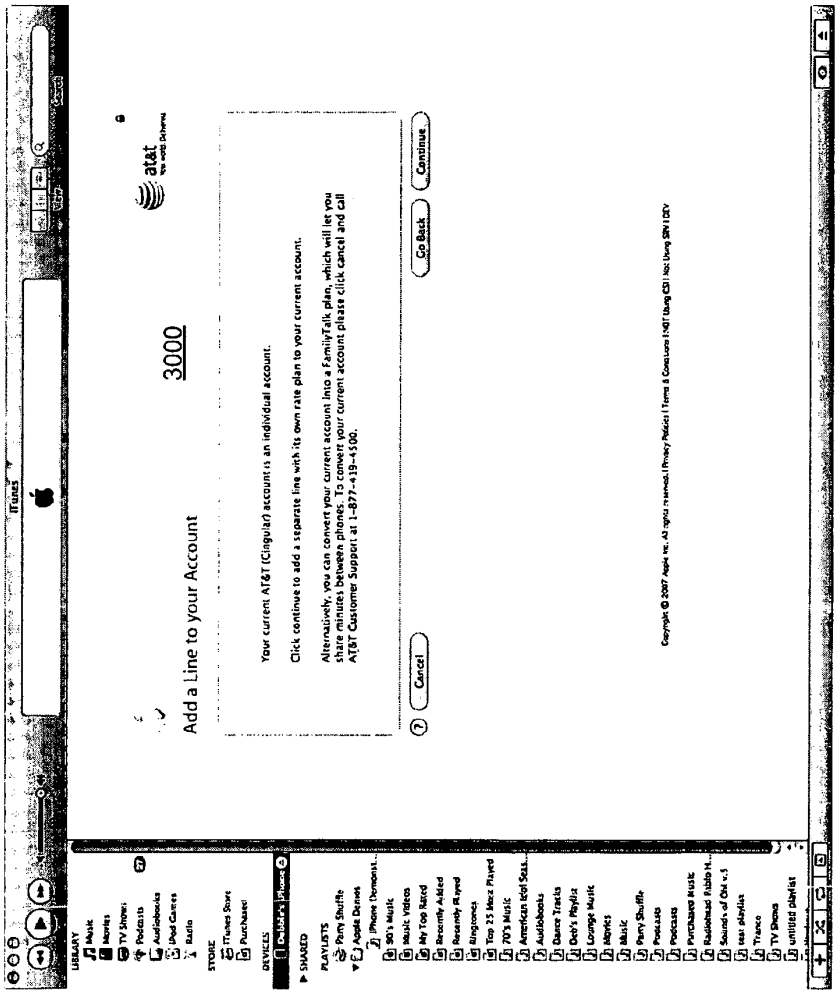

iTunes
LIBRARY
Music
Movies
TV Shows
Podcasts
Audiobooks
iPod Games
Radio
STORE
iTunes Store
Purchased
DEVICES
SHARED
PLAYLISTS
Party Shuffle
Apple Demos
Add a Line to your Account
3000
Your current AT&T (Cingular) account is an individual account.
Click continue to add a separate line with its own rate plan to your current account.
Alternatively, you can convert your current account into a FamilyTalk plan, which will let you share minutes between phones. To convert your current account please click cancel and call AT&T Customer Support at 1-877-419-4500.
Cancel
Go Back
Continue

FIG. 30

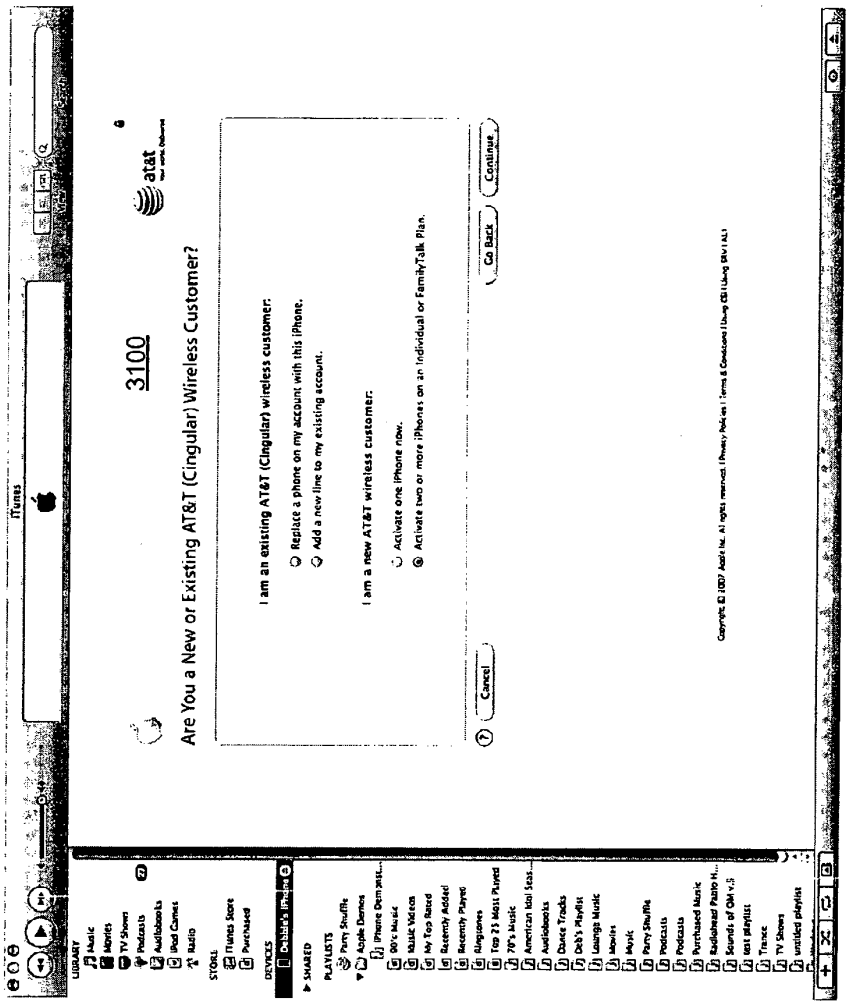


FIG. 31

BNSDOCID: <EP_____1942698A1_I_>

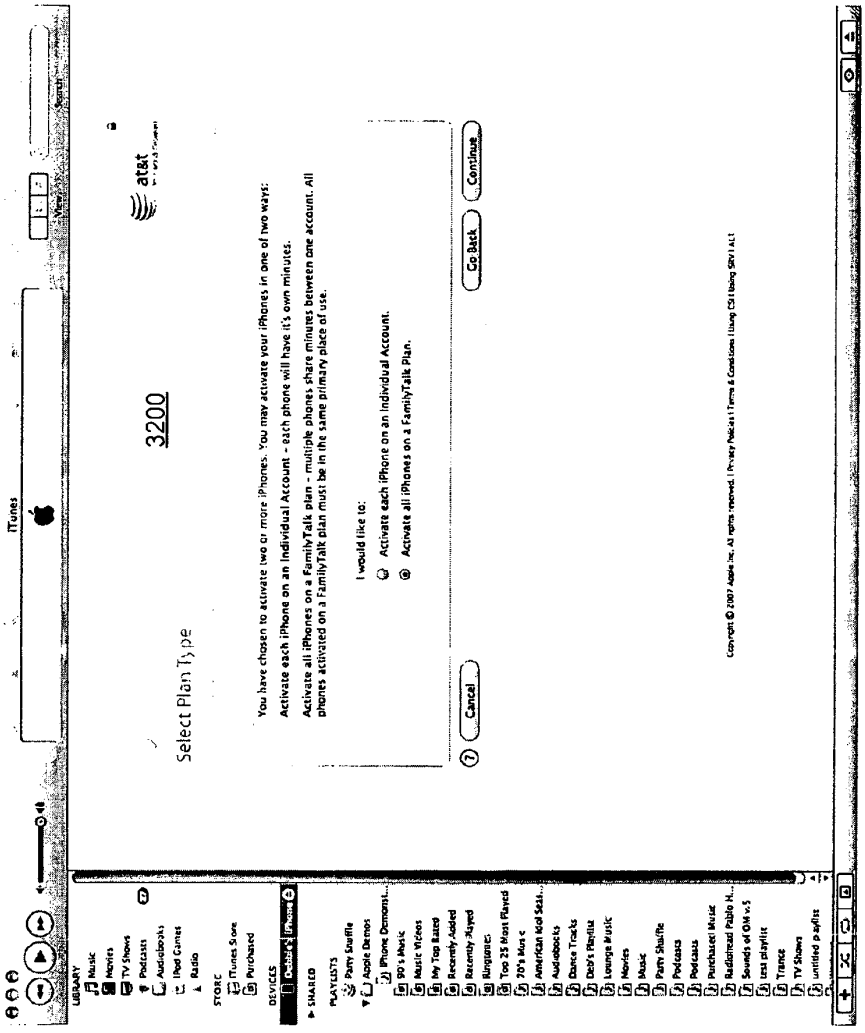


FIG. 32

BNSDOCID: <EP_____1942698A1_I_>

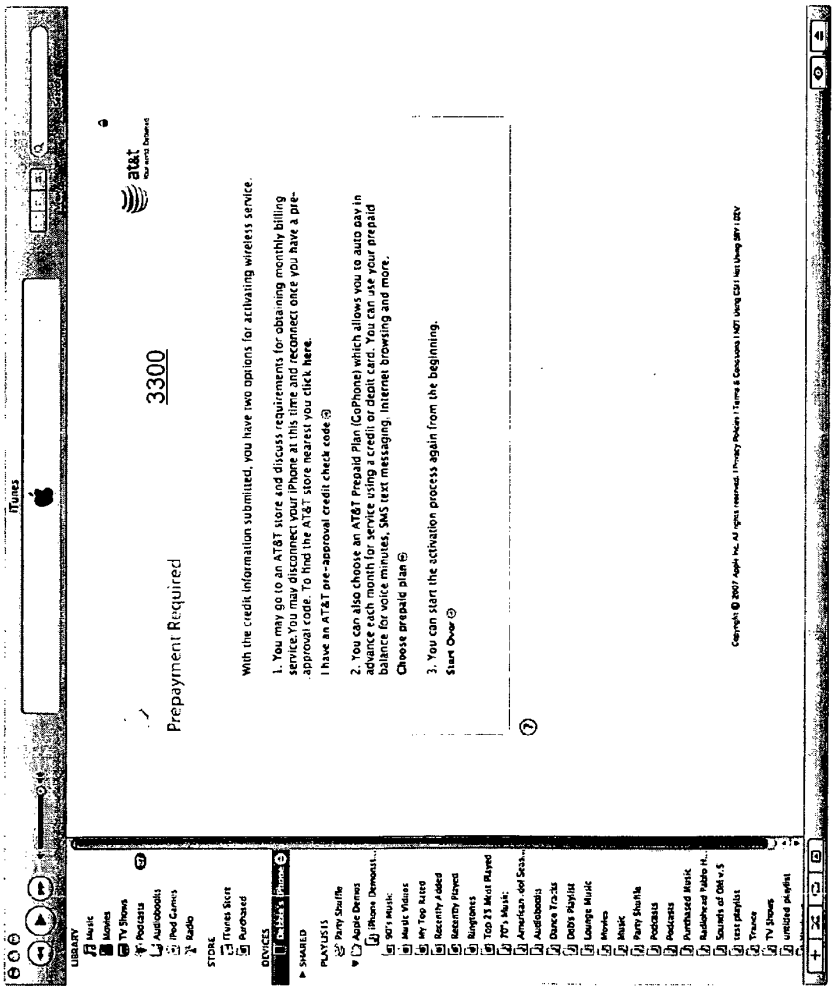


FIG. 33

BNSDOCID: <EP_____1942698A1_I_>

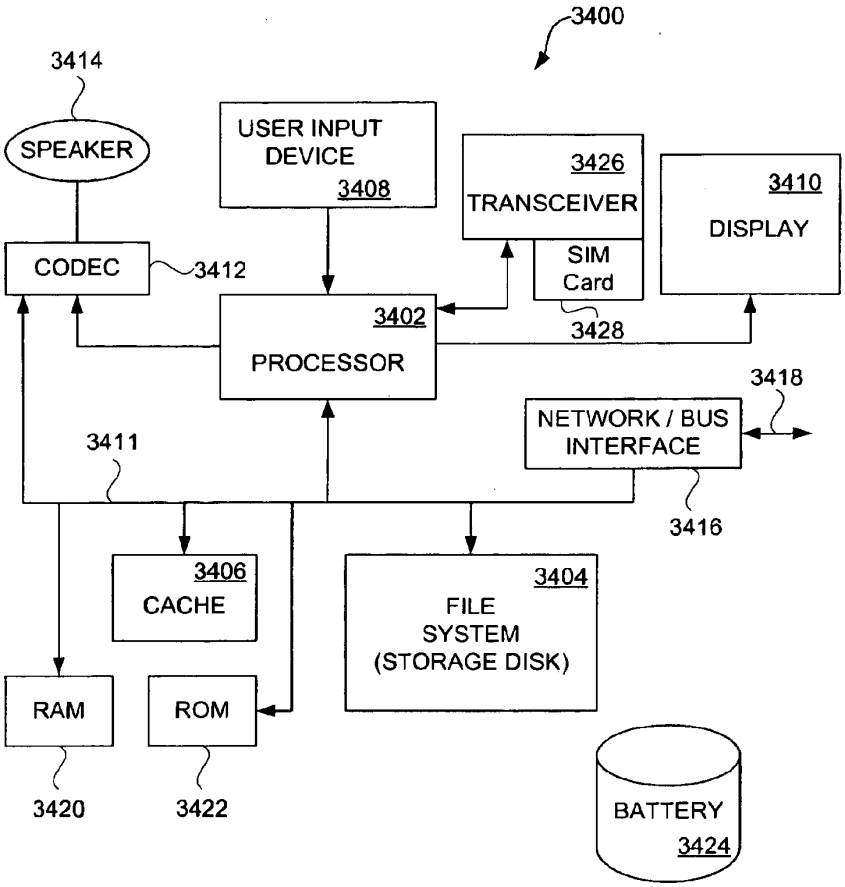


FIG. 34

BNSDOCID: <EP_____1942698A1_I_>

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 08 25 0053

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 2003/083068 A1 (WONG GREGORY A [US]) 1 May 2003 (2003-05-01) * paragraphs [0003] - [0007] * * paragraphs [0018] - [0023] * * figure 2 *	1-68	INV. H04Q7/38
X	US 2006/143098 A1 (LAZARIDIS MIHAL [CA]) 29 June 2006 (2006-06-29) * paragraph [0020] * * paragraph [0030] * * paragraphs [0049], [0050] * * paragraph [0060] * * paragraphs [0075], [0076] * * paragraphs [0087] - [0110] *	1-68	
X	US 2002/085530 A1 (TOYOSHIMA AKIHIKO [JP]) 4 July 2002 (2002-07-04) * paragraphs [0020] - [0022] *	1-68	
X	US 5 386 455 A (COOPER GERSHON N [US]) 31 January 1995 (1995-01-31) * column 1, line 38 - column 2, line 15 * * column 3, line 38 - column 5, line 49 * * figure 3 *	1-68	TECHNICAL FIELDS SEARCHED (IPC) H04Q H04M H04L
X	US 7 054 642 B1 (MATZ WILLIAM R [US] ET AL) 30 May 2006 (2006-05-30) * column 4, lines 39-52 *	1-68	
A	US 2004/235458 A1 (WALDEN CHARLES LEE [US] ET AL) 25 November 2004 (2004-11-25) * paragraphs [0005], [0006] * * paragraph [0011] * * paragraphs [0021] - [0023] * * claim 24 *	1-68	

-/--

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	16 April 2008	Hegeman, Hans

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)

4

BNSDOCID: <EP_____1942698A1_I_>

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 08 25 0053

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
A	WO 01/15414 A (GTE LABORATORIES INC [US]) 1 March 2001 (2001-03-01) * the whole document *	1-68	
A	WO 03/041443 A (SIMPLE PRODUCTS INC [US]) 15 May 2003 (2003-05-15) * the whole document *	1-68	
A	US 2004/176133 A1 (LIPSIT JAMES MASON [US]) 9 September 2004 (2004-09-09) * the whole document *	1-68	
A	EP 0 367 361 A (GTE MOBILNET INC [US]) 9 May 1990 (1990-05-09) * the whole document *	1-68	
			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
The Hague	16 April 2008	Hegeman, Hans

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)

4

BNSDOCID: <EP_____1942698A1_I_>

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 08 25 0053

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.

16-04-2008

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2003083068 A1	01-05-2003	US 2006142007 A1	29-06-2006
US 2006143098 A1	29-06-2006	NONE	
US 2002085530 A1	04-07-2002	NONE	
US 5386455 A	31-01-1995	NONE	
US 7054642 B1	30-05-2006	NONE	
US 2004235458 A1	25-11-2004	CA 2526680 A1 EP 1627539 A2 WO 2004107107 A2	09-12-2004 22-02-2006 09-12-2004
WO 0115414 A	01-03-2001	AU 6893900 A CA 2382298 A1 US 2001041591 A1	19-03-2001 01-03-2001 15-11-2001
WO 03041443 A	15-05-2003	US 2003092435 A1	15-05-2003
US 2004176133 A1	09-09-2004	NONE	
EP 0367361 A	09-05-1990	CA 2001857 A1 US 4958368 A	30-04-1990 18-09-1990

EPO FORM P0459

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

BNSDOCID: <EP_____1942698A1_I_>

REFERENCES CITED IN THE DESCRIPTION

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

Patent documents cited in the description

- US 76744707 A **[0088]**
- US 87931907 P **[0131]**
- US 67908207 A **[0131]**

Electronic Acknowledgement Receipt	
EFS ID:	31741525
Application Number:	15582350
International Application Number:	
Confirmation Number:	7797
Title of Invention:	Wirless Network Buffered Message System
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:	RALEP007C11C3C2C3C2
Receipt Date:	08-FEB-2018
Filing Date:	28-APR-2017
Time Stamp:	16:01:03
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)	P007C11C3C2C3C2.pdf	1054409 8bcec162ea4082257950a56a76fed304aa7795d5	no	5

Warnings:

Information:					
2	Foreign Reference	2095.pdf	9614977 9f371bf4ea0c289ac564aeba3ae2f306a3292b14	no	54
Warnings:					
Information:					
3	Foreign Reference	2096.pdf	4907249 5333d14d9890f1f3087752c23cd0692d086834f1	no	30
Warnings:					
Information:					
4	Foreign Reference	2097.pdf	5055092 48ff78fc65477c69338f1ae4f44454d2354083d9	no	29
Warnings:					
Information:					
5	Foreign Reference	2098.pdf	13411096 d640be147b894d8c3f2ad40fd7969e670da1b102	no	72
Warnings:					
Information:					
			Total Files Size (in bytes):	34042823	

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
15/582,350	04/28/2017	Gregory G. Raleigh	RALEP007C11C3C2C3C2

CONFIRMATION NO. 7797

106963
Headwater Research LLC
1011 Pruitt Place
Tyler, TX 75703

PUBLICATION NOTICE

OC000000095507265

Title: Wirless Network Buffered Message System

Publication No.US-2017-0332240-A1
Publication Date:11/16/2017

NOTICE OF PUBLICATION OF APPLICATION

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

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

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Public Records Division. The Public Records Division can be reached by telephone at (571) 272-3150 or (800) 972-6382, by facsimile at (571) 273-3250, by mail addressed to the United States Patent and Trademark Office, Public Records Division, 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 https://portal.uspto.gov/pair/PublicPair. 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 (03-15)
Approved for use through 07/31/2016. 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	15582350
Filing Date	2017-04-28
First Named Inventor	Gregory G. Raleigh
Art Unit	2447
Examiner Name	not yet assigned
Attorney Docket Number	RALEP007C11C3C2C3C2

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	6760417	B1	2004-07-06	Wallenius, Jukka	
	2	7539862	B2	2009-05-26	Edgett et al.	
	3	7721296	B2	2010-05-18	Ricagni, Giuseppe	
	4	7873346	B2	2011-01-18	Petersson et al.	
	5	7873540	B2	2011-01-18	Arumugam, Avin	
	6	8091087	B2	2012-01-03	Ali et al.	
	7	8146142	B2	2012-03-27	Lortz et al.	
	8	8190087	B2	2012-05-29	Fisher et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Gregory G. Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	9	8214890	B2	2012-07-03	Kirovski et al.	
	10	8285992	B2	2012-10-09	Mathur et al.	
	11	8588240	B2	2013-11-19	Ramankutty et al.	
	12	8676682	B2	2014-03-18	Kalliola, Janne	
	13	8818394	B2	2014-08-26	Bienas et al.	
	14	9064275	B1	2015-06-23	Lu et al.	
	15	9286604	B2	2016-03-15	Aabye et al.	
	16	9589117	B2	2017-03-07	Ali 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	20100284388	A1	2010-11-11	Fantini et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Gregory G. Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	2	20020099848	A1	2002-07-25	Lee, Hoon	

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]
	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	15582350
	Filing Date	2017-04-28
	First Named Inventor	Gregory G. Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

CERTIFICATION STATEMENT

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

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

OR

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

See attached certification statement.

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

☒ A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/James E. Harris/	Date (YYYY-MM-DD)	2017-11-09
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 Acknowledgement Receipt

EFS ID:	30906228
Application Number:	15582350
International Application Number:	
Confirmation Number:	7797
Title of Invention:	Wirless Network Buffered Message System
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:	RALEP007C11C3C2C3C2
Receipt Date:	09-NOV-2017
Filing Date:	28-APR-2017
Time Stamp:	15:49:12
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)	P007C11C3C2C3C2.pdf	1054408 cc9ee1ef440c71bba15d24f16801c96ce9eebfd5	no	5

Warnings:

Information:	
Total Files Size (in bytes):	1054408

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	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
15/582,350	04/28/2017	2447	1600	RALEP007C11C3C2C3C2	18	1

CONFIRMATION NO. 7797

106963
Headwater Research LLC
1011 Pruitt Place
Tyler, TX 75703

UPDATED FILING RECEIPT

OC000000093338852

Date Mailed: 08/10/2017

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 Research LLC, Tyler, TX;

Power of Attorney: The patent practitioners associated with Customer Number 106963

Domestic Priority data as claimed by applicant

This application is a CON of 15/239,398 08/17/2016 PAT 9641957
which is a CON of 14/979,233 12/22/2015 PAT 9532161
which is a CON of 14/667,353 03/24/2015 PAT 9232403
which 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 for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: Yes

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

If Required, Foreign Filing License Granted: 05/05/2017

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 15/582,350**

Projected Publication Date: 11/16/2017

Non-Publication Request: No

Early Publication Request: Yes
**** SMALL ENTITY ****
Title

Wirless Network Buffered Message System

Preliminary Class

709

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.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 15/582,350

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.

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 15/582,350	Filing Date 04/28/2017	☐ To be Mailed

ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) 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	08/08/2017	(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.

LDRC
/EVA GILLIS/

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.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Raleigh	Examiner:	not yet assigned
Serial No.:	15/582,350	Art Unit:	2447
Filed:	April 28, 2017	Conf. No.:	7797
Title:	Automated Device Provisioning and Activation		

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

PRELIMINARY AMENDMENT AND RESPONSE TO NOTICE TO FILE MISSING PARTS

In response to the Notice to File Missing Parts dated May 8, 2017 (the "Notice"), the no-fee deadline for response being July 10, 2017, please enter the following amendments and remarks:

Amendments to the Specification begin on page 2.

Amendments to the Abstract begin on page 3.

Amendments to the Claims begin on page 4.

Remarks begin on page 8.

AMENDMENTS TO THE SPECIFICATION

In the Title:

Please replace the application title with the following new title:

Wireless Network Buffered Message System

AMENDMENTS TO THE ABSTRACT

In the Abstract:

Please replace the abstract with the following abstract:

A network server system maintains secure Internet data message links with respective device link agents on each of many wireless end-user devices. Through a network interface, the server system receives messages from network elements, for which delivery is requested to specific software components on specific ones of the devices. A message buffer system buffers such messages for delivery, and logic determines whether one of several potential triggers has happened to cause the system to deliver buffered messages to a particular one of the devices. For at least some messages, receiving the message at the buffer will not trigger delivery. At least one trigger identifies a time-critical message, however, which can cause all buffered messages for a particular device to be delivered. Such a system balances wireless network efficiency and opportunistic delivery with a potential for fast message delivery, when needed.

AMENDMENTS TO THE CLAIMS

1. (Canceled).

2. (New) A networked system comprising:

i) a network server system including

a link interface to maintain a respective secure Internet data message link between the link interface and a respective device link agent on each of a plurality of wireless end-user devices, each of the wireless end-user devices comprising multiple software components authorized to receive messages via the device link agent on that device;

a network interface to receive messages from a plurality of network elements, for delivery to respective ones of the software components identified in the messages, each network element authorized to send messages via the link interface to one or more of the software components on one or more of the wireless end-user devices; and

a message buffer system including a memory and logic,

the memory to buffer content from the received network element messages for which delivery is requested to any of the wireless end-user devices,

the logic to determine when one of a plurality of message delivery triggers for a given one of the wireless end-user devices has occurred, wherein for at least some of the received network element messages, the receipt of such a message by the message buffer system is not a message delivery trigger, and for at least one of the message delivery triggers, the trigger is an occurrence of an asynchronous event with time-critical messaging needs, and

upon determining that one of the message delivery triggers has occurred for the given one of the wireless end-user devices, the logic further to supply one or more messages comprising the buffered content for the given one of the wireless end-user devices to the transport services stack for delivery on the secure message link maintained between the transport services stack and a device link agent on the given one of the wireless end-user devices; and

ii) the device link agents on the respective wireless end-user devices, each of the device link agents configured to

maintain the respective secure Internet data message link over a wireless network to the link interface,

receive secure Internet data messages from the network server system over the respective secure Internet data message link, including messages collected from multiple ones of the network elements and messages corresponding to multiple ones of the software components authorized to receive messages via the device link agent on that respective device, wherein at least a first subset of the secure Internet data messages contain both a unique identifier for a corresponding one of the software agents and data to be consumed by that software component, the data supplied from a respective network element corresponding to that software component, and

for software components that are authorized to access messages received via the device link agent, cause messages with a unique identifier corresponding to a given one of those software applications to be securely delivered to a software process corresponding to the given software component.

3. (New) The networked system of claim 2, wherein one of the message delivery triggers is the expiration of a periodic timer.

4. (New) The networked system of claim 3, wherein the period of the timer is fractionally shorter than a maximum data message interval beyond which the Internet data message link to the given device is taken down.

5. (New) The networked system of claim 2, wherein one of the message delivery triggers is the receipt of a transmission on the respective secure Internet data message link from the device link agent of the given one of the wireless end-user devices, or a response generated to a transmission received from that device link agent.

6. (New) The networked system of claim 2, wherein one of the message delivery triggers is a heartbeat message generated by the given device link agent, or a request received from the given device link agent.

7. (New) The networked system of claim 2, wherein one of the message delivery triggers is the receipt of a particular message from one of the network elements.

8. (New) The networked system of claim 2, further comprising a secure server to store a secure authorization list, the secure authorization list indicating the authorized software components and the authorized network elements that are allowed to communicate using the network server system.

9. (New) The networked system of claim 8, further comprising the respective device link agent on each wireless end-user device receiving access authorization information from the secure server, the access authorization indicating, respectively for each wireless end-user device, the software components authorized to receive messages via the device link agent on that device.

10. (New) The networked system of claim 2, wherein a second subset of the secure Internet data messages contain a user message from a network element, the user message intended for display on a user interface of a given one of the wireless end-user devices.

11. (New) The networked system of claim 2, wherein one of the software components on a given one of the wireless end-user devices is a policy control agent, and the data to be consumed by the policy control agent comprises service settings and/or configuration information for the given device.

12. (New) The networked system of claim 2, the link interface to encrypt messages identified for delivery to each given one of the wireless end-user devices to create secure Internet data messages, the device link agent on each given device further configured to decrypt the received secure Internet data messages for that device prior to delivering those messages to a respective software process.

13. (New) The networked system of claim 12, wherein the encrypted messages are transported to the device link agent using one or more of encryption on a transport services stack, IP (Internet Protocol) layer encryption, and tunneling.

14. (New) The networked system of claim 2, wherein the device link agent on a given device executes in a secure execution environment, and at least one of the software components on that device executes outside of the secure execution environment.

15. (New) The networked system of claim 2, wherein the device link agent on a given one of the devices is further configured to receive, from one or more of the software components on that device, upload messages, each of the upload messages identifying a corresponding one of the network elements to which the device respective software component has requested delivery, the device link agent on that device transmitting the upload messages to the network message server over the respective secure Internet data message link, for delivery by the network message server to the respective identified network elements.

16. (New) The networked system of claim 15, the device link agent on the given device further configured to buffer one or more of the upload messages for transmission to the network message server at a time selected by a heartbeat mechanism.

17. (New) The networked system of claim 2, at least a given one of the devices further comprising a secure interprocess communication service separately secured from the secure Internet data message link, the device link agent for the given device causing messages to be securely delivered to a software process by initiating delivery of each such message on the secure interprocess communication service.

18. (New) The networked system of claim 2, wherein at least one of the secure Internet data messages comprises multiple identifier/data pairs.

19. (New) The networked system of claim 2, the message buffer system logic to determine, for each of the wireless end-user devices, when one of a plurality of message delivery triggers has occurred, at least one of the triggers for each given device specific to one or more states of that given device.

REMARKS

Claim 1 has been canceled, and new claims 2-19 have been added. No new matter has been added. Applicant respectfully requests the entry of the amendments herein.

Applicant is also submitting the required fees and surcharge, as noted in the Notice.

The Commissioner is authorized to charge any fee deficiency or credit any overpayment to Deposit Account 50-5876.

Respectfully submitted,

Date: August 8, 2017

By: /James E. Harris/

James E. Harris
Reg. No. 40,013
Patent Counsel
Headwater Research LLC
1011 Pruitt Place
Tyler, TX 75703
(903) 201-6212

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: Aug. 8, 2017 By: /Ann Taylor/
Ann Taylor

Electronic Patent Application Fee Transmittal

Application Number:	15582350
Filing Date:	28-Apr-2017
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:	RALEP007C11C3C2C3C2

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:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
PUBL. FEE- EARLY, VOLUNTARY, OR NORMAL	1504	1	0	0
LATE FILING FEE FOR OATH OR DECLARATION	2051	1	70	70
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Extension - 1 month with $0 paid	2251	1	100	100
Miscellaneous:				
		Total in USD ($)		**1700**

Electronic Acknowledgement Receipt	
EFS ID:	30022507
Application Number:	15582350
International Application Number:	
Confirmation Number:	7797
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:	RALEP007C11C3C2C3C2
Receipt Date:	08-AUG-2017
Filing Date:	28-APR-2017
Time Stamp:	18:24:38
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$1700
RAM confirmation Number	080917INTEFSW00005768505876
Deposit Account	505876
Authorized User	Ann Taylor
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.16 (National application filing, search, and examination fees) 37 CFR 1.17 (Patent application and reexamination processing fees)	

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Extension of Time	P007C11C3C2C3C2_Extension.pdf	163886 a7ce34f8e134463761193fdd5fbbf37362055a8d	no	2
Warnings:					
Information:					
2	Applicant Response to Pre-Exam Formalities Notice	P007C11C3C2C3C2_NFMP.pdf	72145 45dfe94b93ddeee44720fbefe4facac764486fb8	no	2
Warnings:					
Information:					
3	Assignee showing of ownership per 37 CFR 3.73	P007C11C3C2C3C2_Stmt.pdf	120077 0b5dce393e8454acf8239c1ea05e1a2819944531	no	3
Warnings:					
Information:					
4	Preliminary Amendment	P007C11C3C2C3C2_PreliminaryAmendment.pdf	105773 1c4fbabc16609fcbaab1b3f5d2e55cf30c9a8797	no	8
Warnings:					
Information:					
5	Fee Worksheet (SB06)	fee-info.pdf	42297 ae8ac3de1cfed4083373a248dcd88d1afcd9911f	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	504178		

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/22 (03-13)
Approved for use through 7/31/2016. 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.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)	Docket Number (Optional) RALEP007C11C3C2C3C2
Application Number 15/582,350	Filed April 28, 2017
For Automated Device Provisioning and Activation	
Art Unit 2447	Examiner not yet assigned

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above-identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

		Fee	Small Entity Fee	Micro Entity Fee	
☑	One month (37 CFR 1.17(a)(1))	$200	$100	$50	$ 100
☐	Two months (37 CFR 1.17(a)(2))	$600	$300	$150	$
☐	Three months (37 CFR 1.17(a)(3))	$1,400	$700	$350	$
☐	Four months (37 CFR 1.17(a)(4))	$2,200	$1,100	$550	$
☐	Five months (37 CFR 1.17(a)(5))	$3,000	$1,500	$750	$

☑ Applicant asserts small entity status. See 37 CFR 1.27.

☐ Applicant certifies micro entity status. See 37 CFR 1.29.
Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

☐ A check in the amount of the fee is enclosed.

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

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☑ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 505876.

☑ Payment made via EFS-Web.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

☐ applicant.

☑ attorney or agent of record. Registration number 40013.

☐ attorney or agent acting under 37 CFR 1.34. Registration number _____.

/James E. Harris/	August 8, 2017
Signature	Date
James E. Harris	903-201-6212
Typed or printed name	Telephone Number

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

☐ * Total of _____ forms are submitted.

This collection of information is required by 37 CFR 1.136(a). 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 6 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop PCT, 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 disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
15/582,350	04/28/2017	Gregory G. Raleigh	RALEP007C11C3C2C3C2

CONFIRMATION NO. 7797

106963
Headwater Research LLC
1011 Pruitt Place
Tyler, TX 75703

FORMALITIES LETTER

OC000000091156834

Date Mailed: 05/08/2017

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The statutory basic filing fee is missing.
- The application search fee must be submitted.
- The application examination fee must be submitted.
- Surcharge as set forth in 37 CFR 1.16(f) must be submitted.
  The surcharge is due for any one of:
  - late submission of the basic filing fee, search fee, or examination fee,
  - late submission of inventor's oath or declaration,
  - filing an application that does not contain at least one claim on filing, or
  - submission of an application filed by reference to a previously filed application.

SUMMARY OF FEES DUE:

The fee(s) required within **TWO MONTHS** from the date of this Notice to avoid abandonment is/are itemized below. Small entity discount is in effect. If applicant is qualified for micro entity status, an acceptable Certification of Micro Entity Status must be submitted to establish micro entity status. (See 37 CFR 1.29 and forms PTO/SB/15A and 15B.)

- $ **70** basic filing fee.
- $ **800** for **159** electronically equivalent pages in excess of **100** application size fee.
- $ **70** surcharge.
- $ **300** search fee.
- $ **360** examination fee.
- $(**0**) previous unapplied payment amount.
- $ **1600** TOTAL FEE BALANCE DUE.

Replies must be received in the USPTO within the set time period or must include a proper Certificate of Mailing or Transmission under 37 CFR 1.8 with a mailing or transmission date within the set time period. For more information and a suggested format, see Form PTO/SB/92 and MPEP 512.

Replies should be mailed to:

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web, including a copy of this Notice and selecting the document description "Applicant response to Pre-Exam Formalities Notice". https://sportal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html

For more information about EFS-Web please call the USPTO Electronic Business Center at 1-866-217-9197 or visit our website at http://www.uspto.gov/ebc.

If you are not using EFS-Web to submit your reply, you must include a copy of this notice.

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

/swong/

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)

Applicant/Patent Owner: Headwater Research LLC

Application No./Patent No.: 15/582,350 Filed/Issue Date: April 28, 2017

Titled: Automated Device Provisioning and Activation

Headwater Research 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 _____, Frame _____, 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: Inventor (Raleigh) To: Headwater Partners I LLC

   The document was recorded in the United States Patent and Trademark Office at

   Reel 042231, Frame 0565, or for which a copy thereof is attached.

2. From: Headwater Partners I LLC To: Headwater Research LLC

   The document was recorded in the United States Patent and Trademark Office at

   Reel 042231, Frame 0594, or for which a copy thereof is attached.

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

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

STATEMENT UNDER 37 CFR 3.73(c)

3. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

4. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

5. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

6. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

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

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

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

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

/James E. Harris/	Aug. 8, 2017
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 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.

PTO/SB/08a (03-15)
Approved for use through 07/31/2016. 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	15582350
Filing Date	2017-04-28
First Named Inventor	Raleigh
Art Unit	2447
Examiner Name	not yet assigned
Attorney Docket Number	RALEP007C11C3C2C3C2

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	5131020	A	1992-07-14	Liebesny et al.	
	2	5283904		1994-02-01	CARSON, David G. et al.	
	3	5325532	A	1994-06-28	Crosswy et al.	
	4	5572528	A	1996-11-05	Shuen, Pauline	
	5	5577100		1996-11-19	McGREGOR et al.	
	6	5594777		1997-01-14	Makkonen, Matti et al.	
	7	5617539	A	1997-04-01	Ludwig et al.	
	8	5630159	A	1997-05-13	Zancho, William F.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	9	5633484	A	1997-05-27	Zancho, William F. et al.	
	10	5633868	A	1997-05-27	Baldwin et al.	
	11	5754953	A	1998-05-19	Briancon et al.	
	12	5774532	A	1998-06-30	Gottlieb et al.	
	13	5794142		1998-08-11	VANTTILA et al.	
	14	5814798	A	1998-09-29	Zancho, William F.	
	15	5889477		1999-03-30	Fastenrath, Ulrich	
	16	5892900		1999-04-06	GINTER et al.	
	17	5903845		1999-05-11	BUHRMANN et al.	
	18	5915008	A	1999-06-22	Dulman, Scott	
	19	5933778		1999-08-03	BUHRMANN et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	20	5940472		1999-08-17	NEWMAN et al.	
	21	5974439	A	1999-10-26	Bollella, Gregory	
	22	5983270	A	1999-11-09	Abraham et al.	
	23	6035281		2000-03-07	Crosskey, James P. et al.	
	24	6038452		2000-03-14	Strawczynski, Leo et al.	
	25	6038540	A	2000-03-14	Krist et al.	
	26	6047268		2000-04-04	BARTOLI et al.	
	27	6058434	A	2000-05-02	Wilt et al.	
	28	6061571	A	2000-05-09	Tamura, Hideo	
	29	6064878		2000-05-16	DENKER, John Stewart et al.	
	30	6078953		2000-06-20	VAID et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	31	6081591		2000-06-27	SKOOG, Frederick H.	
	32	6098878		2000-08-08	DENT et al.	
	33	6104700	A	2000-08-15	Haddock, Stephen R. et al.	
	34	6115823	A	2000-09-05	Velasco et al.	
	35	6119933	A	2000-09-19	Wong et al.	
	36	6125391	A	2000-09-26	Meltzer et al.	
	37	6141565	A	2000-10-31	Feuerstein et al.	
	38	6141686		2000-10-31	JACKOWSKI et al.	
	39	6148336		2000-11-14	THOMAS et al.	
	40	6154738		2000-11-28	CALL, Charles Gainor	
	41	6157636	A	2000-12-05	Voit et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	42	6185576	B1	2001-02-06	Mcintosh, Lowrie	
	43	6198915		2001-03-06	McGREGOR et al.	
	44	6219786	B1	2001-04-17	Cunningham et al.	
	45	6226277		2001-05-01	Chuah, Mooi Choo	
	46	6263055		2001-07-17	GARLAND et al.	
	47	6292828		2001-09-18	Williams, David L.	
	48	6317584		2001-11-13	ABU-AMARA et al.	
	49	6381316		2002-04-30	JOYCE, Simon James et al.	
	50	6393014	B1	2002-05-21	Daly et al.	
	51	6397259	B1	2002-05-28	Lincke et al.	
	52	6401113	B2	2002-06-04	Lazaridis et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	53	6418147		2002-07-09	WIEDEMAN, Robert A.	
	54	6438575	B1	2002-08-20	Khan et al.	
	55	6445777	B1	2002-09-03	Clark, Curtis	
	56	6449479		2002-09-10	SANCHEZ, Eduardo	
	57	6466984	B1	2002-10-15	Naveh et al.	
	58	6477670		2002-11-05	Ahmadvand, Nima	
	59	6502131		2002-12-31	VAID, Aseem et al.	
	60	6505114		2003-01-07	LUCIANI, Sergio	
	61	6510152	B1	2003-01-21	Gerszberg et al.	
	62	6522629	B1	2003-02-18	Anderson, Sr., Ronald D.	
	63	6532235		2003-03-11	BENSON et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	64	6532579		2003-03-11	SATO et al.	
	65	6535855	B1	2003-03-18	Cahill et al.	
	66	6539082		2003-03-25	LOWE et al.	
	67	6542500	B1	2003-04-01	Gerszberg et al.	
	68	6542992		2003-04-01	Peirce, Kenneth L. et al.	
	69	6546016	B1	2003-04-08	Gerszberg et al.	
	70	6563806		2003-05-13	YANO et al.	
	71	6570974	B1	2003-05-27	Gerszberg et al.	
	72	6574321		2003-06-03	COX et al.	
	73	6574465		2003-06-03	MARSH et al.	
	74	6578076	B1	2003-06-10	Putzolu, David Matthew	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	75	6581092		2003-06-17	MOTOYAMA, Tetsuro	
	76	6598034	B1	2003-07-22	Kloth, Axel K.	
	77	6601040	B1	2003-07-29	Kolls, H. Brock	
	78	6603969		2003-08-05	VUORISTO et al.	
	79	6606744		2003-08-12	MIKURAK, Michael G.	
	80	6628934	A	2003-09-30	Rosenberg et al.	
	81	6631122		2003-10-07	ARUNACHALAM, Vaidhyanathan et al.	
	82	6636721	B2	2003-10-21	Threadgill et al.	
	83	6639975		2003-10-28	O'NEAL et al.	
	84	6640097		2003-10-28	Corrigan, Louis et al.	
	85	6640334	B	2003-10-28	Rasmussen, John H.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	86	6650887		2003-11-18	McGREGOR et al.	
	87	6651101		2003-11-18	GAI et al.	
	88	6654786	B1	2003-11-25	Fox et al.	
	89	6654814		2003-11-25	Britton, Kathryn H. et al.	
	90	6658254		2003-12-02	PURDY et al.	
	91	6662014	B1	2003-12-09	Walsh, Patrick Jay	
	92	6678516		2004-01-13	Nordman, Ian et al.	
	93	6683853		2004-01-27	Kannas, Chris et al.	
	94	6684244		2004-01-27	GOLDMAN et al.	
	95	6690918	B2	2004-02-10	Evans et al.	
	96	6697821	B2	2004-02-24	Ziff et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	97	6725031		2004-04-20	WATLER et al.	
	98	6725256	B1	2004-04-20	Albal et al.	
	99	6735206	B1	2004-05-11	Oki et al.	
	100	6748195	B1	2004-06-08	Phillips, W. Garland	
	101	6748437	B1	2004-06-08	Mankude et al.	
	102	6751296	B1	2004-06-15	Albal et al.	
	103	6754470		2004-06-22	Hendrickson, Keith et al.	
	104	6757717	B1	2004-06-29	Goldstein, Leonid	
	105	6763000		2004-07-13	WALSH, Peter J.	
	106	6763226	B1	2004-07-13	McZeal Jr., Alfred	
	107	6765864		2004-07-20	NATARAJAN et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	108	6765925		2004-07-20	Sawyer, Wilson et al.	
	109	6782412		2004-08-24	BROPHY, Kevin et al.	
	110	6785889		2004-08-31	WILLIAMS, Peter	
	111	6792461	B1	2004-09-14	Hericourt, Olivier	
	112	6829596		2004-12-07	FRAZEE, Steve	
	113	6829696		2004-12-07	BALMER et al.	
	114	6839340		2005-01-04	Voit, Eric A. et al.	
	115	6873988	B2	2005-03-29	Herrmann et al.	
	116	6876653		2005-04-05	AMBE, Shekhar et al.	
	117	6879825	B1	2005-04-12	Daly, Brian Kevin	
	118	6882718	B1	2005-04-19	Smith, Benjamin V.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	119	6885997	B1	2005-04-26	Roberts, David T.	
	120	6901440	B1	2005-05-31	Bimm et al.	
	121	6920455		2005-07-19	WESCHLER, Paul	
	122	6922562		2005-07-26	Ward, Stephen L. et al.	
	123	6928280		2005-08-09	Xanthos, James et al.	
	124	6934249	B1	2005-08-23	Bertin, Olivier et al.	
	125	6934751	B2	2005-08-23	Jayapalan et al.	
	126	6947723		2005-09-20	Gurnani, Roger et al.	
	127	6947985	B2	2005-09-20	Hegli et al.	
	128	6952428		2005-10-04	NECKA et al.	
	129	6957067		2005-10-18	Iyer, Pradeep J. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	130	6959393	B2	2005-10-25	Hollis et al.	
	131	6965667		2005-11-15	TRABANDT et al.	
	132	6965872		2005-11-15	Grdina, Jerome M.	
	133	6967958		2005-11-22	ONO, Yoshiyuki et al.	
	134	6970692	B2	2005-11-29	Tysor, Arthur James	
	135	6982733	B1	2006-01-03	McNally et al.	
	136	6983370	B2	2006-01-03	Eaton et al.	
	137	6996062	B1	2006-02-07	Freed et al.	
	138	6996076		2006-02-07	FORBES et al.	
	139	6996393		2006-02-07	Pyhalammi, Seppo et al.	
	140	6998985		2006-02-14	REISMAN et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	141	7002920		2006-02-21	Ayyagari, Deepak et al.	
	142	7007295	B1	2006-02-28	Rose et al.	
	143	7013469	B2	2006-03-14	Smith et al.	
	144	7017189	B1	2006-03-21	DeMello et al.	
	145	7024200		2006-04-04	McKENNA et al.	
	146	7024460	B2	2006-04-04	Koopmas et al.	
	147	7027055	B2	2006-04-11	Anderson et al.	
	148	7027408		2006-04-11	NABKEL et al.	
	149	7032072	B1	2006-04-18	Quinn et al.	
	150	7039027	B2	2006-05-02	Bridgelall, Raj	
	151	7039037		2006-05-02	Wang, Jiwei R. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	152	7039403		2006-05-02	Wong, Gregory A.	
	153	7039713	B1	2006-05-02	Van Gunter, David et al.	
	154	7042988		2006-05-09	JUITT et al.	
	155	7043225	B1	2006-05-09	Patel et al.	
	156	7043226		2006-05-09	Yamauchi, Toshiaki	
	157	7043268	B2	2006-05-09	Yukie et al.	
	158	7047276	B2	2006-05-16	Liu et al.	
	159	7058022	B1	2006-06-06	Carolan et al.	
	160	7058968		2006-06-06	ROWLAND et al.	
	161	7068600		2006-06-27	CAIN, Joseph Bibb	
	162	7069248		2006-06-27	HUBER, Adriano	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	163	7082422	B1	2006-07-25	Zirngibl et al.	
	164	7084775	B1	2006-08-01	Smith, Michael R.	
	165	7092696		2006-08-15	HOSAIN et al.	
	166	7095754	B2	2006-08-22	Benveniste, Mathilde	

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	20080250053	A	2008-10-09	Aaltonen, Janne et al.	
	2	20080256593		2008-10-16	VINBERG et al.	
	3	20080259924	A1	2008-10-23	Gooch et al.	
	4	20080262798		2008-10-23	KIM, Eun Ah et al.	
	5	20080263348	A	2008-10-23	Zaltsman et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	6	20080268813		2008-10-30	MAES, Stephane H.	
	7	20080270212	A	2008-10-30	Blight et al.	
	8	20080279216	A1	2008-11-13	Sharif-Ahmadi et al.	
	9	20080282319	A1	2008-11-13	Fontijn et al.	
	10	20080293395	A1	2008-11-27	Mathews et al.	
	11	20080298230		2008-12-04	LUFT et al.	
	12	20080305793		2008-12-11	GALLAGHER et al.	
	13	20080311885		2008-12-18	DAWSON et al.	
	14	20080313315	A	2008-12-18	Karaoguz et al.	
	15	20080313730		2008-12-18	Iftimie, Sorin et al.	
	16	20080316923		2008-12-25	FEDDERS et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	17	20080318547		2008-12-25	BALLOU et al.	
	18	20080318550		2008-12-25	DeATLEY, Dallas	
	19	20080319879		2008-12-25	CARROLL et al.	
	20	20080320497	A1	2008-12-25	Tarkoma et al.	
	21	20090005000	A	2009-01-01	Baker, Matthew et al.	
	22	20090005005		2009-01-01	FORSTALL et al.	
	23	20090006116	A	2009-01-01	Baker, Matthew et al.	
	24	20090006200	A	2009-01-01	Baker, Matthew et al.	
	25	20090006229	A1	2009-01-01	Sweeney et al.	
	26	20090013157		2009-01-08	BEAULE, Stephane	
	27	20090016310	A1	2009-01-15	Rasal, Digambar L.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	28	20090036111	A1	2009-02-05	Danford et al.	
	29	20090042536	A1	2009-02-12	Bernard et al.	
	30	20090044185	A1	2009-02-12	Krivopaltsev, Eugene	
	31	20090046707	A1	2009-02-19	Smires et al.	
	32	20090046723		2009-02-19	RAHMAN, Reshad A. et al.	
	33	20090047989	A1	2009-02-19	Harmon et al.	
	34	20090048913	A1	2009-02-19	Shenfield et al.	
	35	20090049156	A1	2009-02-19	Aronsson et al.	
	36	20090049518	A1	2009-02-19	Roman et al.	
	37	20090054030		2009-02-26	GOLDS, David	
	38	20090065571	A1	2009-03-12	Jain, Deepak	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	39	20090067372		2009-03-12	SHAH, Keyur C. et al.	
	40	20090068984		2009-03-12	BURNETT, R. Alan	
	41	20090070379	A1	2009-03-12	Rappaport, Theodore R.	
	42	20090077622		2009-03-19	BAUM et al.	
	43	20090079699		2009-03-26	SUN, Jian	
	44	20090113514		2009-04-30	HU, Q. James	
	45	20090125619		2009-05-14	ANTANI, Snehal S.	
	46	20090132860	A1	2009-05-21	LIU et al.	
	47	20090149154	A1	2009-06-11	Bhasin et al.	
	48	20090157792		2009-06-18	Fiatal, Trevor	
	49	20090163173	A1	2009-06-25	Williams, Timothy D.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	50	20090172077		2009-07-02	ROXBURGH, David et al.	
	51	20090180391		2009-07-16	PETERSEN et al.	
	52	20090181662	A1	2009-07-16	Fleischman et al.	
	53	20090197585		2009-08-06	AARON, Jeffrey A.	
	54	20090197612	A1	2009-08-06	Kiiskinen, Arto	
	55	20090203352	A1	2009-08-13	Fordon et al.	
	56	20090217364	A1	2009-08-27	Salmela et al.	
	57	20090219170		2009-09-03	CLARK, Ryan C. et al.	
	58	20090248883		2009-10-01	SURYANARAYANA et al.	
	59	20090254857	A	2009-10-08	Romine et al.	
	60	20090257379		2009-10-15	ROBINSON et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	61	20090271514		2009-10-29	THOMAS et al.	
	62	20090282127	A	2009-11-12	Leblanc et al.	
	63	20090286507		2009-11-19	O'NEIL et al.	
	64	20090287921		2009-11-19	ZHU et al.	
	65	20090288140		2009-11-19	HUBER et al.	
	66	20090291665	A1	2009-11-26	Gaskarth et al.	
	67	20090299857		2009-12-03	BRUBAKER, Curtis M.	
	68	20090307696	A1	2009-12-10	Vals et al.	
	69	20090307746		2009-12-10	DI, Jinwen et al.	
	70	20090315735		2009-12-24	BHAVANI, Neeraj S. et al.	
	71	20090320110	A1	2009-12-24	NICOLSON et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	72	20100017506		2010-01-21	FADELL, Anthony	
	73	20100020822		2010-01-28	ZERILLO, Anthony J. et al.	
	74	20100027469		2010-02-04	GURAJALA, Ravindra Babu et al.	
	75	20100027559		2010-02-04	LIN, Hung-Ming et al.	
	76	20100030890	A	2010-02-04	Dutta et al.	
	77	20100041364		2010-02-18	LOTT, Robert Wayne et al.	
	78	20100041365	A1	2010-02-18	Lott et al.	
	79	20100042675		2010-02-18	FUJII, Hiroshi	
	80	20100043068		2010-02-18	VARADHAN et al.	
	81	20100071053		2010-03-18	ANSARI et al.	
	82	20100075666	A1	2010-03-25	Garner, Neil Robert	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	83	20100080202		2010-04-01	Hanson, Mark	
	84	20100082431		2010-04-01	RAMER et al.	
	85	20100103820		2010-04-29	FULLER et al.	
	86	20100121744	A1	2010-05-13	Belz et al.	
	87	20100131584		2010-05-27	Johnson, William J.	
	88	20100144310		2010-06-10	BEDINGFIELD, James Carlton	
	89	20100151866	A1	2010-06-17	Karpov et al.	
	90	20100153781		2010-06-17	HANNA, Stephen R.	
	91	20100167696	A	2010-07-01	Smith, Christopher David et al.	
	92	20100188975		2010-07-29	RALEIGH, Gregory G.	
	93	20100188990		2010-07-29	RALEIGH, Gregory G.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	94	20100188992		2010-07-29	RALEIGH, Gregory G.	
	95	20100188994		2010-07-29	RALEIGH, Gregory G.	
	96	20100190469	A1	2010-07-29	Vanderveen et al.	
	97	20100191576		2010-07-29	RALEIGH, Gregory G.	
	98	20100191612		2010-07-29	RALEIGH, Gregory G.	
	99	20100191846		2010-07-29	RALEIGH, Gregory G.	
	100	20100192170		2010-07-29	RALEIGH, Gregory G.	
	101	20100192212		2010-07-29	RALEIGH, Gregory G.	
	102	20100195503		2010-08-05	RALEIGH, Gregory G.	
	103	20100197268		2010-08-05	RALEIGH, Gregory G.	
	104	20100198698		2010-08-05	RALEIGH et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	105	20100198939		2010-08-05	RALEIGH, Gregory G.	
	106	20100241544		2010-09-23	Benson, Dan et al.	
	107	20100248719	A1	2010-09-30	Scholaert, Hugh	
	108	20100284327	A	2010-11-11	Miklos, Gyorgy	
	109	20100287599	A1	2010-11-11	He et al.	
	110	20100325420		2010-12-23	KANEKAR, Tushar	
	111	20110013569	A	2011-01-20	Scherzer, Shimon et al.	
	112	20110019574	A	2011-01-27	Malomsoky et al.	
	113	20110081881	A	2011-04-07	Baker, Matthew Donald et al.	
	114	20110082790	A	2011-04-07	Baker, Matthew Donald et al.	
	115	20110110309	A	2011-05-12	Bennett, James D.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	116	20110126141		2011-05-26	KING et al.	
	117	20110145920	A1	2011-06-16	Mahaffey et al.	
	118	20110159818	A	2011-06-30	Scherzer, Shimon et al.	
	119	20110173678		2011-07-14	KAIPPALLIMALIL, John et al.	
	120	20110264923	A	2011-10-27	Kocher et al.	
	121	20120020296	A	2012-01-26	Scherzer, Shimon et al.	
	122	20120144025	A1	2012-06-07	Melander et al.	
	123	20120166364	A1	2012-06-28	Ahmad et al.	
	124	20120196644	A	2012-08-02	Scherzer, Shimon et al.	
	125	20120238287	A	2012-09-20	Scherzer, Shimon	
	126	20130029653	A	2013-01-31	Baker, Matthew Donald et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	127	20130058274	A	2013-03-07	Scherzer, Shimon et al.	
	128	20130065555	A	2013-03-14	Baker, Matthew Donald et al.	
	129	20130072177	A1	2013-03-21	Ross et al.	
	130	20130084835	A	2013-04-04	Scherzer, Shimon et al.	
	131	20130144789		2013-06-06	Aaltonen, Janne et al.	
	132	20130326356	A9	2013-12-05	Zheng et al.	
	133	20140073291	A1	2014-03-13	Hildner et al.	
	134	20140241342	A1	2014-08-28	Constantinof, Cristian	

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	2002093877	WO	A1	2002-11-21	Nokia Corp.		

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	2	2003014891	WO		2003-02-20	The Boeing Company		
	3	2003017063	WO	A2	2003-02-27	Apogee Networks		
	4	2003017065	WO	A2	2003-02-27	Apogee Networks		
	5	2003058880	WO		2003-07-17	Telia AB		
	6	2004028070	WO		2004-04-01	Credant Technologies, Inc.		
	7	2004064306	WO		2004-07-29	Motorola Inc.		
	8	2004077797	WO		2004-09-10	Boston Communications Group, Inc. (Erskine)		
	9	2004095753	WO		2004-11-04	Motorola Inc.		
	10	2005008995	WO		2005-01-27	Starhub Ltd.		
	11	2005053335	WO	A1	2005-06-09	Nokia Corp.		
	12	2005083934	WO	A1	2005-09-09	Research In Motion Ltd.		

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	13	2006004467	WO		2006-01-12	Telefonaktiebolaget LM Ericsson		
	14	2006004784	WO	A1	2006-01-12	Japan Communications Inc.		
	15	2006012610	WO	A2	2006-02-02	Citrix Systems, Inc.		
	16	2006050758	WO		2006-05-18	Telefonaktiebolaget LM Ericsson		
	17	2006073837	WO		2006-07-13	Symbol Technologies, Inc.		
	18	2006077481	WO		2006-07-27	TrueContext Corporation		
	19	2006093961	WO	A1	2006-09-08	Kyocera Wireless Corp.		
	20	2006120558	WO		2006-11-16	Nokia Corp.		
	21	2006130960	WO		2006-12-14	Mobidia, Inc.		
	22	2007001833	WO		2007-01-04	Symbol Technologies, Inc.		
	23	2007014630	WO		2007-02-08	Telefonaktiebolaget LM Ericsson		

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	24	2007018363	WO		2007-02-15	Upresto, Inc.		
	25	2007053848	WO		2007-05-10	Mobile Armor, LLC		
	26	2007068288	WO		2007-06-21	Telefonaktiebolaget LM Ericsson		
	27	2007069245	WO		2007-06-21	Yoggie Security Systems, Inc.		
	28	2007097786	WO	A	2007-08-30	Sony Ericsson Mobile Communications AB		
	29	2007107701	WO		2007-09-27	British Telecommunications Public Limited Company		
	30	2007120310	WO		2007-10-25	Qualcomm Inc.		
	31	2007124279	WO		2007-11-01	Cisco Technology, Inc., et al.		
	32	2007126352	WO		2007-11-08	Telefonaktiebolaget LM Ericsson		
	33	2007133844	WO	A	2007-11-22	Camiant, Inc.		
	34	2008017837	WO		2008-02-14	Symbian Software Limited		

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	35	2008051379	WO		2008-05-02	Verizon Services Corp.			
	36	2008066419	WO		2008-06-05	Telefonaktiebolaget LM Ericsson			
	37	2008080139	WO		2008-07-03	Integrated Mobile, Inc.			
	38	2008080430	WO		2008-07-10	Telecom Italia S.P.A.			
	39	2008099802	WO		2008-08-21	NEC Corporation			
	40	2009008817	WO	A1	2009-01-15	Ericsson			
	41	2009091295	WO	A1	2009-07-23	Telefonaktiebolaget LM Ericsson			
	42	2010088413	WO		2010-08-05	Headwater Partners I LLC			

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	STEGLICH, Stephan, "I-Centric User Interaction," November 21, 2003	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	2	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	
	3	VAN EIJK, et al., "GigaMobile, Agent Technology for Designing Personalized Mobile Service Brokerage," July 1, 2002	
	4	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	
	5	Windows7 Power Management, published April 2009	
	6	ZHU et al., "A Survey of Quality of Service in IEEE 802.11 Networks," IEEE Wireless Communications, August 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	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

CERTIFICATION STATEMENT

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

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

OR

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

See attached certification statement.

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

☒ A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/James E. Harris/	Date (YYYY-MM-DD)	2017-08-08
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.

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

PTO/SB/08a (03-15)
Approved for use through 07/31/2016. 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	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

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	20010048738	A	2001-12-06	Baniak, Paul G. et al.	
	2	20010053694		2001-12-20	IGARASHI, Yoichiro et al.	
	3	20020022472		2002-02-21	WATLER et al.	
	4	20020049074	A	2002-04-25	Eisinger, Bernd et al.	
	5	20020116338		2002-08-22	GONTHIER, Jean-Charles et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	6	20020120370	A1	2002-08-29	Parupudi et al.	
	7	20020120540		2002-08-29	KENDE et al.	
	8	20020131404		2002-09-19	MEHTA et al.	
	9	20020138599	A1	2002-09-26	Dilman et al.	
	10	20020138601		2002-09-26	PIPONIUS et al.	
	11	20020154751	A1	2002-10-24	Thompson et al.	
	12	20020161601	A	2002-10-31	Nauer, Bernhard et al.	
	13	20020164983		2002-11-07	Raviv, Li-On et al.	
	14	20020176377		2002-11-28	HAMILTON, Thomas E.	
	15	20020188732	A1	2002-12-12	Buckman et al.	
	16	20020191573	A1	2002-12-19	Whitehill et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	17	20020199001		2002-12-26	WENOCUR et al.	
	18	20030004937		2003-01-02	SALMENKAITA et al.	
	19	20030005112		2003-01-02	KRAUTKREMER, Todd Joseph	
	20	20030013434		2003-01-16	ROSENBERG et al.	
	21	20030018524		2003-01-23	FISHMAN et al.	
	22	20030028623	A1	2003-02-06	Hennessey et al.	
	23	20030046396		2003-03-06	RICHTER et al.	
	24	20030050070		2003-03-13	MASHINSKY et al.	
	25	20030050837		2003-03-13	KIM, Do Sik	
	26	20030084321	A1	2003-05-01	Tarquini et al.	
	27	20030088671		2003-05-08	KLINKER et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	28	20030133408		2003-07-17	CHENG et al.	
	29	20030134650	A1	2003-07-17	Sundar et al.	
	30	20030159030	A1	2003-08-21	Evans, Junius A.	
	31	20030161265		2003-08-28	CAO et al.	
	32	20030171112		2003-09-11	Lupper, Alfred et al.	
	33	20030182420		2003-09-25	JONES et al.	
	34	20030182435		2003-09-25	REDLICH et al.	
	35	20030184793	A1	2003-10-02	Pineau, Richard A.	
	36	20030188006	A	2003-10-02	Bard, Steven R.	
	37	20030188117	A	2003-10-02	Yoshino et al.	
	38	20030220984		2003-11-27	JONES et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	39	20030224781		2003-12-04	MILFORD et al.	
	40	20030229900		2003-12-11	REISMAN, Richard	
	41	20030233332	A	2003-12-18	Keeler, James D. et al.	
	42	20030236745		2003-12-25	HARTSELL et al.	
	43	20040019539		2004-01-29	RAMAN et al.	
	44	20040021697		2004-02-05	BEATON et al.	
	45	20040030705		2004-02-12	BOWMAN-AMUAH, Michel K.	
	46	20040039792	A1	2004-02-26	Nakanishi, Tomoaki	
	47	20040044623		2004-03-04	WAKE et al.	
	48	20040047358		2004-03-11	CHEN et al.	
	49	20040054779	A1	2004-03-18	Takeshima et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	50	20040073672		2004-04-15	FASCENDA, Anthony C.	
	51	20040082346		2004-04-29	SKYTT et al.	
	52	20040098715		2004-05-20	AGHERA et al.	
	53	20040102182	A	2004-05-27	Reith, Lothar et al.	
	54	20040103193		2004-05-27	PANDYA et al.	
	55	20040107360		2004-06-03	HERRMANN et al.	
	56	20040127200		2004-07-01	SHAW et al.	
	57	20040127208	A1	2004-07-01	Nair et al.	
	58	20040132427		2004-07-08	Lee, Wan-Yeon et al.	
	59	20040133668	A1	2004-07-08	Nicholas III, Henry T.	
	60	20040137890	A1	2004-07-15	Kalke, Catherine	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	61	20040168052		2004-08-26	CLISHAM et al.	
	62	20040170191	A	2004-09-02	Guo et al.	
	63	20040176104	A1	2004-09-09	Arcens, Suzanne	
	64	20040198331		2004-10-07	COWARD et al.	
	65	20040203755		2004-10-14	BRUNET, Jeffrey et al.	
	66	20040203833	A	2004-10-14	Rathunde, Dale F. et al.	
	67	20040225561	A1	2004-11-11	Hertzberg et al.	
	68	20040225898	A	2004-11-11	Frost, D. et al.	
	69	20040236547		2004-11-25	RAPPAPORT et al.	
	70	20040243680	A1	2004-12-02	Mayer, Georg	
	71	20040243992	A	2004-12-02	Gustafson et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	72	20040249918		2004-12-09	SUNSHINE, Roger N.	
	73	20040255145	A	2004-12-16	Chow, Jerry	
	74	20040259534	A1	2004-12-23	Chaudhari et al.	
	75	20040260766	A1	2004-12-23	Barros et al.	
	76	20040267872	A1	2004-12-30	Serdy et al.	
	77	20050007993		2005-01-13	Chambers, Mahdi et al.	
	78	20050009499		2005-01-13	KOSTER, Karl	
	79	20050021995		2005-01-27	LAL et al.	
	80	20050041617	A1	2005-02-24	Huotari et al.	
	81	20050048950		2005-03-03	MORPER, Hans-Jochen	
	82	20050055291		2005-03-10	BEVENTE et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	83	20050055309		2005-03-10	WILLIAMS et al.	
	84	20050055595	A	2005-03-10	Frazer et al.	
	85	20050060266		2005-03-17	DEMELLO et al.	
	86	20050060525	A1	2005-03-17	Schwartz et al.	
	87	20050075115	A1	2005-04-07	Corneille et al.	
	88	20050079863	A	2005-04-14	Macaluso, Anthony G.	
	89	20050091505	A1	2005-04-28	Riley et al.	
	90	20050096024	A1	2005-05-05	Bicker et al.	
	91	20050097516		2005-05-05	DONNELLY et al.	
	92	20050107091		2005-05-19	VANNITHAMBY et al.	
	93	20050108075	A1	2005-05-19	Douglis et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	94	20050111463	A1	2005-05-26	Leung et al.	
	95	20050128967		2005-06-16	SCOBBIE, Donald MacGregor	
	96	20050135264	A1	2005-06-23	Popoff et al.	
	97	20050163320	A1	2005-07-28	Brown et al.	
	98	20050166043		2005-07-28	ZHANG et al.	
	99	20050183143		2005-08-18	ANDERHOLM et al.	
	100	20050186948	A	2005-08-25	Gallagher et al.	
	101	20050198377		2005-09-08	FERGUSON et al.	
	102	20050216421		2005-09-29	BARRY et al.	
	103	20050228985		2005-10-13	YLIKOSKI et al.	
	104	20050238046		2005-10-27	HASSAN et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	105	20050239447	A1	2005-10-27	Holzman et al.	
	106	20050245241	A1	2005-11-03	Durand et al.	
	107	20050246282		2005-11-03	NASLUND et al.	
	108	20050250508		2005-11-10	GUO et al.	
	109	20050250536	A1	2005-11-10	Deng et al.	
	110	20050254435		2005-11-17	MOAKLEY et al.	
	111	20050266825		2005-12-01	CLAYTON, Steve	
	112	20050266880		2005-12-01	GUPTA, Vivek G.	
	113	20060014519		2006-01-19	MARSH et al.	
	114	20060019632		2006-01-26	CUNNINGHAM et al.	
	115	20060020787	A1	2006-01-26	Choyi et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	116	20060026679		2006-02-02	ZAKAS, Philip H.	
	117	20060030306	A1	2006-02-09	Kuhn, Brian Gerald	
	118	20060034256		2006-02-16	ADDAGATLA et al.	
	119	20060035631	A1	2006-02-16	White et al.	
	120	20060040642		2006-02-23	BORIS et al.	
	121	20060045245		2006-03-02	AARON et al.	
	122	20060048223		2006-03-02	LEE et al.	
	123	20060068796	A	2006-03-30	Millen, Stephanie L. et al.	
	124	20060072451	A1	2006-04-06	Ross, Alan D.	
	125	20060072550	A1	2006-04-06	Davis et al.	
	126	20060072646		2006-04-06	FEHER, Kamilo	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	127	20060075506	A1	2006-04-06	Sanda et al.	
	128	20060085543		2006-04-20	HRASTAR et al.	
	129	20060095517	A1	2006-05-04	O'Connor et al.	
	130	20060098627	A1	2006-05-11	Karaoguz et al.	
	131	20060099970	A1	2006-05-11	Morgan et al.	
	132	20060112016		2006-05-25	ISHIBASHI, Yoshihito	
	133	20060114821	A1	2006-06-01	Willey et al.	
	134	20060114832	A	2006-06-01	Hamilton et al.	
	135	20060126562	A1	2006-06-15	Liu, Huitao	
	136	20060135144	A	2006-06-22	Jothipragasam, Premkumar	
	137	20060136882	A1	2006-06-22	Noonan et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	138	20060143066	A1	2006-06-29	Calabria	
	139	20060143098		2006-06-29	LAZARIDIS, Mihal	
	140	20060156398	A	2006-07-13	Ross et al.	
	141	20060160536	A	2006-07-20	Chou, Joey	
	142	20060165060		2006-07-27	DUA, Robin	
	143	20060168128	A	2006-07-27	Sistla et al.	
	144	20060173959	A	2006-08-03	Mckelvie et al.	
	145	20060174035	A	2006-08-03	Tufail, Mudassir	
	146	20060178917		2006-08-10	MERRIAM et al.	
	147	20060178918		2006-08-10	MIKURAK, Michael G.	
	148	20060182137	A1	2006-08-17	Zhou et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	149	20060183462		2006-08-17	KOLEHMAINEN, Mikko	
	150	20060190314		2006-08-24	HERNANDEZ, Rick	
	151	20060190987	A1	2006-08-24	Ohta et al.	
	152	20060199608		2006-09-07	DUNN et al.	
	153	20060200663	A1	2006-09-07	Thornton, Andrew J.	
	154	20060206709	A1	2006-09-14	Labrou et al.	
	155	20060206904		2006-09-14	WATKINS et al.	
	156	20060218395		2006-09-28	MAES, Stephane H.	
	157	20060233108		2006-10-19	KRISHNAN, Murali R.	
	158	20060233166		2006-10-19	BOU-DIAB et al.	
	159	20060236095		2006-10-19	SMITH et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	160	20060242685		2006-10-26	HEARD et al.	
	161	20060258341		2006-11-16	MILLER et al.	
	162	20060277590	A1	2006-12-07	Limont et al.	
	163	20060291419	A1	2006-12-28	McConnell et al.	
	164	20060291477		2006-12-28	CROAK et al.	
	165	20070005795	A1	2007-01-04	Gonzalez, Ruben	
	166	20070019670		2007-01-25	FALARDEAU, Eric	
	167	20070022289		2007-01-25	ALT et al.	
	168	20070025301	A	2007-02-01	Petersson et al.	
	169	20070033194	A	2007-02-08	Srinivas et al.	
	170	20070033197	A	2007-02-08	Scherzer, Shimon et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	171	20070036312		2007-02-15	CAI et al.	
	172	20070055694		2007-03-08	RUGE et al.	
	173	20070060200	A1	2007-03-15	Boris et al.	
	174	20070061243	A1	2007-03-15	Ramer et al.	
	175	20070061800	A1	2007-03-15	Cheng et al.	
	176	20070061878		2007-03-15	HAGIU, Costin et al. et al.	
	177	20070073899	A1	2007-03-29	Judge et al.	
	178	20070076616		2007-04-05	NGO et al.	
	179	20070093243		2007-04-26	KAPADEKAR et al.	
	180	20070100981		2007-05-03	ADAMCZYK et al.	
	181	20070101426		2007-05-03	LEE et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	182	20070104126		2007-05-10	CALHOUN et al.	
	183	20070109983	A	2007-05-17	Shankar, Rohit et al.	
	184	20070130283	A1	2007-06-07	Klein et al.	
	185	20070130315		2007-06-07	FRIEND et al.	
	186	20070140113		2007-06-21	GEMELOS, Steven	
	187	20070140145	A	2007-06-21	Kumar et al.	
	188	20070140275		2007-06-21	BOWMAN et al.	
	189	20070143824	A1	2007-06-21	Shahbazi, Majid	
	190	20070147317	A	2007-06-28	Smith et al.	
	191	20070147324		2007-06-28	McGary, Faith	
	192	20070155365	A	2007-07-05	Kim, Sung-Jun et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	193	20070165630	A1	2007-07-19	Rasanen et al.	
	194	20070168499	A	2007-07-19	Chu, Jing-Long	
	195	20070174490	A1	2007-07-26	Choi et al.	
	196	20070192460	A1	2007-08-16	Choi et al.	
	197	20070198656		2007-08-23	MAZZAFERRI et al.	
	198	20070201502	A1	2007-08-30	Abramson, Nathan	
	199	20070213054	A1	2007-09-13	Han, Seung-Wook	
	200	20070220251		2007-09-20	ROSENBERG et al.	
	201	20070226225		2007-09-27	YIU et al.	
	202	20070226775	A	2007-09-27	Andreasen et al.	
	203	20070234402	A1	2007-10-04	Khosravi et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	204	20070243862		2007-10-18	COSKUN et al.	
	205	20070248100		2007-10-25	ZUBERI et al.	
	206	20070254675		2007-11-01	ZORLU OZER et al.	
	207	20070255769	A1	2007-11-01	Agrawal et al.	
	208	20070255797	A1	2007-11-01	Dunn et al.	
	209	20070255848		2007-11-01	SEWALL et al.	
	210	20070257767	A1	2007-11-08	Beeson, Curt	
	211	20070259656	A	2007-11-08	Jeong, Jong Woo	
	212	20070259673		2007-11-08	WILLARS et al.	
	213	20070263558		2007-11-15	SALOMONE, Leonardo	
	214	20070266422	A1	2007-11-15	Germano et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	215	20070274327		2007-11-29	KAARELA et al.	
	216	20070280453		2007-12-06	Kelley, Sean S.	
	217	20070282896		2007-12-06	WYDROUG et al.	
	218	20070293191	A1	2007-12-20	Mir et al.	
	219	20070294395		2007-12-20	STRUB et al.	
	220	20070294410	A1	2007-12-20	Pandya et al.	
	221	20070297378	A1	2007-12-27	Poyhonen et al.	
	222	20070298764		2007-12-27	CLAYTON, Steve	
	223	20070299965	A1	2007-12-27	Nieh et al.	
	224	20070300252		2007-12-27	Acharya, Swarup et al.	
	225	20080005285		2008-01-03	ROBINSON et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	226	20080005561		2008-01-03	BROWN et al.	
	227	20080010379	A	2008-01-10	Zhao, Hang	
	228	20080010452		2008-01-10	HOLTZMAN et al.	
	229	20080018494	A1	2008-01-24	Waite et al.	
	230	20080022354	A	2008-01-24	Grewal, Karanvir et al.	
	231	20080025230	A	2008-01-31	Patel et al.	
	232	20080032715	A1	2008-02-07	Jia et al.	
	233	20080034063	A1	2008-02-07	Yee, Robert	
	234	20080034419	A	2008-02-07	Mullick et al.	
	235	20080039102		2008-02-14	SEWALL et al.	
	236	20080049630		2008-02-28	KOZISEK et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	237	20080050715	A1	2008-02-28	Golczewski et al.	
	238	20080051076		2008-02-28	O'Shaughnessy, John et al.	
	239	20080052387		2008-02-28	HEINZ et al.	
	240	20080056273	A	2008-03-06	Pelletier et al.	
	241	20080059474		2008-03-06	LIM, Keng	
	242	20080059743		2008-03-06	BYCHKOV et al.	
	243	20080060066		2008-03-06	WYNN et al.	
	244	20080062900		2008-03-13	RAO, Bindu Rama	
	245	20080064367		2008-03-13	NATH et al.	
	246	20080066149		2008-03-13	LIM, Keng	
	247	20080066150		2008-03-13	LIM, Keng	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	248	20080066181	A1	2008-03-13	Haveson et al.	
	249	20080070550	A	2008-03-20	Hose, David Alan	
	250	20080077705	A1	2008-03-27	Li et al.	
	251	20080080457	A1	2008-04-03	Cole, Terry L.	
	252	20080081606		2008-04-03	COLE, Terry L.	
	253	20080082643		2008-04-03	STORRIE et al.	
	254	20080083013		2008-04-03	SOLIMAN et al.	
	255	20080085707		2008-04-10	FADELL, Tony	
	256	20080089295	A	2008-04-17	Keeler, James D. et al.	
	257	20080089303	A1	2008-04-17	Wirtanen et al.	
	258	20080095339		2008-04-24	ELLIOTT et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	259	20080096559	A1	2008-04-24	Phillips et al.	
	260	20080098062		2008-04-24	BALIA, Hinal K.	
	261	20080109679		2008-05-08	WRIGHT et al.	
	262	20080120129	A	2008-05-22	Seubert et al.	
	263	20080120668		2008-05-22	Yau, Frank Chuen-Foo	
	264	20080120688		2008-05-22	QIU et al.	
	265	20080125079	A1	2008-05-29	O'Neil et al.	
	266	20080126287	A1	2008-05-29	Cox et al.	
	267	20080127304		2008-05-29	GINTER et al.	
	268	20080130534		2008-06-05	TOMIOKA, Tazuko	
	269	20080130656		2008-06-05	KIM et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	270	20080132201		2008-06-05	KARLBERG, Johan	
	271	20080132268		2008-06-05	CHOI-GROGAN et al.	
	272	20080134330		2008-06-05	KAPOOR et al.	
	273	20080139210	A	2008-06-12	Gisby et al.	
	274	20080147454		2008-06-19	WALKER et al.	
	275	20080160958		2008-07-03	ABICHANDANI et al.	
	276	20080162637		2008-07-03	ADAMCZYK et al.	
	277	20080162704		2008-07-03	POPLETT et al.	
	278	20080164304		2008-07-10	NARASIMHAN et al.	
	279	20080166993	A1	2008-07-10	Gautier et al.	
	280	20080167027		2008-07-10	GAUTIER et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	281	20080167033		2008-07-10	BECKERS, Michel	
	282	20080168275	A1	2008-07-10	DeAtley et al.	
	283	20080168523		2008-07-10	ANSARI et al.	
	284	20080177998		2008-07-24	APSANGI et al.	
	285	20080178300	A1	2008-07-24	Brown et al.	
	286	20080183812		2008-07-31	PAUL et al.	
	287	20080184127		2008-07-31	RAFEY et al.	
	288	20080189760		2008-08-07	ROSENBERG et al.	
	289	20080201266	A	2008-08-21	Chua et al.	
	290	20080207167		2008-08-28	BUGENHAGEN, Michael K.	
	291	20080212470		2008-09-04	CASTANEDA et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	292	20080212751	A1	2008-09-04	Chung, Simon	
	293	20080219268		2008-09-11	DENNISON, Larry R.	
	294	20080221951		2008-09-11	STANFORTH et al.	
	295	20080222692		2008-09-11	ANDERSSON et al.	
	296	20080225748		2008-09-18	KHEMANI et al.	
	297	20080229385		2008-09-18	FEDER et al.	
	298	20080229388		2008-09-18	MAES, Stephane H.	
	299	20080235511		2008-09-25	O'BRIEN, William G. et al.	
	300	20080240373		2008-10-02	WILHELM, Robert 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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	1	2688553	CA	A1	2008-12-04	Yoggie Security Systems, Inc.		
	2	101035308	CN	A	2006-03-09	Huawei Tech. Co. Ltd.		
	3	101080055	CN	A	2007-11-28	Tencent Technology (Shenzhen) Co., Ltd.		
	4	101115248	CN	A	2008-01-30	Lenovo Beijing Ltd.		
	5	101123553	CN	A	2007-09-11	SouTheast University		
	6	101127988	CN	A	2008-02-20	ZTE Corporation		
	7	101155343	CN	B	2006-09-29	Huawei Tech. Co. Ltd.		
	8	101183958	CN	A	2008-05-21	Huawei Tech. Co. Ltd.		
	9	101335666	CN	A	2008-12-31	Hangzhou H3C Technologies Co., Ltd.		
	10	101341764	CN	A	2009-01-07	Telefonaktiebolaget LM Ericsson		
	11	101815275	CN	A	2010-08-25	Yang, Liu		

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	12	1310401	CN	A	2001-08-29	Wang, Di Xing		
	13	1345154A	CN		2002-04-17	Datang Microelectronics Tech. Co.		
	14	1508734	CN	A	2004-06-30	Chinese Creative Corp.		
	15	1538730	CN	A	2004-10-20	Zhongxing Communication Co., Ltd.		
	16	1567818	CN	A	2005-01-19	Huawei Tech. Co. Ltd.		
	17	1801829	CN	A	2006-07-12	Kunda Computer Technology (Kunshan) Co., Ltd.		
	18	1802839	CN	A	2006-07-12	Motorola Inc.		
	19	1867024	CN	A	2006-11-22	Huawei Technologies Co., Ltd.		
	20	1878160	CN	A	2006-12-13	Huawei Technologies Co., Ltd.		
	21	1889777	CN	A	2006-07-19	Huawei Tech. Co. Ltd.		
	22	1937511	CN	A	2007-03-28	ZTE		

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	23	1289326	EP	A1	2003-03-05	Motorola, Inc.		
	24	1463238	EP		2004-09-29	Alcatel		
	25	1503548	EP	A1	2005-02-02	FG Microtec GmbH		
	26	1545114	EP	A1	2005-06-22	Alcatel		
	27	1739518	EP		2007-01-03	Research In Motion Limited		
	28	1772988	EP		2007-04-11	Huawei Technologies Co., Ltd.		
	29	1850575	EP	A1	2007-10-31	Research In Motion		
	30	1887732	EP	A1	2008-02-13	Huawei Technologies Co., Ltd.		
	31	1978772	EP		2008-10-08	British Telecommunications Public Limited Company		
	32	2007065	EP	A1	2008-12-24	Huawei Technologies Co., Ltd.		
	33	2005339247	JP	A	2005-12-08	Secured Communications		

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	34	2006041989	JP		2006-02-09	Fujitsu Ltd.		
	35	2006155263	JP	A	2006-06-15	NEC Corporation		
	36	2006197137	JP		2006-07-27	NTT Docomo Inc.		
	37	2006344007	JP	A	2006-12-21	Hitachi Ltd.		
	38	2007318354	JP	A	2007-12-06	Fujitsu Ten Ltd.		
	39	2008301121	JP	A	2008-12-11	Kyocera Corp.		
	40	2009111919	JP		2009-05-21	Kyocera Communications Systems		
	41	2009212707	JP	A	2009-09-17	Fujitsu Ltd.		
	42	2009218773	JP		2009-09-24	Advanced Telecommunication Research Institute Inte		
	43	2009232107	JP	A	2009-10-08	Fujitsu Ltd.		
	44	3148713	JP	B2	2001-03-26	ATR Kankyo Tekio Tsushin Kenkyusho		

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	45	0208863	WO		2002-01-31	Telemac Corp.		
	46	1998058505	WO		1998-12-23	Sonera Oy		
	47	1999027723	WO		1999-06-03	Telefonaktiebolaget LM Ericsson		
	48	1999065185	WO		1999-12-16	British Telecommunications Public Limited Company		
	49	2002045315	WO	A2	2002-06-06	Micromuse		
	50	2002067616	WO	A1	2002-08-29	Sonera Oyj		

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	"ASA/PIX: Allow Split Tunneling for VPN Clients on the ASA Configuration Example," Document ID 70917, January 10, 2008	
	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	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	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	'Jentro Technologies launches Zenlet platform to accelerate location-based content delivery to mobile devices," The Mobile Internet, Boston, MA, Feb. 2008	
	6	'The Construction of Intelligent Residential District in Use of Cable Television Network," Shandong Science, Vol. 13, No. 2, June 2000	
	7	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	
	8	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	
	9	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	
	10	ALONISTIOTI et al., "Intelligent Architectures Enabling Flexible Service Provision and Adaptability," 2002	
	11	Amazon Technologies, Inc., "Kindle™ User's Guide," 3rd Edition, Copyright 2004-2009	
	12	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)	
	13	Blackberry Mobile Data System, version 4.1, Technical Overview, 2006	
	14	CHANDRASEKHAR et al., "Femtocell Networks: A Survey," June 28, 2008	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	15	CHAOUCHI et al., "Policy Based Networking in the Integration Effort of 4G Networks and Services," 2004 IEEE	
	16	Cisco Systems, Inc., "Cisco Mobile Exchange (CMX) Solution Guide: Chapter 2 - Overview of GSM, GPRS, and UMTS," November 4, 2008	
	17	Client Guide for Symantec Endpoint Protection and Symantec Network Access Control, 2007	
	18	DIKAIAKOS et al., "A Distributed Middleware Infrastructure for Personalized Services," November 24, 2003	
	19	Dixon et al., "Triple Play Digital Services: Comcast and Verizon (Digital Phone, Television, and Internet), August 2007	
	20	Ehnert, "Small application to monitor IP trafic on a Blackberry - 1.01.03 ", March 27, 2008; http://www.ehnert.net/MiniMoni/	
	21	European Commission, "Data Roaming Tariffs - Transparency Measures," obtained from EUROPA - Europe's Information Society Thematic Portal website, June 24, 2011: "http://ec.europa.eu/information_society/activities/roaming/data/measures/index_en.htm."	
	22	FAROOQ et al., "An IEEE 802.16 WiMax Module for the NS-3 Simulator," March 2-6, 2009	
	23	Fujitsu, "Server Push Technology Survey and Bidirectional Communication in HTTP Browser," January 9, 2008 (JP)	
	24	HAN et al., "Information Collection Services for Qos-Aware Mobile Applications," 2005	
	25	HARTMANN et al., "Agent-Based Banking Transactions & Information Retrieval - What About Performance Issues?" 1999	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	26	Hewlett-Packard Development Company, LP, "IP Multimedia Services Charging," white paper, January 2006	
	27	HOSSAIN et al., "Gain-Based Selection of Ambient Media Services in Pervasive Environments," Mobile Networks and Applications. 03 October 2008	
	28	Jing et al., "Client-Server Computing in Mobile Environments," GTE Labs. Inc., Purdue University, ACM Computing Surveys, Vol. 31, No. 2, June 1999	
	29	Kasper et al., "Subscriber Authentication in mobile cellular Networks with virtual software SIM Credentials using Trusted Computing," Fraunhofer-Institute for Secure Information Technology SIT, Darmstadt, Germany; ICACT 2008	
	30	Kassar et al., "An overview of vertical handover decision strategies in heterogeneous wireless networks," ScienceDirect, University Pierre & Marie Curie, Paris, France, 6/5/2007	
	31	Kim, "Free wireless a high-wire act; MetroFi needs to draw enough ads to make service add profits," San Francisco Chronicle, Aug. 21, 2006	
	32	KNIGHT et al., "Layer 2 and 3 Virtual Private Networks: Taxonomy, Technology, and Standarization Efforts," IEEE Communications Magazine, June 2004	
	33	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	
	34	KOUTSOPOULOU et al., "Middleware Platform for the Support of Charging Reconfiguration Actions," 2005	
	35	Kuntze et al., "Trustworthy content push," Fraunhofer-Institute for Secure Information Technology SIT; Germany; WCNC 2007 proceedings, IEEE	
	36	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	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	37	LI, Yu, "Dedicated E-Reading Device: The State of the Art and The Challenges," Scroll, Vol. 1, No. 1, 2008	
	38	Loopt User Guide, metroPCS, 7/17/2008	
	39	Muntermann et al., "Potentiale und Sicherheitsanforderungen mobiler Finanzinformationsdienste und deren Systeminfrastrukturen," Chair of Mobile Commerce & Multilateral Security, Goethe Univ. Frankfurt, 2004	
	40	NetLimiter Lite 4.0.19.0; http://www.heise.de/download/netlimiter-lite-3617703.html from vol. 14/2007	
	41	NILSSON et al., "A Novel MAC Scheme for Solving the QoS Parameter Adjustment Problem in IEEE802.11e EDCA," February 2006	
	42	Nuzman et al., "A compund model for TCP connection arrivals for LAN and WAN applications," Oct. 22, 2002	
	43	Open Mobile Alliance (OMA), Push Architecture, Candidate Version 2.2; Oct. 2, 2007; OMA-AD-Push-V2_2-20071002-C	
	44	OPPLIGER, Rolf, "Internet Security: Firewalls and Bey," Communications of the ACM, May 1997, Vol. 40. No. 5	
	45	RAO et al., "Evolution of Mobile Location-Based Services," Communication of the ACM, December 2003	
	46	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	
	47	Rivadeneyra et al., "A communication architecture to access data services through GSM," San Sebastian, Spain, 1998	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	48	Sabat, "The evolving mobile wireless value chain and market structure," Nov. 2002	
	49	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	
	50	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	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

CERTIFICATION STATEMENT

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

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

OR

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

See attached certification statement.

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

☒ A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/James E. Harris/	Date (YYYY-MM-DD)	2017-08-08
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 (03-15)
Approved for use through 07/31/2016. 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	15582350
Filing Date	2017-04-28
First Named Inventor	Raleigh
Art Unit	2447
Examiner Name	not yet assigned
Attorney Docket Number	RALEP007C11C3C2C3C2

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	7102620	B2	2006-09-05	Harries, Andrew Stanely Guy et al.	
	2	7110753	B2	2006-09-19	Campen, Kenneth Brian	
	3	7113780	B2	2006-09-26	Mckenna Daniel et al.	
	4	7113997		2012-09-26	Jayapalan, Jay et al.	
	5	7133386	B2	2006-11-07	Holur et al.	
	6	7133695	B2	2006-11-07	Beyda, William J.	
	7	7136361	B2	2006-11-14	Benveniste, Mathilde	
	8	7139569	B2	2006-11-21	Kato, Akira	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	9	7142876		2006-11-28	TROSSEN et al.	
	10	7149229	B1	2006-12-12	Leung, Kent K.	
	11	7149521	B2	2006-12-12	Sundar et al.	
	12	7151764	B1	2006-12-19	Heinonen et al.	
	13	7158792		2007-01-02	COOK et al.	
	14	7162237	B1	2007-01-09	Silver et al.	
	15	7167078		2007-01-23	POURCHOT, Shawn C.	
	16	7174156	B1	2007-02-06	Mangal, Manish	
	17	7174174		2007-02-06	BORIS et al.	
	18	7177919	B1	2007-02-13	Truong et al.	
	19	7180855		2007-02-20	LIN , Wei	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	20	7181017		2007-02-20	Nagel, Robert H. et al.	
	21	7191248	B2	2007-03-13	Chattopadhyay et al.	
	22	7197321		2007-03-27	ERSKINE et al.	
	23	7200112	B2	2007-04-03	Sundar et al.	
	24	7203169	B1	2007-04-10	Okholm, Jon et al.	
	25	7203721	B1	2007-04-10	Ben-Efraim et al.	
	26	7203752	B2	2007-04-10	Rice et al.	
	27	7212491		2007-05-01	Koga, Takahiro	
	28	7219123	B1	2007-05-15	Fiechter et al.	
	29	7222190	B2	2007-05-22	Klinker et al.	
	30	7222304	B2	2007-05-22	Beaton et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	31	7224968	B2	2007-05-29	Dobson et al.	
	32	7228354		2007-06-05	CHAMBLISS, David Darden et al.	
	33	7236780		2007-06-26	Benco, David S.	
	34	7242668	B2	2007-07-10	Kan et al.	
	35	7242920		2007-07-10	MORRIS, Robert P.	
	36	7245901		2007-07-17	McGREGOR et al.	
	37	7248570	B2	2007-07-24	Bahl et al.	
	38	7251218		2007-07-31	Jorgensen, Jacob W.	
	39	7260382	B1	2007-08-21	Lamb et al.	
	40	7266371	B1	2007-09-04	Amin et al.	
	41	7269157	B2	2007-09-11	Klinker et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	42	7271765	B2	2007-09-18	Stilp et al.	
	43	7272660	B1	2007-09-18	Powers et al.	
	44	7280816		2007-10-09	FRATTI et al.	
	45	7280818		2007-10-09	CLAYTON, Steve	
	46	7283561		2007-10-16	Picher-Dempsey, Heidi	
	47	7283963		2007-10-16	FITZPATRICK, John E. et al.	
	48	7286834	B2	2007-10-23	Walter	
	49	7286848	B2	2007-10-23	Vireday, Richard P. et al.	
	50	7289489		2007-10-30	KUNG et al.	
	51	7290283		2007-10-30	COPELAND III, John A.	
	52	7310424		2007-12-18	Gehring, Stephan Walter et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	53	7313237	B2	2007-12-25	Bahl, Paramvir et al.	
	54	7317699		2008-01-08	GODFREY et al.	
	55	7318111	B2	2008-01-08	Zhao, Wen	
	56	7320029	B2	2008-01-15	Rinne 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	7336960		2008-02-26	ZAVALKOVSKY et al.	
	61	7340772	B2	2008-03-04	Panasyuk et al.	
	62	7346410		2008-03-18	UCHIYAMA, Kenji	
	63	7349695		2008-03-25	OOMMEN et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	64	7353533		2008-04-01	WRIGHT et al.	
	65	7356011		2008-04-08	Waters, Christopher J.F. et al.	
	66	7356337		2008-04-08	FLORENCE, Shahar	
	67	7366497		2008-04-29	NAGATA, Hideaki	
	68	7366654	B2	2008-04-29	Moore, Robert C.	
	69	7369848	B2	2008-05-06	Jiang, Yue Jun	
	70	7369856	B2	2008-05-06	Ovadia, Shlomo	
	71	7373136		2008-05-13	WATLER et al.	
	72	7373179		2008-05-13	Stine, Ted et al.	
	73	7379731	B2	2008-05-27	Natsuno et al.	
	74	7388950		2008-06-17	ELSEY et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	75	7389412	B2	2008-06-17	Sharma et al.	
	76	7391724	B2	2008-06-24	Alakoski et al.	
	77	7395244	B1	2008-07-01	Kingsford, Bryan	
	78	7401338		2008-07-15	BOWEN et al.	
	79	7403763		2008-07-22	MAES, Stephane H.	
	80	7409447	B	2008-08-05	Assadzadeh, Alireza	
	81	7409569	B2	2008-08-05	Illowsky et al.	
	82	7411930	B2	2008-08-12	Montojo et al.	
	83	7418253		2008-08-26	KAVANAH, Alan	
	84	7418257		2008-08-26	Kim, Myong-Ju	
	85	7421004		2008-09-02	FEHER, Kamilo	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	86	7423971	B1	2008-09-09	Mohaban et al.	
	87	7428750	B1	2008-09-23	Dunn et al.	
	88	7440433	B2	2008-10-21	Rink et al.	
	89	7444669	B1	2008-10-28	Bahl, Paramvir et al.	
	90	7450591		2008-11-11	KORLING et al.	
	91	7450927		2008-11-11	CRESWELL et al.	
	92	7454191	B2	2008-11-18	Dawson et al.	
	93	7457265		2008-11-25	Julka, Vibhor et al.	
	94	7457870	B1	2008-11-25	Lownsbrough et al.	
	95	7460837	B2	2008-12-02	Diener, Neil R.	
	96	7466652	B2	2008-12-16	Lau et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	97	7472189		2008-12-30	Mallya, Arvind R. et al.	
	98	7478420	B2	2009-01-13	Wright, Michael et al.	
	99	7486185		2009-02-03	CULPEPPER et al.	
	100	7486658	B2	2009-02-03	Kumar, Rajneesh	
	101	7493659	B1	2009-02-17	Wu, Handong et al.	
	102	7496652		2009-02-24	Pezzutti, David	
	103	7499438		2009-03-03	Hinman, Brian L. et al.	
	104	7499537		2009-03-03	ELSEY et al.	
	105	7502672	B1	2009-03-10	Kolls, H. Brock	
	106	7505795	B1	2009-03-17	Lim et al.	
	107	7508799	B2	2009-03-24	Sumner et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	108	7512128	B2	2009-03-31	DiMambro et al.	
	109	7512131	B2	2009-03-31	Svensson et al.	
	110	7515608		2009-04-07	Yuan, Yuan et al.	
	111	7515926	B2	2009-04-07	Bu et al.	
	112	7516219		2009-04-07	MOGHADDAM et al.	
	113	7522576	B2	2009-04-21	Du et al.	
	114	7526541	B2	2009-04-28	Roese et al.	
	115	7529204	B2	2009-05-05	Bourlas, Yair et al.	
	116	7535880		2009-05-19	Hinman, Brian L. et al.	
	117	7536695	B2	2009-05-19	Alam et al.	
	118	7539132	B2	2009-05-26	Werner et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	119	7540408	B2	2009-06-02	Levine, Judah et al.	
	120	7545782		2009-06-09	Rayment, Stephen G. et al.	
	121	7546460		2009-06-09	Maes, Stephane H.	
	122	7546629		2009-06-09	ALBERT, Anthony et al.	
	123	7548976	B2	2009-06-16	Bahl, Paramvir et al.	
	124	7551922		2009-06-23	Roskowski, Steve et al.	
	125	7554983	B1	2009-06-30	Muppala, Suresh	
	126	7555757	B2	2009-06-30	Smith et al.	
	127	7561899	B2	2009-07-14	Lee, Changseok	
	128	7562213	B1	2009-07-14	Timms, Natalie	
	129	7564799	B2	2009-07-21	Holland et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	130	7565141		2009-07-21	Macaluso, Anthony G.	
	131	7574509	B2	2009-08-11	Nixon et al.	
	132	7574731		2009-08-11	FASCENDA, Anthony C.	
	133	7577431	B2	2009-08-18	Jiang, Yue Jun	
	134	7580356	B1	2009-08-25	Mishra et al.	
	135	7580857		2009-08-25	VanFLEET et al.	
	136	7583964	B2	2009-09-01	Wong, Gregory A.	
	137	7586871	B2	2009-09-08	Hamilton et al.	
	138	7593417		2009-09-22	Wang, James et al.	
	139	7593730	B2	2009-09-22	Khandelwal, Deepak et al.	
	140	7596373	B2	2009-09-29	Mcgregor, Christopher et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	141	7599288		2009-10-06	COLE, Raymond E. et al.	
	142	7599714	B2	2009-10-06	Kuzminskiy, Alexandr	
	143	7602746	B2	2009-10-13	Calhoun et al.	
	144	7609650		2009-10-27	ROSKOWSKI, Steve et al.	
	145	7609700		2009-10-27	Ying, Wen-Ping et al.	
	146	7610047	B2	2009-10-27	Hicks III et al.	
	147	7610328		2009-10-27	HAASE et al.	
	148	7610396	B2	2009-10-27	Taglienti et al.	
	149	7614051	B	2009-11-03	Glaum et al.	
	150	7616962	B2	2009-11-10	Oswal, Anand K. et al.	
	151	7617516		2009-11-10	HUSLAK et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	152	7620041		2009-11-17	Dunn, Jeffrey H. et al.	
	153	7620065		2009-11-17	FALARDEAU, Eric	
	154	7620162		2009-11-17	AARON et al.	
	155	7627314		2009-12-01	Carlson, Steven I. et al.	
	156	7627767	B2	2009-12-01	Sherman et al.	
	157	7627872	B2	2009-12-01	Hebeler et al.	
	158	7633438		2009-12-15	Tysowski, Piotr Konrad	
	159	7634388		2009-12-15	Archer, Charles J. et al.	Entire Document
	160	7636574		2009-12-22	Poosala, Viswanath	
	161	7636626	B2	2009-12-22	Oesterling et al.	
	162	7643411	B2	2010-01-05	Andreasen et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	163	7644151		2010-01-05	JERRIM, John et al.	
	164	7644267		2010-01-05	YLIKOSKI, Martti et al.	
	165	7647047		2010-01-12	MOGHADDAM et al.	
	166	7650137		2010-01-19	JOBS et al.	
	167	7653394	B2	2010-01-26	McMillin, Brian K.	
	168	7657920	B2	2010-02-02	Arseneau et al.	
	169	7660419	B1	2010-02-09	Ho, Jin-Meng	
	170	7661124	B2	2010-02-09	Ramanathan et al.	
	171	7664494	B2	2010-02-16	Jiang, Yue Jun	
	172	7668176		2010-02-23	Chuah, Mooi Choo	
	173	7668612	B	2010-02-23	Okkonen, Harri	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	174	7668903		2010-02-23	EDWARDS et al.	
	175	7676673	B2	2010-03-09	Weller et al.	
	176	7680086	B2	2010-03-16	Eglin	
	177	7684370	B2	2010-03-23	Kezys, Vytautas Robertas	
	178	7685131		2010-03-23	Batra, Vishal Singh et al.	
	179	7685254		2010-03-23	Pandya, Ashish A.	
	180	7685530	B2	2010-03-23	Sherrard et al.	
	181	7693720		2010-04-06	KENNEWICK et al.	
	182	7697540	B2	2010-04-13	Haddad et al.	
	183	7710932		2010-05-04	MUTHUSWAMY, Sivakumar et al.	
	184	7711848		2010-05-04	MAES, Stephane H.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	185	7719966	B2	2010-05-18	Luft et al.	
	186	7720206	B2	2010-05-18	Devolites et al.	
	187	7720464	B2	2010-05-18	Batta, Puneet	
	188	7720505		2010-05-18	GOPI et al.	
	189	7720960	B2	2010-05-18	Pruss, Richard Manfred et al.	
	190	7724716	B2	2010-05-25	Fadell, Anthony M.	
	191	7725570		2010-05-25	Lewis, Lundy	
	192	7729326		2010-06-01	Sekhar, Ramesh	
	193	7730123		2010-06-01	ERICKSON, Richard R. et al.	
	194	7734784		2010-06-08	ARAUJO et al.	
	195	7742406	B1	2010-06-22	Muppala, Suresh	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	196	7746854		2010-06-29	AMBE, Shekhar et al.	
	197	7747240		2010-06-29	BRISCOE et al.	
	198	7747699		2010-06-29	PRUEITT et al.	
	199	7747730		2010-06-29	HARLOW, James D.	
	200	7752330	B2	2010-07-06	Olsen et al.	
	201	7756056	B2	2010-07-13	Kim et al.	
	202	7756534		2010-07-13	Anupam, Vinod et al.	
	203	7756757	B1	2010-07-13	Oakes III, Charles Lee	
	204	7760137	B2	2010-07-20	Martucci et al.	
	205	7760711	B1	2010-07-20	Kung et al.	
	206	7760861		2010-07-20	Croak, Marian et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	207	7765294	B2	2010-07-27	Edwards et al.	
	208	7769397	B2	2010-08-03	Funato et al.	
	209	7770785	B2	2010-08-10	Jha et al.	
	210	7774323	B2	2010-08-10	Helfman, Nadav	
	211	7774456	B1	2010-08-10	Lownsbrough, Derek Leigh et al.	
	212	7778176		2010-08-17	Morford, Michael Robert	
	213	7778643		2010-08-17	Laroia, Rajiv et al.	
	214	7792257	B1	2010-09-07	Vanier et al.	
	215	7792538		2010-09-07	Kozisek, Steven E.	
	216	7792708		2010-09-07	ALVA, Jessi	
	217	7797060	B2	2010-09-14	Grgic et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	218	7797204		2010-09-14	BALENT, Bruce F.	
	219	7797401		2010-09-14	STEWART et al.	
	220	7801523		2010-09-21	Kenderov, Stoyan	
	221	7801783	B2	2010-09-21	Kende et al.	
	222	7801985	B1	2010-09-21	Pitkow, Jim et al.	
	223	7802724		2010-09-28	Nohr, Steven Paul	
	224	7805140	B2	2010-09-28	Friday et al.	
	225	7805606	B2	2010-09-28	Birger et al.	
	226	7809351	B1	2010-10-05	Panda et al.	
	227	7817615	B1	2010-10-19	Breau et al.	
	228	7817983	B2	2010-10-19	Cassett et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	229	7822837		2010-10-26	URBAN et al.	
	230	7826427	B2	2010-11-02	Sood et al.	
	231	7826607	B1	2010-11-02	De Carvalho Resende et al.	
	232	7843831	B2	2010-11-30	Morrill et al.	
	233	7843843	B1	2010-11-30	Papp III et al.	
	234	7844034	B1	2010-11-30	Oh et al.	
	235	7844728		2010-11-30	ANDERSON, Thomas W. et al.	
	236	7848768		2010-12-07	OMORI et al.	
	237	7849161	B2	2010-12-07	Koch et al.	
	238	7849477	B2	2010-12-07	Cristofalo et al.	
	239	7853255	B2	2010-12-14	Karaoguz et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	240	7856226		2010-12-21	WONG, Ellis L. et al.	
	241	7860088	B2	2010-12-28	Lioy, Marcello	
	242	7865182		2011-01-04	Macaluso, Anthony G.	
	243	7865187	B2	2011-01-04	Ramer et al.	
	244	7868778		2011-01-11	KENWRIGHT, David Norris	
	245	7873001	B2	2011-01-18	Silver, Andrew	
	246	7873344		2011-01-18	BOWSER, Robert et al.	
	247	7873705		2011-01-18	KALISH, Dan	
	248	7877090		2011-01-25	Maes, Stephane H.	
	249	7881199		2011-02-01	KRSTULICH, Zlatko	
	250	7881697	B2	2011-02-01	Baker, Matthew Donald et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	251	7882029		2011-02-01	WHITE, Craig R.	
	252	7882247	B2	2011-02-01	Sturniolo et al.	
	253	7886047		2011-02-08	POTLURI, Dora	
	254	7889384	B2	2011-02-15	Armentrout et al.	
	255	7890084		2011-02-15	Dudziak, Thaddeus Jude et al.	
	256	7890111		2011-02-15	Bugenhagen, Michael K.	
	257	7894431	B2	2011-02-22	Goring et al.	
	258	7899039	B2	2011-03-01	Andreasen et al.	
	259	7899438	B2	2011-03-01	Baker, Matthew Donald et al.	
	260	7903553		2011-03-08	Liu, Enhui	
	261	7907970		2011-03-15	Park, Vincent D. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	262	7911975		2011-03-22	DROZ, Patrick et al.	
	263	7912025		2011-03-22	Pattenden, Christopher E. S. et al.	
	264	7912056		2011-03-22	BRASSEM, Wayne	
	265	7920529		2011-04-05	MAHLER, Roger et al.	
	266	7921463		2011-04-05	Sood, Kapil et al.	
	267	7925740	B2	2011-04-12	Nath et al.	
	268	7925778	B1	2011-04-12	Wijnands et al.	
	269	7929959	B2	2011-04-19	DeAtley, Dallas et al.	
	270	7929960		2011-04-19	MARTIN et al.	
	271	7929973		2011-04-19	Zavalkovsky, Arthur et al.	
	272	7930327	B2	2011-04-19	Craft David et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	273	7930446	B2	2011-04-19	Kesselman, Alex et al.	
	274	7933274	B2	2011-04-26	Verma et al.	
	275	7936736	B2	2011-05-03	Proctor, Jr. et al.	
	276	7937069		2011-05-03	RASSAM, Frederic	
	277	7937450	B2	2011-05-03	Janik, Craig M.	
	278	7940685	B1	2011-05-10	Breslau, Lee et al.	
	279	7940751		2011-05-10	Hansen, Christopher J.	
	280	7941184		2011-05-10	PRENDERGAST et al.	
	281	7944948		2011-05-17	Chow, Albert T. et al.	
	282	7945238	B2	2011-05-17	Baker, Matthew Donald et al.	
	283	7945240		2011-05-17	KLOCK, Jacqueline et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	284	7945945		2011-05-17	Graham, Richard et al.	
	285	7948952		2011-05-24	HURTTA, Tuija et al.	
	286	7948953	B2	2011-05-24	Melkote, Keerti G. et al.	
	287	7948968		2011-05-24	Voit, Eric A. et al.	
	288	7949529		2011-05-24	WEIDER et al.	
	289	7953808		2011-05-31	SHARP et al.	
	290	7953877	B2	2011-05-31	Vemula et al.	
	291	7957020		2011-06-07	MINE, Ryuta et al.	
	292	7957381	B2	2011-06-07	Clermidy et al.	
	293	7957511		2011-06-07	DRUDIS et al.	
	294	7958029	B1	2011-06-07	Bobich et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	295	7962622		2011-06-14	Friend, John et al.	
	296	7965983		2011-06-21	SWAN, Tim et al.	
	297	7966405	B2	2011-06-21	Sundaresan et al.	
	298	7969950	B2	2011-06-28	Iyer, Pradeep J. et al.	
	299	7970350		2011-06-28	SHEYNMAN, Arnold	
	300	7970426		2011-06-28	Poe, Brian R. 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					

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	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	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	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

CERTIFICATION STATEMENT

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

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

OR

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

See attached certification statement.

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

☒ A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/James E. Harris/	Date (YYYY-MM-DD)	2017-08-08
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 (03-15)
Approved for use through 07/31/2016. 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	15582350
Filing Date	2017-04-28
First Named Inventor	Raleigh
Art Unit	2447
Examiner Name	not yet assigned
Attorney Docket Number	RALEP007C11C3C2C3C2

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	7974624		2011-07-05	Gallagher, Michael D. et al.	
	2	7975184		2011-07-05	GOFF et al.	
	3	7978627		2011-07-12	TAYLOR, William Scott et al.	
	4	7978686	B2	2011-07-12	Goyal et al.	
	5	7979069	B2	2011-07-12	Hupp et al.	
	6	7984130		2011-07-19	BOGINENI et al.	
	7	7984511	B2	2011-07-19	Kocher Paul et al.	
	8	7986935		2011-07-26	D'SOUZA et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	9	7987496	B2	2011-07-26	Bryce et al.	
	10	7987510	B2	2011-07-26	Kocher et al.	
	11	7990049	B2	2011-08-02	Shioya, Shunsuke	
	12	8000276	B2	2011-08-16	Scherzer, Shimon et al.	
	13	8000318		2011-08-16	Wiley, William L. et al.	
	14	8005009		2011-08-23	McKee, Neil et al.	
	15	8005459		2011-08-23	BALSILLIE, Jim	
	16	8005726	B1	2011-08-23	Bao, Yulin	
	17	8005913	B1	2011-08-23	Carlander, Carrie	
	18	8005988		2011-08-23	MAES, Stephane H.	
	19	8010080		2011-08-30	THENTHIRUPERAI et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	20	8010081		2011-08-30	ROSKOWSKI, Steve	
	21	8010082	B2	2011-08-30	Sutaria et al.	
	22	8010990	B2	2011-08-30	Ferguson et al.	
	23	8015133		2011-09-06	WU et al.	
	24	8015234		2011-09-06	LUM et al.	
	25	8019687		2011-09-13	WANG et al.	
	26	8019820		2011-09-13	Son, Giyeong et al.	
	27	8019846	B2	2011-09-13	Roelens et al.	
	28	8019868		2011-09-13	RAO, Goutham et al.	
	29	8023425		2011-09-20	RALEIGH, Gregory G.	
	30	8024397		2011-09-20	ERICKSON, Richard R. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	31	8027339	B2	2011-09-27	Short, Joel E. et al.	
	32	8031601	B2	2011-10-04	Feroz et al.	
	33	8032168	B2	2011-10-04	Ikaheimo, Jorma	
	34	8032409	B1	2011-10-04	Mikurak, Michael G.	
	35	8032899	B2	2011-10-04	Archer, Charles J. et al.	
	36	8036387	B2	2011-10-11	Kudelski et al.	
	37	8044792	B2	2011-10-25	Orr et al.	
	38	8045973	B2	2011-10-25	Chambers, Michael D.	
	39	8046449	B2	2011-10-25	Yoshiuchi, Hideya	
	40	8050275		2011-11-01	IYER, Jayaraman R.	
	41	8050690	B2	2011-11-01	Neeraj, Chawla	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	42	8050705	B2	2011-11-01	Sicher et al.	
	43	8059530		2011-11-15	Cole, Terry L.	
	44	8060463		2011-11-15	Spiegel, Joel R.	
	45	8064418	B2	2011-11-22	Maki, Lasse	
	46	8065365	B2	2011-11-22	Saxena et al.	
	47	8068824		2011-11-29	SHAN, Xueshan et al.	
	48	8068829	B2	2011-11-29	Lemond, Eric et al.	
	49	8073427	B2	2011-12-06	Koch et al.	
	50	8073721		2011-12-06	Lewis, Lundy	
	51	8078140	B2	2011-12-13	Baker, Matthew Donald et al.	
	52	8078163	B2	2011-12-13	Lemond, Eric et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	53	8085808	B2	2011-12-27	Brusca et al.	
	54	8086398	B2	2011-12-27	Sanchez et al.	
	55	8086497	B1	2011-12-27	Oakes III, Charles Lee	
	56	8086791	B2	2011-12-27	Caulkins, Jason	
	57	8090359		2012-01-03	Proctor Jr., James Arthur et al.	
	58	8090616		2012-01-03	Proctor Jr., James Arthur et al.	
	59	8094551		2012-01-10	HUBER, Kurt Donald et al.	
	60	8095112	B2	2012-01-10	Chow, Richard et al.	
	61	8095640	B2	2012-01-10	Guingo et al.	
	62	8095666		2012-01-10	SCHMIDT et al.	
	63	8098579		2012-01-17	Ray, Amar N. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	64	8099077		2012-01-17	CHOWDHURY et al.	
	65	8099517		2012-01-17	JIA et al.	
	66	8102814		2012-01-24	RAHMAN, Shahriar I. et al.	
	67	8103285	B2	2012-01-24	Kalhan, Amit	
	68	8104080	B2	2012-01-24	Burns et al.	
	69	8107953	B2	2012-01-31	Zimmerman et al.	
	70	8108520		2012-01-31	Ruutu, Jussi et al.	
	71	8112435	B2	2012-02-07	Epstein et al.	
	72	8116223		2012-02-14	TIAN, Dan et al.	
	73	8116749		2012-02-14	Proctor Jr., James Arthur et al.	
	74	8116781	B2	2012-02-14	Chen, Xixian et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	75	8122128		2012-02-21	Burke, II, Robert M. et al.	
	76	8122249		2012-02-21	Falk, Rainer et al.	
	77	8125897	B2	2012-02-28	Ray et al.	
	78	8126123		2012-02-28	Cai, Yigang et al.	
	79	8126396	B2	2012-02-28	Bennett, James D.	
	80	8126476	B2	2012-02-28	Vardi, Yosef et al.	
	81	8126722		2010-02-28	ROBB, Terence Alan et al.	
	82	8130793	B2	2012-03-06	Edwards, Stephen K. et al.	
	83	8131256		2012-03-06	MARTTI, Jyrki et al.	
	84	8131281	B1	2012-03-06	Hildner et al.	
	85	8131840	B1	2012-03-06	Denker, Richard E.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	86	8131858	B2	2012-03-06	Agulnik et al.	
	87	8132256	B2	2012-03-06	Bari, Farooq	
	88	8134954	B2	2012-03-13	Godfrey, James A. et al.	
	89	8135388		2012-03-13	Gailloux, Michael A. et al.	
	90	8135392		2012-03-13	MARCELLINO et al.	
	91	8135657		2012-03-13	Kapoor, Harsh et al.	
	92	8140690	B2	2012-03-20	Ly et al.	
	93	8144591		2012-03-27	GHAI et al.	
	94	8145194	B2	2012-03-27	Yoshikawa et al.	
	95	8149823		2012-04-03	Turcan, Diane Brown et al.	
	96	8150394	B2	2012-04-03	Bianconi et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	97	8150431		2012-04-03	Wolovitz, Lionel et al.	
	98	8151205	B2	2012-04-03	Follmann et al.	
	99	8155155		2012-04-10	Chow, Albert T. et al.	
	100	8155620		2012-04-10	Wang, Jun et al.	
	101	8155666	B2	2012-04-10	Alizadeh-Shabdiz, Farshid	
	102	8155670		2012-04-10	Fullam, Scott et al.	
	103	8156206		2012-04-10	KILEY, Kevin J. et al.	
	104	8159520	B1	2012-04-17	Dhanoa et al.	
	105	8160056	B2	2012-04-17	Van der Merwe et al.	
	106	8160598	B2	2012-04-17	Savoor, Raghvendra	
	107	8165576		2012-04-24	Raju, Vishwanath et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	108	8166040	B2	2012-04-24	Brindisi, Richard G. et al.	
	109	8166554	B2	2012-04-24	John, Pramod	
	110	8170553		2012-05-01	BENNETT, James D.	
	111	8174378	B2	2012-05-08	Richman et al.	
	112	8174970	B2	2012-05-12	Adamczyk, Maria et al.	
	113	8175574	B1	2012-05-08	Panda et al.	
	114	8180881	B2	2012-05-15	Seo et al.	
	115	8180886	B2	2012-05-15	Overcash et al.	
	116	8184530		2012-05-22	SWAN, Tim L. et al.	
	117	8184590		2012-05-22	Rosenblatt, Ariel	
	118	8185093		2012-05-22	Uheng, Yu-Syuan et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	119	8185127	B1	2012-05-22	Cai, Zheng et al.	
	120	8185152		2012-05-22	GOLDNER, Alla	
	121	8185158		2012-05-22	Tamura, Motoshi et al.	
	122	8190122	B1	2012-05-29	Alexander et al.	
	123	8190675		2012-05-29	TRIBBETT, David	
	124	8191106	B2	2012-05-29	Choyi et al.	
	125	8191116		2012-05-29	Gazzard, Daryl	
	126	8191124	B2	2012-05-29	Wynn et al.	
	127	8194549	B2	2012-06-05	Huber et al.	
	128	8194553		2012-06-05	LIANG, Zhi Yong et al.	
	129	8194581	B1	2012-06-05	Schroeder et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	130	8195153	B1	2012-06-05	Frencel et al.	
	131	8195163	B2	2012-06-05	Gisby, Doug et al.	
	132	8195661	B2	2012-06-05	Kalavade, Asawaree	
	133	8196199	B2	2012-06-05	Hrastar et al.	
	134	8200163	B2	2012-06-12	Hoffman, George E.	
	135	8200200	B1	2012-06-12	Belser et al.	
	136	8200509	B2	2012-06-12	Kenedy, Andrew Alexander et al.	
	137	8200775		2012-06-12	MOORE, James F.	
	138	8200818	B2	2012-06-12	Freund et al.	
	139	8204190		2012-06-19	Bang, Jung-Hee et al.	
	140	8204505	B2	2012-06-19	Jin et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	141	8208788	B2	2012-06-26	Ando et al.	
	142	8208919		2012-06-26	KOTECHA, Lalit Ratilal	
	143	8213296		2012-07-03	SHANNON, Frank M. et al.	
	144	8213363		2012-07-03	Ying, Wen-Ping et al.	
	145	8214536		2012-07-03	ZHAO, Wen	
	146	8219134	B2	2012-07-10	Maharajh et al.	
	147	8223655	B2	2012-07-17	Heinz et al.	
	148	8224382		2012-07-17	Bultman, Michael J.	
	149	8224773		2012-07-17	Spiegel, Joel R.	
	150	8228818	B2	2012-07-24	Chase et al.	
	151	8229394	B2	2012-07-24	Karlberg, Johan	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	152	8229914	B2	2012-07-24	Ramer et al.	
	153	8233433	B2	2012-07-31	Kalhan, Amit	
	154	8233883		2012-07-31	De Froment, Eric	
	155	8233895		2012-07-31	Tysowski, Piotr Konrad	
	156	8238287		2012-08-07	Gopi, Paramesh et al.	
	157	8239520		2012-08-07	GRAH, Adrian	
	158	8242959	B2	2012-08-14	Mia, Rashidus S. et al.	
	159	8244241		2012-08-14	Montemurro, Michael	
	160	8249601	B2	2012-08-21	Emberson et al.	
	161	8254880	B2	2012-08-28	Aaltonen et al.	
	162	8254915		2012-08-28	Kozisek, Steven E.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	163	8255515		2012-08-28	MELMAN, David et al.	
	164	8255534	B2	2012-08-28	Assadzadeh, Alireza	
	165	8255689		2012-08-28	KIM, Eun Ah et al.	
	166	8259692	B2	2012-09-04	Bajko, Gabor	
	167	8264965	B2	2012-09-11	Dolganow et al.	
	168	8265004		2012-09-11	Toutonghi, Michael J.	
	169	8266681		2012-09-11	Deshpande, Sumit B. et al.	
	170	8270955	B2	2012-09-18	Ramer et al.	
	171	8270972	B2	2012-09-18	Otting, Marcia J. et al.	
	172	8271025	B2	2012-09-18	Brisebois et al.	
	173	8271045		2012-09-18	Parolkar, Satish et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	174	8271049		2012-09-18	SILVER, Andrew et al.	
	175	8271992	B2	2012-09-18	Chatley, Scott P. et al.	
	176	8275415	B2	2012-09-25	Huslak, Nicholas S.	
	177	8279067		2012-10-02	BERGER, Thomas R. et al.	
	178	8279864		2012-10-02	Wood, Daniel M.	
	179	8280354		2012-10-02	Smith, Christopher et al.	
	180	8284740		2012-10-09	O'CONNOR, Dennis M.	
	181	8285249	B2	2012-10-09	Baker, Matthew Donald et al.	
	182	8291238		2012-10-16	GINTER, Karl L. et al.	
	183	8291439	B2	2012-10-16	Jethi et al.	
	184	8296404		2012-10-23	McDysan, Dave et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	185	8300575	B2	2012-10-30	Willars, Per	
	186	8307067	B2	2012-11-06	Ryan, Nicholas M.	
	187	8315198	B2	2012-11-20	Corneille et al.	
	188	8315593	B2	2012-11-20	Gallant et al.	
	189	8315999	B2	2012-11-20	Chatley, Scott P. et al.	
	190	8320244	B2	2012-11-27	Muqattash et al.	
	191	8320949		2012-11-27	Matta, Sudheer Poorna Chandra	
	192	8325638		2012-12-04	Jin, Haipeng et al.	
	193	8325906	B2	2012-12-04	Fullarton et al.	
	194	8326319	B2	2012-12-04	Davis, Richard W.	
	195	8326828	B2	2012-12-04	Zhou et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	196	8331223	B2	2012-12-11	Hill et al.	
	197	8331293		2012-12-11	Sood, Kapil	
	198	8332375		2012-12-11	Chatley, Scott P. et al.	
	199	8339991	B2	2012-12-25	Biswas et al.	
	200	8340678	B1	2012-12-25	Pandey, Vinod	
	201	8340718		2012-12-25	Colonna, Massimo et al.	
	202	8346210	B2	2013-01-01	Balsan et al.	
	203	8347104	B2	2013-01-01	Pathiyal, Krishna K.	
	204	8347378	B2	2013-01-01	Merkin et al.	
	205	8350700		2013-01-08	Fast, Raymond D. et al.	
	206	8351592	B2	2013-01-08	Freeny Jr et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	207	8351898	B2	2013-01-08	Raleigh, Gregory G.	
	208	8352360	B2	2013-01-08	De Judicibus et al.	
	209	8352980		2013-01-08	Howcroft, Jerald Robert	
	210	8355696	B1	2013-01-15	Olding et al.	
	211	8356336	B2	2013-01-15	Johnston, Keith et al.	
	212	8358638	B2	2013-01-22	Scherzer, Tamir et al.	
	213	8358975	B2	2013-01-22	Bahl et al.	
	214	8363658		2013-01-29	Delker, Jason R. et al.	
	215	8363799	B2	2013-01-29	Gruchala et al.	
	216	8364806		2013-01-29	Short, Joel E. et al.	
	217	8370477		2013-02-05	Short, Joel E. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	218	8370483	B	2013-02-05	Choong Jason et al.	
	219	8374090		2013-02-12	Morrill, Robert J. et al.	
	220	8374592		2013-02-12	Proctor, Jr. James A. et al.	
	221	8375128	B2	2013-02-12	Tofighbakhsh et al.	
	222	8375136	B2	2013-02-12	Roman et al.	
	223	8380247	B2	2013-02-19	Engstrom	
	224	8385199	B1	2013-02-26	Coward et al.	
	225	8385896		2013-02-26	Proctor Jr., James A. et al.	
	226	8385964	B2	2013-02-26	Haney, Richard D.	
	227	8386386		2013-02-26	Zhu, Kevin	
	228	8396929		2013-03-12	Helfman, Nadav et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	229	8402165	B2	2013-03-19	Deu-Ngoc et al.	
	230	8402540		2013-03-19	Kapoor, Harsh et al.	
	231	8406736	B2	2013-03-26	Das et al.	
	232	8407763	B2	2013-03-26	Weller et al.	
	233	8411587		2013-04-02	Curtis, William et al.	
	234	8411691	B2	2013-04-02	Aggarwal	
	235	8418168	B2	2013-04-09	Tyhurst et al.	
	236	8423016		2013-04-16	BUCKLEY, Adrian et al.	
	237	8429403		2013-04-23	Moret, Eric et al.	
	238	8437734		2013-05-07	Ray, Amar N. et al.	
	239	8442015	B2	2013-05-14	Behzad et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	240	8446831	B2	2013-05-21	Kwan et al.	
	241	8447607	B2	2013-05-21	Weider, Chris et al.	
	242	8447980		2013-05-21	Godfrey, James A. et al.	
	243	8448015	B2	2013-05-21	Gerhart, David	
	244	8461958	B2	2013-06-11	Saenz et al.	
	245	8463232	B2	2013-06-11	Tuli et al.	
	246	8468337	B2	2013-06-18	Gaur, Santosh P. et al.	
	247	8472371		2013-06-25	Bari, Farooq et al.	
	248	8477778		2013-07-02	Lehmann Jr., L. Curtis et al.	
	249	8483135		2013-07-09	Cai, Yigang et al.	
	250	8483694	B2	2013-07-09	Lewis et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	251	8484327	B2	2013-07-09	Werner et al.	
	252	8488597	B2	2013-07-16	Nie et al.	
	253	8489110	B2	2013-07-16	Frank et al.	
	254	8489720	B1	2013-07-16	Morford, Michael et al.	
	255	8494559	B1	2013-07-23	Malmi	
	256	8495181	B2	2013-07-23	Venkatraman et al.	
	257	8495227		2013-07-23	Kaminsky, David L. et al.	
	258	8495360		2013-07-23	Falk, Rainer et al.	
	259	8495700	B2	2013-07-23	Shahbazi, Majid	
	260	8503358	B2	2013-08-06	Hanson et al.	
	261	8503455	B2	2013-08-06	Heikens, Heico	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	262	8504032	B2	2013-08-06	Lott et al.	
	263	8504687	B2	2013-08-06	Maffione et al.	
	264	8504729		2013-08-06	Pezzutti, David A.	
	265	8505073	B2	2013-08-06	Taglienti et al.	
	266	8509082	B2	2013-08-13	Heinz, John M. et al.	
	267	8514927	B2	2013-08-20	Sundararajan et al.	
	268	8520589		2013-08-27	Bhatt, Yogesh et al.	
	269	8521110		2013-08-27	Rofougaran, Ahmadreza	
	270	8521775	B1	2013-08-27	Poh et al.	
	271	8522039	B2	2013-08-27	Hyndman et al.	
	272	8522249	B2	2013-08-27	Beaule, Stephane	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	273	8522337	B2	2013-08-27	Adusumilli et al.	
	274	8523547	B2	2013-09-03	Pekrul, Merton W.	
	275	8526329	B2	2013-09-03	Mahany, Ronald L. et al.	
	276	8526350	B2	2013-09-03	Xue, Qi et al.	
	277	8527410	B2	2013-09-03	Markki et al.	
	278	8527662	B2	2013-09-03	Biswas et al.	
	279	8528068	B1	2013-09-03	Weglein et al.	
	280	8531954	B2	2013-09-10	McNaughton et al.	
	281	8532610	B2	2013-09-10	Manning Cassett et al.	
	282	8533775	B2	2013-09-10	Alcorn et al.	
	283	8538394	B2	2013-09-17	Zimmerman et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	284	8538421	B2	2013-09-17	Brisebois et al.	
	285	8538458	B2	2013-09-17	Haney, Richard D.	
	286	8539544	B2	2013-09-17	Garimella et al.	
	287	8543265	B2	2013-09-24	Ekhaguere et al.	
	288	8543814	B2	2013-09-24	Laitinen et al.	
	289	8544105	B2	2013-09-24	Mclean et al.	
	290	8548427	B2	2013-10-01	Chow et al.	
	291	8554876	B2	2013-10-08	Winsor, Gerald W.	
	292	8561138	B2	2013-10-15	Rothman, Michael M. et al.	
	293	8565746	B2	2013-10-22	Hoffman, George E.	
	294	8566236	B2	2013-10-22	Busch, James David	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	295	8571474	B2	2013-10-29	Chavez et al.	
	296	8571501	B2	2013-10-29	Miller et al.	
	297	8571598	B2	2013-10-29	Valavi, John J.	
	298	8571993	B2	2013-10-29	Kocher et al.	
	299	8572117	B2	2013-10-29	Rappaport, Theodore S.	
	300	8572256	B2	2013-10-29	Babbar, Uppinder Singh	

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]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	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	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

CERTIFICATION STATEMENT

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

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

OR

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

See attached certification statement.

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

☒ A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/James E. Harris/	Date (YYYY-MM-DD)	2017-08-08
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 (03-15)
Approved for use through 07/31/2016. 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	15582350
Filing Date	2017-04-28
First Named Inventor	Raleigh
Art Unit	2447
Examiner Name	not yet assigned
Attorney Docket Number	RALEP007C11C3C2C3C2

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	8583499		2013-11-12	De Judicibus, Dario et al.	
	2	8589955	B2	2013-11-19	Roundtree et al.	
	3	8600895	B2	2013-12-03	Felsher, David Paul	
	4	8601125	B2	2013-12-03	Huang et al.	
	5	8605691	B2	2013-12-10	Soomro et al.	
	6	8634425	B2	2014-01-21	Gorti et al.	
	7	8635164	B2	2014-01-21	Rosenhaft et al.	
	8	8639215	B2	2014-01-28	McGregor et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	9	8644702	B1	2014-02-04	Kalajan, Kevin E.	
	10	8644813	B1	2014-02-04	Gailloux et al.	
	11	8645518	B	2014-02-04	David, Scott L.	
	12	8655357	B1	2014-02-18	Gazzard et al.	
	13	8660853	B2	2014-02-25	Robb et al.	
	14	8666395	B2	2014-03-04	Silver, Andrew	
	15	8667542	B1	2014-03-04	Bertz et al.	
	16	8670334	B	2014-03-11	Keohane et al.	
	17	8675852	B2	2014-03-18	Maes, Stephane H.	
	18	8676925	B	2014-03-18	Liu et al.	
	19	8693323		2014-04-08	McDysan, David E.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	20	8694772	B2	2014-04-08	Kao et al.	
	21	8700729	B2	2014-04-15	Dua, Robin	
	22	8701015	B2	2014-04-15	Bonnat, Pierre	
	23	8706863		2014-04-22	Fadell, Anthony	
	24	8713535	B2	2014-04-29	Malhotra et al.	
	25	8713641	B1	2014-04-29	Pagan et al.	
	26	8719397	B2	2014-05-06	Levi et al.	
	27	8719423	B2	2014-05-06	Wyld	
	28	8725899	B	2014-05-13	Short et al.	
	29	8730842	B2	2014-05-20	Collins et al.	
	30	8731519	B2	2014-05-20	Flynn et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	31	8732808	B2	2014-05-20	Sewall et al.	
	32	8739035	B2	2014-05-27	Trethewey, Jim	
	33	8744339	B2	2014-06-03	Halfmann et al.	
	34	8761711	B2	2014-06-24	Grignani et al.	
	35	8780857	B2	2014-07-15	Balasubramanian et al.	
	36	8787249	B2	2014-07-22	Giaretta et al.	
	37	8793304	B2	2014-07-29	Lu et al.	
	38	8811338	B2	2014-08-19	Jin et al.	
	39	8811991	B2	2014-08-19	Jain et al.	
	40	8819253	B2	2014-08-26	Simeloff et al.	
	41	8825109	B2	2014-09-02	Montemurro et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	42	8826411	B2	2014-09-02	Moen et al.	
	43	8831561	B2	2014-09-09	Sutaria et al.	
	44	8838752	B2	2014-09-16	Lor et al.	
	45	8855620	B2	2014-10-07	Sievers et al.	
	46	8862751	B2	2014-10-14	Faccin et al.	
	47	8875042	B2	2014-10-28	LeJeune et al.	
	48	8880047	B2	2014-11-04	Konicek et al.	
	49	8908516	B2	2014-12-09	Tzamaloukas et al.	
	50	8930238	B2	2015-01-06	Coffman et al.	
	51	8943551	B2	2015-01-27	Ganapathy et al.	
	52	8948726	B2	2015-02-03	Smith et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	53	8966018	B2	2015-02-24	Bugwadia et al.	
	54	8971912	B2	2015-03-03	Chou et al.	
	55	8977284	B2	2015-03-10	Reed, Mark J.	
	56	8995952	B1	2015-03-31	Baker et al.	
	57	9002342	B2	2015-04-07	Tenhunen et al.	
	58	9014973	B2	2015-04-21	Ruckart, John	
	59	9015331	B2	2015-04-21	Lai et al.	
	60	9030934	B2	2015-05-12	Shah et al.	
	61	9049010		2015-06-02	Jueneman et al.	
	62	9111088	B2	2015-08-18	Ghai et al.	
	63	9172553	B2	2015-10-27	Dawes et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	64	9325737	B2	2016-04-26	Gutowski et al.	
	65	9326173	B2	2016-04-26	Luft, Achim	
	66	9344557	B2	2016-05-17	Gruchala et al.	
	67	9367680	B2	2016-06-14	Mahaffey et al.	
	68	9413546	B2	2016-08-09	Meier et al.	
	69	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

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]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

	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	15582350
	Filing Date	2017-04-28
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C3C2

CERTIFICATION STATEMENT

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

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

OR

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

See attached certification statement.

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

☒ A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/James E. Harris/	Date (YYYY-MM-DD)	2017-08-08
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.

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
9 June 2005 (09.06.2005)

PCT

(10) International Publication Number
WO 2005/053335 A1

(51) International Patent Classification[7]: H04Q 7/32

(21) International Application Number:
PCT/EP2004/013101

(22) International Filing Date:
19 November 2004 (19.11.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/724,569 26 November 2003 (26.11.2003) US

(71) Applicant *(for all designated States except US)*: **NOKIA CORPORATION** [FI/FI]; Keilalahdentie 4, FIN-02150 Espoo (FI).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **ENGELS, Ralf** [DE/DE]; Im Mittelbühl 26, 89160 Dornstadt (DE).

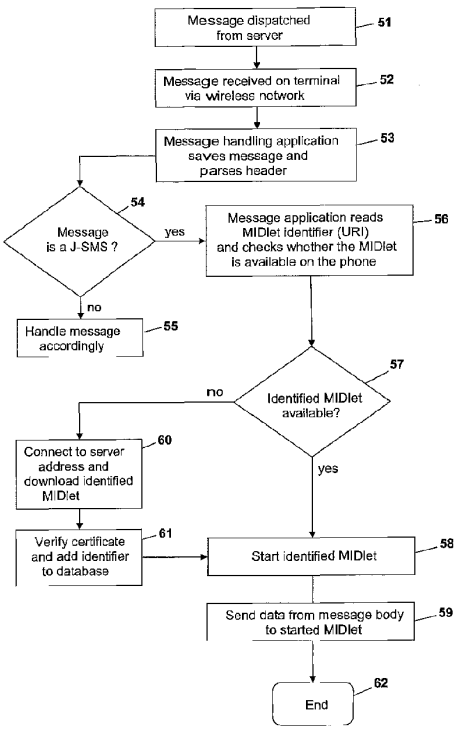
(74) Agent: **VAN WALSTIJN, B., Gerard, G.**; Walstijn Intellectual Property ApS, Parkovsvej 3, DK-2820 Gentofte (DK).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI,

[Continued on next page]

(54) Title: FLEXIBLE MESSAGING SYSTEM



(57) Abstract: A universal messaging system for wireless networks that can handle a great variety of different content. The messaging system operates with messages that include an application identifier in the header for an application in platform independent code. The message body contains data to be used by the identified application. The mobile terminals for operation on the wireless network are provided with native software and with a virtual machine capable of executing platform independent code. The identifier allows the mobile terminal to start the correct application for using the data contained in the message body. A uniform recourse identifier (URI) is used to identify the application and to provide an address at which the application can be downloaded if it is not yet available on the message receiving mobile terminal.

WO 2005/053335 A1

FR, GB, GR, HU, IE, IS, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

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

FLEXIBLE MESSAGING SYSTEM

The present invention relates to the use of messaging for sending and receiving various items in a wireless communication network.

BACKGROUND ART

Smart Messaging is a concept developed by Nokia for sending and receiving ring tones, picture messages, operator logos, business cards, calendar requests, and Internet settings over the Short Message Service (SMS). Since its introduction in 1997, Smart Messaging has become an extremely popular terminal-specific content delivery technology and the de facto standard for the industry. Examples of different SMS type messages are: Business Card format, Calendar format, Ringing tone format, OTA Bitmap format, CLI Icon format, Operator logo format, Picture Message format and Downloadable Profile message format. There are advanced message types that allow e.g. a network operator to send a complex set of configuration information like "GPRS settings" to a mobile phone. The software on the phones presently on the market is programmed to handle, on average, about 6 to 8 of these different message types. The message types that a phone can handle is determined by the manufacturer, depending on the target customer group, since it is not realistic to attempt to provide a phone that can handle all available message types.

There is presently a fast increase in the number of applications for mobile phones, such as e.g. background images, screen savers, location based services, financial services, operator controlled updating or settings/phonebook contents, etc. that have created a need to increase in the number of message types. It is

CONFIRMATION COPY

however problematical to harmonize these message types between the different phone manufacturers, despite the dominance of the Nokia Smart Messaging Concept. The present SMS standard may be augmented as described below to provide for more flexible handling of increasing demand.

Accordingly, a need exists for a universal messaging system for wireless networks that can handle a great variety of different content.

DISCLOSURE OF THE INVENTION

The devices and method described below provide for a method of handling incoming messages received on a mobile communication terminal via a wireless network, the terminal having native software and a virtual machine capable of executing applications in platform independent object code. The method comprises the step of receiving and storing a message that comprises a header and a message body. The header contains an identifier for an application in platform independent object code to be executed by the virtual machine. In the next step it is verified if the identified application is available on the terminal, and the identified application is started when available on the terminal.

Thus, the terminal is able to automatically start the application required for using the data in the message body of a received message, regardless of the type and version of the native software of the terminal unless the required application is not available on the terminal. Therefore, the header may further contain an address at which the identified application can be downloaded from a server that is accessible through the wireless network, and the method further comprises the steps of connecting

to the terminal to the server at the address contained in the header, downloading the identified application when the identified application was not available on the terminal, and starting the identified application when downloaded.

Thus, the required application can automatically be downloaded if it is not already available on the terminal. Since the application is in platform independent object code, there is no platform compatibility problems, and because the download address is contained in the header the user does not need to search for it.

Preferably, the message body contains data to be used by the identified application.

The platform independent object code can be Java™, in particular Java™ 2 Platform, Micro Edition (J2METM) from Sun Microsystems Inc. but other platform independent object codes can be used.

The virtual machine preferably is a K Virtual Machine™ (KVM). The identified application can be a Java™ application, a Java™ applet or a Java™ MIDlet.

The devices and method described below provide for a mobile communication terminal that can operate with a flexible messaging concept for a wireless network. This terminal has native software and a virtual machine. The virtual machine is capable of executing applications in platform independent object code. The terminal also has a message handling application in the native software or in an application run by the virtual machine. The message handling application is capable of sending and receiving messages via the wireless network, and the

message handling application is programmed to start an application written in the independent object code when a corresponding identifier is contained the header of a received message.

Thus, the terminal is able to automatically start the application required for using the data in the message body of a received message, regardless of the type and version of the native software of the terminal if the required application is available on the terminal.

The message handling application can also be programmed to download the identified application from a server that is accessible via the wireless network at an address contained in the header when the identified application is not already available on the terminal.

The message handling application is programmed to verify the certification of the downloaded application.

The mobile communication terminal may further comprise an application identifier database listing the identifiers of all the applications in platform independent object code that are available on the terminal.

The message to be used with a flexible messaging concept for mobile terminals that operate on a wireless network is describe in detail below, and provides a format suitable for transmission through a wireless network to a mobile communication terminal, the terminal having native software and an virtual machine capable of handling platform independent object code and the message having a syntax comprising a header part and message body part. The header contains an identifier for an application in platform independent object code to be executed by the

virtual machine in the mobile communication terminal that receives the message.

Preferably, the header includes an address at which the identified application can be downloaded from a server that is accessible through the wireless network. The message body may contain data to be used by the identified application.

The message header may include a URI that serves as identifier and contains the address at which the identified application can be downloaded from a server.

The message can be an SMS message with a port address in octets 4-5 that identifies it as a message containing an identifier for an application in platform independent object code to be started upon receipt of the message. The identified application can be a Java™ applet or MIDlet, preferably in the Java™ 2, Micro Edition, Mobile Information Device Profile (MIDP) format.

The message may also contain a signed certificate issued by a recognized certification authority and including a public key from the signatory. In addition, the message may include field communication of an unique sender identifier in the form of a telephone number of an originating mobile phone, or other unique identifier for mobile terminals and/or computers.

On this background, it is an object of the present invention to provide.

With the system described herein, a flexible messaging method for mobile terminals that operate on a wireless network achieved by providing a method of enabling an application in platform independent object code to be run

on a mobile communication terminal comprising the steps of sending a message from a server via the wireless network to a mobile communication terminal, the terminal being provided with a virtual machine capable of executing applications in platform independent object code. The message contains a header with an identifier for the application to be started on the mobile communication terminal and a message body with the data to be used by the identified application.

Thus, the system and methods described herein make it possible to send a message with data to be used by a specific application to a mobile communication terminal, without needing to know first which platform is installed in the terminal.

The message header may further contain an address at which the identified application can be obtained from a server that is accessible through the wireless network, and thus the method may further comprise the step of uploading the identified application to the mobile communication terminal when the mobile terminal connects to the server at the address in the header.

Thus, it is rendered possible to transfer an application to a mobile terminal without being required to know the platform installed on the terminal. There is also no risk of installing the application twice on the same terminal.

Further objects, features, advantages and properties of the flexible messaging system according to the invention will become apparent from the detailed description.

BRIEF DESCRIPTION OF THE DRAWINGS

In the following detailed portion of the present description, the invention will be explained in more detail with reference to the exemplary embodiments shown in the drawings, in which

Fig. 1 shows the architecture of a wireless cellular communication network for use with the present invention,
Fig. 2 shows a mobile phone in accordance with the present invention,
Fig. 3 is a block diagram showing the basic components of the mobile phone of Fig. 2,
Fig. 4 shows the software architecture of the mobile phone of Fig. 2,
Fig. 5 is a flowchart illustrating the message handling procedure according to a preferred embodiment of the present invention,
Fig. 6 shows a sequence diagram of an example of the use of the flexible messaging system according to the invention, and
Fig. 7 shows a sequence diagram of a further example of the use of the flexible messaging system according to the invention.

DETAILED DESCRIPTION

Fig. 1 illustrates a network architecture for use with the present invention. The telecommunication system includes a wireless cellular network 16 and a data network 24. The wireless cellular network 16 can be implemented in a conventional wireless cellular telephone network that has been enhanced to carry data. A wireless network capable of carrying circuit-switched data can be used for this purpose. More preferably, however, the wireless cellular network provides a packet-switched data

service. An example of a wireless infrastructure includes UMTS (Universal Mobile Telephone System), a 3rd Generation wireless system based on GSM (Global System for Mobile communications). GSM adds a packet network overlay known as GRPS (GSM Packet Radio Service) to a wireless circuit voice network. The data network can e.g. be the Internet.

The cellular network comprises a large number of base stations 20 (only two are shown) that are provided with a transceiver for handling mobile phone communications. The base stations 20 are connected to a mobile switching centre 21. Each of the base stations 20 has its own control channel frequency (control channel frequencies can be reused for distant cells).

The base stations 20 are provided with an SMS/MMS message controller (not shown) and an SMS/MMS message transmission driver to allow it to send message to a mobile phone 1 and to receive messages from a mobile phone 1.

The mobile switching centre 21 is connected to a data 22 switching node that connects the cellular communication network 16 with the data network 24. Different servers 25,26,27,28 described in more detail below, are connected to the data network.

Fig. 2 shows a preferred embodiment of a mobile phone 1 according to the invention. The mobile phone 1, comprises a user interface having a keypad 2, a display 3, an on/off button 4 (present in the top of the phone) a speaker 5, and a microphone 6 (only the opening present in the bottom of the phone is visible). The mobile phone 1 according to the preferred embodiment is adapted for communication via a cellular network, such as the GSM

900/1800 MHz network, but could just as well be adapted for use with a Code Division Multiple Access (CDMA) network.

According to a preferred embodiment, the keypad 2 has a first group 7 of keys as alphanumeric keys, two softkeys 9, a cursor navigation key 10 (scroll up/down), and on-hook and off-hook keys 12. The present functionality of the softkeys 9 is shown in separate fields (softkey-labels) in the display 3 just above the softkeys 9. The softkeys 9 are multifunction keys and their present function depends on the state of the mobile phone 1. The softkeys 9 give access to the menu, the phonebook and call can activate actions related to call handling and message handling. A releasable battery pack 14 is placed on the rear side of the mobile phone 1.

Fig. 3 schematically shows the most important components of a preferred embodiment of the mobile phone 1, said components being essential to the understanding of the invention. The processor 18 controls the communication with the network via the transmitter/receiver circuit 19 and an internal antenna 15.

The microphone 6 transforms the user's speech into analogue signals, the analogue signals formed thereby are A/D converted in an A/D converter (not shown) before the speech is encoded in a digital signal processing unit 14 (DSP). The encoded speech signal is transferred to the processor 18, which i.e. supports the GSM terminal software. The processor 18 also forms the interface to the peripheral units of the apparatus, including a RAM memory 17a and a Flash ROM memory 17b, a SIM card 16, the display 3 and the keypad 2 (as well as data, power supply, etc.). The DSP 14 speech-decodes the signal,

which is transferred from the processor 18 to the speaker 5 via a D/A converter (not shown).

Fig. 4 illustrates the software architecture of the mobile phone 1. The software architecture comprises an operating system, in a preferred embodiment the Symbian™ 7.0 OS that provides the platform for the native software. The native software comprises a number of native applications of which a few can be mentioned: User interface, KVM support, a call handling, phone book, message handling and a MIDlet database. The listed native applications are, however, merely exemplary, there could be more as well as fewer native applications.

A Connected Limited Device Configuration (CLDC) provides the runtime environment for Java™ applications. CLDC is one of the most appropriate configurations for mobile phones available for Java™, since it is tailored for devices with 160-512 KB memory battery powered, slow, possibly intermittent, connection.

The CLDC comprises a K Java™ Virtual Machine (KVM) and a set of libraries and Application Program Interfaces (APIs). The libraries and APIs are specified in the Mobile Information Device Profile (MIDP) sitting on top of the CLDC. The MIDP is a vertical extension of CLDC. Together they provide a run-time environment for Java™ Applets and MIDlets (MIDlet: an application written for the Mobile Information Device profile (MIDP)) on the mobile phone concerned.

The MIDlets are in code that is created by a Java™ compiler. This code can be run on any platform that has a KVM installed. A MIDlet will run the same in any KVM, regardless of the hardware and software underlying the system. The MIDLETS are therefore ideal for extending

the functionality of mobile phones, also because their relatively small size renders them suitable for downloading to the phone. In the present embodiment, a calculator MIDlet and two other MIDlets X2 and X3 have been downloaded to the mobile phone 1. The MIDlets co-exist with other applications on the mobile phone 1 such as the Original Equipment Manufacturer (OEM) Specific Applications. In the present embodiment a Java™ xhtml micro browser applet has been installed by the OEM.

The message handling application is capable of receiving, creating and sending text messages in the SMS standard (Short Message Service (SMS) part of the Global System for Mobile communications (GSM) digital standard - well known in the art). The message handling application may also be able to handle other message formats for exchanging information between mobile phones/servers such as the more recent MIME (Multipurpose Internet Mails Extensions) and MMS (Multimedia Messaging Service) standards. The message handling application may run in the native software or in an application run by the virtual machine.

The mobile phone 1 can send and receive data using the General Packet Radio Service (GRPS) for e.g. downloading MIDlets or other applications and is Wireless Application Protocol (WAP) enabled. A micro-browser written in Java™ is one of the OEM-specific applications.

The present invention provides for a new SMS message type in which the message header contains a MIDlet identifier and an address at which the identified MIDlet can be downloaded from a server that is connected to the wireless cellular network. This header is in addition the now-standard SMS header and the user data header. The message body contains the data to be used by the

identified MIDlet. The new SMS message type will be referred to hereafter as a Java-message (J-SMS).

The syntax of the J-SMS in a preferred embodiment is as follows:

<sms>::=

<sms-header>

<sms-data>

<sms-header>::= standard sms header described somewhere else

<sms-data>::

<user-data-header>

<user-data>

<user-data-header>::= user data header as described in smart messaging specification

<user-data>::=

<j-sms-header>

<j-sms-data>

<j-sms-header>::=

<j-sms-header-length>

<j-sms-version>

<j-sms-flags>

<j-sms-uris>

<j-sms-certificates>

<j-sms-header-length>::=two bytes giving the length of the j-sms header

<j-sms-version>::=one byte with the version of the j-sms protocol (01)

<j-sms-flags>::=one byte with flags for the message. Sum of the following:

1: the message includes certificates and a checksum

2: the message can be displayed as text

4: the message can be discarded if not able to display

<j-sms-uris>::=

<number of uris>

*<uri_s>**

<number of uris>::=one byte with the number of uris

<uri_s>::=uri's terminated with \n

<j-sms-certificates>

<checksum>

*<certificate>**

<checksum>::=checksum of the whole user data block (user data header plus user data) excluding this checksum

<certificate>::=certificate in base64 encoding terminated by \n

<j-sms-data>::=data that is to be transferred to the MIDlet

An example of a J-SMS in accordance with a preferred embodiment of the present invention in the form of an application port addressing scheme as defined in GSM 03.40 is listed below:

Octet Number	Value	Description
1	0B	Length of the User Data Header
2	05	Information Element Identifier (IEI; application port addressing scheme, 16-bit port address)
3	04	Information Element Data Length (IEDL)
4 - 5	2136	Information Element Data (octets 4 & 5 → 2136 - destination port)

6 - 7	00 00	Information Element Data (octets 6 & 7 → 0000 - originator port)
8	00	Information Element Identifier (IEI; concatenated short message, 8-bit reference number)
9	03	Information Element Data Length (IEDL; 3 octets)
10	01	Information Element Data (concatenated short message reference number)
11	02	Information Element Data (total number of concatenated messages (0-255))
12	01	Information Element Data (sequence number of current short message)
13	30	MIDlet message version number. ISO-8859-1 character "0"
14	00	Message flags where the following bits have the meaning: 1. message includes certificate 2. message data can be displayed as text 3. message can be discarded if not able to display 4. reserved for future use.
15	01	Number of following URIs
16..	"http://www.d2.de/greetingcard.jat"	The URI of the MIDlet used to display the content. Terminated by a newline (0x0A) character.
..	http://www.d2.de/greeting/picture1.jpg "Hi there, how are you doing ?".	MIDlet message data in a format defined only by the MIDlet.

The port number in octet 4-5 defines the SMS message type. The number used in this example is arbitrary and has not been reserved for the message type according to the present invention. Regular port numbers are reserved in the NBS port number space at the Internet Assigned Numbers Authority (IANA).

Octets 1 to 12 are in use in conventional SMS types, and for further information on their function reference is made to the GSM 03.40 specification, hereby incorporated by reference.

Octet 13 identifies the MIDlet message version number.

Octet 14 contains message flags where the following bits have the meaning:

1. message includes certificate
2. message data can be displayed as text
3. message can be discarded if not able to display
4. reserved for future use.

Octet 15 defines the number of Uniform Resource Identifiers (URIs) contained in the message. Octet 16 contains the first URI, followed by the message body with the data to be used by the identified MIDlet.
The message handling application detects the message type through the port number in octet 4-5. If the port number is (in present example) 2136 (HEX) the message is treated as a J-SMS. SMS messages with other port numbers in octet 4-5 are handled by the message handling application in the respective intended way, which is though not described here since this other types of the message handling are well known from e.g. the SMART MESSAGING SPECIFICATION, Revision 3.0.0, 2000-12-18, hereby incorporated by reference.

The MIDlet to be executed upon receipt of the message is defined by the URI in octet 16. The data to be used during the execution of the identified MIDlet is contained in the message body in the following octets. The data may comprise image files, formatted text files, audio files database files, or any other type of file executable on the terminal, or it may contain links to

such files. Referring to the table, greeting card MIDlet identified in octet 16 is needed to display the greeting card which includes an image file and associated text. The greeting card image file "picture1.jpg" is provide by an identification of the URI "http://www.d2.de/greeting/picture1.jpg," and the accompanying text "Hi there, how are you doing?" is provided as a text file within the message itself.

The following example illustrates the practical application of the J-SMS type messages. A first mobile subscriber A wishes to send his friend, mobile subscriber B, an e-postcard. Subscriber A visits the WAP-site of a postcard server 25 using the micro browser on his mobile phone 1. There, he selects the type of e-postcard to be sent, e.g. the graphics, accompanying tune, animation, font type, color, etc. The server 25 prompts subscriber A to enter a message text, that may or may not be used in combination with text integrated in the selected e-postcard. The server 25 also prompts subscriber A to enter the intended recipient's name and phone number. When the server 25 has received these data and an accept from subscriber A it sends a J-SMS to subscriber B. The header of the J-SMS contains an identifier for a postcard displaying MIDlet, and an address where the postcard displaying MIDlet can be downloaded from a server, in this case a MIDlet server 26, but it could just as well have been the postcard server 25. The URI serves as MIDlet identifier and as download address.

The postcard displaying MIDlet is an application that displays the postcard as selected and composed by subscriber A correctly on any mobile device with a Java™ Virtual Machine. The postcard contains text and may contain graphics, backgrounds, animations, music, etc.

The message body contains the data for the postcard displaying MIDlet.

Fig. 5 is a flowchart that illustrates the procedure after dispatch of the J-SMS (step 51). Upon receipt of the J-SMS by the mobile phone 1 of subscriber B (step 52) the message handling application saves the message and examines the message header (step 53), parsing the message header for the information indicated in table above. Then, the message handling application determines the message type by checking the port number in octets 4-5 (step 54).

If the message is not a J-SMS, but e.g. a profile or a text message, the message handling application handles the message accordingly (step 55), as is well-known in the art and therefore not further explained here.

If the message handling application finds port number 2136 (HEX) in octet 4-5 the message is handled as a J-SMS. The message handling application reads the first URI included in the message. The URI serves as the MIDlet identifier. The mobile phone 1 maintains a small MIDlet database (one of the native applications) that lists the URIs of all the MIDlets that have been downloaded to the phone. The URI of OEM installed MIDlets is preferably also listed in the MIDlet database. The message handling application checks the MIDlet database for the presence of the URI included in the header (step 56).

After checking the MIDlet database, the message handling application can determine (step 57) if the identified MIDlet, in this example the postcard displaying MIDlet, is available on the mobile phone 1.

If the identified MIDlet is available, the message handling application starts the postcard displaying MIDlet (step 58). The message handling application then sends the data in the message body to the postcard displaying MIDlet (step 59) which uses it to display the postcard as selected and composed by subscriber A, including the image on the picture1.jpg file and the personal text "Hi there, how are you doing?" (step 59A in Figure 5).

If the URI identified MIDlet was not found in the MIDlet database in step 56, the message handling application connects e.g. via GPRS to the address in the URI at which the identified midlet can be downloaded and downloads the identified MIDlet. In this example the postcard displaying MIDlet is downloaded from the MIDlet server 26 (step 60). In the download request the message handling application may provide information about the requesting phone. The MIDlet sever 26 uploads the postcard handling MIDlet to the mobile phone 1.

Next, the message handling application adds the URI of the downloaded MIDlet to the MIDlet database and verifies that the certificate accompanying the MIDlet is signed and issued by an recognized certificate authority to ensure the integrity of the MIDlet (step 61).

A certificate issued by a recognized certificate authority is added to the signed MIDlet. The carrier, or the software developer, creates a signing-key pair and obtains a certificate from a recognized certificate authority. The carrier or developer computes a signature of the MIDlet suite JAR, then places that signature and the corresponding certificate in the application descriptor.

The signed MIDlet suite assures the user that the contents of the MIDlet suite have not been tampered with, and that the MIDlet suite comes from an trusted source. The MIDP implementation on the device can verify the identity of the developer by verifying the developer's signature. It can use the developer's public key added to the Java Application Descriptor (JAD) to verify the integrity of the MIDlet suite itself. For further details on the certification of MIDlets reference is made to the MIDP 2.0 specification (hereby incorporated by reference).

The MIDlet is then handled in accordance with the permission levels indicated in the certificate. The permissions may comprise allowed permissions and user permissions (the ones for which the user will be consulted). The permission levels are stepped in the following order: Network operators (highest level), OEM (mid level), signed but not by Network operator or OEM (lowest level). Depending on these levels the phone prompts for permission for sensitive operations to e.g. opening an HTTP connection, to delete or change phone numbers, etc.

After the certificate verification the message handling application starts the postcard displaying MIDlet (step 58), sends the data in the message body to the postcard displaying MIDlet (step 59) and the postcard is displayed.

The procedure can be repeated if subscriber B replies by sending an e-postcard back to subscriber A, a function that may be built into the postcard displaying application. Otherwise, the message handling application ends in step 62.

There can be more than one MIDlet identifier (URI) included in a single J-SMS. The message application will execute the identified MIDlets in the order in which they are listed in the J-SMS. In the above example the URI has been used both to identify the MIDlet and to provide the address at which the MIDlet can be downloaded. It is however possible to use a separate identifier and address. The MIDlet that is started by the J-SMS may also download further information or other data.

Another example of the use of the present invention is illustrated in Fig. 6 with the following scenario. An e-mail provider wishes to send e-mail messages to mobile subscribers. The standard SMS e-mail message is not sufficient for the operator's requirements because more features should be implemented e.g. starting an xhtml browser to read the e-mail, displaying the header of the new received e-mail, displaying the provider logo, showing an in-tray with received e-mails in every user's e-mail folder. After receipt of an e-mail intended for a mobile subscriber, the operator's e-mail server 27 sends a J-SMS that starts a MIDlet that displays the text "e-mail received" on the display of the mobile phone together with an audible notification and prompts the user if the e-mail should be opened. If the user affirms but the required enhanced e-mail MIDLET (an xhtml Java™ browser) is not installed on the user's mobile phone, the mobile phone requests a download of the enhanced e-mail MIDlet from the URI listed in the e-mail message, processes the download to install the enhanced e-mail MIDLET, and thereafter executes the enhanced e-mail MIDLET to process the e-mail data. The xhtml browser exchanges e-mail data via GPRS between the mobile phone 1 and the e-mail server 27 and displays the e-mail data. The xhtml browser operates as a sophisticated e-mail client that offers the user more flexibility and comfort

than the simple e-mail displaying capacities of conventional SMS. The steps of requesting the MIDlet from the MIDlet server and the subsequent download as shown in Fig. 6 are bypassed if the xhtml browser MIDlet is already available on the mobile phone 1.

A further example of the use of the present invention is illustrated in Fig. 7 with the following scenario. A network operator wishes to offer a new service to its customers. This new service sends special offers from the operator's web-shop to the mobile phone of the customers. This service is realized by the provider sending J-SMSs including name, price and description (photo) of the offered items from its web-shop server (e.g., block 28 of Figure 1). The J-SMS includes an identifier of an advertisement displaying MIDlet that displays this information in a clean way, stores past offers for reference and allows the subscriber to order the items at the web-shop. The steps of requesting the MIDlet from the MIDlet server and the subsequent download as shown in Fig. 7 are bypassed if the advertisement displaying MIDlet is already available on the mobile phone 1.

The integrity verification does not need to be exclusively applied to the MIDlets, it can also be implemented in the J-SMS itself by adding a certificate from a recognized certificate authority and an encrypted checksum of the whole message to the J-SMS. The validity of the certificate can be verified by opening the signature with the public key that is included in the J-SMS. In this embodiment of the J-SMS the verification can be carried out before downloading the MIDlet concerned. Thus, some unnecessary downloads of uncertified MIDlets can be avoided.

As illustrated above, the messaging system provides a message format for use in a mobile phone system wherein mobile phones are capable of running a variety of applications to process a variety of files, and are capable of running a message handling application for receiving messages. The message format comprises a header portion for identifying the message to the message handling application and a message data portion. The message data portion further comprises (1) a message data file portion which may optionally contain message text files, message images, message audio, message database files or the like, or identification of message files and locations from which said message files or the like may be downloaded to the phone, as desired by the originator of the message and (2) a message data header portion which contains an identification for any application needed in order to process files contained or identified in the message data file portion, and also contains information regarding locations from which said application may be downloaded to the phone. In addition, the message format may comprise a user data header according the SMS specification, and various other headers as dictated by the particular message contents.

Although the present invention has been described in detail for purpose of illustration, it is understood that such detail is solely for that purpose, and variations can be made therein by those skilled in the art without departing from the scope of the invention. The message type is not limited to the SMS standard, and may be implemented in MMS or EMS standards. The applications that are executed after receipt of a message do not need to be MIDlets, they could just as well be Java™ applets or other applications in platform independent code. The platform independent runtime environment does not need to be Java™ based, other runtime environments for platform

independent code can be used. Thus, while the preferred embodiments of the devices and methods have been described in reference to the environment in which they were developed, they are merely illustrative of the principles of the inventions. Other embodiments and configurations may be devised without departing from the scope of the appended claims.

CLAIMS:

1. A method of handling incoming messages received on a mobile communication terminal via a wireless network, the terminal having native software and a virtual machine capable of executing platform independent object code, comprising the steps of:

receiving and storing a message that comprises a header and a message body, the header containing an identifier for an application in platform independent object code that can be executed by the virtual machine,

verifying if the identified application is available on the terminal, and

starting the identified application when available on the terminal

2. A method according to claim 1, wherein the header further contains an address at which the identified application can be downloaded from a server that is accessible through the wireless network, and further comprising the steps of:

connecting to the terminal to the server at the address contained in the header and downloading the identified application when the identified application was not available on the terminal, and

starting the identified application when downloaded.

3. A method according to claim 1, wherein the message body contains data to be used by the identified application.

4. A method according to claim 2, wherein the message body contains data to be used by the identified application.

5. A method according to claim 3, wherein the message body contains greeting card data that is to be used by a greeting card displaying application identified in the header.

6. A method according to claim 4, wherein the message body contains greeting card data that is to be used by a greeting card displaying application identified in the header.

7. A method according to claim 3, wherein the message body contains phone number data that is to be used by a phonebook updating application identified in the header.

8. A method according to claim 4, wherein the message body contains phone number data that is to be used by a phonebook updating application identified in the header.

9. A method according to claim 3, wherein the message body contains e-mail data that is to be used by an e-mail displaying application identified in the header.

10. A method according to claim 4, wherein the message body contains e-mail data that is to be used by an e-mail displaying application identified in the header.

11. A method according to any of claims 1 to 10, wherein the platform independent object code is Java™, preferably in the Java™ 2, Micro Edition format.

12. A method according to any of claims 1 to 10, wherein the virtual machine is a Java Virtual Machine, preferably a K Virtual Machine™ (KVM) .

13. A method according to any of claims 1 to 10, wherein the identified application is a MIDlet.

14. A method according to any of claims 1 to 10, further comprising the step of verifying the certification of the identified application.

15. A mobile communication terminal for operation with a wireless network, the terminal having:

native software,

a virtual machine capable of executing platform independent object code,

a message handling application in the native software or in an application under the virtual machine, the message handling application being capable of sending and receiving messages via the wireless network, and

the message handling application being programmed to start an application written in the independent object code when a corresponding identifier is contained the header of a received message.

16. A mobile communication terminal according to claim 15, wherein the message handling application is programmed to download the identified application from a server that is accessible via the wireless network at an address contained in the header when the identified application is not already available on the terminal.

17. A mobile communication terminal according to claim 15, wherein the platform independent object code is Java™, preferably in the Java™ 2, Micro Edition format.

18. A mobile communication terminal according to claim 17, wherein the virtual machine is a Java™ Virtual Machine, preferably a K Virtual Machine™ (KVM).

19. A mobile communication terminal according to any of claims 15 to 18, wherein the identified application is a MIDlet.

20. A mobile communication terminal according to any of claims 15 to 18, wherein the message handling application is programmed to verify the certification of the downloaded application.

21. A mobile communication terminal according to any of claims 15 to 18, wherein the message application is programmed to send the data in the message body to the identified application.

22. A mobile communication terminal according to any of claims 15 to 18, further comprising an application identifier database listing the identifiers of all the applications in platform independent object code that are available on the terminal.

23. A message for transmission through a wireless network to a mobile communication terminal, the terminal having native software and a virtual machine capable of executing applications in platform independent object code, the message having a syntax comprising:

a header part, and

a message body part,

the header containing an identifier for an application in platform independent object code to be executed by the virtual machine on the mobile communication terminal that receives the message.

24. A message according to claim 23, wherein the header includes an address at which the identified application can be downloaded from a server that is accessible through the wireless network.

25. A message according to claim 23 or 24, wherein the message header contains a URI that serves as identifier and contains the address at which the identified application can be downloaded from a server.

26. A message according to any of claims 23 or 24, wherein the message body contains data to be used by the identified application.

27. A message according to any of claims 23 or 24, wherein the message is an SMS message with a port address in octets 4-5 that identifies it as a message containing an identifier for an application to be started upon receipt of the message.

28. A message according to any of claims 23 or 24, wherein the identified application is a Java™ applet or a MIDlet, preferably in the Java™ 2, Micro Edition, Mobile Information Device Profile (MIDP) format.

29. A message according to any of claims 23 or 24, further containing a signed certificate issued by a recognized certification authority that includes a public key from the signatory.

30. A method of enabling an application in platform independent object code to be run on a mobile communication terminal comprising the steps of:

sending a message from a server via the wireless network to the mobile communication terminal that is provided with a virtual machine capable of executing applications in platform independent object code, the message containing:

a header with an identifier for the application to be executed by the virtual machine and

a message body with the data to be used by the identified application.

31. A method according to claim 30, wherein the message header further contains an address at which the identified application can be obtained from a server that is accessible through the wireless network, further comprising the step of:

uploading the identified application to the mobile communication terminal when the mobile terminal connects to the server at the address contained in the header.

32. A method according to claim 30, wherein the server that uploads the identified application is not the same as the server sending the message.

33. A method according to claim 30, wherein the uploaded application is a MIDLet, preferably in the Java™ 2, Micro Edition, Mobile Information Device Profile (MIDP) format.

34. A message format for use in a mobile phone system wherein mobile phones are capable of running a variety of applications to process a variety of files, and are capable of running a message handling application for receiving messages, said message format comprising:

a header portion for identifying the message to the message handling application;

a message data portion, said message data portion further comprising;

a message data file portion which may optionally contain message text files, message images,

message audio, message database files or the like, or identification of message files and locations from which said message files or the like may be downloaded to the phone, as desired by the originator of the message; and

a message data header portion, wherein said message data header portion contains an identification for any application needed in order to process files contained or identified the message data file portion, and also contains information regarding locations from which said application may be downloaded to the phone.

35. A method of transmitting messages to a mobile phone in a mobile phone system wherein mobile phones are capable of running a variety of applications to process a variety of files, and are capable of running a message handling application for receiving messages; said method comprising the steps of:

creating a message in a message format comprising:

a header portion for identifying the message to the message handling application

a message data portion, said message data portion further comprising;

a message data file portion which may optionally contain message text files, message images, message audio, message database files or the like, or identification of message files and locations from which said message files or the like may be downloaded to the phone, as desired by the originator of the message; and

a message data header portion, wherein said message data header portion contains an

identification for any application needed in order to process files contained or identified the message data file portion, and also contains information regarding locations from which said application may be downloaded to the phone; and

transmitting the message to a mobile phone.

36. A method of operating a mobile phone comprising;

programming the phone to receive messages having a format such that the messages comprise an SMS header portion and an SMS data portion, wherein the SMS data portion comprises a first portion comprising message handling information and a second portion comprising message data for eventual display to the mobile phone user, wherein the message handling information comprises information identifying an application needed to display the message data or otherwise process the message data with an application, and information identifying a location from which the application may be downloaded to the phone; and wherein the message data comprises message files comprising message text files, message images, message audio, message database files or the like, or identification of locations from which said message files or the like may be downloaded to the phone;

further programming the phone to determine if the application needed to display or otherwise use the message data is installed on the phone, and, if not, to download the application from the

location identified in the message handling information;

further programming the phone to display or otherwise use the message files or the like if they are already in the message data, or, if not, to download the message files from the locations identified in the message data;

operating the phone to receive a message, and thereafter operating the phone to determine if the application needed to use the message files is installed on the phone, and, if not, to download the application; and thereafter operating the phone to display or otherwise use the message files if they are contained in the message data, and, if not, to download the message files from the location identified in the message data and thereafter display or otherwise use the message files.

37. The message format of claim 34 wherein the messages are provided in an SMS format.

38. The message format of claim 34 wherein the messages are provided in an MMS format.

39. The message format of claim 34 wherein the messages are provided in an EMS format.

40. The method of claim 35 or 36 wherein the messages are provided in an SMS format.

41. The method of claim 35 or 36 wherein the messages are provided in an MMS format.

42. The method of claim 35 or 36 wherein the messages are provided in an EMS format.

43. The message format of claim 34 wherein the message header is an SMS header, and wherein the message format further comprises a user data header.

44. The method of claim 35 further comprising creating the message in a message format comprising a user data header.

45. The method of claim 36 wherein the message header is an SMS header, and wherein the message format further comprises a user data header.

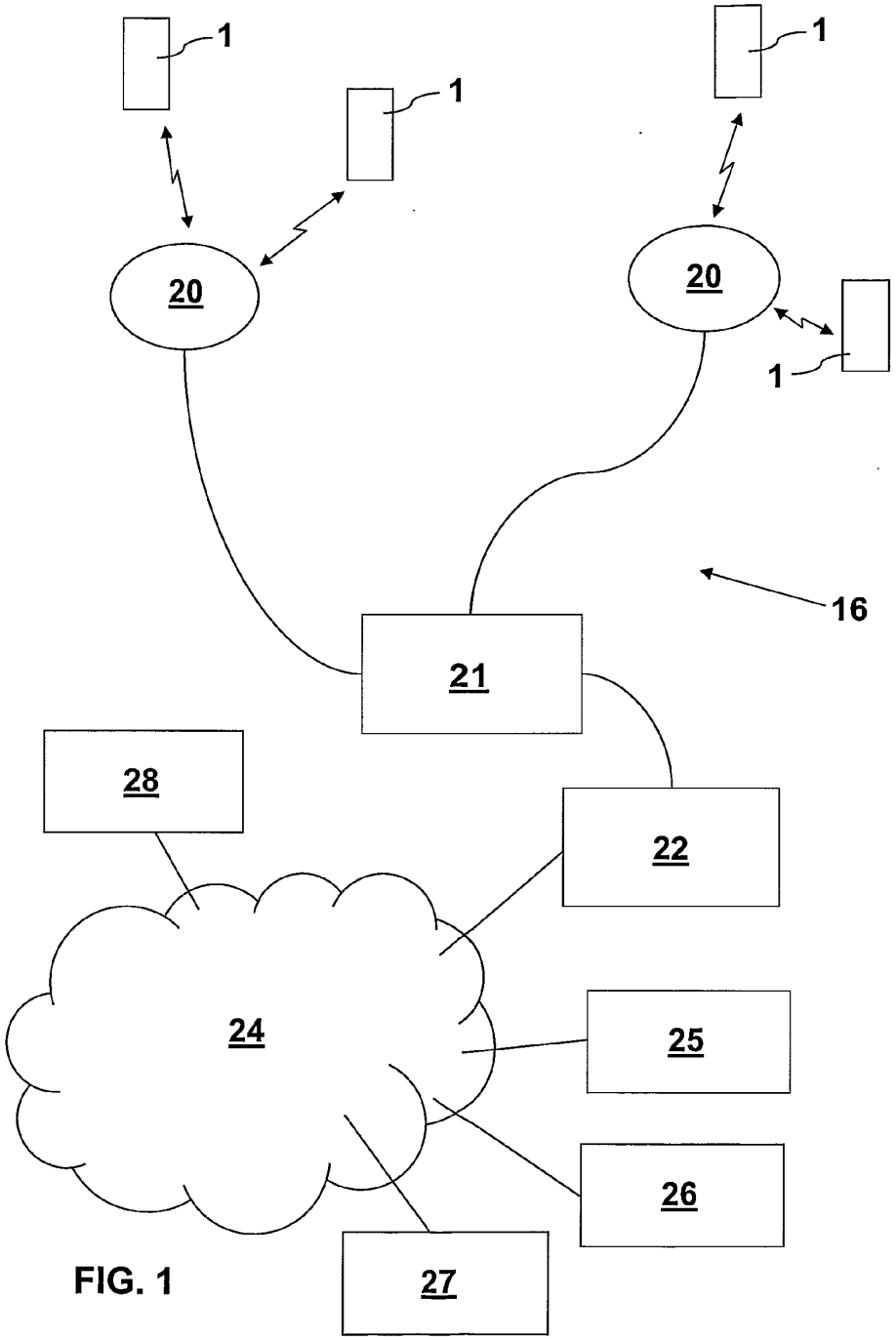


FIG. 1

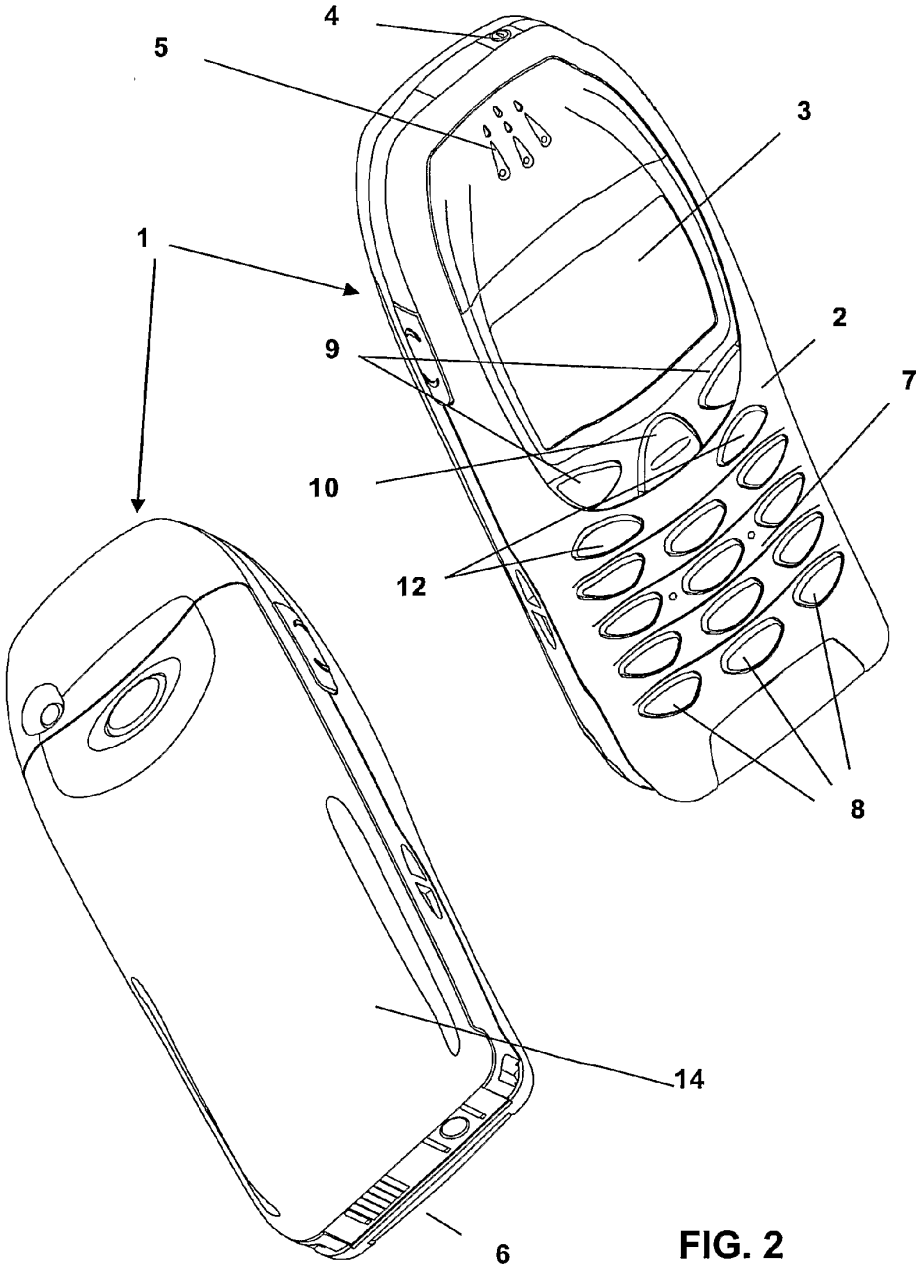


FIG. 2

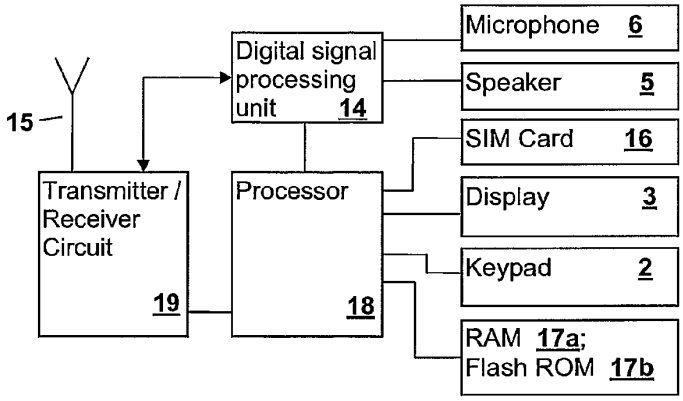

15
Digital signal processing unit 14
Microphone 6
Speaker 5
SIM Card 16
Display 3
Keypad 2
RAM 17a; Flash ROM 17b
Transmitter / Receiver Circuit 19
Processor 18

FIG. 3

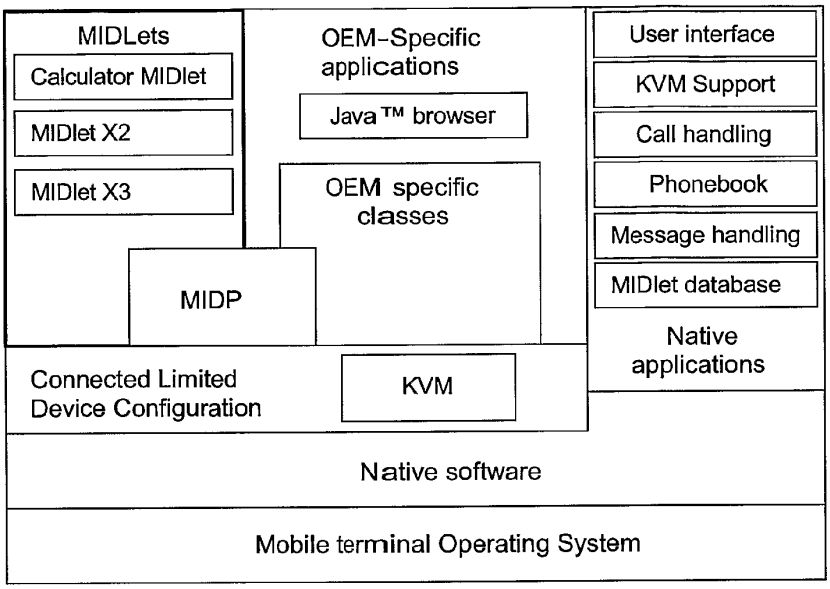

MIDLets
Calculator MIDlet
MIDlet X2
MIDlet X3
OEM-Specific applications
Java™ browser
OEM specific classes
MIDP
User interface
KVM Support
Call handling
Phonebook
Message handling
MIDlet database
Native applications
Connected Limited Device Configuration
KVM
Native software
Mobile terminal Operating System

FIG. 4

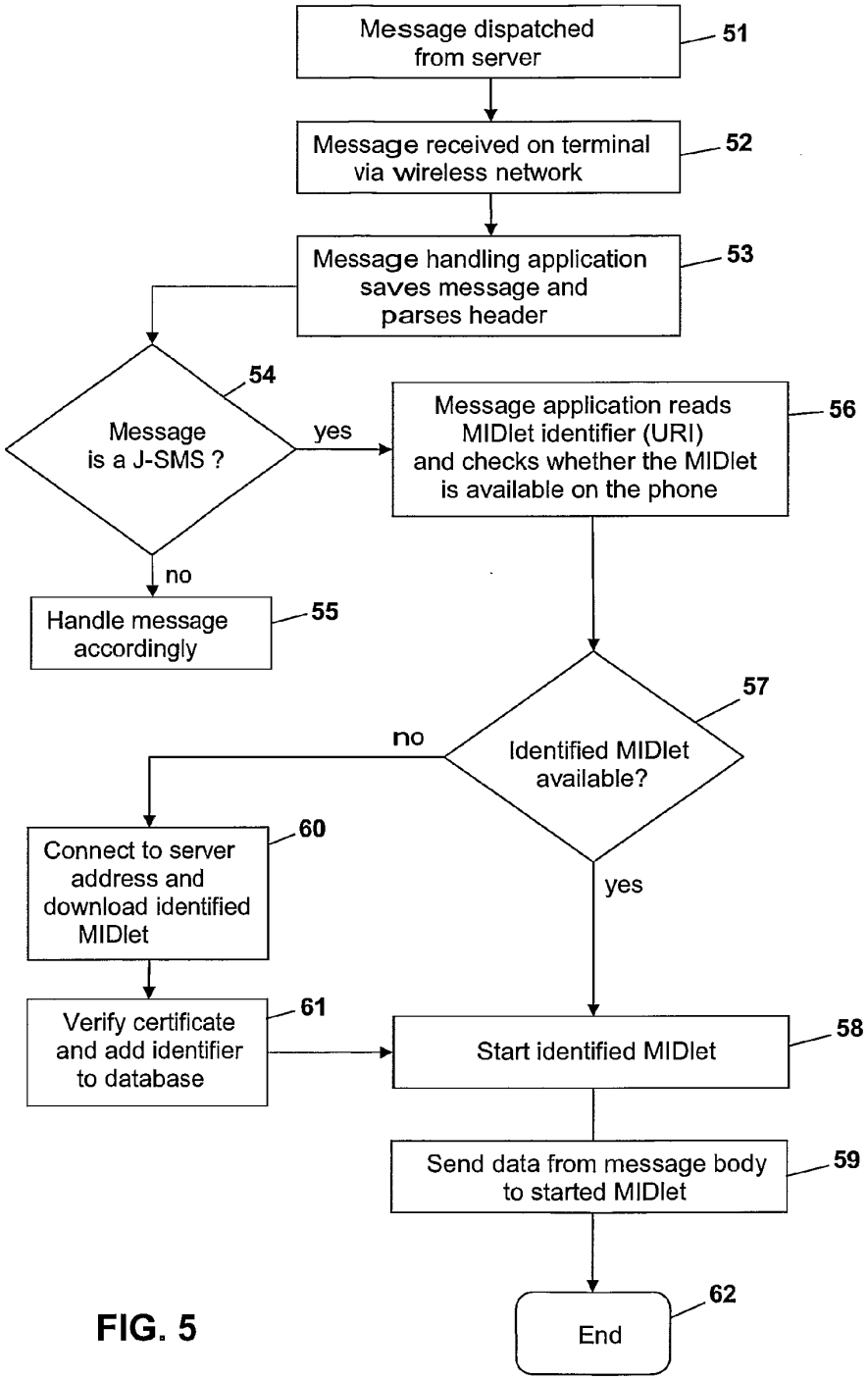

Message dispatched from server
51
Message received on terminal via wireless network
52
Message handling application saves message and parses header
53
54
Message is a J-SMS ?
yes
Message application reads MIDlet identifier (URI) and checks whether the MIDlet is available on the phone
56
no
Handle message accordingly
55
57
Identified MIDlet available?
no
yes
Connect to server address and download identified MIDlet
60
Verify certificate and add identifier to database
61
Start identified MIDlet
58
Send data from message body to started MIDlet
59
End
62

FIG. 5

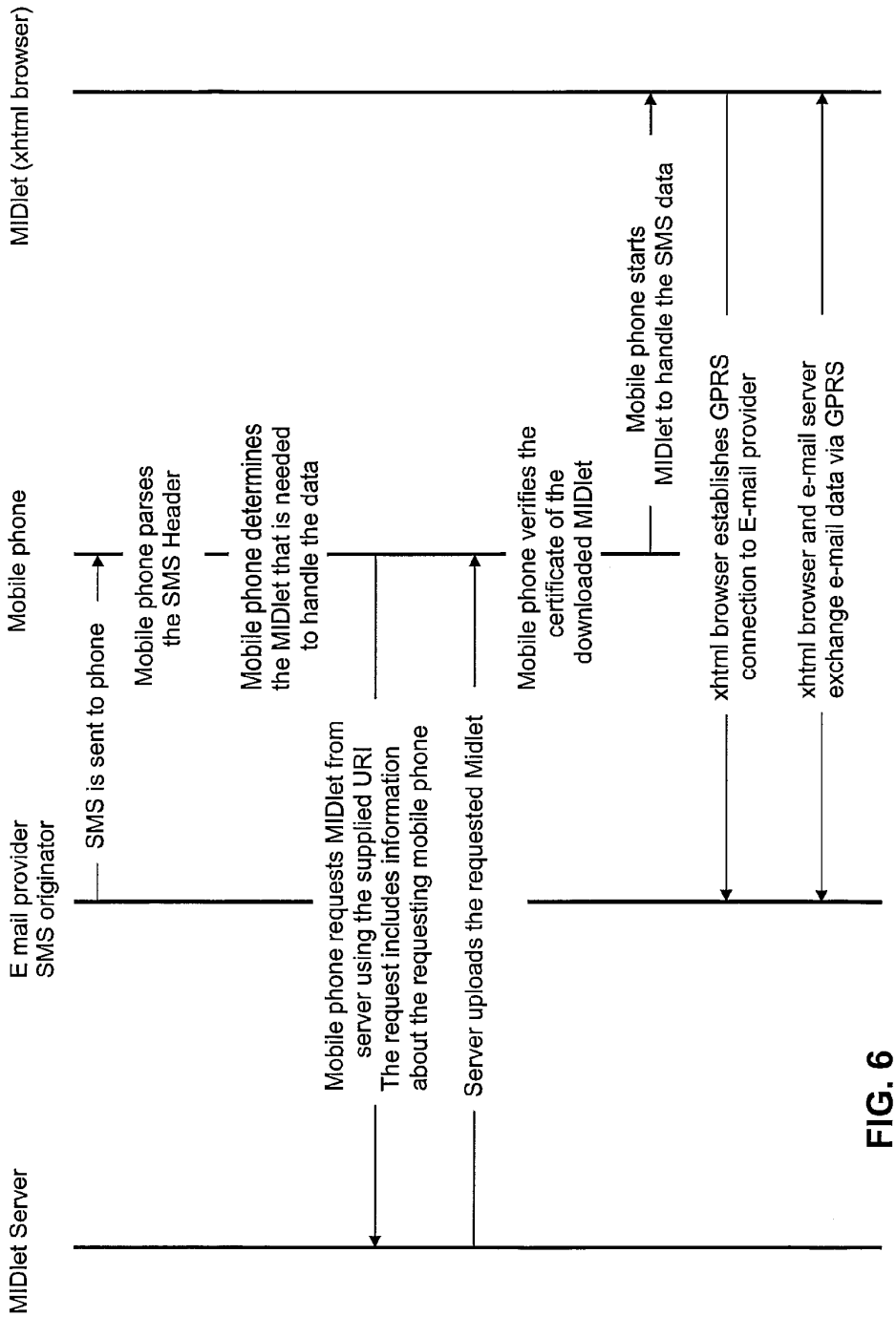

MIDlet Server
E mail provider
SMS originator
Mobile phone
MIDlet (xhtml browser)
SMS is sent to phone
Mobile phone parses the SMS Header
Mobile phone determines the MIDlet that is needed to handle the data
Mobile phone requests MIDlet from server using the supplied URI
The request includes information about the requesting mobile phone
Server uploads the requested Midlet
Mobile phone verifies the certificate of the downloaded MIDlet
Mobile phone starts MIDlet to handle the SMS data
xhtml browser establishes GPRS connection to E-mail provider
xhtml browser and e-mail server exchange e-mail data via GPRS

FIG. 6

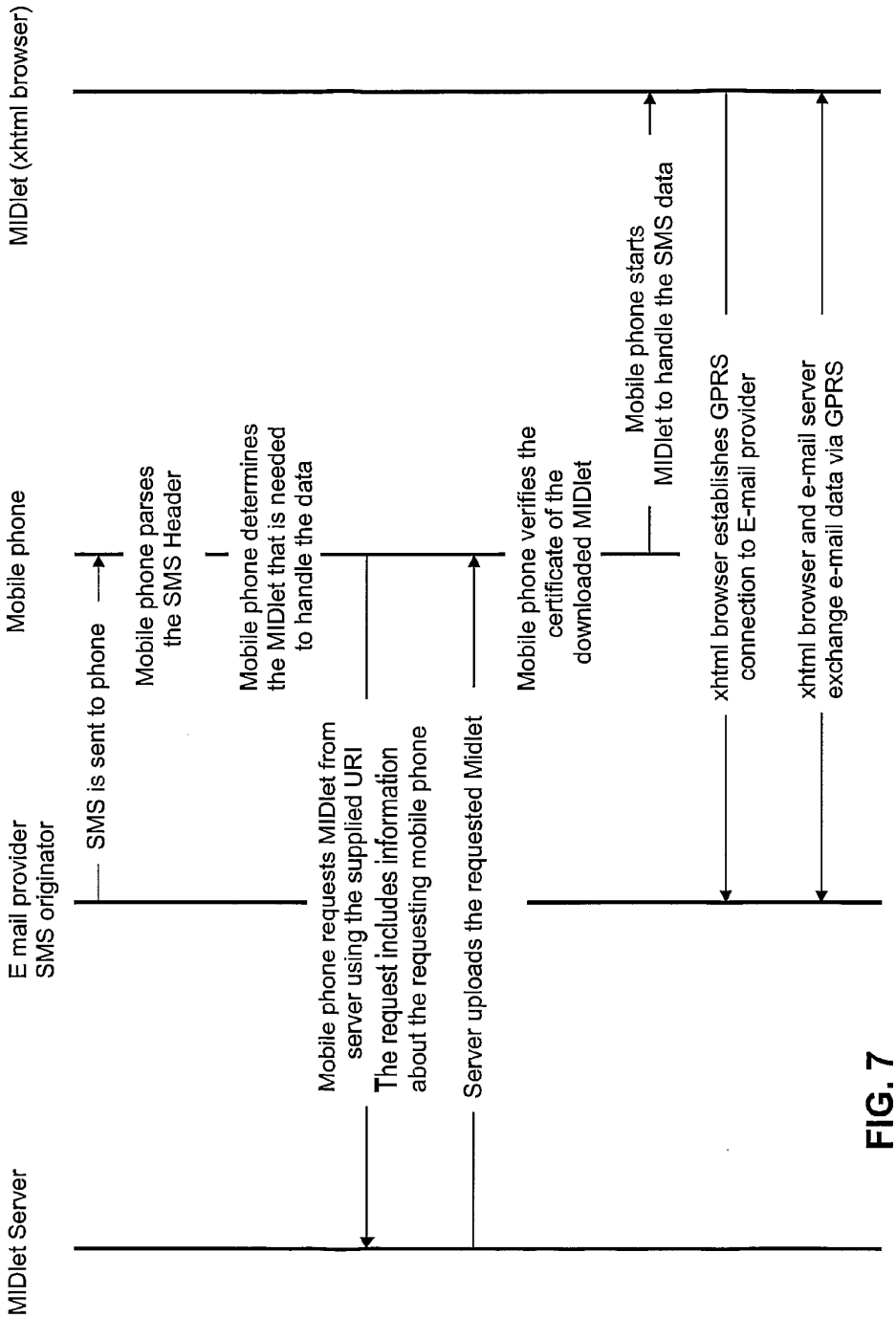

MIDlet Server
E mail provider
SMS originator
Mobile phone
MIDlet (xhtml browser)
SMS is sent to phone
Mobile phone parses the SMS Header
Mobile phone determines the MIDlet that is needed to handle the data
Mobile phone requests MIDlet from server using the supplied URI
The request includes information about the requesting mobile phone
Server uploads the requested Midlet
Mobile phone verifies the certificate of the downloaded MIDlet
Mobile phone starts MIDlet to handle the SMS data
xhtml browser establishes GPRS connection to E-mail provider
xhtml browser and e-mail server exchange e-mail data via GPRS

FIG. 7

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2004/013101

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04Q7/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04Q

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

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

EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 98/34422 A (NOKIA MOBILE PHONES LIMITED; WELLS, MARK; HUBER, ROLF) 6 August 1998 (1998-08-06) page 5, line 4 - line 17 page 15, line 5 - page 17, line 2 page 27, line 7 - last line figure 4 ----- -/--	1,3,5,7, 9,11-15, 17-23, 26-30, 32,33

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 March 2005	30/03/2005

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Müller, N

2

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2004/013101

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	SONERA MEDIALAB: "Mobile Java Application Development White Paper" 'Online! 12 September 2002 (2002-09-12), , XP002320888 Retrieved from the Internet: URL:http://www.medialab.sonera.fi/workspace/MobileJavaAppDevelopment.pdf> 'retrieved on 2005-03-10! Chapters 1 and 2	1,3,5,7, 9,11-15, 17-23, 26-30, 32,33
A	EP 1 143 688 A (CLIENT ELECTRONICS GMBH) 10 October 2001 (2001-10-10) page 2, paragraph 10 - page 3, paragraph 20 page 3, paragraph 25 - page 5, paragraph 44 figures 1-3,5	1-45
A	US 2002/123335 A1 (LUNA MICHAEL E.S ET AL) 5 September 2002 (2002-09-05) page 1, paragraph 13 - paragraph 14 page 2, paragraph 16 page 2, paragraph 21 - paragraph 23 page 3, paragraph 27 figure 2	1-45
A	US 2002/138545 A1 (ANDREAKIS DEAN W ET AL) 26 September 2002 (2002-09-26) page 1 - page 2, paragraph 10 page 2 - page 3, paragraph 19 page 3, paragraph 22 - paragraph 24	1-45

2

Form PCT/ISA/210 (continuation of second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP2004/013101

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9834422 A	06-08-1998	US 6125281 A	26-09-2000
		AU 6214998 A	25-08-1998
		WO 9834422 A2	06-08-1998
		EP 0956719 A2	17-11-1999
		JP 2001509981 T	24-07-2001
		US 6078820 A	20-06-2000
EP 1143688 A	10-10-2001	EP 1143688 A1	10-10-2001
US 2002123335 A1	05-09-2002	US 2002068554 A1	06-06-2002
		US 2003023849 A1	30-01-2003
		EP 1308858 A2	07-05-2003
		CN 1270452 A	18-10-2000
		EP 1043906 A2	11-10-2000
		JP 2000358282 A	26-12-2000
		EP 1286514 A2	26-02-2003
US 2002138545 A1	26-09-2002	CN 1460213 A	03-12-2003
		EP 1374082 A1	02-01-2004
		JP 2004519780 T	02-07-2004
		MX PA02011541 A	06-06-2003
		WO 02077843 A1	03-10-2002

Form PCT/ISA/210 (patent family annex) (January 2004)

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
31 January 2002 (31.01.2002)

PCT

(10) International Publication Number
WO 02/08863 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number: PCT/US01/23226

(22) International Filing Date: 23 July 2001 (23.07.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/220,241 21 July 2000 (21.07.2000) US

(71) Applicant: **TELEMAC CORPORATION** [US/US]; 6701 Center Drive West, Suite 700, Los Angeles, CA 90045 (US).

(72) Inventors: **WATLER, Theodore, W.**; 5341 E. 4th Street, Long Beach, CA 90814-1920 (US). **HANLEY, Jerry**; 1315 Franklin Street, #D, Santa Monica, CA 90404 (US).

(74) Agents: **NG, Horace** et al.; Townsend and Townsend and Crew LLP, Two Embarcadero Center, 8th Floor, San Francisco, CA 94111-3834 (US).

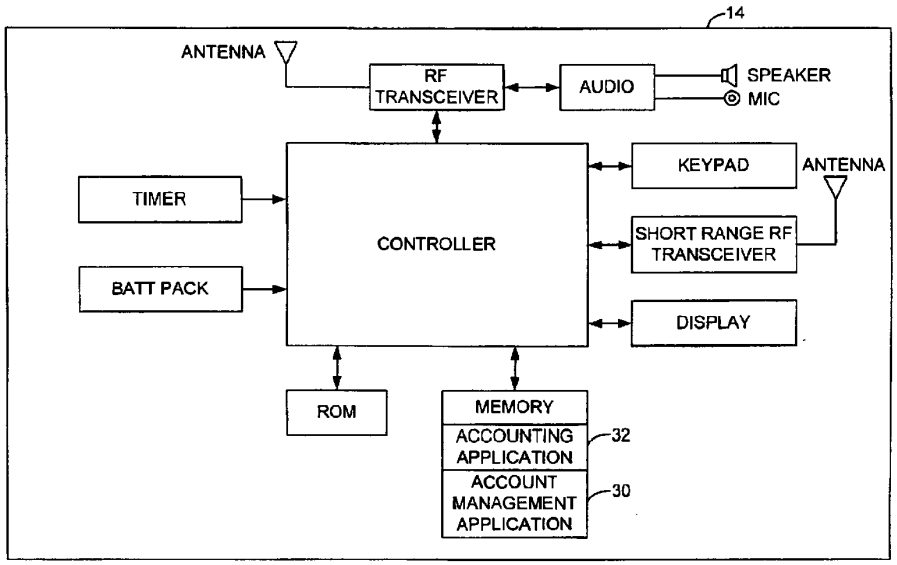
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU,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

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

Published:
— *without international search report and to be republished upon receipt of that report*

[Continued on next page]

(54) Title: MULTIPLE VIRTUAL WALLETS IN WIRELESS DEVICES



(57) Abstract: A system having a wireless device capable of monitoring and tracking its own usage and account activities is disclosed. The wireless device includes an account management application and accounting applications. The account management application manages a variety of accounts in conjunction with the accounting applications and is used by a user to determine how each call/transaction is to be paid for. For example, the user of the wireless device may wish to pay for business calls using a first account and personal calls using a second account.

WO 02/08863 A2

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.

MULTIPLE VIRTUAL WALLETS IN WIRELESS DEVICES

CROSS-REFERENCES TO RELATED APPLICATION

[01] This application claims the benefit of priority under 35 U.S.C. § 119 from U.S. Provisional Patent Application Serial No. 60/220,241 filed on July 21, 2000, the disclosure of which is hereby incorporated by reference in its entirety for all purposes.

BACKGROUND OF THE INVENTION

[02] The present invention generally relates to a system with an account management protocol for wireless devices, and in particular, to a system with an account management protocol which is used to monitor and track usage and account activities of a wireless device.

[03] More specifically, the account management system is adapted for a mobile phone so as to allow the usage and account activities of the mobile phone to be tracked and monitored on an individual basis. A number of accounting systems are described in U.S. Patent Nos. 5,325,418 (the '418 Patent), 5,625,669 (the '669 Patent), 5,577,100 (the '100 Patent), and 6198,915 B1 (the '915 Patent), which are incorporated herein by reference. The '418 and '669 Patents describe accounting systems with features that have particular application to post-paid mobile phone services, such as a mobile phone rental service or controlled mobile phone services. In a controlled mobile phone service, capturing phone call data and calculating phone charges for each call enable service providers (or corporations in an intra-corporate system) to limit, or at least monitor, mobile phone usage before the periodic billing cycle. For example, if mobile phone usage exceeds a pre-established limit, the mobile phone could be temporarily disabled or restricted until an interim payment or additional credit sources are obtained. In an intra-corporate system, a warning message could be sent to a corporate authority that could then either authorize additional use or temporarily disable the mobile phone. In such systems, phone call data is stored in the mobile phone and then transmitted to a host processor that calculates charges. The host processor is typically located on a network that is separate from the mobile phone.

[04] Since the issuance of the '418 and '669 Patents, the state of the art has advanced to a point where an accounting application in the mobile phone is able to calculate calling charges internally. As described in the '100 and '915 Patents, such

systems minimize the communication traffic required between the service provider's host processor and the mobile phone and thus expand the overall traffic handling capacity of the mobile phone system. The '100 and '915 Patents describe accounting systems with features that have particular application to pre-paid mobile phone services.

[05] Due to the increasing ease of use and lower costs, the proliferation and use of mobile phones is going to continue. Many companies nowadays provide employees with mobile phones in order to ensure that such employees remain in contact. Since carrying two mobile phones is quite impractical, these employees inevitably tend to use their company-provided mobile phones for both business and personal calls. Hence, in order to prevent abuses and/or provide accurate accounting, it would be desirable to have the ability to monitor proper usage and account activities of company-provided mobile phones.

[06] Furthermore, some mobile phones on the market today provide a two-line or multi-line capability. With a two-line phone, the two phone lines could be dedicated to handle a first type and a second type of calls respectively. As a result, account activities for different types of calls may need to be monitored separately. Therefore, it would be desirable to provide a mobile phone system that is capable of handling and monitoring different types of usage and account activities for wireless devices.

SUMMARY OF THE INVENTION

[07] The system of the present invention relates to wireless communication systems having wireless devices, particularly mobile phones, that are part of a wireless communication network. In particular, the present invention relates to a wireless device, such as a mobile phone, that includes an internal account management application for internal management of a variety of accounts. In an exemplary embodiment, the account management application interacts with an accounting application for calculation of communication charges on the fly. Such mobile phones are typically cellular telephones in a cellular phone network, radio telephones in a personal communication service network or other communication system, where the mobile phone is moveable from place to place.

[08] Use of the system of the present invention is intended for mobile phones, where real time calculation of calling charges is desirable to limit phone usage or to immediately bill for phone usage where the billings of the public switched service providers and participating wireless service providers are not yet available.

BNSDOCID: <WO_____0208863A2_I_>

[09] The account management system includes an account management application, carried internally in the wireless device, that manages a variety of accounts. The account management application interacts with one or more accounting applications, such as, a complex billing algorithm with multiple factor accounting protocol to account for local charges, roaming charges when the wireless device moves from one zone to another, long distance charges, international charges including country independent local charges, and surcharges which may be per call or rate based. The complex billing algorithm can be expanded to accommodate special charges of service providers or called stations or special discounts or premiums for data transfer calls.

[10] The accounting applications related to mobile phone usage may include a rate schedule. A rate schedule in the wireless device may be periodically updated by wireless communications with the service provider's host processor or customer service representative. The accounting applications related to m-commerce transactions obtain the amount to be deducted from a pre-defined communication protocol with the vendor's transaction device or customer service representative.

[11] It is to be understood that the accounting applications may reside either in the wireless device or on a network which is accessible to the wireless device. Depending on design specification or constraints, the functionality of the account management application may be incorporate into the accounting application.

[12] It is to be further understood that the wireless device with the account management system can be implemented into existing wireless communication networks without substantial modification to the network and can be implemented into most existing wireless devices with minimal modification, primarily by internal reprogramming of the wireless device. Modification to most existing wireless devices is even more minimal when existing accounting applications residing on a network are utilized by the wireless device.

[13] A wireless device such as a mobile phone currently includes an internal processor and sufficient internal memory to incorporate the programming and data storage necessary to accomplish the real time accounting. The account management application and the complex algorithms providing the multiple factor accounting capabilities are sufficiently compact that storage and processing of the call data is enabled in real time with sufficient accuracy to account for multiple charges from multiple service providers even for a roaming phone. The accounting and account management

BNSDOCID: <WO_____0208863A2_I_>

applications should utilize an encryption system to permit secure programming and transactions over the airways.

[14] The accounting and account management system as described herein provides customers and businesses with greater flexibility in managing costs of mobile phone use and m-commerce transactions, especially where costs must be segregated into different accounts by multiple criteria such as business versus personal, or by different profit centers within the same business. The increased flexibility also includes different methods for controlling costs with respect to each account such as pre-paid service or post-paid service with usage limits. The present invention describes a system in which an individual wireless device could be utilized in a controlled service mode for certain purposes such as business calls, in a pre-paid service mode for other purposes such as private calls, and have additional secure electronic accounts for other m-commerce transactions.

[15] The system of the present invention is adapted for analog or digital cellular telephones, radiophones in personal communication service networks and other wireless communication systems. The system is also adapted for other wireless devices, such as personal digital assistants, that are used for m-commerce transactions through short-range radio frequency communication protocols or data bearer communication services such as short message service.

[16] Reference to the remaining portions of the specification, including the drawings and claims, will realize other features and advantages of the present invention. Further features and advantages of the present invention, as well as the structure and operation of various embodiments of the present invention, are described in detail below with respect to accompanying drawings, like reference numbers indicate identical or functionally similar elements.

BRIEF DESCRIPTION OF THE DRAWINGS

[17] Fig. 1 is a simplified schematic diagram illustrating a typical wireless telecommunication arrangement;

[18] Fig. 2 is a simplified schematic diagram illustrating a typical arrangement for sending data bearer messages such as short message service to a wireless device;

[19] Fig. 3 is a simplified schematic diagram illustrating a typical wireless transaction arrangement; and

BNSDOCID: <WO_____0208863A2_I_>

[20] Fig. 4 is a simplified schematic diagram showing an exemplary embodiment of a wireless device in accordance with the present invention.

DETAILED DESCRIPTION OF THE INVENTION

[21] Fig. 1 is a simplified schematic diagram illustrating a typical wireless telecommunication arrangement. A network 10 communicates with a wireless device 14, such as a mobile phone, via a transmission station 12. The transmission station 12 uses over-the-air communications to communicate with the wireless device 14. Over-the-air communication protocols which can be used to implement wireless communications between the wireless device 14 and the network 10 include, for example, GSM, CDMA, TDMA, UMTS, etc. A person of ordinary skill in the art will know of other ways and methods to implement over-the-air communications.

[22] Fig. 2 is a simplified schematic diagram illustrating a typical arrangement for sending data bearer messages such as short message service to a wireless device 14. An application program 16 residing on a host processor 18 uses a communication link 20, such as a TCP/IP link over the Internet, to communicate with a data bearer message controller 22 within the network 10 to transmit a data bearer message such as a short message service message to the wireless device 14, such as a mobile phone, via a transmission station 12.

[01] Fig. 3 is a simplified schematic diagram illustrating a typical wireless transaction arrangement. A vending machine 24 with a short range radio communication transceiver and the wireless device 14, such as a mobile phone with a short range radio communication transceiver, communicate using a short range radio communication link 26. Short range radio communication links which can be used to implement wireless communications between the wireless device 14 and the vending machine 24 include, for example, Bluetooth ™ wireless communication links. A person of ordinary skill in the art will know of other ways and methods to communicate transactional data between two devices. As another example, vending machine 24 and wireless device 14, each with the appropriate transceiver, can communicate transactional data using a data bearer message service such as short message service.

[24] Referring to Fig. 4, there is shown an exemplary embodiment of the wireless device 14 in accordance with the present invention. According to the exemplary embodiment, the wireless device 14 includes an account management application 30 which permits the usage and account activities of the wireless device 14 to be tracked and

BNSDOCID: <WO_____0208863A2_I_>

monitored on an individual basis. The account management application 30 functions as multiple virtual wallets and is capable of maintaining a number of different accounts which are chargeable for calls or transactions handled by the wireless device 14. The different accounts include, for example, traditional postpaid account, postpaid monitored or controlled usage account, and prepaid account.

[25] The account management application 30 can reside on executable memory within the wireless device 14. Such memory can be one of any type such as ROM, EPROM, or flash memory. The account management application 30 can store dynamic data in RAM and utilize nonvolatile memory such as EEPROM or flash memory to store control data. Alternatively, the account management application 30 can reside on a smart card, such as a universal subscriber identification module (USIM) or Universal Identity Module (UIM), which is attachable to the wireless device 14.

[26] According to an exemplary embodiment, the account management application 30 further interacts with other applications, such as the accounting application 32 described below, so as to properly manage and process the different accounts. The accounting application 32 is capable of calculating calling charges in real time or on the fly. An example of the accounting application 32 is the complex billing algorithm described in the '100 Patent. The complex billing algorithm factors the multiple variables of a telephone call from a mobile phone into a billing equation that virtually mirrors the factors considered by public switched network providers and participating wireless service providers, (of which there may be more than one in a single call). The resultant call charge accurately approximates the summation of real charges that will be billed by the participating service providers thereby enabling an instantaneous calculation and display of calling charges. The complex billing algorithm can be expanded to accommodate special charges of service providers or called stations or special discounts or premiums for data transfer calls. The accounting application 32 can reside on executable memory within the wireless device 14. Such memory can be one of any type such as ROM, EPROM, or flash memory. The accounting application 32 can store dynamic data in RAM and utilize nonvolatile memory such as EEPROM or flash memory to store control data. Alternatively, the accounting application 32 can reside on a smart card, such as a universal subscriber identification module (USIM) or Universal Identity Module (UIM), which is attachable to the wireless device 14. In the alternative, it is to be also understood that the accounting application 32 may reside on the network 10. A

BNSDOCID: <WO_____0208863A2_I_>

person of ordinary skill in the art will know of ways and methods to obtain and retrieve calling charge information from an accounting application 32 residing on the network 10.

[27] It is to be further understood that the accounting applications 32 may reside either in the wireless device 14 or on the network 10 which is accessible to the wireless device 14. Depending on design specification or constraints, the functionality of the account management application 30 may be incorporated into or combined with the accounting application 32.

[28] The wireless device 14 can be programmed using systems such as that described in U.S. Patent No. 6,243,574 B1. In addition to installing account management application 30 and accounting applications 32, programming can include providing data, such as initial monetary values for pre-paid accounts or credit limits, to the wireless device 14. Alternatively, the wireless device 14 can be programmed over the air using DTMF signals, or a data bearer communication service such as short message service, initiated from an application program 16 residing on a host processor 18 such as described in the '100 Patent.

[29] The wireless device 14 is preferably a contemporary unit with an LCD display screen for display of numeric or alphanumeric data, such as a user menu and warning messages; a keypad for entry of data, such as menu selections; and a timer for determining the duration of calls thereby allowing calling charges to be calculated. In the alternative, a person of ordinary skill in the art will know that timer information can be obtained from the network 10.

[30] In an exemplary embodiment, the account management application 30 charges a call or transaction to the account selected by a user. The account selection is accomplished via a user interface. The user interface permits the user to interact with the account management application 30 and select which one of the accounts is to be used for each call or transaction. Furthermore, the user interface also allows the user to perform certain account management functions. For example, the user, via the user interface, may transfer balances between accounts or perform other typical accounting functions. As another example, the user, via the user interface, may change the account to which a particular call has been charged. Preferably, the user interface is implemented in the form of a menu of available accounts presented on the LCD screen of the wireless device 14.

[31] In an exemplary mode of operation, the usage and account activities of the wireless device 14 are monitored and tracked as follows. In the situation where an outgoing call is to be made via the wireless device 14, before such call is made, the user

BNSDOCID: <WO_____0208863A2_I_>

using the user interface selects which account is to be charged for that call. Once the account is selected, the user then continues with the normal procedures to make the call. If, for example, a prepaid account is selected, the accounting application 32 then calculates the charges to be debited and the account management application 30 accordingly debits the selected prepaid account.

[32] Similarly, in the situation where an incoming call is to be received by the wireless device 14, before such call is answered, the user using the user interface selects which account is to be charged for that call. Once the account is selected, the user then continues with the normal procedures to receive the call. If, for example, a postpaid account is selected, the charges for the call are calculated and the account management application 30 accordingly updates the postpaid account.

[33] As described above, a selected account is charged for a call handled by the wireless device 14. However, it should be understood that an account may also be charged for any transaction handled by the wireless device 14. That is, the account management application 30 is also able to monitor and track transactions handled by the wireless device 14. For example, referring to Fig. 3, if the wireless device 14 is used to communicate with the vending machine 24 to make a purchase, an appropriate account on the wireless device 14 can similarly be charged for making that purchase.

[34] Alternatively, the account management application 30 may automatically select the account to be charged from a multifactor algorithm. For example, where the wireless device 14 is a multi-line mobile phone, the account management application 30 detects which line of the multi-line mobile phone is in use and charges the account associated with that line. The calling charges to be applied to that account is determined by the accounting application 32. For example, the account management application 30 may select and apply a postpaid account for calls made or received on one line and select and apply a prepaid account for calls made or received on another line.

[35] In another exemplary embodiment, the account management application 30 is able to determine the telephone number of the device which originated the call using the network 10 automatic number identification features, and charge the account associated with that telephone number in a table stored on EEPROM or flash memory within the wireless device 14. In the event that the originating telephone number was not found in the table, a default account is then charged or the user is prompted to select an account to be charged for the call. The timing of the prompt may vary depending on design. For example, the prompt may occur after the call is concluded, if the available

BNSDOCID: <WO_____0208863A2_I_>

prepaid fund and/or credit limit of all potentially chargeable accounts was sufficient. Alternatively, the timing of the prompt may also occur at the preprogrammed time for warning of exhaustion of the available prepaid fund and/or credit limit based on the account, out of all potentially chargeable accounts, which first reaches the time for such warning. It is understood that the multifactor algorithm may include one or more of the above factors, as well as other factors appropriate for selecting the account to be charged.

[36] In an exemplary embodiment , the account management application 30 maintains each account according to an algorithm programmed by the service provider or by authorized corporate personnel. For example, an application program 16 residing on a host processor 18 can provide secure access to authorized corporate personnel to allow such personnel to enter control data with respect to each account. The application program 16 can initiate the transmission of a data bearer message, such as a short message service message, which, when received by the wireless device 14, accordingly reprograms the wireless device 14 with such control data. For example, one account may be set up to be a traditional postpaid account with a limit on usage and a second account may be set up to be a prepaid account. Corporate procedures may require the user to use the first account only for legitimate business calls. The user's compliance with such procedures may be monitored through call detail records stored on the wireless device 14 and transmitted to a host processor as described in the '418 and '669 Patents.

[37] It is understood that the call detail records can be stored on RAM or other memory within the wireless device 14, or alternatively, the call detail records can be stored on a smart card, such as a universal subscriber identification module (USIM), which is attachable to the wireless device 14.

[38] The control data transmitted to the wireless device 14 can also be used to determine the consequence of the user reaching a usage limit. For example, one such consequence is for the account management application 30 to generate and transmit an SMS message, or other data bearer message, to the appropriate corporate authority warning that the user had exceeded the usage limit and that review of the call detail records is warranted. Another such consequence is for the account management application 30 to temporarily restrict operation of the wireless device 14, allowing only emergency calls and calls to customer representatives until the restriction is removed. Corporate procedures may permit personal calls on the same wireless device 14 if the user utilizes the second account, the prepaid account. Authorized corporate personnel may receive acceptable forms of payment from the user, and, using the application program

BNSDOCID: <WO_____0208863A2_I_>

16, transmit control data to the wireless device 14 adding funds to the prepaid account accordingly, similar to the description in the '100 Patent.

[39] In another exemplary embodiment, an application program 16 on a host processor 18 is able to provide secure access to authorized personnel of a service provider or, in an intra-corporate system, of the corporation to change control data with respect to each account. The application program 16 can initiate the transmission of a data bearer message, such as a short message service message, which, when received by the wireless device 14, accordingly reprograms the wireless device 14 with such control data. Examples of such changes include changes in the rate tables utilized by the accounting application 32, changes in credit limits for controlled post-paid accounts, and changes in paid funds in pre-paid accounts etc. Alternatively, the users may be provided with over the air access to application program 16 on the host processor 18 to make limited changes, such as using credit cards or prepaid calling cards to add funds to pre-paid accounts, similar to the description provided in the '100 Patent. Furthermore, the updated rate table may be transmitted to the wireless device 14 when the user applies for an increase in the internal phone account.

[40] In an exemplary embodiment, the account management application 30 is able to generate audio warnings through the speaker of the wireless device 14 and/or warning messages displayed on the LCD screen of the wireless device 14 so as to inform the user that s/he is about to exhaust the credit limit or prepaid funds. The warning messages may include information identifying the applicable account and the amount of remaining funds or credit.

[41] The system of the present invention provides substantial flexibility by the features described above. For example, a user of the wireless device 14 is given the flexibility to pay for each call differently on an ad hoc basis. A user may wish to separate and pay for the calls based on the nature of each call. Business and personal calls handled by the same wireless device 14 may be paid from different accounts. A business call is to be paid from one account and a personal call is to be paid from another account. A user may also wish to use different accounts to pay for different calls; one call may be paid from a prepaid account, while another call may be charged to a postpaid account.

[42] It is understood that the examples and embodiments described herein are for illustrative purposes only and that various modifications or changes in light thereof will be suggested to persons skilled in the art and are to be included within the spirit and purview of this application and scope of the appended claims. All publications, patents,

BNSDOCID: <WO 0208863A2_I_>

and patent applications cited herein are hereby incorporated by reference for all purposes in their entirety.

BNSDOCID: <WO_____0208863A2_I_>

WHAT IS CLAIMED IS:

1. A system for handling a plurality of account activities, comprising:
a wireless device capable of performing a plurality of billable operations;
an account management application residing in the wireless device;
wherein the account management application is configured to manage a plurality of accounts; and
wherein each billable operation performed by the wireless device is selectively charged to one of the plurality of accounts.

2. The system according to claim 1 further comprising:
a user interface configured to allow a user to determine how each billable operation performed by the wireless device is to be selectively charged to one of the plurality of accounts.

3. The system according to claim 1 wherein the account management application automatically selects one of the plurality of accounts to be charged for at least one of the plurality of billable operations in accordance with an algorithm.

4. The system according to claim 1 further comprising:
an accounting application configured to calculate charges for each billable operation performed by the wireless device;
wherein the account management application functions in cooperation with the accounting application to manage the plurality of accounts.

5. The system according to claim 1wherein the plurality of billable operations includes making or receiving a voice or data communication.

6. The system according to claim 5 wherein how each billable operation performed by the wireless device is to be selectively charged to one of the plurality of accounts depends on origin or destination of the voice or data communication.

7. The system according to claim 1 wherein the wireless device is a mobile phone.

8. The system according to claim 1 wherein the account management application resides on a smart card attachable to the wireless device.

BNSDOCID: <WO_____0208863A2_I_>

9. The system according to claim 1 wherein the account management application resides on a memory residing in the wireless device.

10. The system according to claim 1 wherein the accounting application resides on a memory residing in the wireless device.

11. The system according to claim 1 wherein the accounting application resides on a network.

12. The system according to claim 1 wherein the account management application is configured so as to allow a user to transfer balances amongst the plurality of accounts.

13. The system according to claim 1 wherein the plurality of accounts includes a postpaid account and a prepaid account.

14. The system according to claim 1 wherein at least one of the plurality of accounts has a usage limit; and

wherein the plurality of billable operations performable by the wireless device is restricted when the usage limit is exceeded.

15. A wireless device configured to perform a plurality of billable operations, comprising:

an account management application residing on the wireless device and configured to maintain a plurality of accounts;

an accounting application configured to calculate charges for each billable operation performed by the wireless device; and

a user interface configured to allow a user to selectively determine how each billable operation performed by the wireless device is to be charged to one of the plurality of accounts;

wherein the account management application and the accounting application function in cooperation with each other in order to maintain the plurality of accounts.

16. The wireless device of claim 15 wherein the plurality of billable operations includes making or receiving a voice or data communication.

BNSDOCID: <WO_____0208863A2_I_>

17. The wireless device of claim 16 wherein how each billable operation performed by the wireless device is to be selectively charged to one of the plurality of accounts depends on origin or destination of the voice or data communication.

18. The wireless device of claim 15 wherein the wireless device is a mobile phone.

19. The wireless device of claim 15 wherein the account management application resides on a smart card attached to the wireless device.

20. The wireless device of claim 15 wherein the account management application resides on a memory residing in the wireless device.

21. The wireless device of claim 15 wherein the accounting application resides on a network.

22. The wireless device of claim 15 wherein the account management application is configured so as to allow the user to transfer balances amongst the plurality of accounts.

23. The wireless device of claim 14 wherein the plurality of accounts includes a postpaid account and a prepaid account.

24. The wireless device of claim 14 wherein at least one of the plurality of accounts has a usage limit; and

wherein the plurality of billable operations performable by the wireless device is restricted when the usage limit is exceeded.

25. A mobile phone comprising:

a first line and a second line both configured to make and receive calls; and

an account management application residing on the mobile phone and configured to manage a plurality of accounts;

wherein calls made or received via the first line is charged to one of the plurality of accounts and calls made or received via the second line is charged to another one of the plurality of accounts.

BNSDOCID: <WO_____0208863A2_I_>

26. The mobile phone of claim 25 further comprising:

a user interface configured to allow a user to selectively determine how each call made or received by the mobile phone is to be charged to one of the plurality of accounts.

27. The mobile phone of claim 25 further comprising:

an accounting application configured to calculate charges for each call made or received by the mobile phone.

28. The mobile phone of claim 25 wherein the account management application resides on a smart card attachable to the mobile phone.

29. The mobile phone of claim 25 wherein the account management application resides on a memory residing in the mobile phone.

30. The mobile phone of claim 27 wherein the accounting application resides on a memory residing in the mobile phone.

31. The mobile phone of claim 27 wherein the accounting application resides on a network.

32. The mobile phone of claim 25 wherein the plurality of accounts includes a postpaid account and a prepaid account.

33. The mobile phone of claim 25 wherein the calls made or received via the first line include business calls and the calls made or received via the second line include personal calls.

34. The mobile phone of claim 25 wherein the account management application is configured so as to allow the user to transfer balances amongst the plurality of accounts.

35. A method for tracking account activities relating to a plurality of billable operations performable by a wireless device, comprising:

selecting one of a plurality of accounts to be charged for a billable operation, wherein the plurality of accounts are maintained on the wireless device;

calculating charges to be paid for the billable operation;

BNSDOCID: <WO_____0208863A2_I_>

causing the wireless device to perform the billable operation; and

updating the selected account.

36. The method according to claim 35 wherein the step of selecting one of the plurality of accounts further comprises:

allowing a user to select one of the plurality of accounts via a user interface.

37. The method according to claim 35 wherein the step of calculating charges to be paid for the billable operation is performed by an accounting application.

38. The method according to claim 35 wherein the accounting application resides on a memory residing in the wireless device.

39. The method according to claim 35 wherein the accounting application resides on a network.

40. The method according to claim 35 wherein the wireless device is a mobile phone.

41. The method according to claim 35 wherein the billable operation includes making or receiving a voice or data communication.

42. The method according to claim 41 wherein the step of selecting one of a plurality of accounts to be charged for the billable operation further comprises:

identifying origin or destination of the voice or data communication;

selecting the one of the plurality of accounts to be charged for the billable operation based on the identified origin or destination of the voice or data communication.

43. The method according to claim 35 further comprising:

restricting ability of the wireless device to perform the billable operation when credit limit of at least one of the plurality of accounts is exceeded.

44. The method according to claim 35 further comprising:

BNSDOCID: <WO_____0208863A2_I_>

restricting ability of the wireless device to perform the billable operation when prepaid level of at least one of the plurality of accounts is exhausted or goes below a pre-established limit.

45. A method for tracking account activities made by a mobile phone having a first line and a second line both configured to make and receive calls, comprising:

assigning a first account to calls made or received via the first line;

assigning a second account to calls made or received via the second line, wherein the first and second accounts are maintained on the mobile phone;

making or receiving a call via either the first line or the second line;

calculating charges to be paid for the call; and

updating either the first account or the second account based on the calculated charges depending on which one of the first and second lines the call is made or received.

BNSDOCID: <WO_____0208863A2_I_>

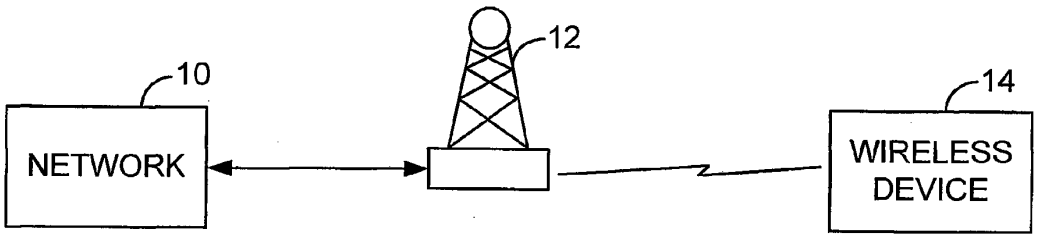


FIG. 1.

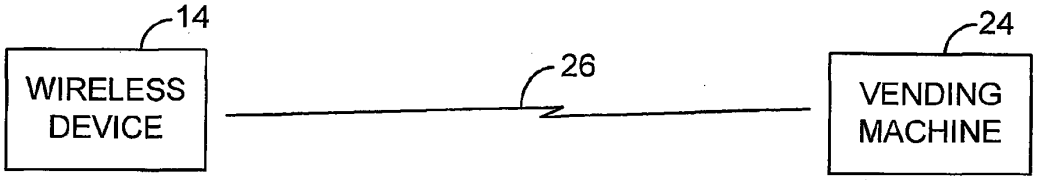


FIG. 3.

BNSDOCID: <WO_____0208863A2_I_>

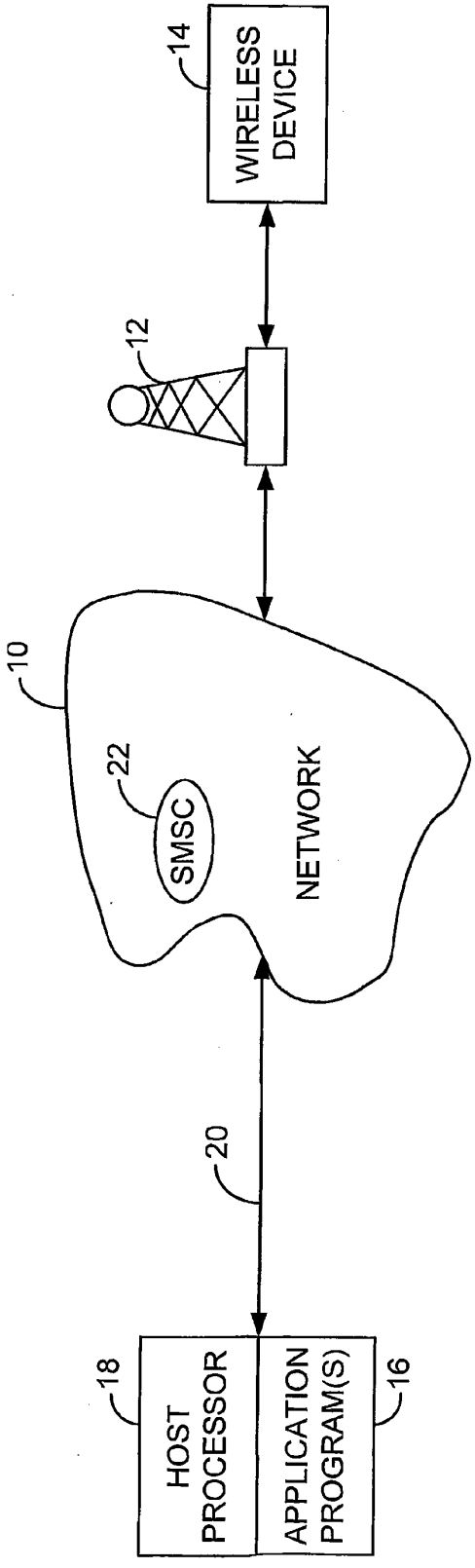


FIG. 2.

BNSDOCID: <WO_____0208863A2_I_>

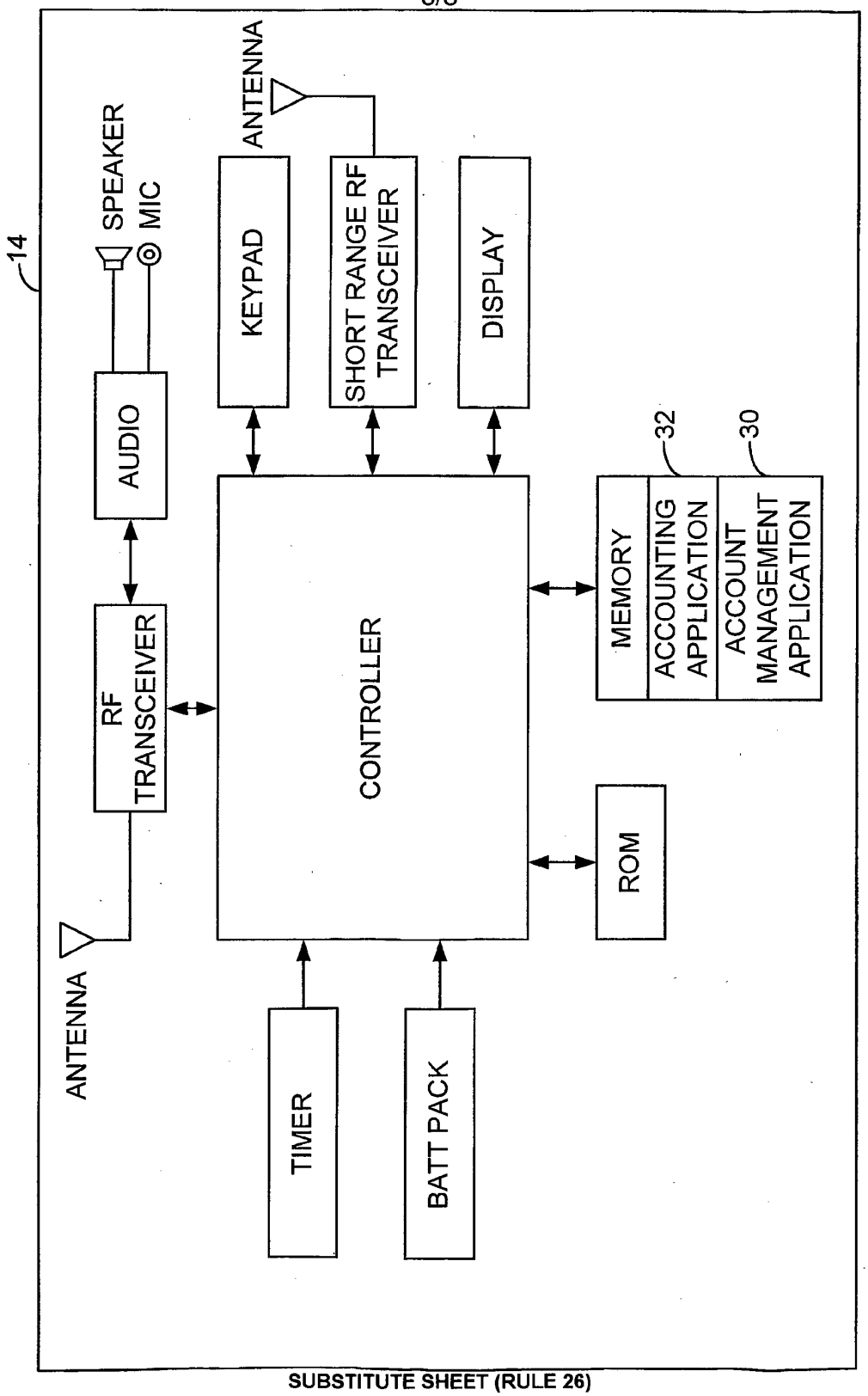


FIG. 4.

BNSDOCID: <WO_____0208863A2_I_>

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
31 January 2002 (31.01.2002)

PCT

(10) International Publication Number
WO 02/08863 A3

(51) International Patent Classification[7]: H04M 15/00

(21) International Application Number: PCT/US01/23226

(22) International Filing Date: 23 July 2001 (23.07.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/220,241 21 July 2000 (21.07.2000) US

(71) Applicant: TELEMAC CORPORATION [US/US]; 6701 Center Drive West, Suite 700, Los Angeles, CA 90045 (US).

(72) Inventors: WATLER, Theodore, W.; 5341 E. 4th Street, Long Beach, CA 90814-1920 (US). HANLEY, Jerry; 1315 Franklin Street, #D, Santa Monica, CA 90404 (US).

(74) Agents: NG, Horace et al.; Townsend and Townsend and Crew LLP, Two Embarcadero Center, 8th Floor, San Francisco, CA 94111-3834 (US).

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

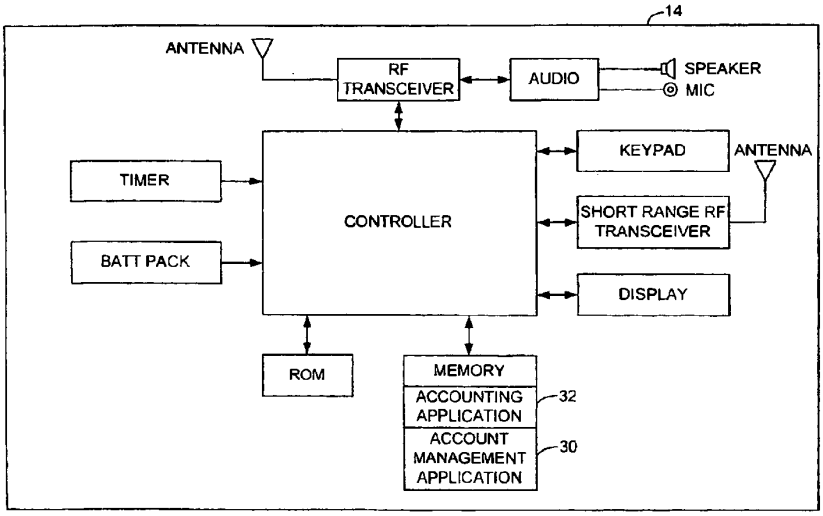
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW,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

Published:
— *with international search report*

(88) Date of publication of the international search report:
30 May 2002

[Continued on next page]

(54) Title: MULTIPLE VIRTUAL WALLETS IN WIRELESS DEVICES



(57) Abstract: A system having a wireless device (14) capable of monitoring and tracking its own usage and account activities is disclosed. The wireless device (14) includes an account management application (30) and accounting applications (32). The account management application (30) manages a variety of accounts in conjunction with the accounting applications (32) and is used by a user to determine how each call/transaction is to be paid for. For example, the user of the wireless device (14) may wish to pay for business calls using a first account and personal calls using a second account.

WO 02/08863 A3

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

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/23226

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : H04M 15/00
US CL : 455/405, 406, 407, 408; 379/114.26

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 455/405, 406, 407, 408, 409, 422, 575; 379/114.01, 114.03, 114.26

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,774,533 A (PATEL) 30 June 1998 (30.06.1998), column 7, lines 8-31, column 17, line 57 - column 18, line 19, and figure 3.	1-45
Y	US 5,956,653 A (LAHTI) 21 September 1999 (21.09.1999), column 2, lines 7-38, and figure 1.	1-45
Y	US 5,428,666 A (FYFE et al) 27 June 1995 (27.06.1995), column 3, line 59 - column 7, line 36, and figures 1-2.	1-45
Y	US 5,109,401 A (HATTORI et al) 28 April 1992 (28.04.1992), see abstract, column 5, line 56 - column 6, line 56, and figure 3.	14, 24, 43, 44
A	US 5,657,373 A (HERMANSSON et al) 12August 1997 (12.08.1997), column 4,1 ine 2 - column 5, line 2.	1-45

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 September 2001 (17.09.2001)	22 JAN 2002
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703)305-3230	Authorized officer Quochien Vuong Telephone No. (703) 306-4530

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

BNSDOCID: <WO_____0208863A3_I_>

Electronic Acknowledgement Receipt

EFS ID:	30024026
Application Number:	15582350
International Application Number:	
Confirmation Number:	7797
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:	RALEP007C11C3C2C3C2
Receipt Date:	08-AUG-2017
Filing Date:	28-APR-2017
Time Stamp:	22:56:04
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	Transmittal Letter	P007C11C3C2C3C2_IDSTransLtr.pdf	59451 57790cf523e66b5644de94ccab695c69a3e7c39d	no	2

Warnings:

Information:					
2	Information Disclosure Statement (IDS) Form (SB08)	P007C11C3C2C3C2_IDS1.pdf	1062864 eff0497e45febb676e67d60960fcaa2d39e7ada3	no	35
Warnings:					
Information:					
3	Information Disclosure Statement (IDS) Form (SB08)	P007C11C3C2C3C2_IDS2.pdf	1066182 500303b74c72067c42367e9cfaedf874d6467c5b	no	40
Warnings:					
Information:					
4	Information Disclosure Statement (IDS) Form (SB08)	P007C11C3C2C3C2_IDS3.pdf	1060964 26f79b2fcbc5921e19e70d38988472b7618e6b9c	no	31
Warnings:					
Information:					
5	Information Disclosure Statement (IDS) Form (SB08)	P007C11C3C2C3C2_IDS4.pdf	1060647 f8520f38dbd60c453b714d00b96dc9561d80b1c8	no	31
Warnings:					
Information:					
6	Information Disclosure Statement (IDS) Form (SB08)	P007C11C3C2C3C2_IDS5.pdf	1055485 76f9b4df447ad59b146d612d4dd4d786fe912ad3	no	10
Warnings:					
Information:					
7	Foreign Reference	2093.pdf	3514622 c65fb898082d5782c1d6c4ab30f0d6f6ceb5ae6b	no	45
Warnings:					
Information:					
8	Foreign Reference	2094.pdf	3952944 dfa7cbac15ff6f3701105acf137953f96f215840	no	25
Warnings:					
Information:					
		Total Files Size (in bytes):	12833159		

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Raleigh	Examiner:	not yet assigned
Serial No.:	15/582,350	Art Unit:	2447
Filed:	April 28, 2017	Conf. No.:	7797
Title:	Automated Device Provisioning and Activation		

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 Nos. 15/239,398 filed August 17, 2016; 14/979,233 filed December 22, 2015; 14/667,353 filed March 24, 2015; 14/263,604 filed April 28, 2014; and 12/380,780 filed March 2, 2009, of which the instant application is from the same direct family. Any foreign or non-patent references not submitted in those family applications 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: August 8, 2017

By: /James E. Harris/
James E. Harris
Reg. No. 40013
Headwater Research LLC
1011 Pruitt Place
Tyler, TX 75703
(903) 201-6212

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: Aug. 8, 2017 By: /Ann Taylor/
Ann Taylor

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
15/582,350	04/28/2017	2447	0.00	RALEP007C11C3C2C3C2	1	1

CONFIRMATION NO. 7797

106963
Headwater Research LLC
1011 Pruitt Place
Tyler, TX 75703

FILING RECEIPT

OC000000091158833

Date Mailed: 05/08/2017

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 Research LLC, Tyler, TX;

Power of Attorney: The patent practitioners associated with Customer Number 106963

Domestic Priority data as claimed by applicant

This application is a CON of 15/239,398 08/17/2016 PAT 9641957
which is a CON of 14/979,233 12/22/2015 PAT 9532161
which is a CON of 14/667,353 03/24/2015 PAT 9232403
which 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 for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: Yes

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

If Required, Foreign Filing License Granted: 05/05/2017

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 15/582,350**

Projected Publication Date: To Be Determined - pending completion of Missing Parts

Non-Publication Request: No

Early Publication Request: Yes
**** SMALL ENTITY ****
Title

Automated Device Provisioning and Activation

Preliminary Class

709

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.

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
15/582,350	04/28/2017	Gregory G. Raleigh	RALEP007C11C3C2C3C2

CONFIRMATION NO. 7797

106963
Headwater Research LLC
1011 Pruitt Place
Tyler, TX 75703

FORMALITIES LETTER

OC000000091156834

Date Mailed: 05/08/2017

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The statutory basic filing fee is missing.
- The application search fee must be submitted.
- The application examination fee must be submitted.
- Surcharge as set forth in 37 CFR 1.16(f) must be submitted.
  The surcharge is due for any one of:
  - late submission of the basic filing fee, search fee, or examination fee,
  - late submission of inventor's oath or declaration,
  - filing an application that does not contain at least one claim on filing, or
  - submission of an application filed by reference to a previously filed application.

SUMMARY OF FEES DUE:

The fee(s) required within **TWO MONTHS** from the date of this Notice to avoid abandonment is/are itemized below. Small entity discount is in effect. If applicant is qualified for micro entity status, an acceptable Certification of Micro Entity Status must be submitted to establish micro entity status. (See 37 CFR 1.29 and forms PTO/SB/15A and 15B.)

- $ **70** basic filing fee.
- $ **800** for **159** electronically equivalent pages in excess of **100** application size fee.
- $ **70** surcharge.
- $ **300** search fee.
- $ **360** examination fee.
- $(**0**) previous unapplied payment amount.
- $ **1600** TOTAL FEE BALANCE DUE.

Replies must be received in the USPTO within the set time period or must include a proper Certificate of Mailing or Transmission under 37 CFR 1.8 with a mailing or transmission date within the set time period. For more information and a suggested format, see Form PTO/SB/92 and MPEP 512.

Replies should be mailed to:

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web, including a copy of this Notice and selecting the document description "Applicant response to Pre-Exam Formalities Notice". https://sportal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html

For more information about EFS-Web please call the USPTO Electronic Business Center at 1-866-217-9197 or visit our website at http://www.uspto.gov/ebc.

If you are not using EFS-Web to submit your reply, you must include a copy of this notice.

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

/swong/

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 15/582,350

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))	1 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.

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 Research LLC
1011 Pruitt Place
Tyler, TX 75703 (USA)

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	January 3, 2017
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:	29069451
Application Number:	15582350
International Application Number:	
Confirmation Number:	7797
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:	RALEP007C11C3C2C3C2
Receipt Date:	28-APR-2017
Filing Date:	
Time Stamp:	19:12:29
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	Application Data Sheet	P007C11C3C2C3C2_ADS.pdf	1823545 ceb55c6cc447d26c30306fe2398449f6246e1fff	no	9

Warnings:

Information:					
2		P007C11C3C2C3C2_Spec.pdf	1089405 697a6eccc8258096ebc0608a8ad145862625122a	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	P007C11C3C2C3C2_RaleighDecl.pdf	104340 45fe2eb014a1714c92385418e355bdfd013a106a	no	1
Warnings:					
Information:					
4	Drawings-only black and white line drawings	P007C11C3C2C3C2_Drawings_Part1.pdf	10373531 e0fc5e83c7051baf9971ec66850158a151bbe2ed	no	54
Warnings:					
Information:					
5	Drawings-only black and white line drawings	P007C11C3C2C3C2_Drawings_Part2.pdf	8159440 2aa88e3fca51a61630c71981434904942cbd5b67	no	52
Warnings:					
Information:					
6	Power of Attorney	P007C11C3C2C3C2_HWR_POA.pdf	1117158 29f7900a48aab77b08ab016fed0337e3ae5a66d0	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	22667419		

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 (11-15)
Approved for use through 04/30/2017. 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	RALEP007C11C3C2C3C2
	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	US

Mailing Address of Inventor:

Address 1	1011 Pruitt Place		
Address 2			
City	Tyler	**State/Province**	TX
Postal Code	75703	**Country**	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	RALEP007C11C3C2C3C2	**Small Entity Status Claimed**	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	106	**Suggested Figure for Publication (if any)**	

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. 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	RALEP007C11C3C2C3C2
	Application Number	
Title of Invention	Automated Device Provisioning and Activation	

Filing By Reference:

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, 365(c), or 386(c) or indicate National Stage entry from a PCT application. Providing benefit claim 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" field blank.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
	Continuation of	15239398	2016-08-17

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. 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	RALEP007C11C3C2C3C2
	Application Number	
Title of Invention	Automated Device Provisioning and Activation	

Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
15239398	Continuation of	14979233	2015-12-22	9532161	2016-12-27
Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
14979233	Continuation of	14667353	2015-03-24	9232403	2016-01-05
Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
14/667353	Continuation of	14263604	2014-04-28	9037127	2015-05-19
Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
14263604	Continuation of	12/380780	2009-03-02	8839388	2014-09-16
Prior Application Status	Expired				Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) 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 or 371(c) 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 or 371(c) 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 or 371(c) 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:

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. 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	RALEP007C11C3C2C3C2
	Application Number	
Title of Invention	Automated Device Provisioning and Activation	

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. 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(i)(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

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.

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. 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	RALEP007C11C3C2C3C2
	Application Number	
Title of Invention	Automated Device Provisioning and Activation	

Authorization or Opt-Out of Authorization to Permit Access:

When this Application Data Sheet is properly signed and filed with the application, applicant has provided written authority to permit a participating foreign intellectual property (IP) office access to the instant application-as-filed (see paragraph A in subsection 1 below) and the European Patent Office (EPO) access to any search results from the instant application (see paragraph B in subsection 1 below).

Should applicant choose not to provide an authorization identified in subsection 1 below, applicant **must opt-out** of the authorization by checking the corresponding box A or B or both in subsection 2 below.

NOTE: This section of the Application Data Sheet is **ONLY** reviewed and processed with the **INITIAL** filing of an application. After the initial filing of an application, an Application Data Sheet cannot be used to provide or rescind authorization for access by a foreign IP office(s). Instead, Form PTO/SB/39 or PTO/SB/69 must be used as appropriate.

1. Authorization to Permit Access by a Foreign Intellectual Property Office(s)

A. Priority Document Exchange (PDX) - Unless box A in subsection 2 (opt-out of authorization) is 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 State Intellectual Property Office of the People's Republic of China (SIPO), the World Intellectual Property Organization (WIPO), and any other foreign intellectual property office participating with the USPTO in a bilateral or multilateral priority document exchange agreement in which a foreign application claiming priority to the instant patent application is filed, access to: (1) the instant patent application-as-filed and its related bibliographic data, (2) any foreign or domestic application to which priority or benefit is claimed by the instant application and its related bibliographic data, and (3) the date of filing of this Authorization. See 37 CFR 1.14(h)(1).

B. Search Results from U.S. Application to EPO - Unless box B in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the EPO access to the bibliographic data and search results from the instant patent application when a European patent application claiming priority to the instant patent application is filed. See 37 CFR 1.14(h)(2).

The applicant is reminded that the EPO's Rule 141(1) EPC (European Patent Convention) requires applicants to submit a copy of search results from the instant application without delay in a European patent application that claims priority to the instant application.

2. Opt-Out of Authorizations to Permit Access by a Foreign Intellectual Property Office(s)

☐ A. Applicant **DOES NOT** authorize the USPTO to permit a participating foreign IP office access to the instant application-as-filed. If this box is checked, the USPTO will not be providing a participating foreign IP office with any documents and information identified in subsection 1A above.

☐ B. Applicant **DOES NOT** authorize the USPTO to transmit to the EPO any search results from the instant patent application. If this box is checked, the USPTO will not be providing the EPO with search results from the instant application.

NOTE: Once the application has published or is otherwise publicly available, the USPTO may provide access to the application in accordance with 37 CFR 1.14.

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. 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	RALEP007C11C3C2C3C2
	Application Number	
Title of Invention	Automated Device Provisioning and Activation	

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.

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 Research LLC		
Mailing Address Information For Applicant:			
Address 1	1011 Pruitt Place		
Address 2			
City	Tyler	**State/Province**	TX
Country	US	Postal Code	75703
Phone Number	903-201-6212	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 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 (11-15)
Approved for use through 04/30/2017. 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	RALEP007C11C3C2C3C2
	Application Number	
Title of Invention	Automated Device Provisioning and Activation	

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. ☐

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 Application Data Sheet must be signed in accordance with 37 CFR 1.33(b). **However, if this Application Data Sheet is submitted with the INITIAL filing of the application and either box A or B is not checked in subsection 2 of the "Authorization or Opt-Out of Authorization to Permit Access" section, then this form must also be signed in accordance with 37 CFR 1.14(c).**

This Application Data Sheet **must** be signed by a patent practitioner if one or more of the applicants is a **juristic entity** (e.g., corporation or association). If the applicant is two or more joint inventors, this form must be signed by a patent practitioner, **all** joint inventors who are the applicant, or one or more joint inventor-applicants who have been given power of attorney (e.g., see USPTO Form PTO/AIA/81) on behalf of **all** joint inventor-applicants.

See 37 CFR 1.4(d) for the manner of making signatures and certifications.

Signature	/James E. Harris/			Date (YYYY-MM-DD)	2017-04-28
First Name	James E.	Last Name	Harris	Registration Number	40013

Additional Signature may be generated within this form by selecting the Add button. Add

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. 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	RALEP007C11C3C2C3C2
	Application Number	
Title of Invention	Automated Device Provisioning and Activation	

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 CooperationTreaty.

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

BACKGROUND OF THE INVENTION

[0001] 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.

[0002] 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

[0003] Various embodiments of the invention are disclosed in the following detailed description and the accompanying drawings.

[0004] FIG. 1 illustrates a simplified (e.g., "flattened") network architecture in accordance with some embodiments.

[0005] FIG. 2 illustrates another simplified (e.g., "flattened") network architecture including an MVNO (Mobile Virtual Network Operator) relationship in accordance with some embodiments.

[0006] FIG. 3 illustrates another simplified (e.g., "flattened") network architecture including two central providers in accordance with some embodiments.

[0007] FIG. 4 illustrates a network architecture including a Universal Mobile Telecommunications System (UMTS) overlay configuration in accordance with some embodiments.

[0008] FIG. 5 illustrates a network architecture including an Evolution Data Optimized (EVDO) overlay configuration in accordance with some embodiments.

[0009] FIG. 6 illustrates a network architecture including a 4G LTE and Wi-Fi overlay configuration in accordance with some embodiments.

[0010] FIG. 7 illustrates a network architecture including a WiMax and Wi-Fi overlay configuration in accordance with some embodiments.

[0011] 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.

[0012] FIG. 9 illustrates a hardware diagram of a device that includes a service processor in accordance with some embodiments.

[0013] FIG. 10 illustrates another hardware diagram of a device that includes a service processor in accordance with some embodiments.

[0014] FIG. 11 illustrates another hardware diagram of a device that includes a service processor in accordance with some embodiments.

[0015] FIG. 12 illustrates another hardware diagram of a device that includes a service processor in accordance with some embodiments.

[0016] 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.

[0017] 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.

[0018] 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.

[0019] FIG. 16 is a functional diagram illustrating a device based service processor and a service controller in accordance with some embodiments.

[0020] FIG. 17 is another functional diagram illustrating the device based service processor and the service controller in accordance with some embodiments.

[0021] 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.

[0022] FIG. 19 is another functional diagram illustrating the service processor and the service controller in accordance with some embodiments.

[0023] FIG. 20 is another functional diagram illustrating the service processor and the service controller in accordance with some embodiments.

[0024] FIG. 21 is another functional diagram illustrating the service processor and the service controller in accordance with some embodiments.

[0025] 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.

[0026] 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.

[0027] 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.

[0028] 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.

[0029] FIGS. 26A through 26H provide tables summarizing various service processor heartbeat functions and parameters in accordance with some embodiments.

[0030] FIGS. 27A through 27P provide tables summarizing various device based service policy implementation verification techniques in accordance with some embodiments.

[0031] FIGS. 28A through 28E provide tables summarizing various techniques for protecting the device based service policy from compromise in accordance with some embodiments.

[0032] 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.

[0033] 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.

[0034] 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.

[0035] 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.

[0036] 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.

[0037] 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.

[0038] 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.

[0039] 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.

[0040] 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.

[0041] FIG. 38 is a functional diagram illustrating a device service processor packet processing flow in accordance with some embodiments.

[0042] FIG. 39 is another functional diagram illustrating the device service processor packet processing flow in accordance with some embodiments.

[0043] FIG. 40 is another functional diagram illustrating the device service processor packet processing flow in accordance with some embodiments.

[0044] FIG. 41 provides a table summarizing various privacy levels for service history reporting in accordance with some embodiments.

[0045] FIGS. 42A through 42J provide tables summarizing various service policy control commands in accordance with some embodiments.

[0046] 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.

[0047] 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.

[0048] 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.

[0049] FIG. 46 is a functional diagram illustrating open, decentralized, device based mobile commerce transactions in accordance with some embodiments.

[0050] FIGS. 47A through 47B are transactional diagrams illustrating open, decentralized, device based mobile commerce transactions in accordance with some embodiments.

[0051] 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.

[0052] FIG. 49 illustrates a network architecture for an open developer platform for virtual service provider (VSP) partitioning in accordance with some embodiments.

[0053] 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.

[0054] 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.

[0055] FIG. 52 illustrates a network architecture for locating service controller device control functions in the access transport network in accordance with some embodiments.

[0056] FIG. 53 illustrates a network architecture for locating service controller device control functions in the radio access network in accordance with some embodiments.

[0057] 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.

[0058] 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.

[0059] FIG. 56 illustrates a 4G/3G/2G DPI/DPC enabled gateway in accordance with some embodiments.

[0060] 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.

[0061] FIG. 58 illustrates another 4G/3G/2G DPI/DPC enabled gateway in accordance with some embodiments.

[0062] 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.

[0063] FIG. 60 illustrates a 4G/3G/2G DPI/DPC enabled gateway and service controller device control system in accordance with some embodiments.

[0064] 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.

[0065] FIG. 62 illustrates another 4G/3G/2G DPI/DPC enabled gateway and service controller device control system in accordance with some embodiments.

[0066] 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.

[0067] 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

[0068] 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.

[0069] 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.

[0070] 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.

[0071] 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.

[0072] 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).

[0073] 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.

[0074] 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.

[0075] 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.

[0076] 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.

[0077] 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.

[0078] 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.

[0079] 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.

[0080] 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.

[0081] 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.

[0082] 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.

[0083] 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.

[0084] 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.

[0085] 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.

[0086] 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).

[0087] 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.

[0088] 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.

[0089] 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

[0090] 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.

[0091] 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.

[0092] 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

[0093] 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.

[0094] 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.

[0095] 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.

[0096] 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.

INCORPORATION BY REFERENCE

[0535] This application incorporates by reference the following US applications:

[0536] Application No. 12/380,780 entitled AUTOMATED DEVICE PROVISIONING AND ACTIVATION, filed March 2, 2009; 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.

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:

- [x] 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.

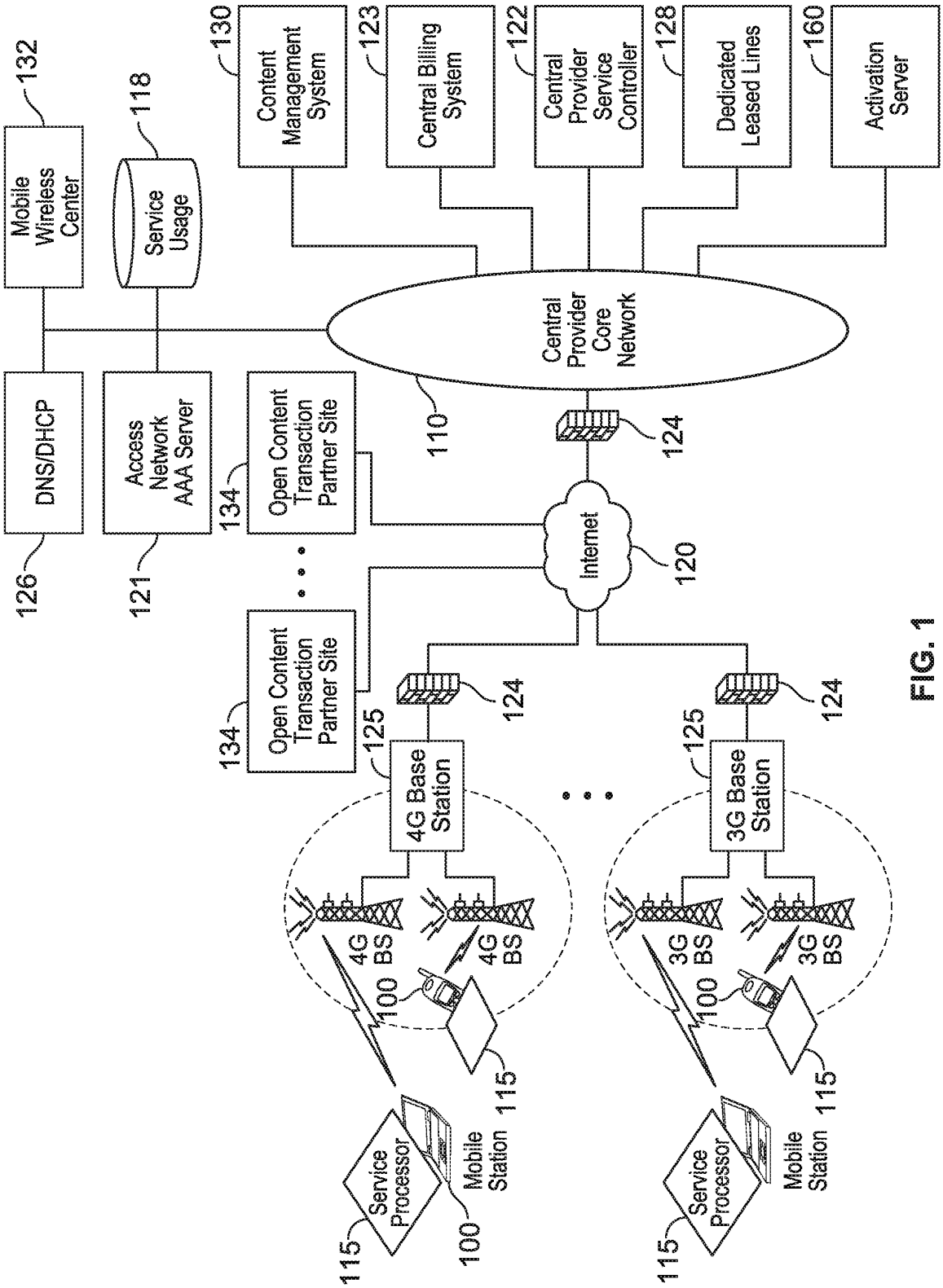

Mobile Wireless Center
132
Service Usage
118
Content Management System
130
Central Billing System
123
Central Provider Service Controller
122
Dedicated Leased Lines
128
Activation Server
160
DNS/DHCP
126
Access Network AAA Server
121
Open Content Transaction Partner Site
134
Central Provider Core Network
110
124
Internet
120
Open Content Transaction Partner Site
134
125
4G Base Station
3G Base Station
4G BS
3G BS
100
115
Service Processor
Mobile Station

FIG. 1

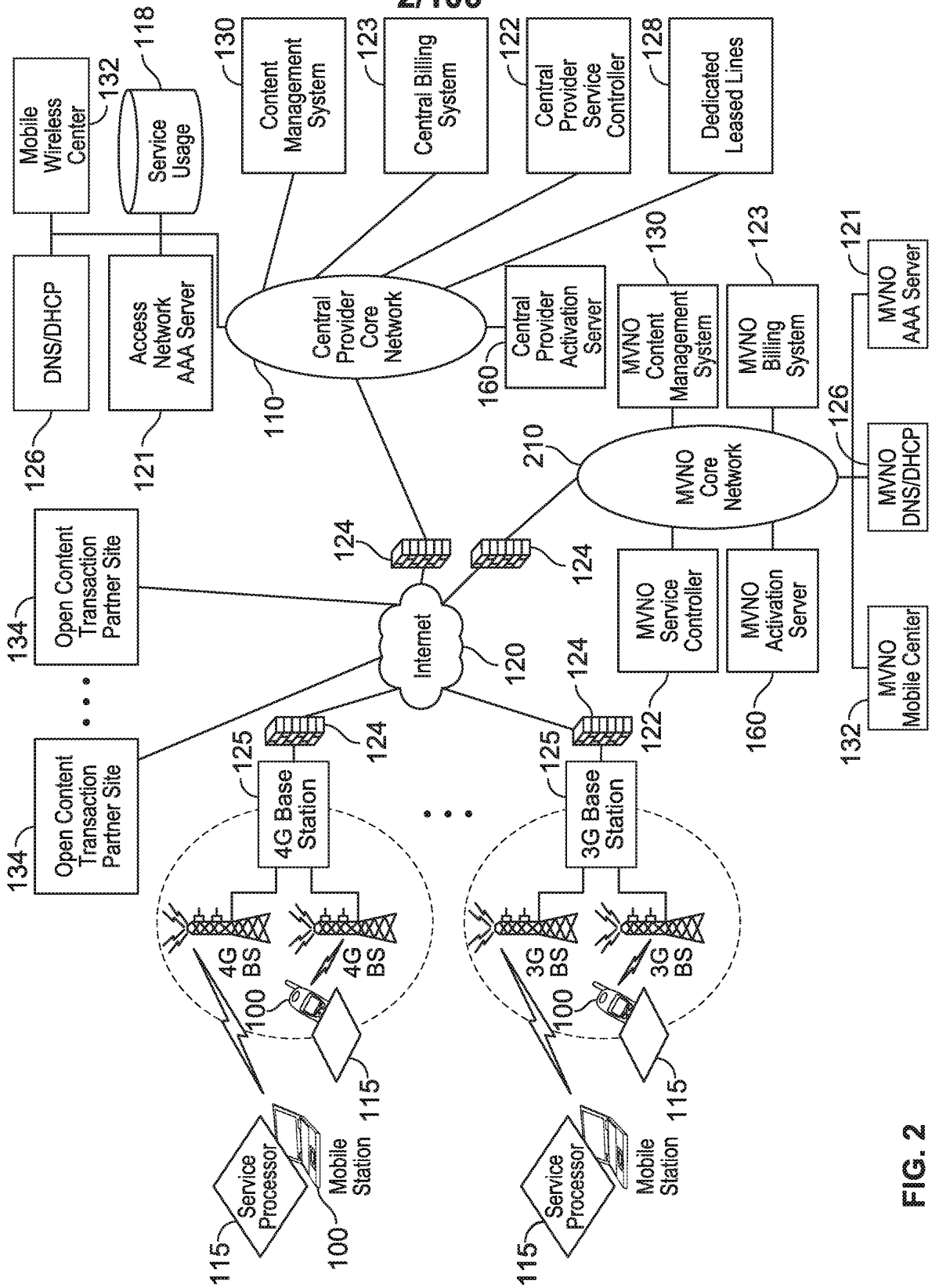

Mobile Wireless Center
132
Service Usage
118
Content Management System
130
Central Billing System
123
Central Provider Service Controller
122
Dedicated Leased Lines
128
DNS/DHCP
126
Access Network AAA Server
121
Central Provider Core Network
110
Central Provider Activation Server
160
MVNO Content Management 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

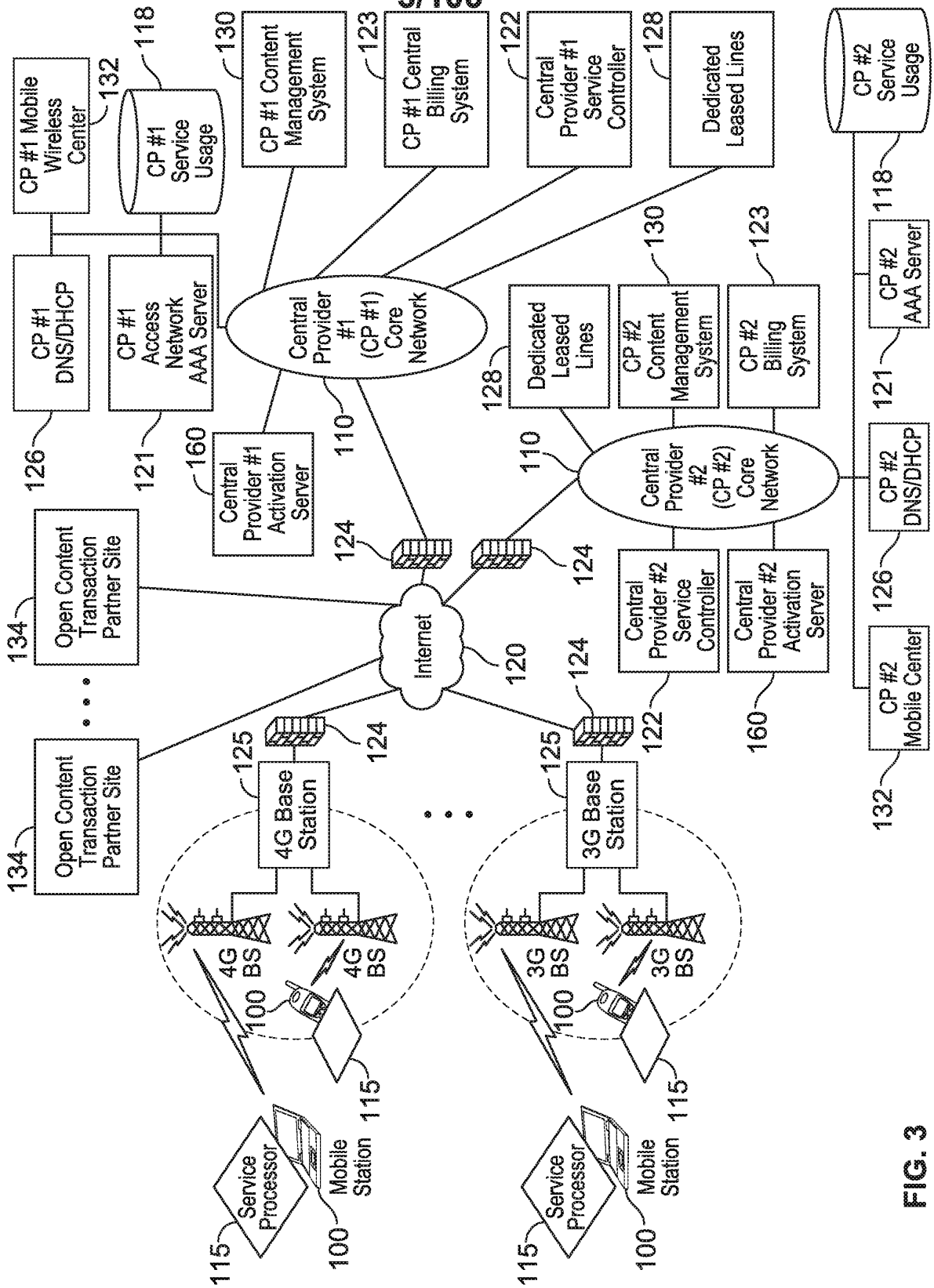

CP #1 Mobile Wireless Center
132
CP #1 Service Usage
118
CP #1 Content Management System
130
CP #1 Central Billing System
123
Central Provider #1 Service Controller
122
Dedicated Leased Lines
128
CP #2 Service Usage
CP #1 DNS/DHCP
126
CP #1 Access Network AAA Server
121
Central Provider #1 Activation 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
4G BS
3G BS
100
115
Service Processor
Mobile Station

FIG. 3

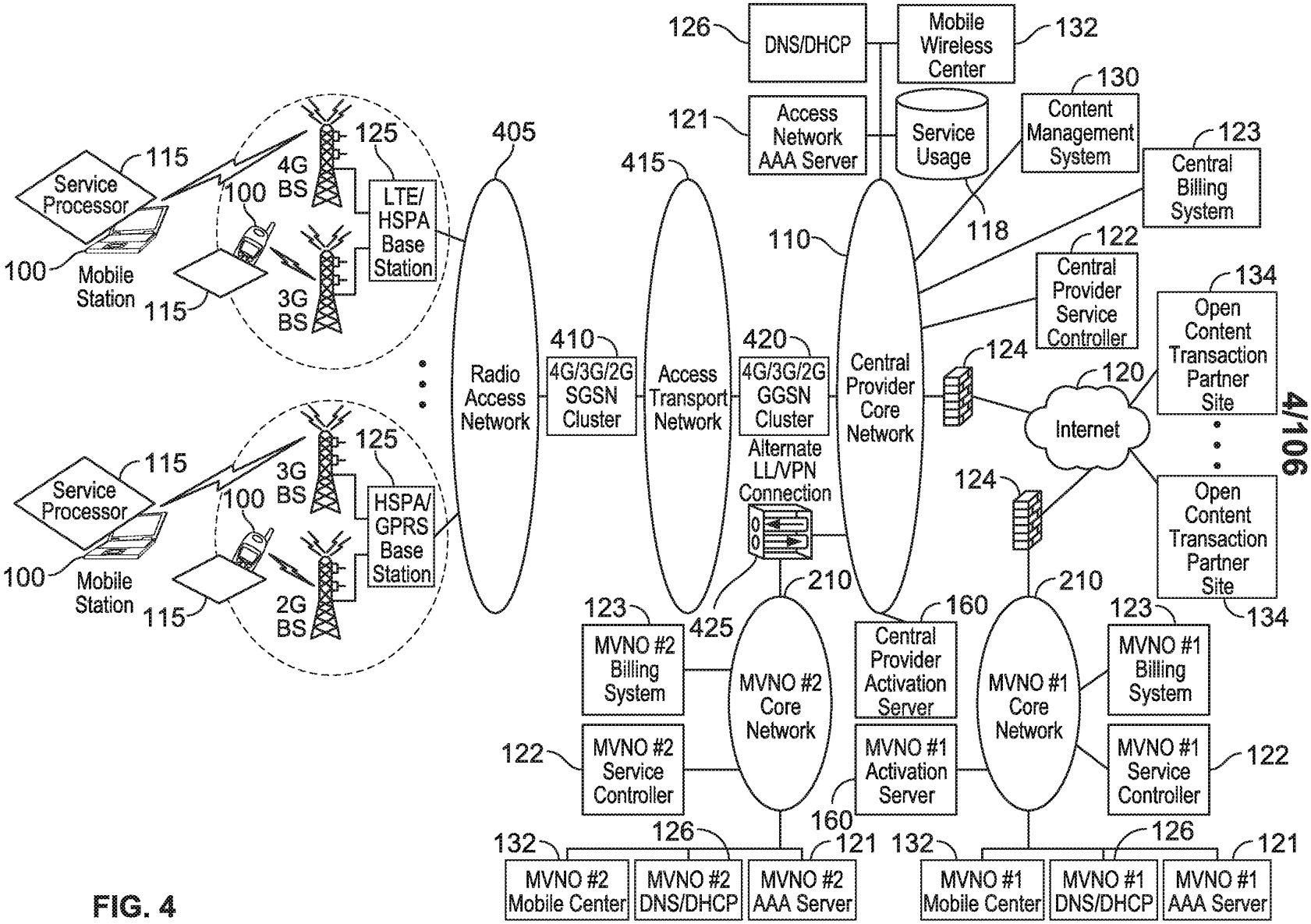


FIG. 4

980

4/106

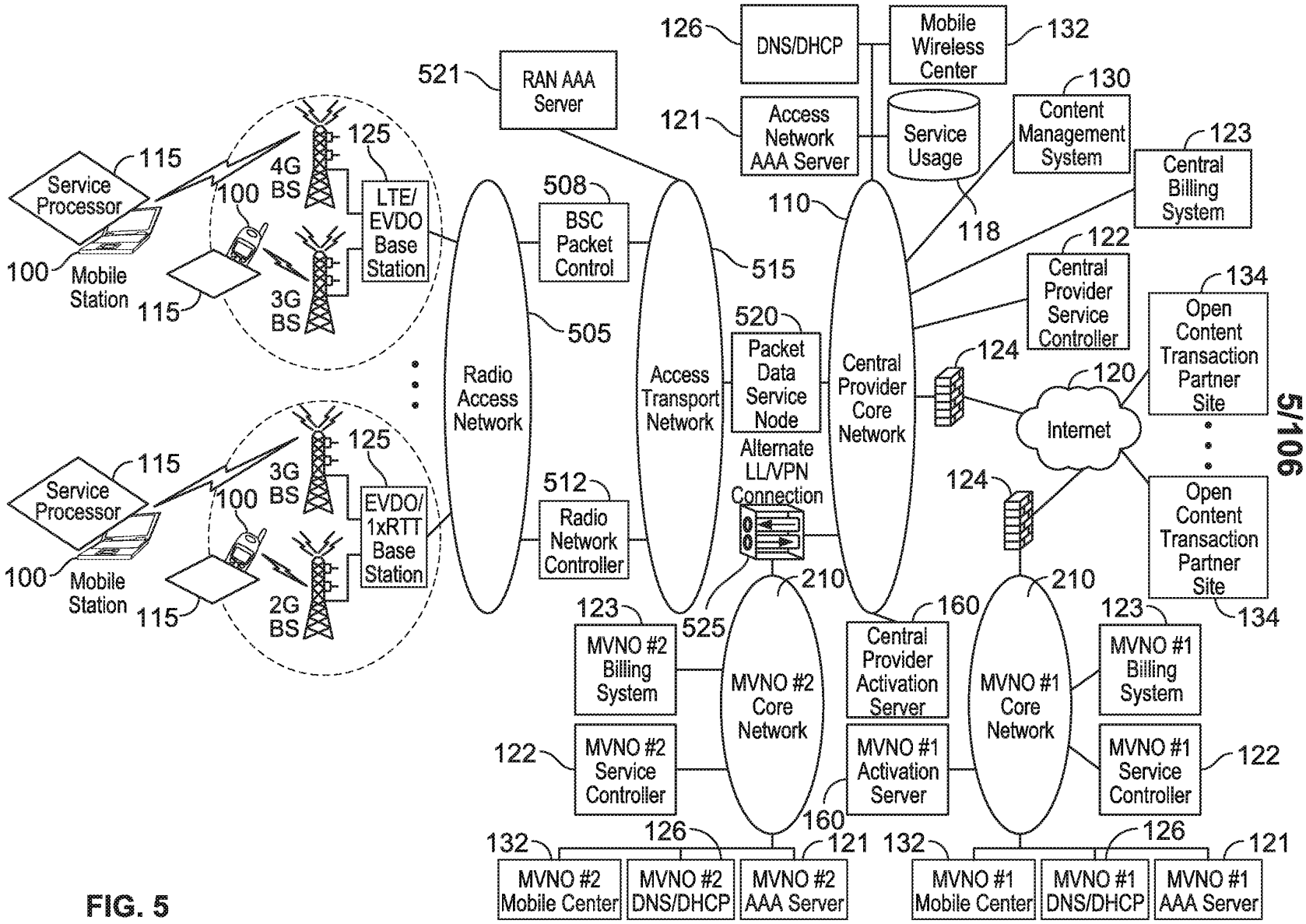


FIG. 5

5/106

981

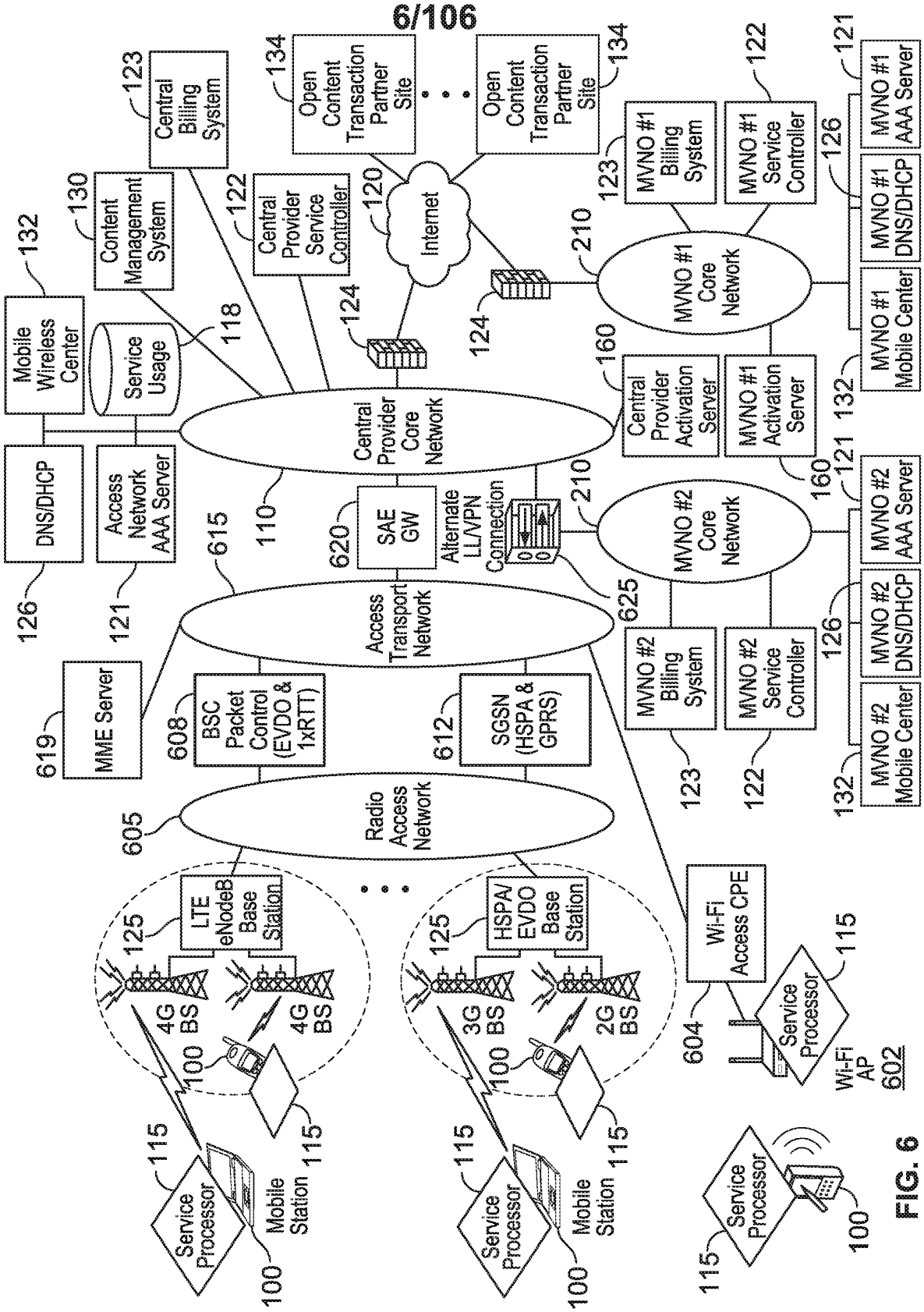

Mobile Wireless Center
132
DNS/DHCP
126
Access Network AAA Server
121
Service Usage
118
Content Management System
130
Central Billing System
123
Central Provider Service Controller
122
Open Content Transaction Partner Site
134
Open Content Transaction Partner Site
134
Internet
120
124
124
Central Provider Core Network
110
MVNO #1 Core Network
210
MVNO #1 Billing System
123
MVNO #1 Service Controller
122
MVNO #1 Mobile Center
132
MVNO #1 DNS/DHCP
126
MVNO #1 AAA Server
121
Central Provider Activation Server
160
MVNO #1 Activation Server
160
615
Access Transport Network
625
MVNO #2 Core Network
210
620
SAE GW
Alternate LL/VPN Connection
MVNO #2 AAA Server
121
MVNO #2 Billing System
123
MVNO #2 Service Controller
122
MVNO #2 DNS/DHCP
126
MVNO #2 Mobile Center
132
619
MME Server
608
BSC Packet Control (EVDO & 1xRTT)
612
SGSN (HSPA & GPRS)
605
Radio Access Network
125
LTE eNodeB Base Station
125
HSPA/ EVDO Base Station
4G BS
4G BS
3G BS
2G BS
100
115
Service Processor
Mobile Station
Wi-Fi Access CPE
604
Service Processor
115
Wi-Fi AP
602

FIG. 6

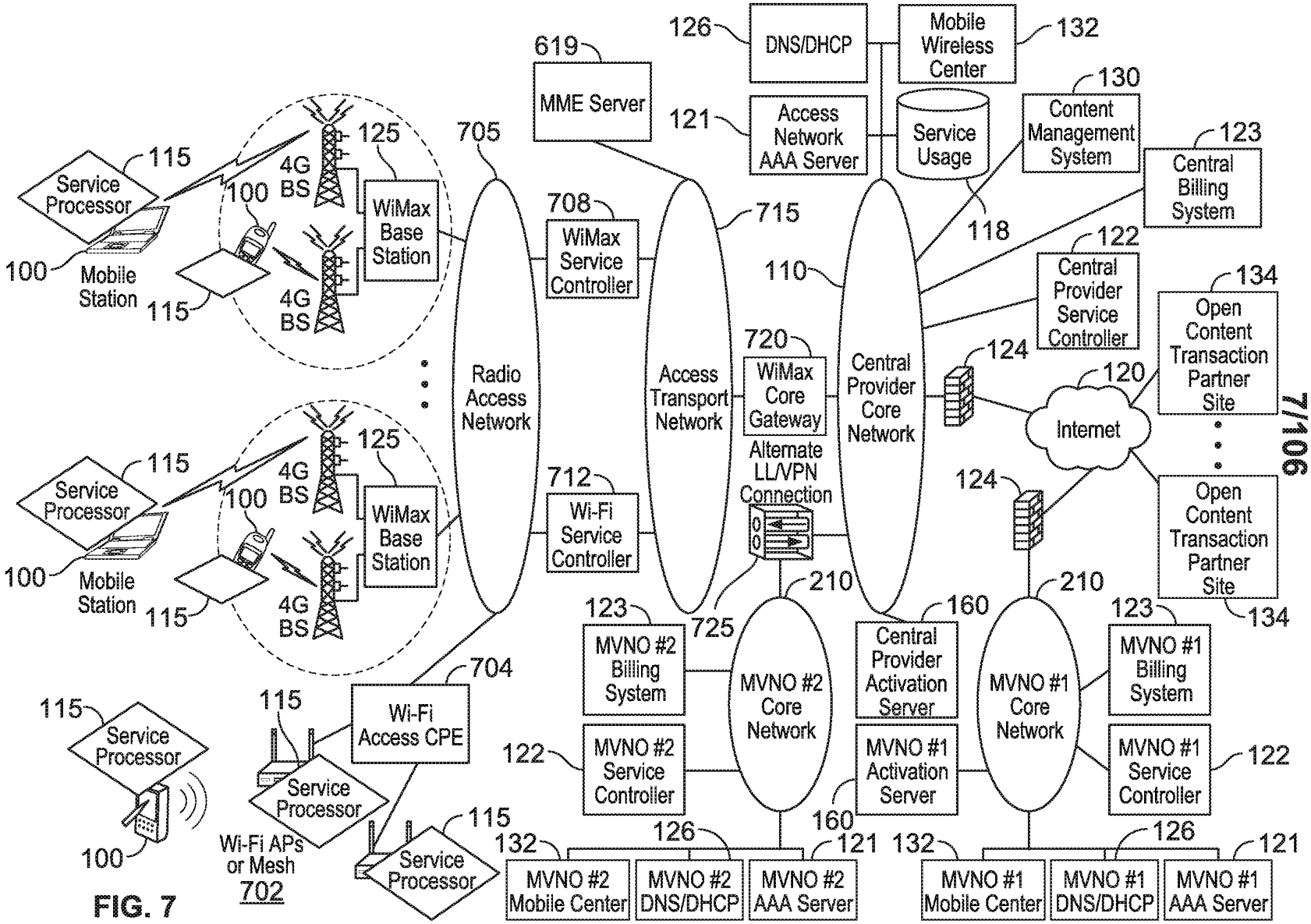

Service Processor
115
100
Mobile Station
4G BS
125
WiMax Base Station
705
Radio Access Network
619
MME Server
708
WiMax Service Controller
712
Wi-Fi Service Controller
715
Access Transport Network
720
WiMax Core Gateway
Alternate LL/VPN Connection
725
110
Central Provider Core Network
126
DNS/DHCP
121
Access Network AAA Server
Mobile Wireless Center
132
Service Usage
118
130
Content Management System
123
Central Billing System
122
Central Provider Service Controller
124
120
Internet
134
Open Content Transaction Partner Site
704
Wi-Fi Access CPE
Wi-Fi APs or Mesh
702
160
Central Provider Activation Server
210
MVNO #2 Billing System
MVNO #2 Core Network
MVNO #2 Service Controller
MVNO #1 Activation Server
MVNO #1 Billing System
MVNO #1 Core Network
MVNO #1 Service Controller
MVNO #2 Mobile Center
MVNO #2 DNS/DHCP
MVNO #2 AAA Server
MVNO #1 Mobile Center
MVNO #1 DNS/DHCP
MVNO #1 AAA Server
7/106

FIG. 7

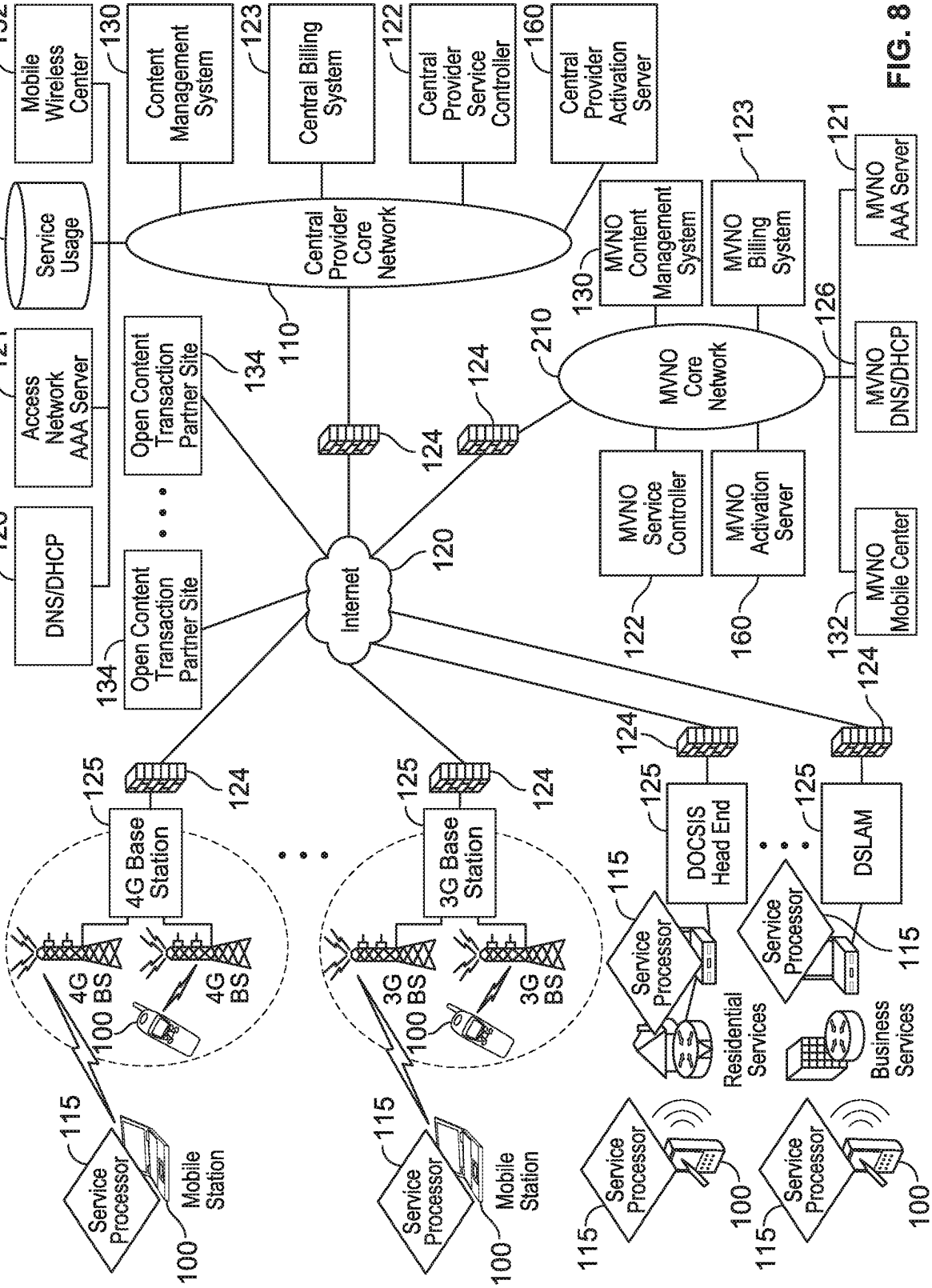

Mobile Wireless Center
132
Content Management System
130
Central Billing System
123
Central Provider Service Controller
122
Central Provider Activation Server
160
Service Usage
118
Central Provider Core Network
110
Access Network AAA Server
121
Open Content Transaction Partner Site
134
DNS/DHCP
126
Internet
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
124
125
4G Base Station
3G Base Station
DOCSIS Head End
DSLAM
4G BS
100
3G BS
100
Service Processor
115
Mobile Station
100
Residential Services
Business Services

FIG. 8

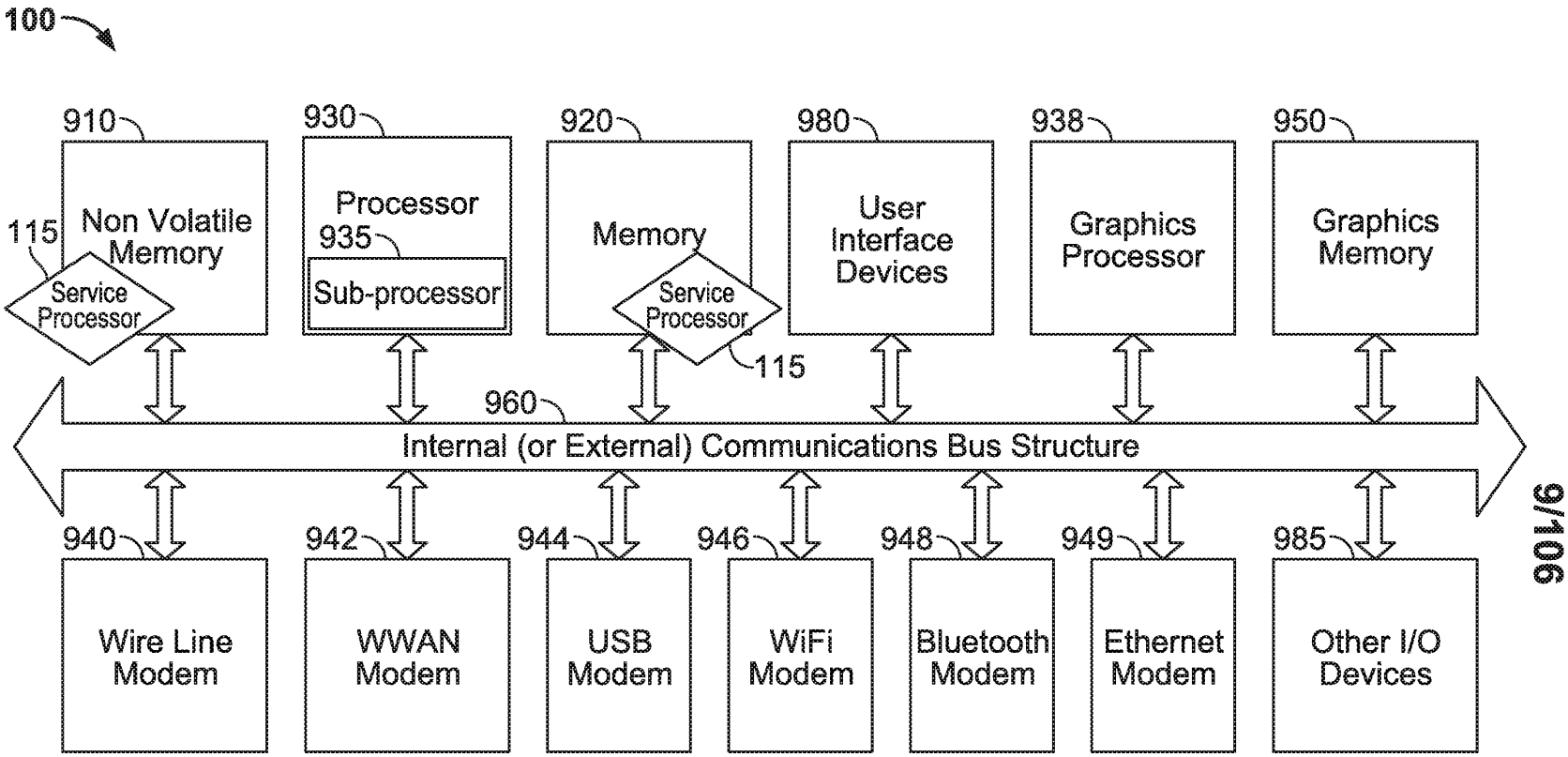

100
910
Non Volatile Memory
115
Service Processor
930
Processor
935
Sub-processor
920
Memory
Service Processor
115
980
User Interface Devices
938
Graphics Processor
950
Graphics Memory
960
Internal (or External) Communications Bus Structure
940
Wire Line Modem
942
WWAN Modem
944
USB Modem
946
WiFi Modem
948
Bluetooth Modem
949
Ethernet Modem
985
Other I/O Devices
985
9/106

FIG. 9

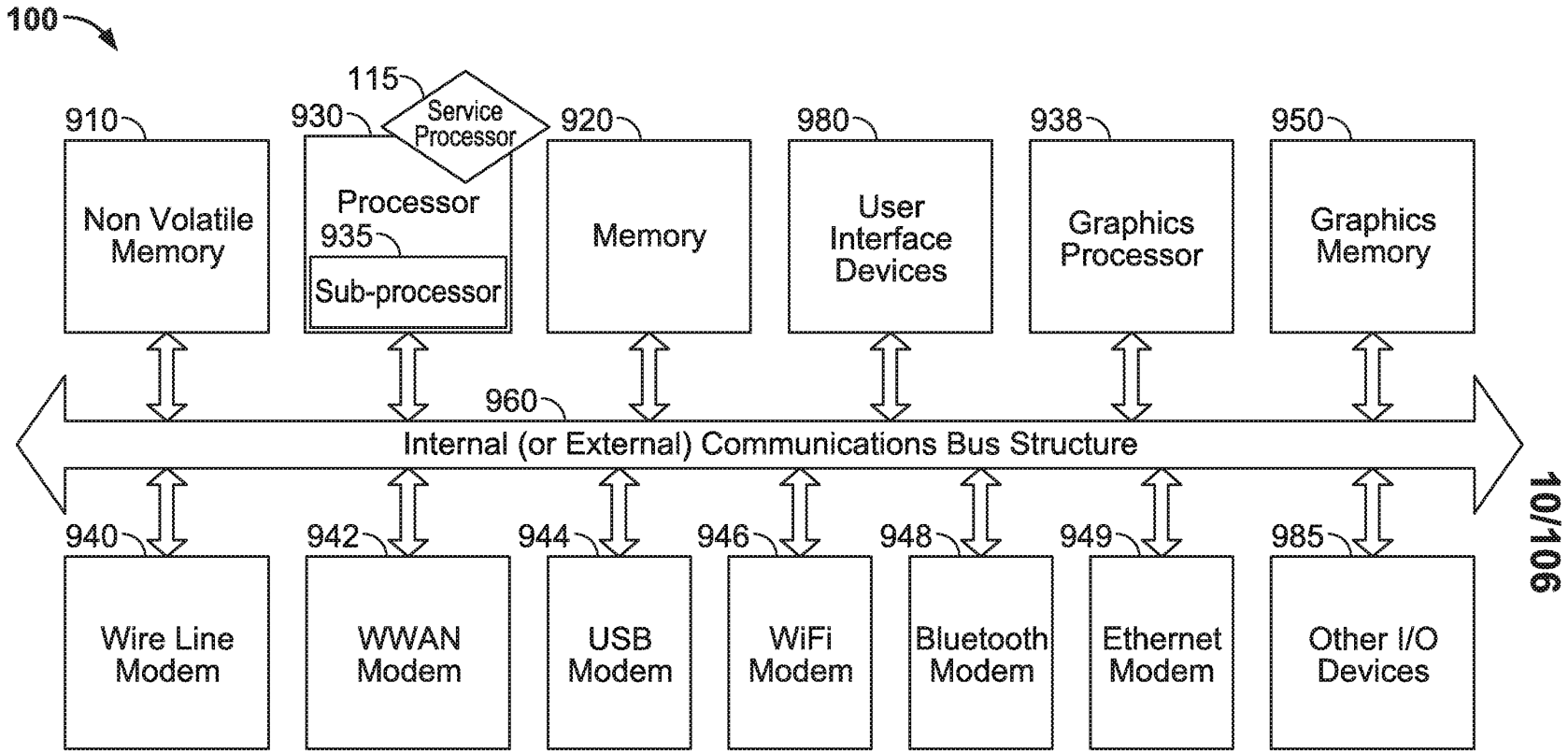

100
115
Service Processor
910
930
920
980
938
950
Non Volatile Memory
Processor
935
Sub-processor
Memory
User Interface Devices
Graphics Processor
Graphics Memory
960
Internal (or External) Communications Bus Structure
940
942
944
946
948
949
985
Wire Line Modem
WWAN Modem
USB Modem
WiFi Modem
Bluetooth Modem
Ethernet Modem
Other I/O Devices
986
10/106

FIG. 10

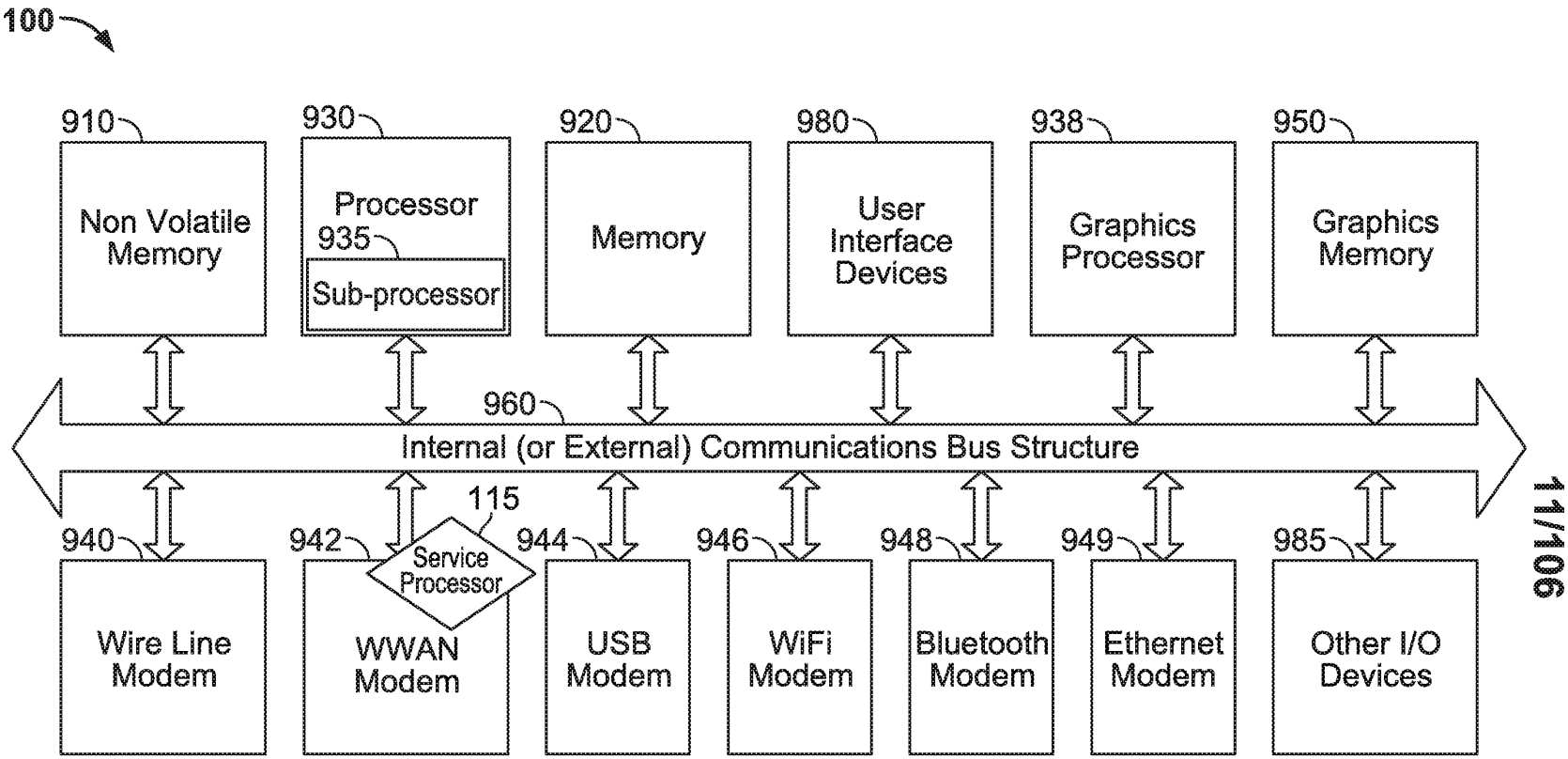

100
910
Non Volatile Memory
930
Processor
935
Sub-processor
920
Memory
980
User Interface Devices
938
Graphics Processor
950
Graphics Memory
960
Internal (or External) Communications Bus Structure
1174
940
Wire Line Modem
942
115
Service Processor
WWAN Modem
944
USB Modem
946
WiFi Modem
948
Bluetooth Modem
949
Ethernet Modem
985
Other I/O Devices
987

FIG. 11

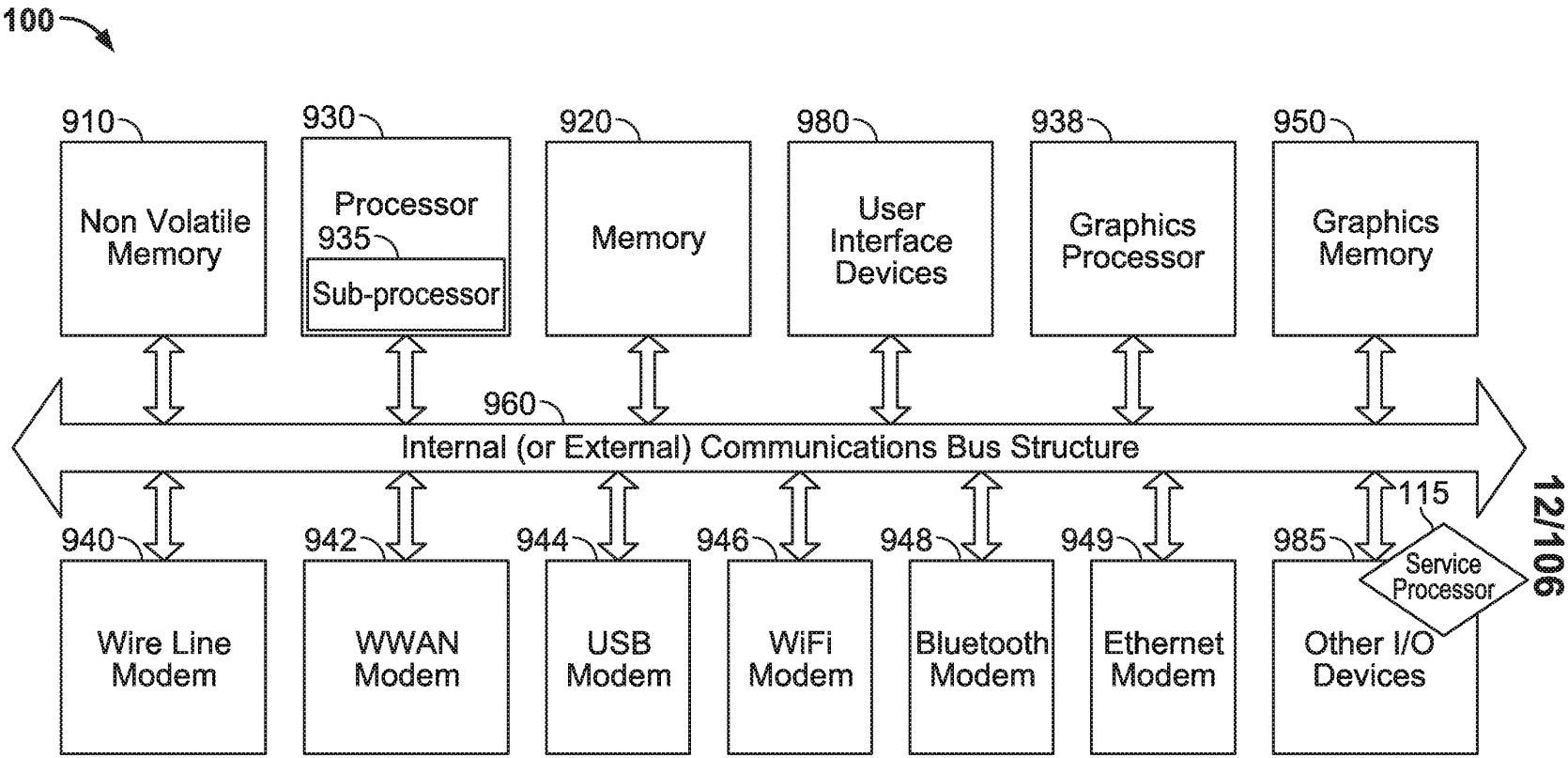

100
910
Non Volatile Memory
930
Processor
935
Sub-processor
920
Memory
980
User Interface Devices
938
Graphics Processor
950
Graphics Memory
960
Internal (or External) Communications Bus Structure
940
Wire Line Modem
942
WWAN Modem
944
USB Modem
946
WiFi Modem
948
Bluetooth Modem
949
Ethernet Modem
985
115
Service Processor
Other I/O Devices
988
12/106

FIG. 12

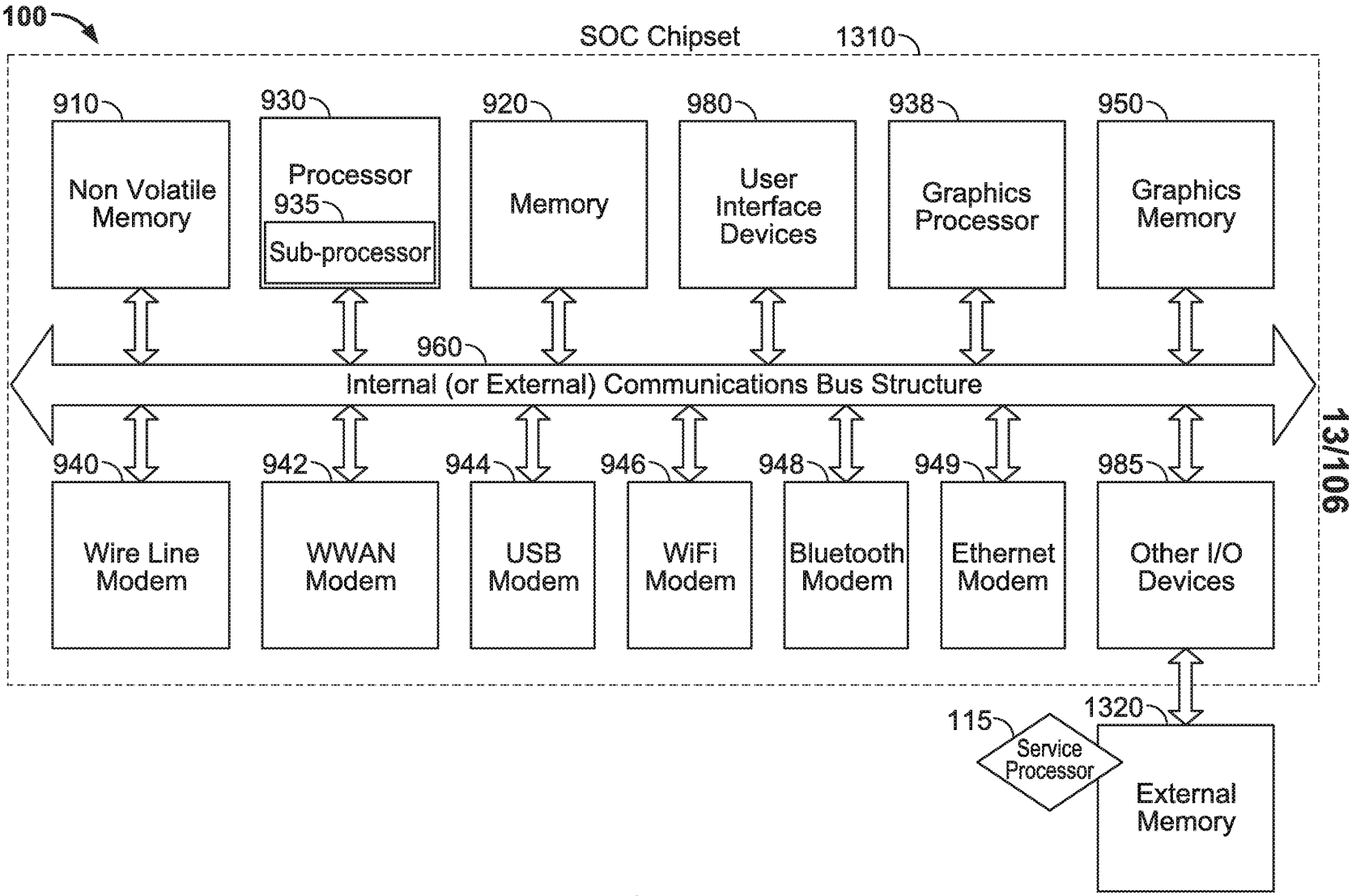

100
SOC Chipset
1310
910
Non Volatile Memory
930
Processor
935
Sub-processor
920
Memory
980
User Interface Devices
938
Graphics Processor
950
Graphics Memory
960
Internal (or External) Communications Bus Structure
940
Wire Line Modem
942
WWAN Modem
944
USB Modem
946
WiFi Modem
948
Bluetooth Modem
949
Ethernet Modem
985
Other I/O Devices
115
Service Processor
1320
External Memory

FIG. 13

686

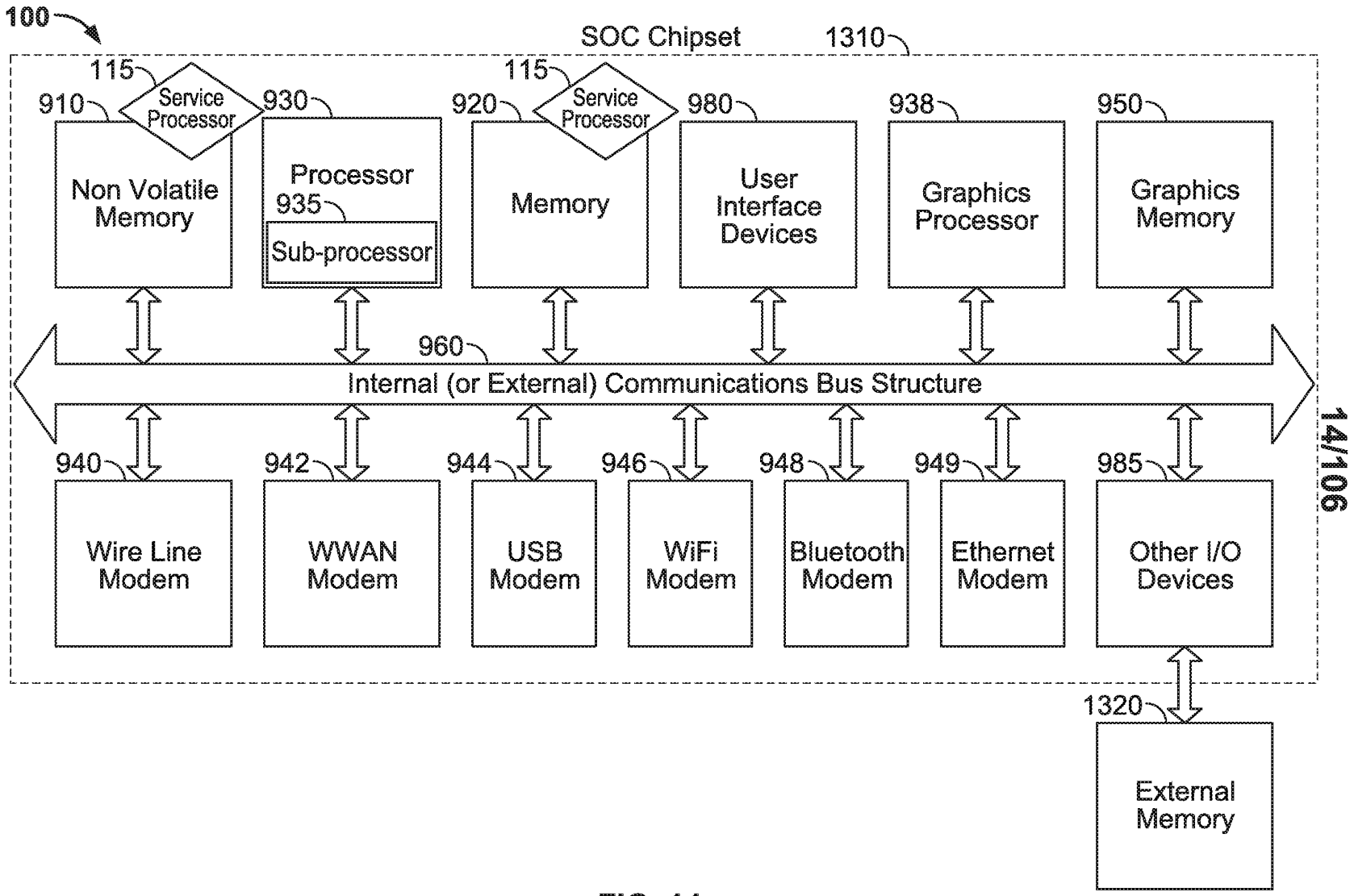

100
SOC Chipset
1310
115
Service Processor
910
Non Volatile Memory
930
Processor
935
Sub-processor
115
Service Processor
920
Memory
980
User Interface Devices
938
Graphics Processor
950
Graphics Memory
960
Internal (or External) Communications Bus Structure
940
Wire Line Modem
942
WWAN Modem
944
USB Modem
946
WiFi Modem
948
Bluetooth Modem
949
Ethernet Modem
985
Other I/O Devices
1320
External Memory
14/106

FIG. 14

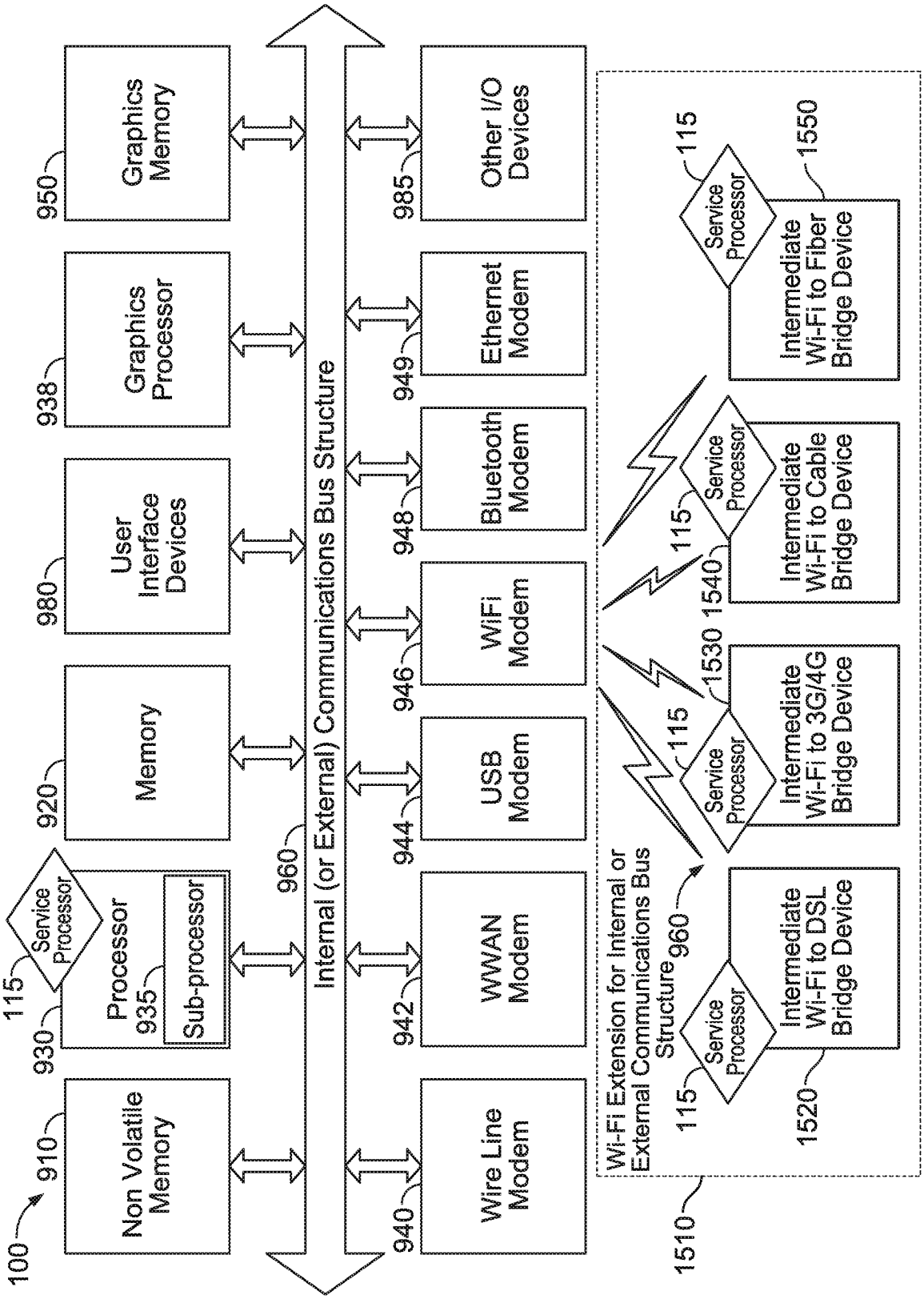

100
910
Non Volatile Memory
930
Processor
935
Sub-processor
115
Service Processor
920
Memory
940
Wire Line Modem
942
WWAN Modem
944
USB Modem
946
WiFi Modem
948
Bluetooth Modem
949
Ethernet Modem
938
Graphics Processor
950
Graphics Memory
980
User Interface Devices
985
Other I/O Devices
960
Internal (or External) Communications Bus Structure
Wi-Fi Extension for Internal or External Communications Bus Structure
1510
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

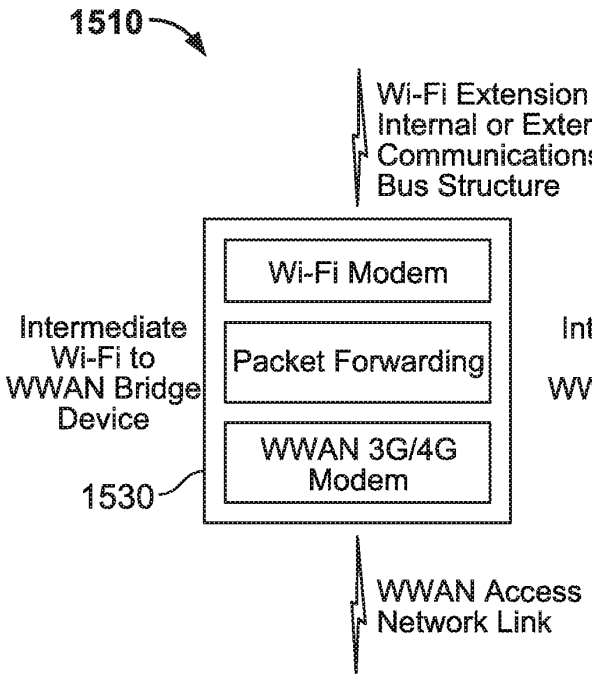


FIG. 15B

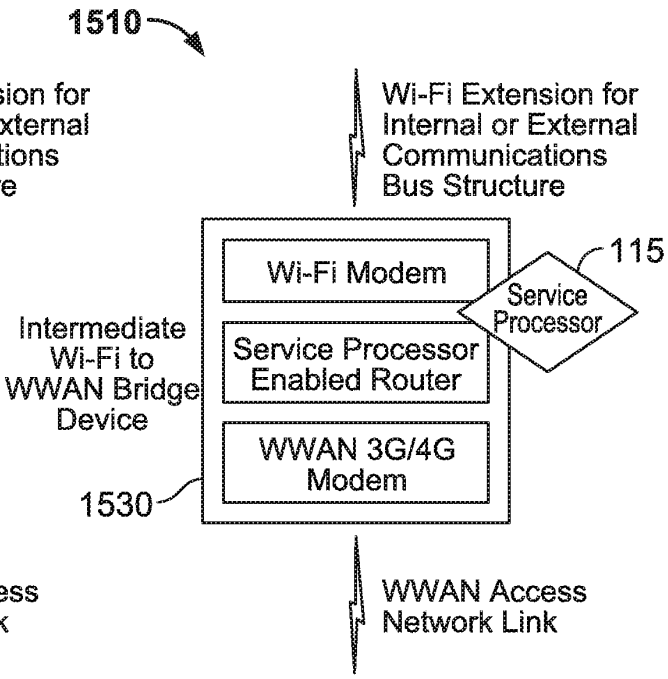


FIG. 15C

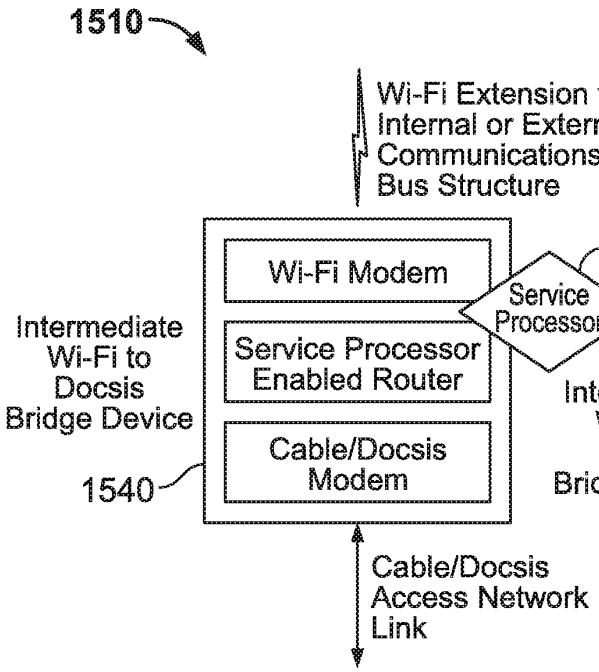


FIG. 15D

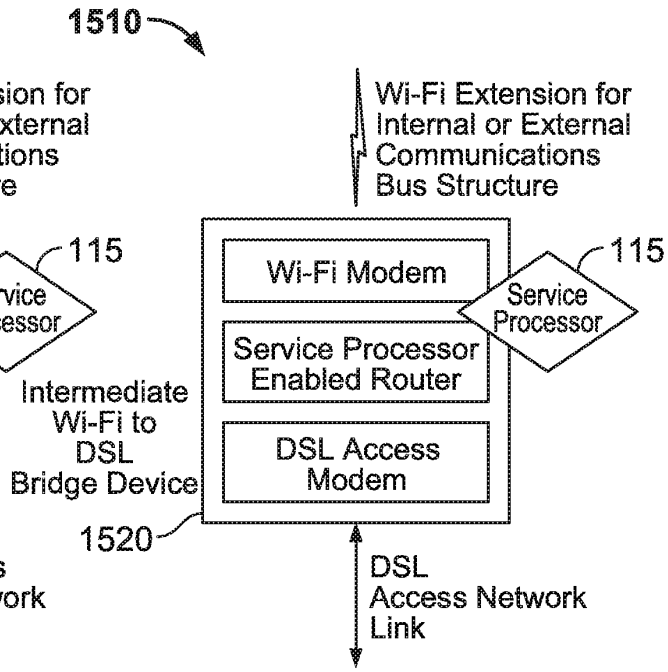


FIG. 15E

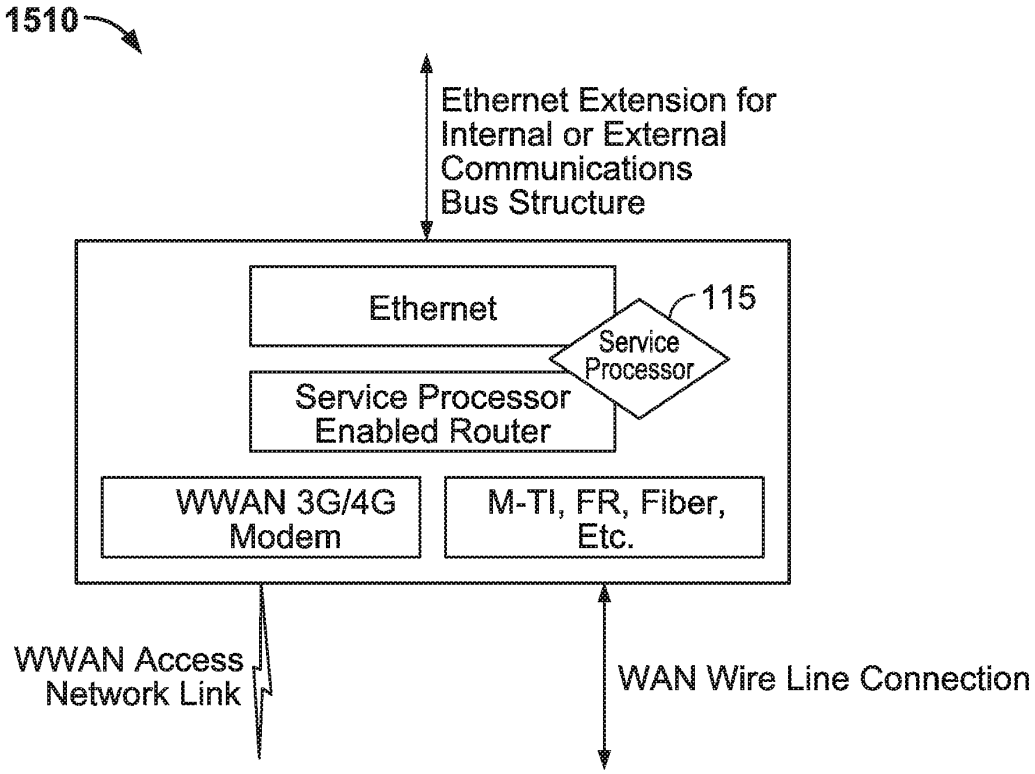

1510
Ethernet Extension for Internal or External Communications Bus Structure
Ethernet
115
Service Processor
Service Processor Enabled Router
WWAN 3G/4G Modem
M-TI, FR, Fiber, Etc.
WWAN Access Network Link
WAN Wire Line Connection

FIG. 15F

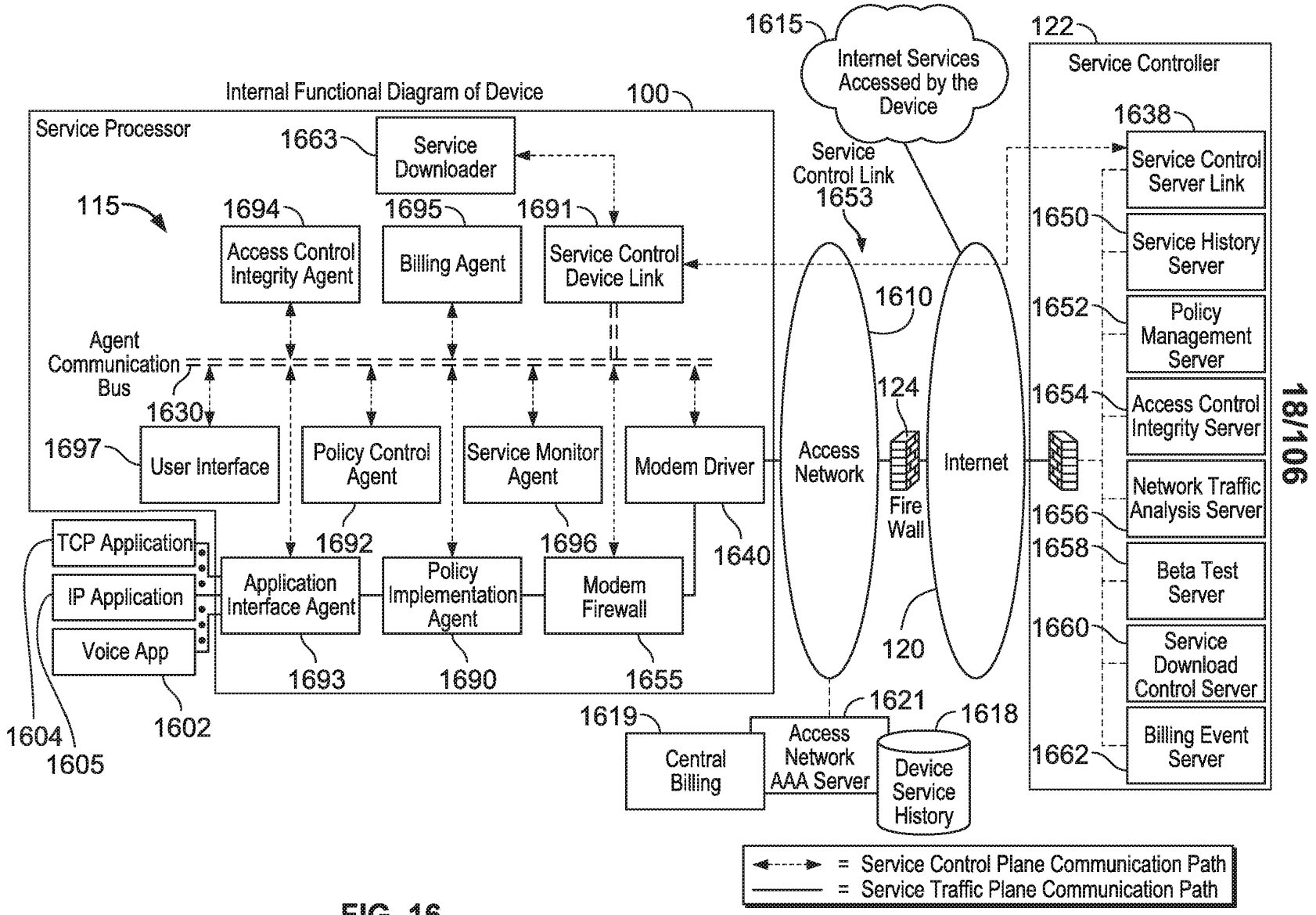

Internal Functional Diagram of Device
100
Service Processor
115
1663
Service Downloader
1694
Access Control Integrity Agent
1695
Billing Agent
1691
Service Control Device Link
Agent Communication Bus
1630
1697
User Interface
Policy Control Agent
Service Monitor Agent
Modem Driver
1692
1696
1640
TCP Application
IP Application
Voice App
Application Interface Agent
Policy Implementation Agent
Modem Firewall
1693
1690
1655
1604
1605
1602
1615
Internet Services Accessed by the Device
Service Control Link
1653
1610
124
Access Network
Fire Wall
Internet
120
1619
Central Billing
1621
Access Network AAA Server
1618
Device Service History
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. 16

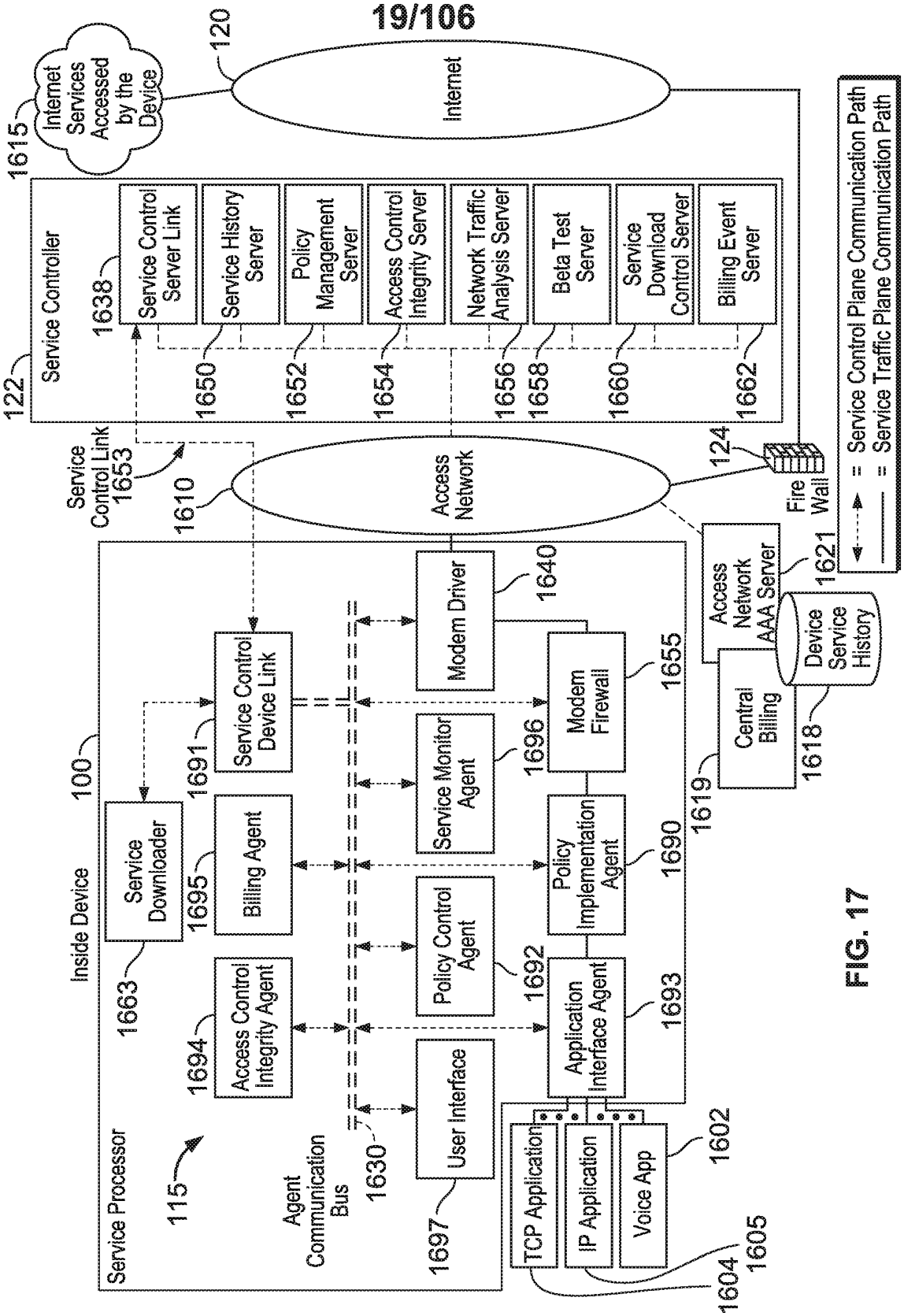

Internet Services Accessed by the Device
1615
120
Internet
Service Controller
122
1638
Service Control Server Link
Service History Server
Policy Management Server
Access Control Integrity Server
Network Traffic Analysis Server
Beta Test Server
Service Download Control Server
Billing Event Server
1650
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
Service Control Device Link
1691
Access Control Integrity Agent
1694
Policy Control Agent
1692
Service Monitor Agent
1696
Modem Driver
1640
Modem Firewall
1655
Policy Implementation Agent
1690
Application Interface Agent
1693
User Interface
1697
Agent Communication Bus
1630
TCP Application
IP Application
Voice App
1602
1604
1605
Access Network AAA Server
1621
Device Service History
1618
Central Billing
1619

FIG. 17

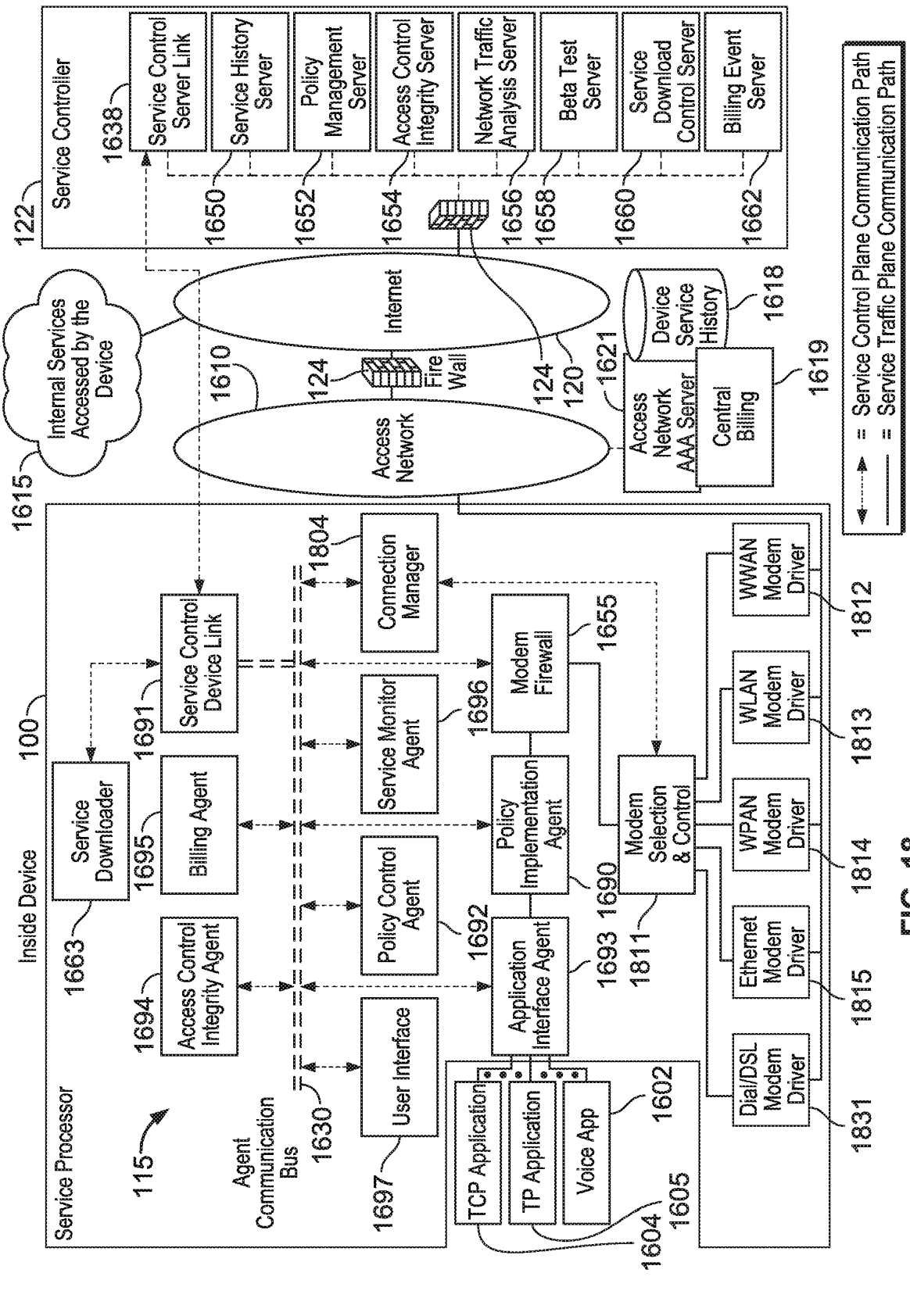

Service Controller
122
Service Control Server Link
1638
Service History Server
Policy Management Server
Access Control Integrity Server
Network Traffic Analysis Server
Beta Test Server
Service Download Control Server
Billing Event Server
1650
1652
1654
1656
1658
1660
1662
Internet
Internal Services Accessed by the Device
1615
1610
124
Fire Wall
Access Network
120
1621
Device Service History
1618
Access Network AAA Server
Central Billing
1619
= Service Control Plane Communication Path
= Service Traffic Plane Communication Path
Inside Device
100
Service Processor
115
Service Downloader
1663
Billing Agent
1695
Service Control Device Link
1691
Connection Manager
1804
Service Monitor Agent
1696
Modem Firewall
1655
Policy Implementation Agent
Modem Selection & Control
1690
Access Control Integrity Agent
1694
Policy Control Agent
1692
Application Interface Agent
1693
1811
Agent Communication Bus
1630
User Interface
1697
TCP Application
TP Application
Voice App
1602
1604
1605
WWAN Modem Driver
1812
WLAN Modem Driver
1813
WPAN Modem Driver
1814
Ethernet Modem Driver
1815
Dial/DSL Modem Driver
1831

FIG. 18

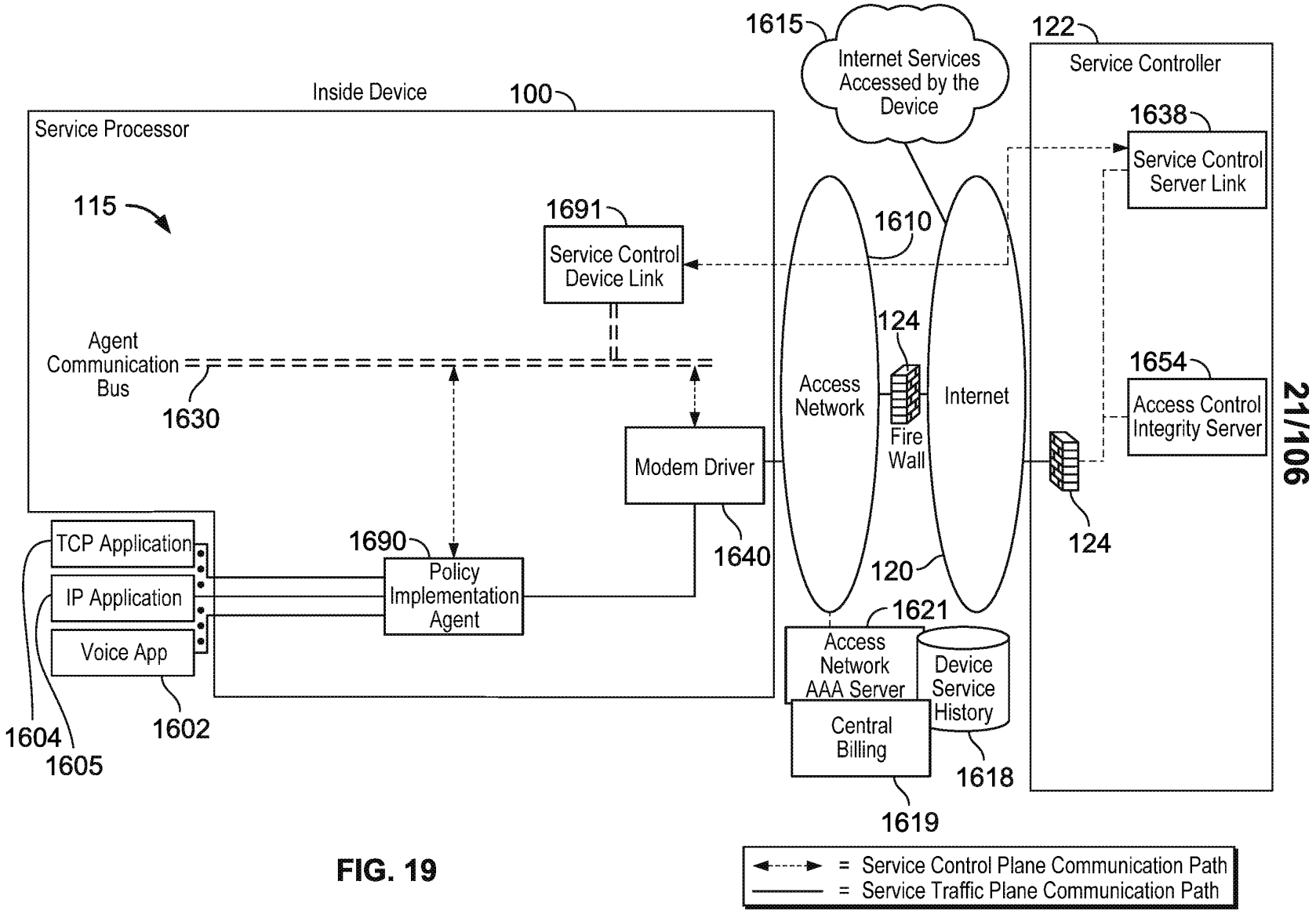

1615
Internet Services Accessed by the Device
122
Service Controller
Inside Device
100
Service Processor
115
1638
Service Control Server Link
1691
Service Control Device Link
1610
124
Agent Communication Bus
1630
Access Network
Internet
Fire Wall
1654
Access Control Integrity Server
21/106
Modem Driver
1640
TCP Application
IP Application
Voice App
1690
Policy Implementation Agent
120
124
1621
Access Network AAA Server
Device Service History
Central Billing
1618
1619
1604
1605
1602
= Service Control Plane Communication Path
= Service Traffic Plane Communication Path

FIG. 19

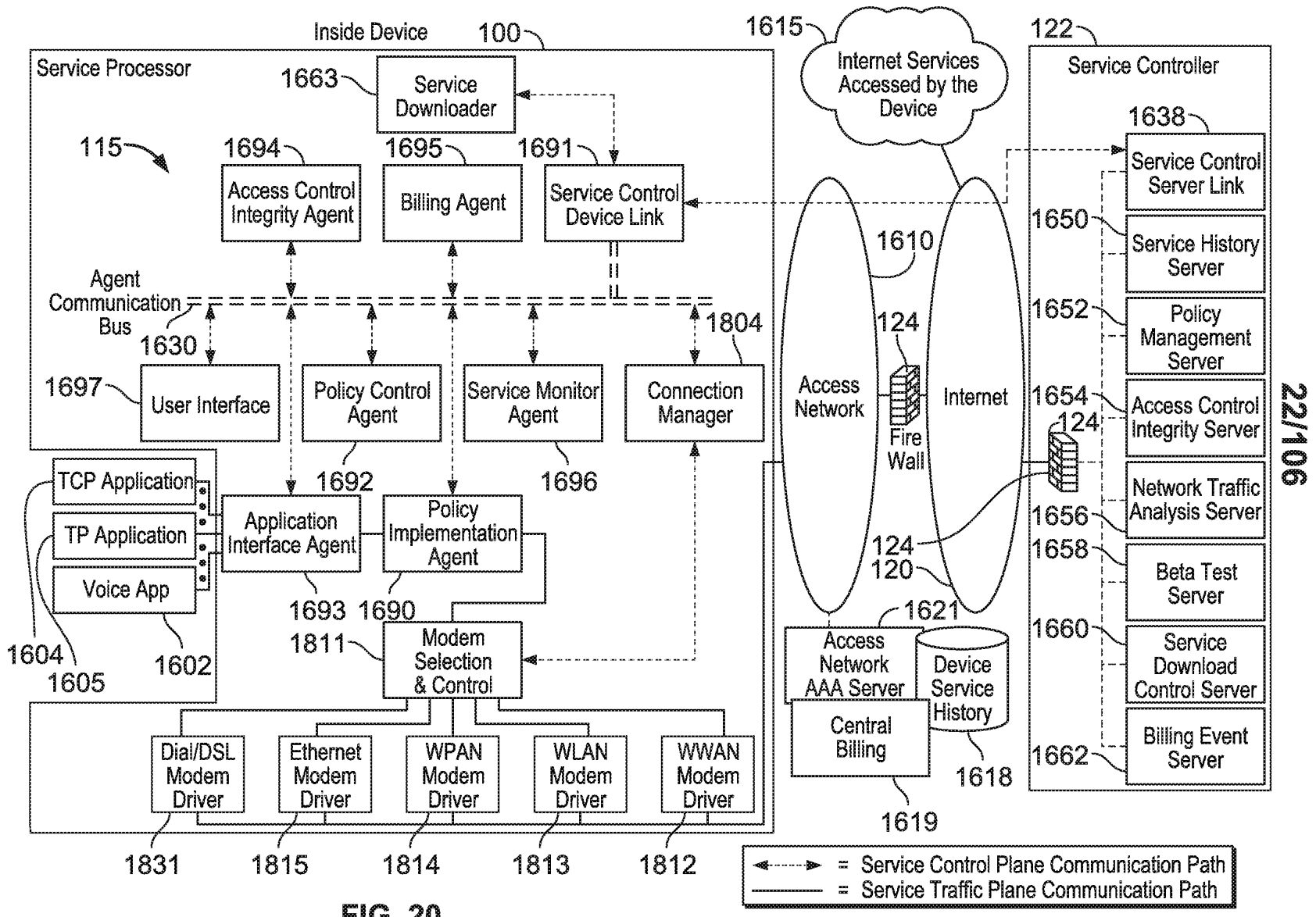

Inside Device
100
Service Processor
1663
Service Downloader
115
1694
Access Control Integrity Agent
1695
Billing Agent
1691
Service Control Device Link
Agent Communication Bus
1630
1804
1697
User Interface
Policy Control Agent
Service Monitor Agent
Connection Manager
1692
1696
TCP Application
TP Application
Voice App
Application Interface Agent
Policy Implementation Agent
1693
1690
1811
Modem Selection & Control
1604
1605
1602
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
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
866
22/106

FIG. 20

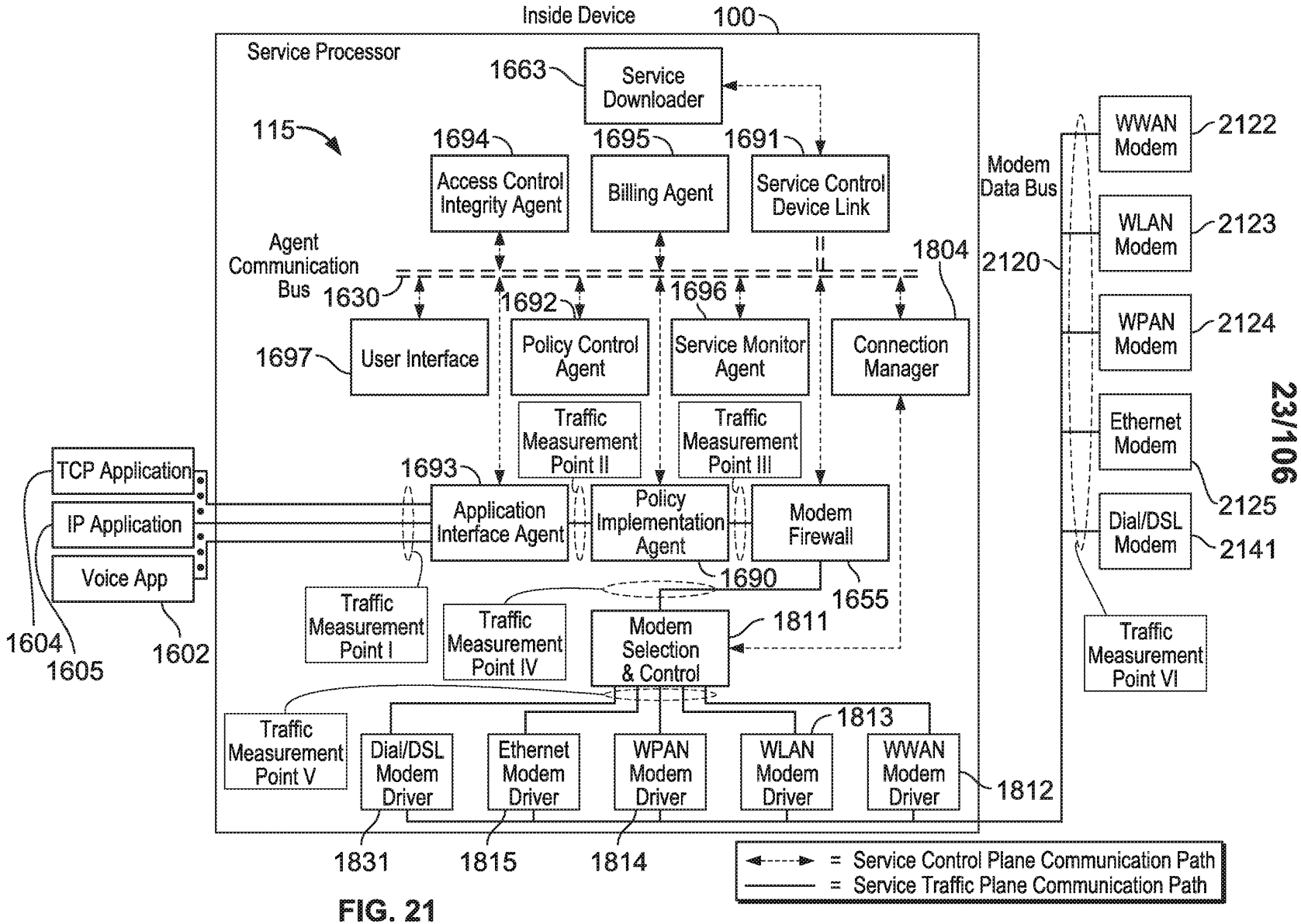

Inside Device
100
Service Processor
115
1663
Service Downloader
1694
Access Control Integrity Agent
1695
Billing Agent
1691
Service Control Device Link
Agent Communication Bus
1630
1692
1696
1804
User Interface
1697
Policy Control Agent
Service Monitor Agent
Connection Manager
Traffic Measurement Point II
Traffic Measurement Point III
TCP Application
IP Application
Voice App
1604
1605
1602
1693
Application Interface Agent
Policy Implementation Agent
Modem Firewall
1690
1655
Traffic Measurement Point I
Traffic Measurement Point IV
Modem Selection & Control
1811
Traffic Measurement Point V
1813
Dial/DSL Modem Driver
Ethernet Modem Driver
WPAN Modem Driver
WLAN Modem Driver
WWAN Modem Driver
1812
1831
1815
1814
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 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.

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.

1001

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.

1002

FIG. 23

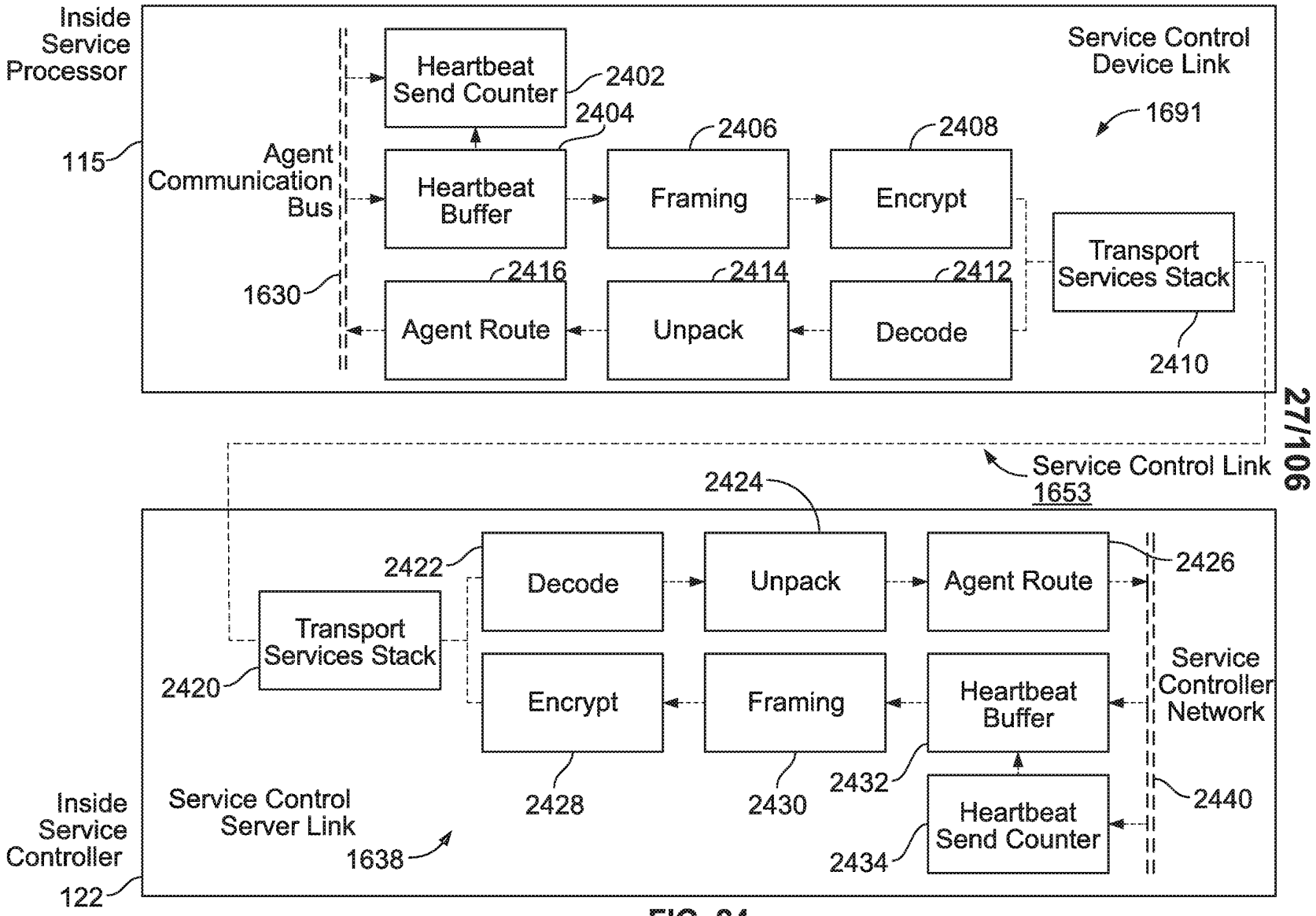

Inside Service Processor
115
Agent Communication Bus
1630
Heartbeat Send Counter
2402
2404
Heartbeat Buffer
2406
Framing
2408
Encrypt
Service Control Device Link
1691
Transport Services Stack
2410
2416
Agent Route
2414
Unpack
2412
Decode
27/106
Service Control Link
1653
2424
2422
Decode
Unpack
Agent Route
2426
Transport Services Stack
2420
Encrypt
Framing
Heartbeat Buffer
Service Controller Network
2428
2430
2432
2440
Heartbeat Send Counter
2434
Inside Service Controller
122
Service Control Server Link
1638

FIG. 24

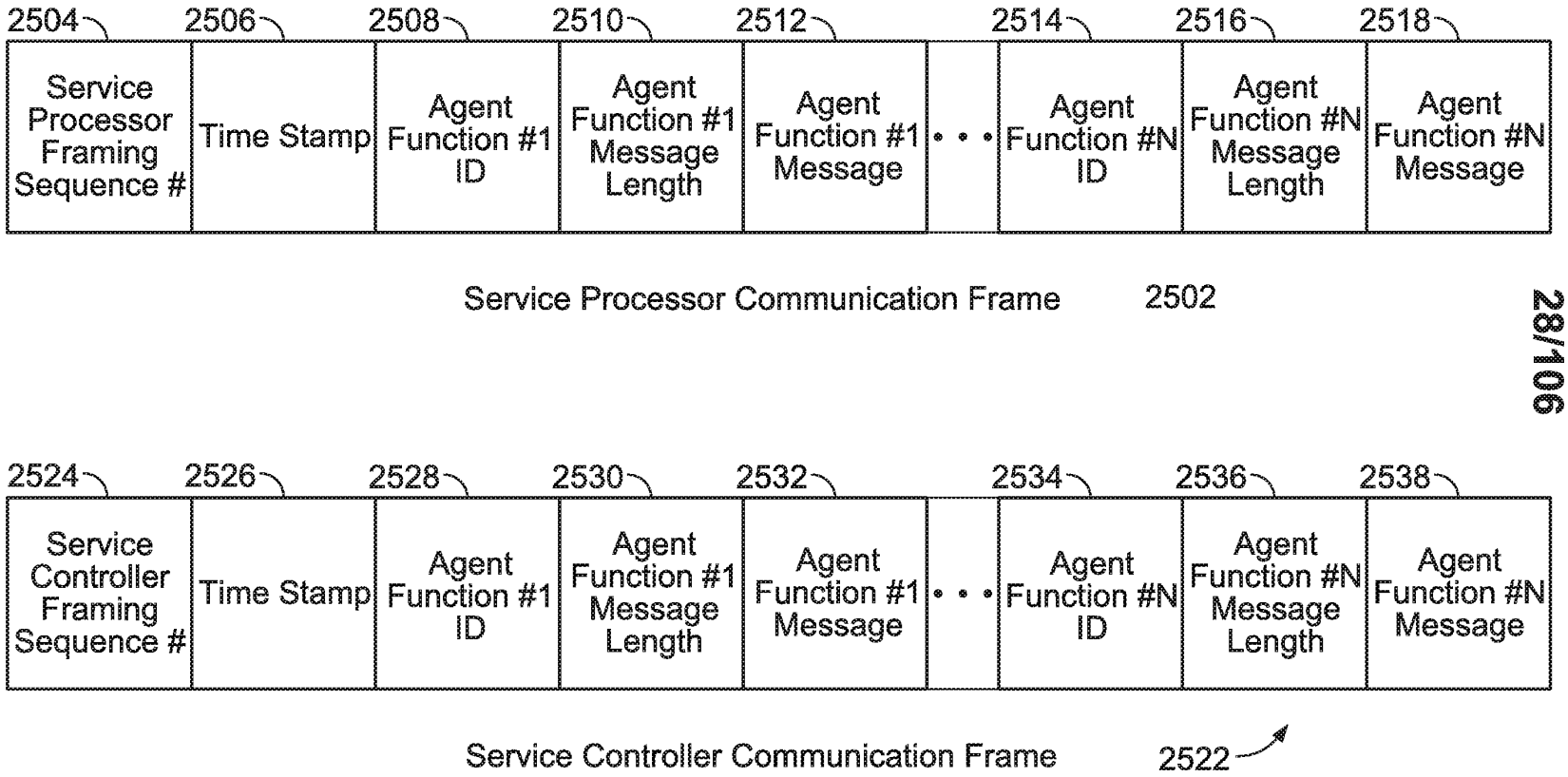

2504
2506
2508
2510
2512
2514
2516
2518
Service Processor Framing Sequence #
Time Stamp
Agent Function #1 ID
Agent Function #1 Message Length
Agent Function #1 Message
• • •
Agent Function #N ID
Agent Function #N Message Length
Agent Function #N Message
Service Processor Communication Frame
2502
2524
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
1004

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.

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.

1006

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.

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.

1008

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.

1009

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.

1010

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.

1012

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

1014

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

1016

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

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

1020

44/106

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.

1022

FIG. 27J

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

		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

1024

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

1025

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

1026

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.

1028

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.

1029

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.

1030

54/109

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

1031

		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.

1032

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.

1033

FIG. 28E

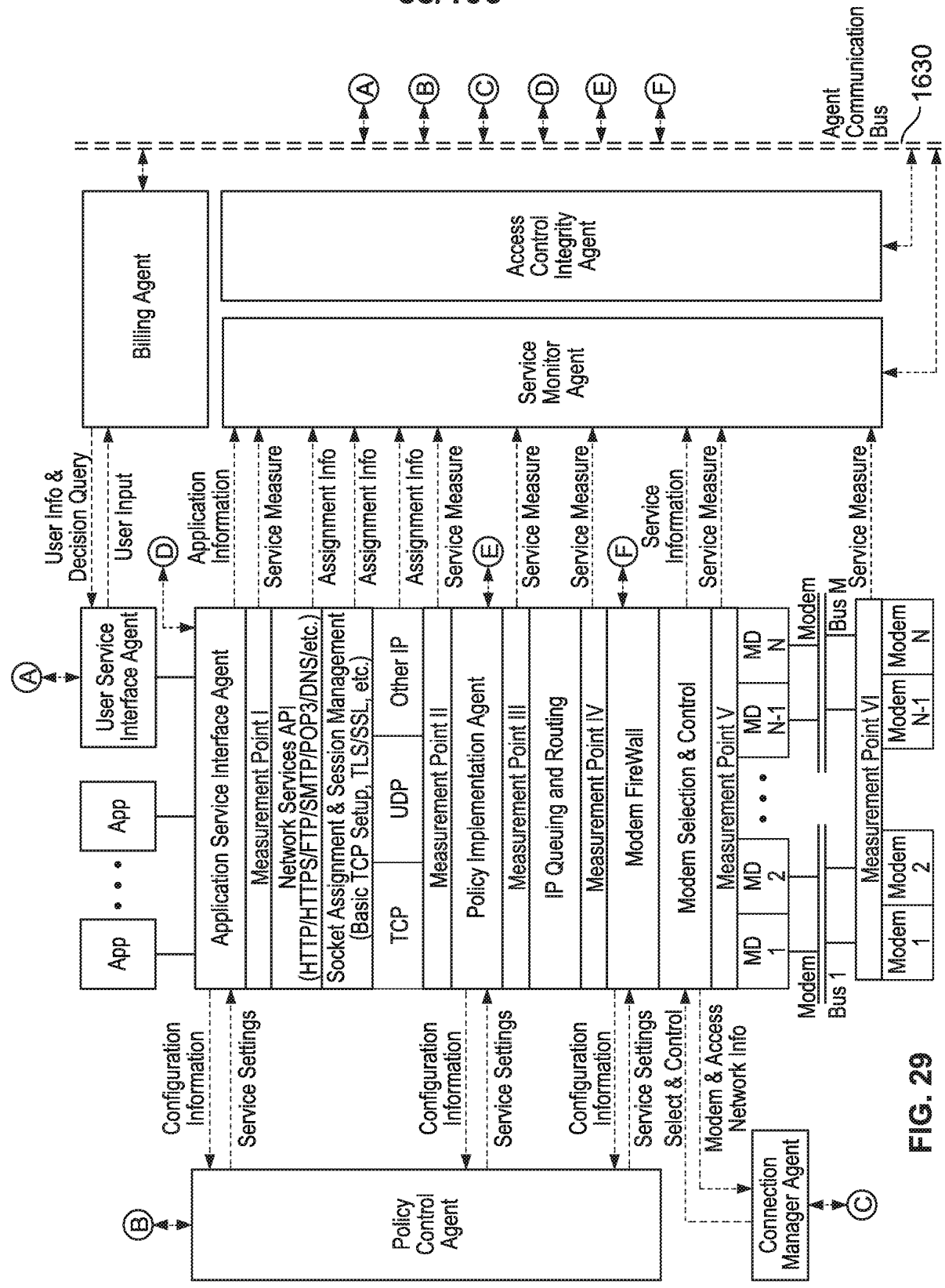

Billing Agent
Access Control Integrity Agent
Service Monitor Agent
User Info & Decision Query
User Input
Application Information
Service Measure
Assignment Info
Service Information
Agent Communication Bus
1630
A
B
C
D
E
F
User Service Interface Agent
App
App
Application Service Interface Agent
Measurement 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

1630
Agent Communication Bus
A
B
C
D
E
F
G
Billing Agent
Access Control Integrity Agent B
Service Monitor Agent B
Access Control Integrity Agent A
Service Monitor Agent A
User Service 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
IP Queuing and Routing
Modem Driver
Modem Bus
Modem Driver
Measurement Point II
Policy Implementation Agent
Measurement Point III
Modem Firewall
Measurement Point IV
Modem MAC/PHY
Configuration Information
Service Settings
Select & Control
Modem & Access Network Info
Service Information
Service Settings
Service Information
Firewall Settings
Policy Control Agent B
Connection Manager Agent
Policy Control Agent A

FIG. 30

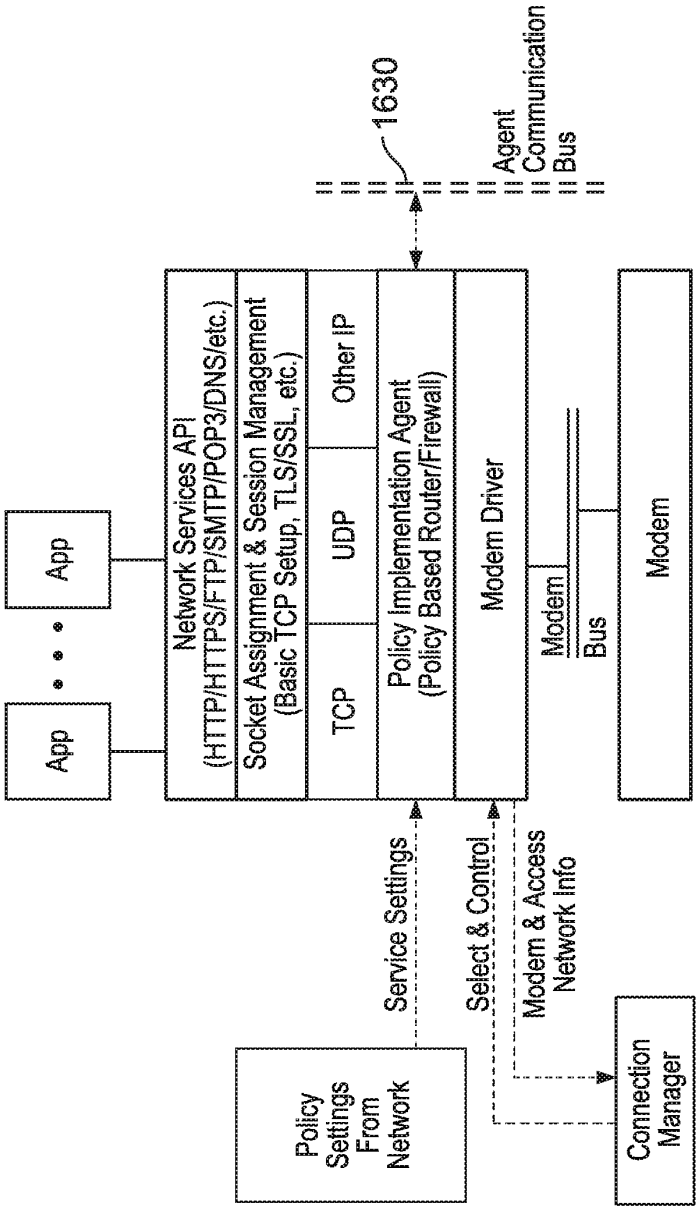

App
App
Network Services API
(HTTP/HTTPS/FTP/SMTP/POP3/DNS/etc.)
Socket Assignment & Session Management
(Basic TCP Setup, TLS/SSL, etc.)
TCP
UDP
Other IP
Policy Implementation Agent
(Policy Based Router/Firewall)
Modem Driver
Modem
Bus
Modem
1630
Agent
Communication
Bus
Policy
Settings
From
Network
Service Settings
Select & Control
Modem & Access
Network Info
Connection
Manager

FIG. 31

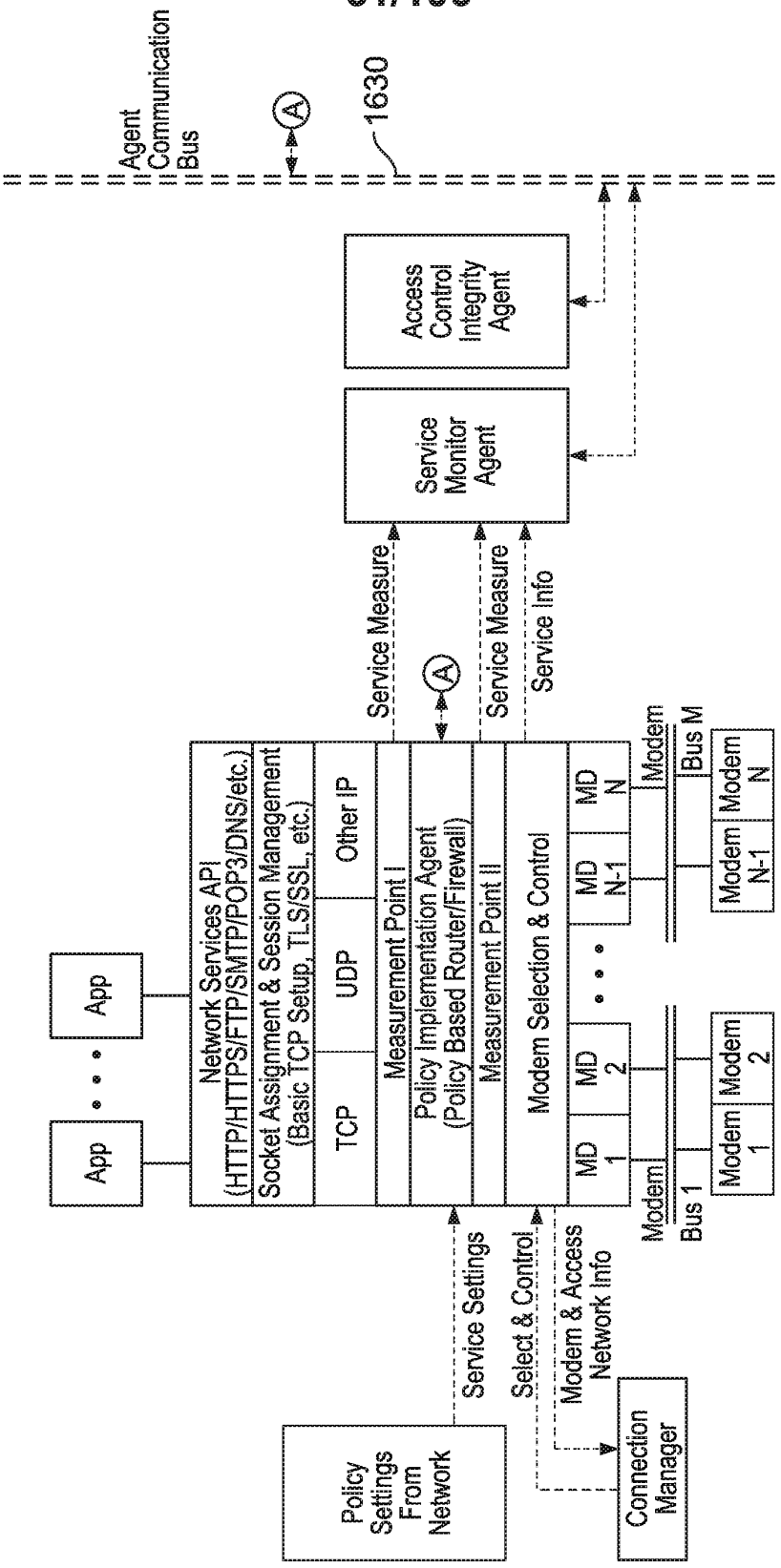

Agent Communication Bus
A
1630
Access Control Integrity Agent
Service Monitor Agent
Service Measure
Service Measure
Service Info
A
App
App
Network Services API (HTTP/HTTPS/FTP/SMTP/POP3/DNS/etc.)
Socket Assignment & Session Management (Basic TCP Setup, TLS/SSL, etc.)
TCP
UDP
Other IP
Measurement Point 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 M
Modem N-1
Modem N
Modem
Bus 1
Modem 1
Modem 2
Service Settings
Select & Control
Modem & Access Network Info
Policy Settings From Network
Connection Manager

FIG. 32

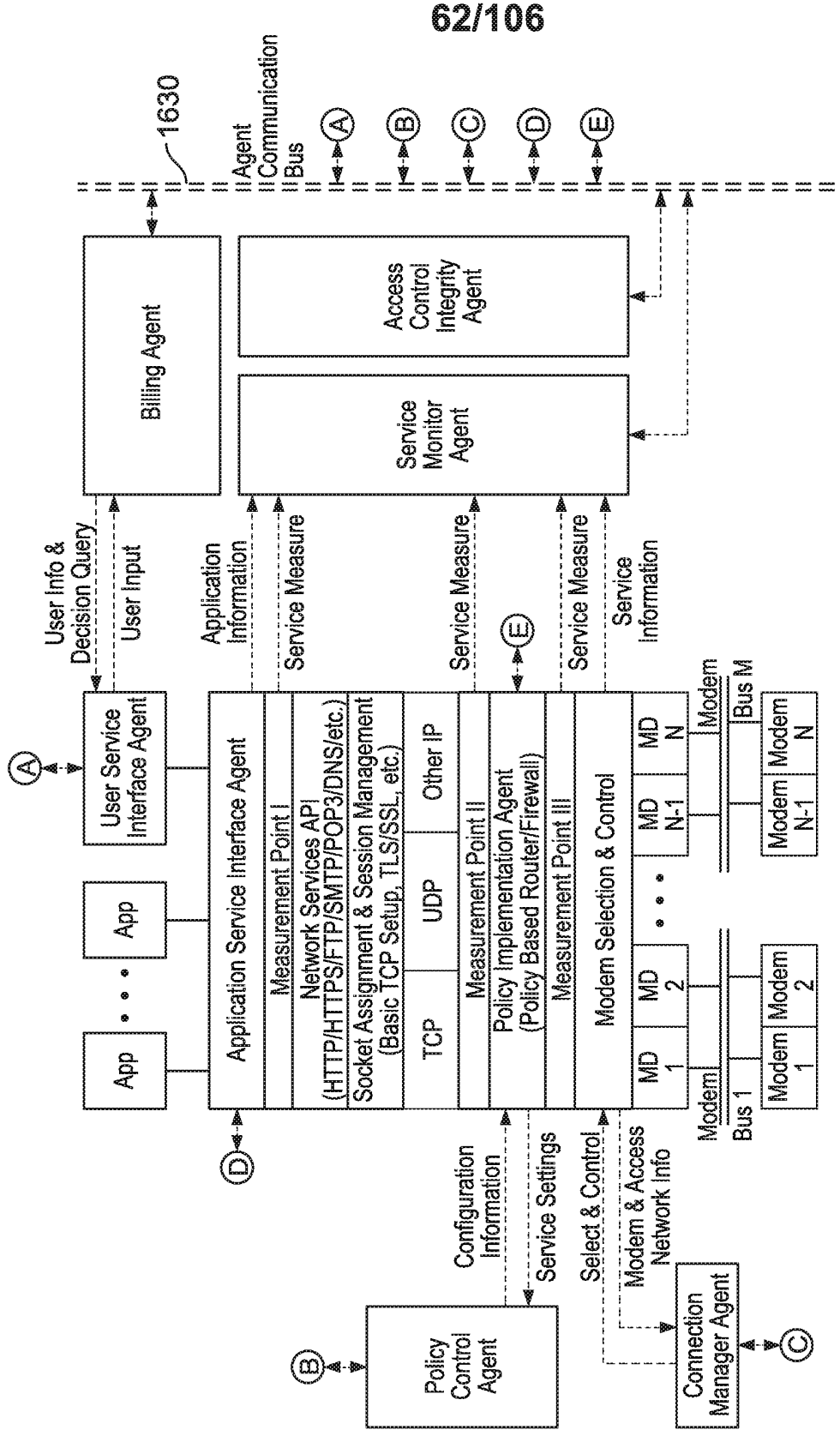

1630
Agent Communication Bus
A
B
C
D
E
Billing Agent
Access Control Integrity Agent
Service Monitor Agent
User Info & Decision Query
User Input
Application Information
Service Measure
Service Measure
Service Measure
Service Information
User Service Interface Agent
App
App
Application Service Interface 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

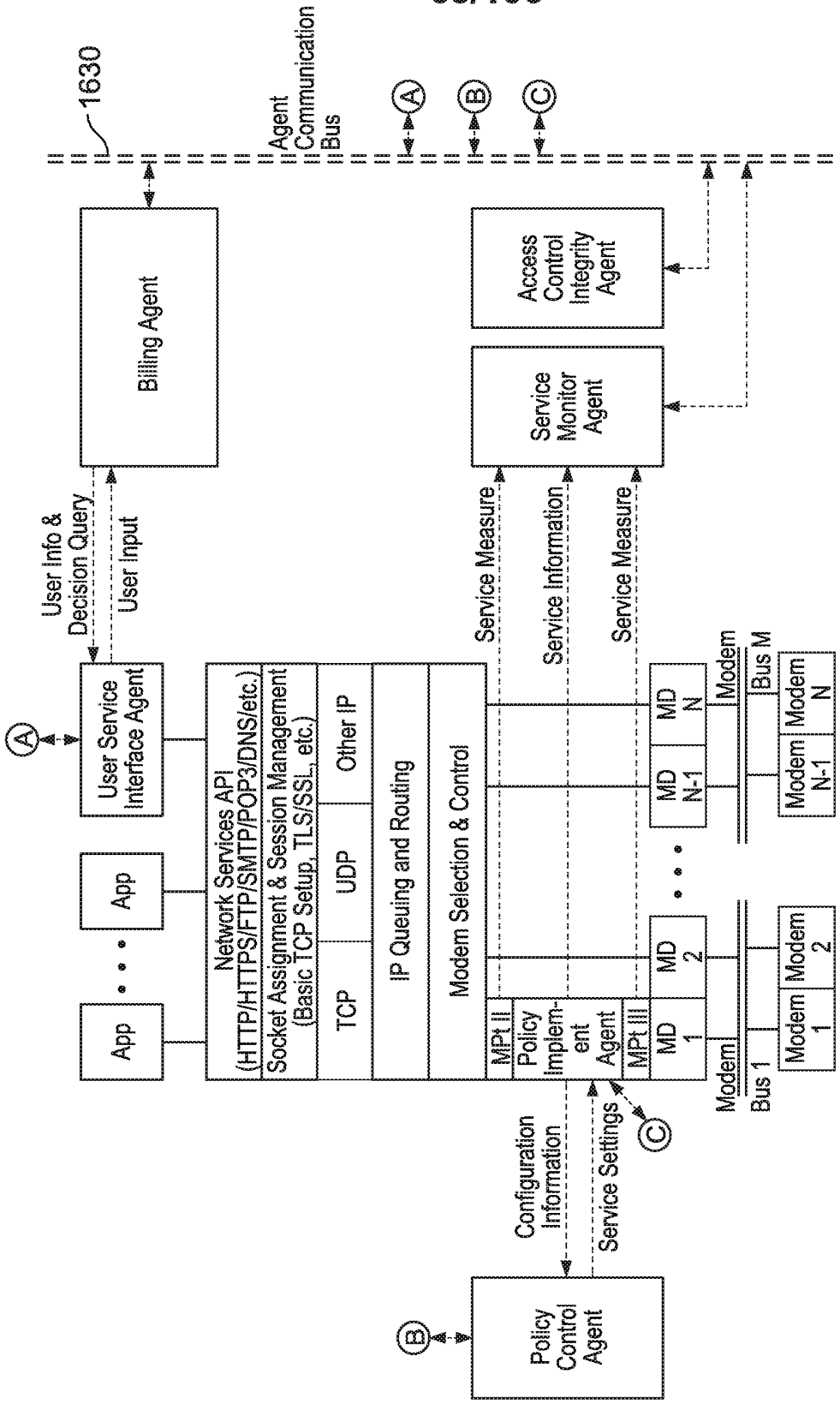

1630
Agent Communication Bus
A
B
C
Billing Agent
User Info & Decision Query
User Input
User Service Interface Agent
App
App
Network Services API (HTTP/HTTPS/FTP/SMTP/POP3/DNS/etc.)
Socket Assignment & Session Management (Basic TCP Setup, TLS/SSL, etc.)
TCP
UDP
Other IP
IP Queuing and Routing
Modem Selection & Control
MPt II
Policy Implem-ent Agent
MPt III
MD 1
MD 2
MD N-1
MD N
Modem Bus 1
Modem Bus M
Modem 1
Modem 2
Modem N-1
Modem N
Service Measure
Service Information
Service Measure
Service Monitor Agent
Access Control Integrity Agent
Configuration Information
Service Settings
Policy Control Agent

FIG. 34

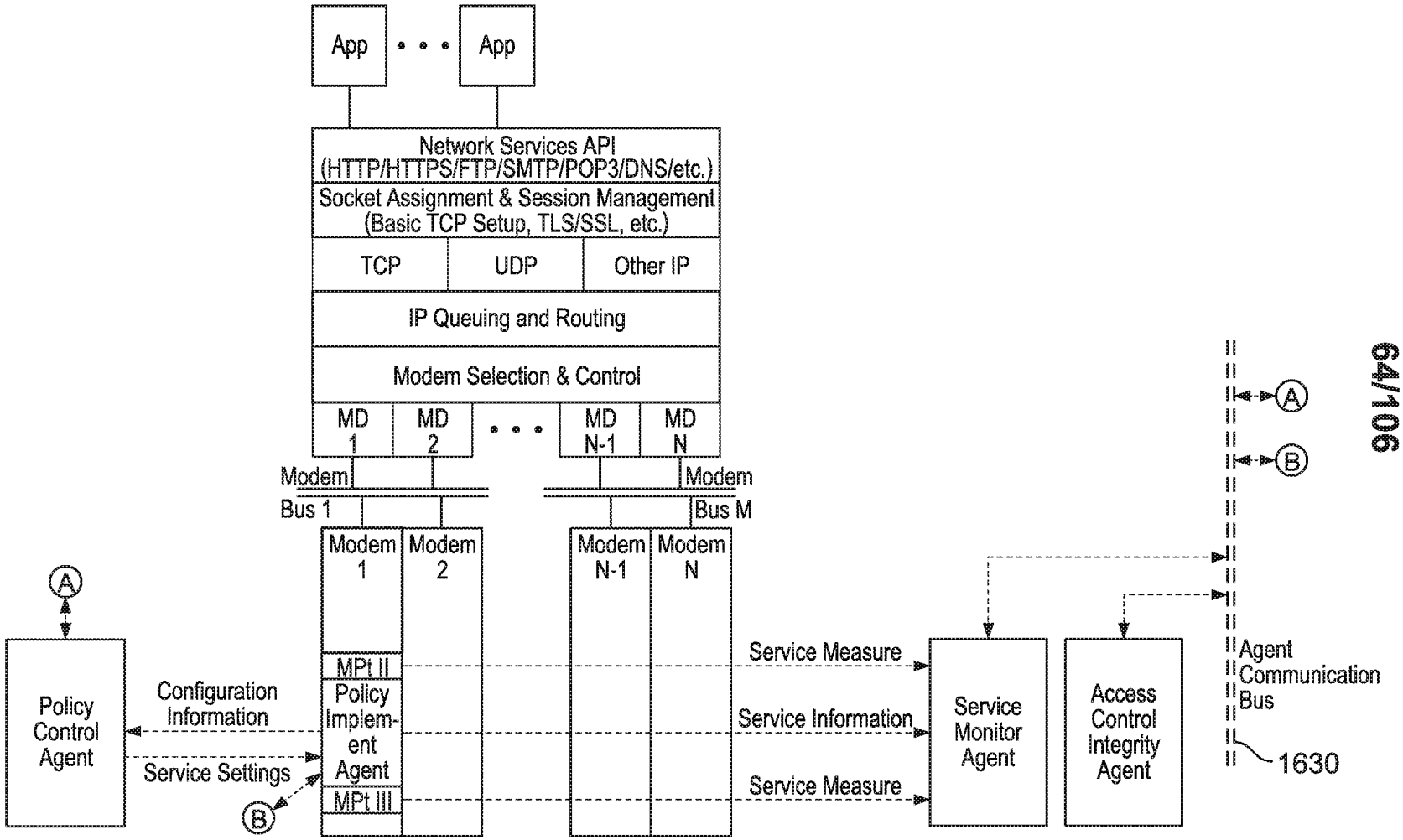

App
App
Network Services API
(HTTP/HTTPS/FTP/SMTP/POP3/DNS/etc.)
Socket Assignment & Session Management
(Basic TCP Setup, TLS/SSL, etc.)
TCP
UDP
Other IP
IP Queuing and Routing
Modem Selection & Control
MD 1
MD 2
MD N-1
MD N
Modem
Bus 1
Modem
Bus M
Modem 1
Modem 2
Modem N-1
Modem N
MPt II
Policy Implem-ent Agent
MPt III
Policy Control Agent
Configuration Information
Service Settings
Service Measure
Service Information
Service Measure
Service Monitor Agent
Access Control Integrity Agent
Agent Communication Bus
1630
A
B
1040
64/106

FIG. 35

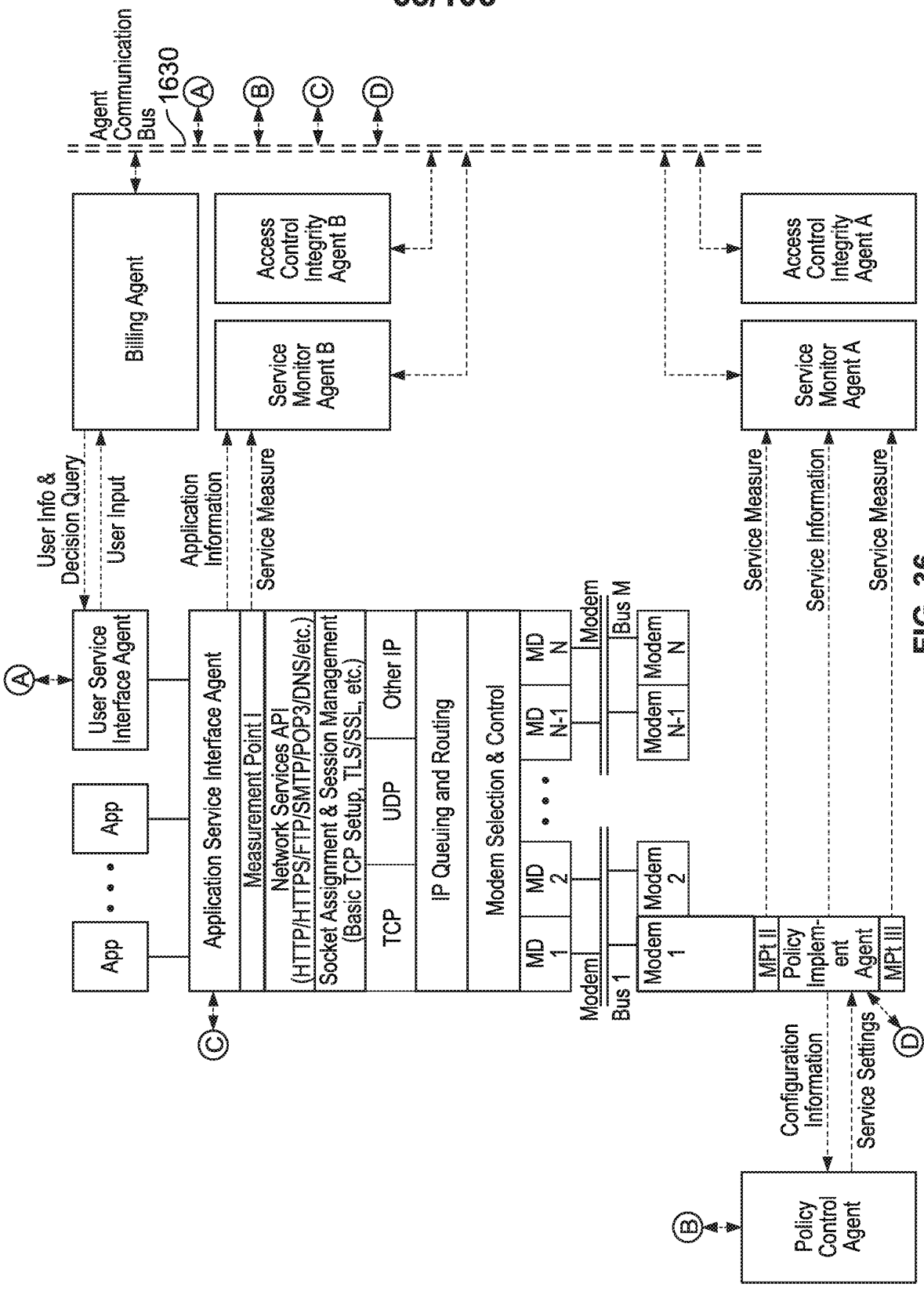

Agent Communication Bus
1630
A
B
C
D
Billing Agent
Access Control Integrity Agent B
Service Monitor Agent B
Access Control Integrity Agent A
Service Monitor Agent A
User Info & Decision Query
User Input
Application Information
Service Measure
Service Measure
Service Information
Service Measure
User Service 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

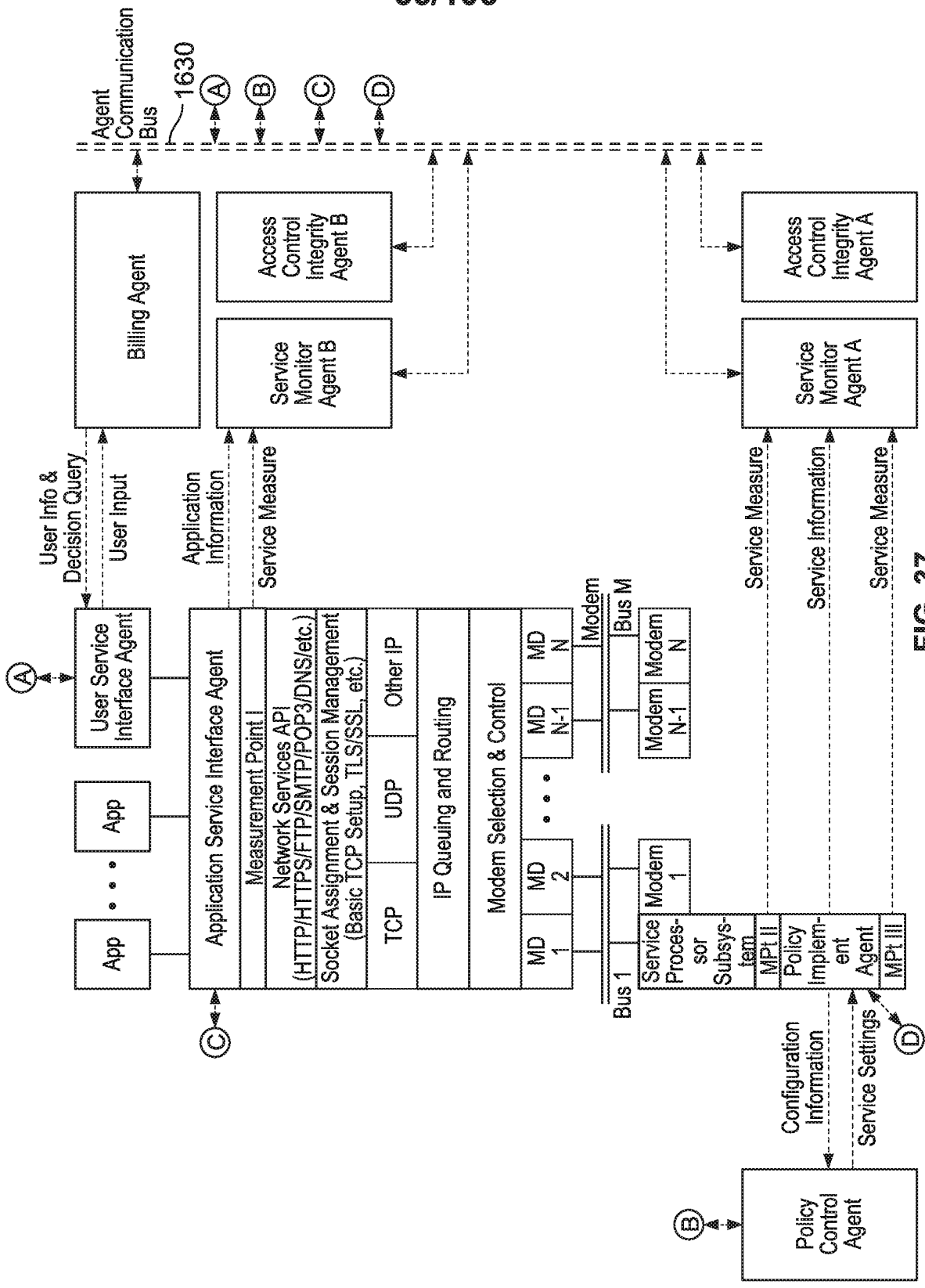

Agent Communication Bus
1630
A
B
C
D
Billing Agent
Access Control Integrity Agent B
Service Monitor Agent B
Access Control Integrity Agent A
Service Monitor Agent A
User Info & Decision Query
User Input
Application Information
Service Measure
Service Measure
Service Information
Service Measure
User Service 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 M
Modem N-1
Modem N
Bus 1
Service Processor Subsystem
Modem 1
MPI II
Policy Implement Agent
MPI III
Configuration Information
Service Settings
Policy Control Agent

FIG. 37

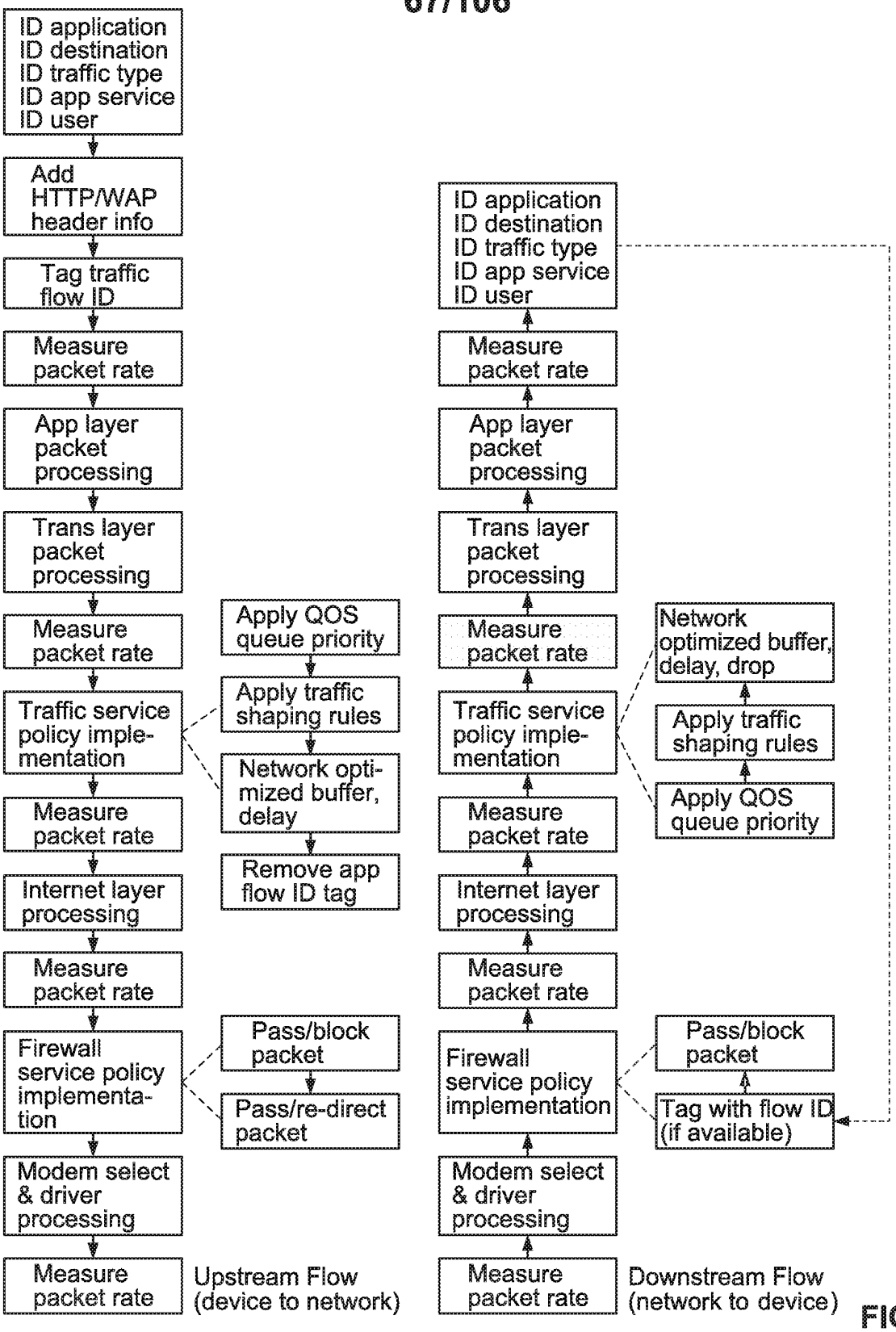

ID application
ID destination
ID traffic type
ID app service
ID user
Add HTTP/WAP header info
Tag traffic flow ID
Measure packet rate
App layer packet processing
Trans layer packet processing
Measure packet rate
Traffic service policy imple-mentation
Apply QOS queue priority
Apply traffic shaping rules
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

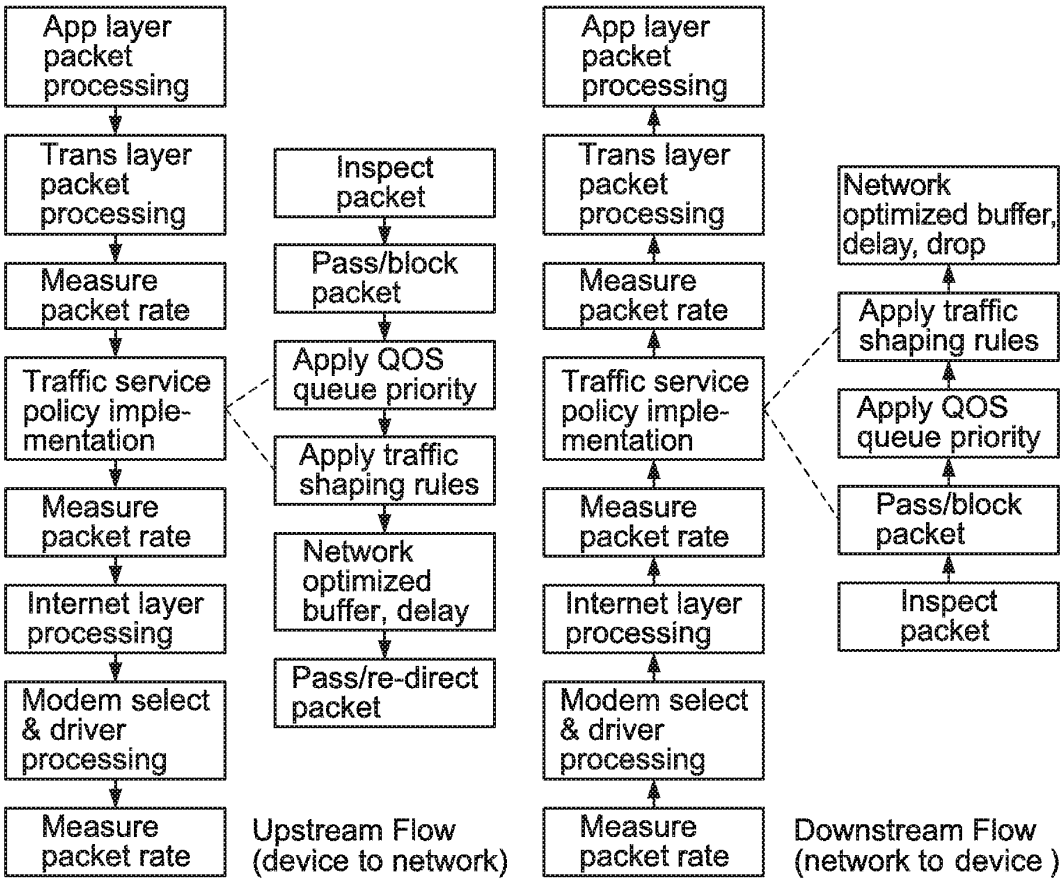

App layer packet processing
Trans layer packet processing
Measure packet rate
Traffic service policy imple-mentation
Measure packet rate
Internet layer processing
Modem select & driver processing
Measure packet rate
Inspect packet
Pass/block packet
Apply QOS queue priority
Apply traffic shaping rules
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

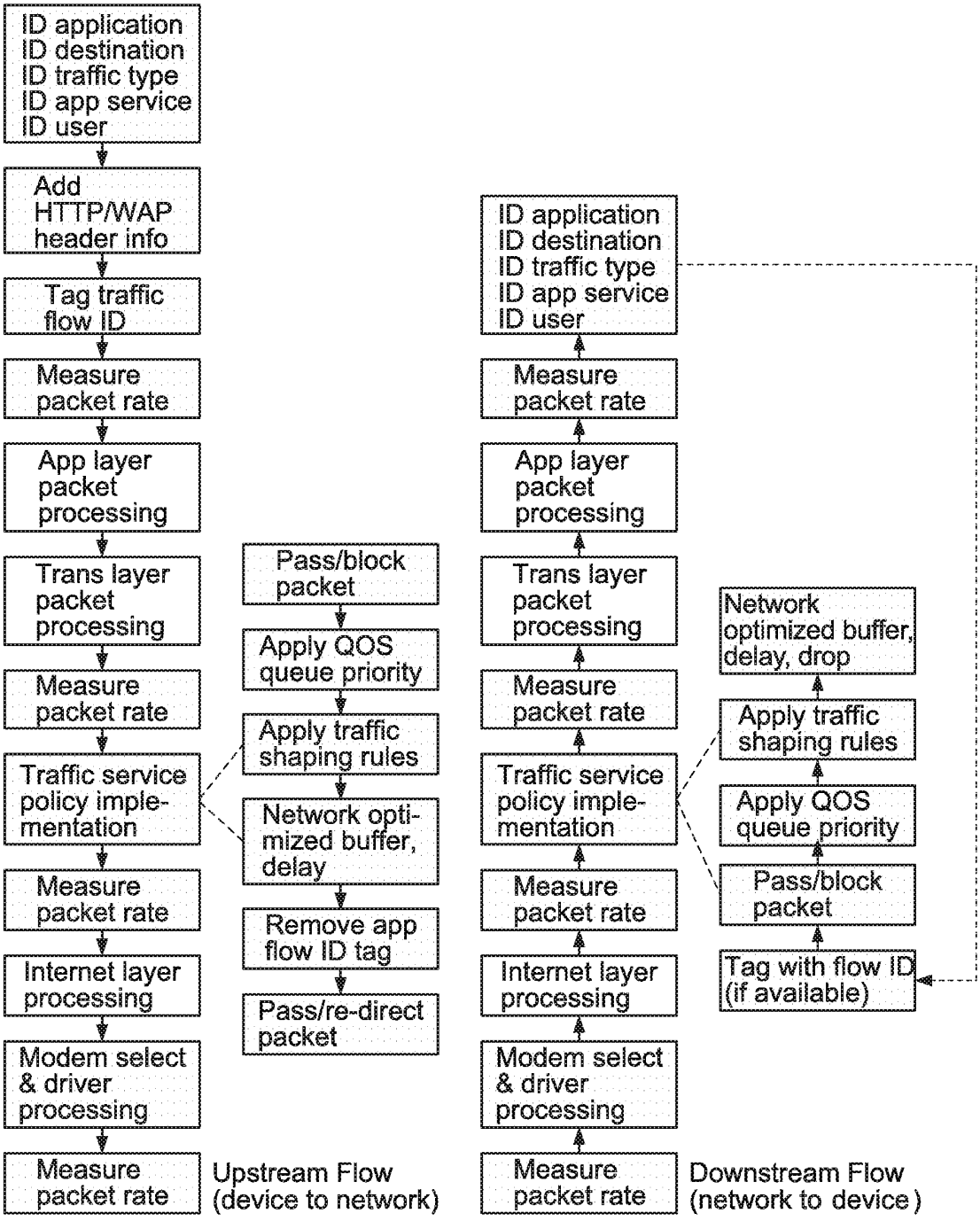

ID application
ID destination
ID traffic type
ID app service
ID user
Add HTTP/WAP header info
Tag traffic flow ID
Measure packet rate
App layer packet processing
Trans layer packet processing
Measure packet rate
Traffic service policy imple-mentation
Measure packet rate
Internet layer processing
Modem 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

1046

70/106

FIG. 41

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.

1047

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.

1048

72/106

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.

1051

75/109

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.

1052

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.

1053

177/206

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

1054

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.

1055

79/106

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.

1056

FIG. 42J

Service Processor Authorization

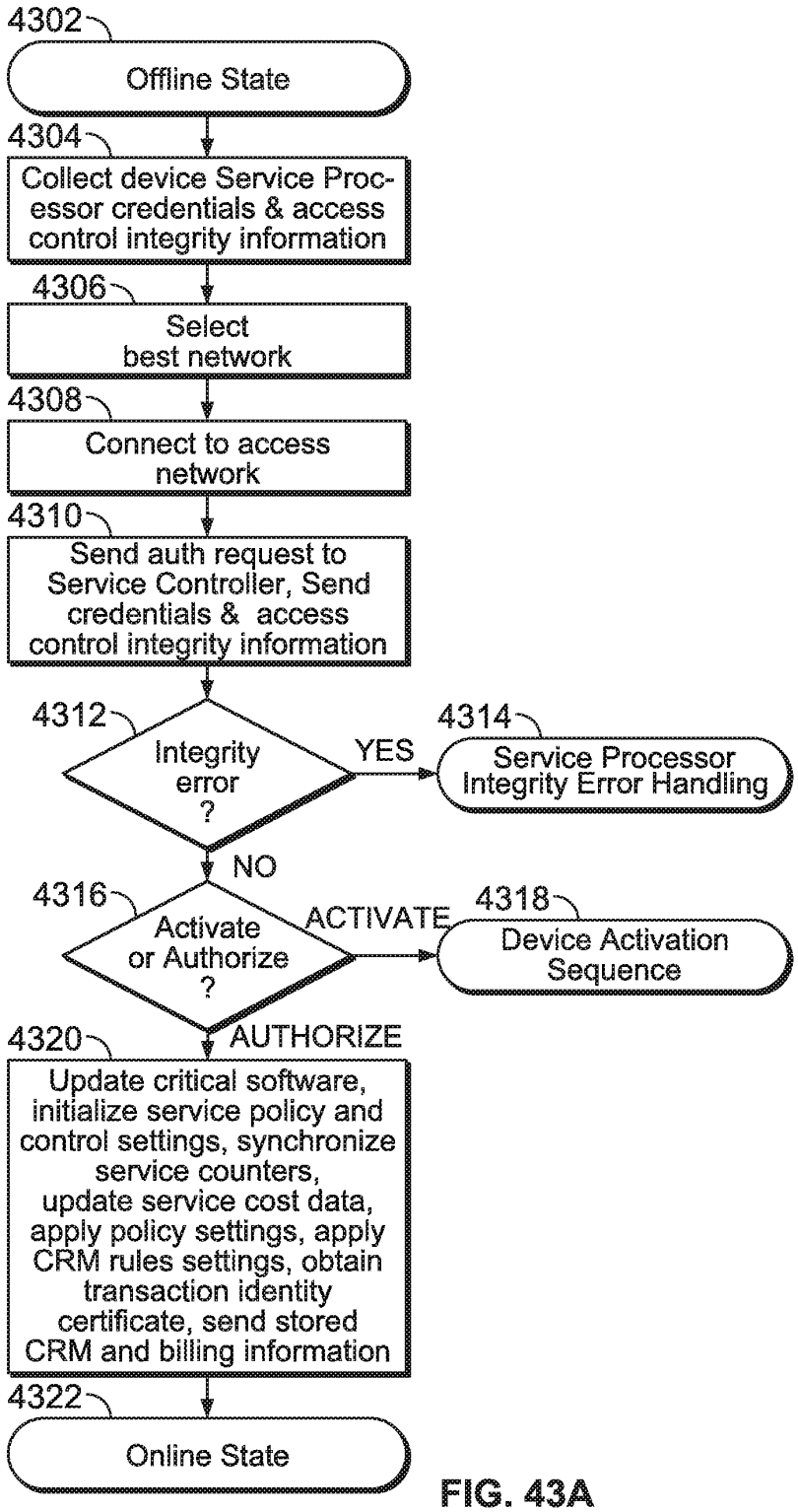


FIG. 43A

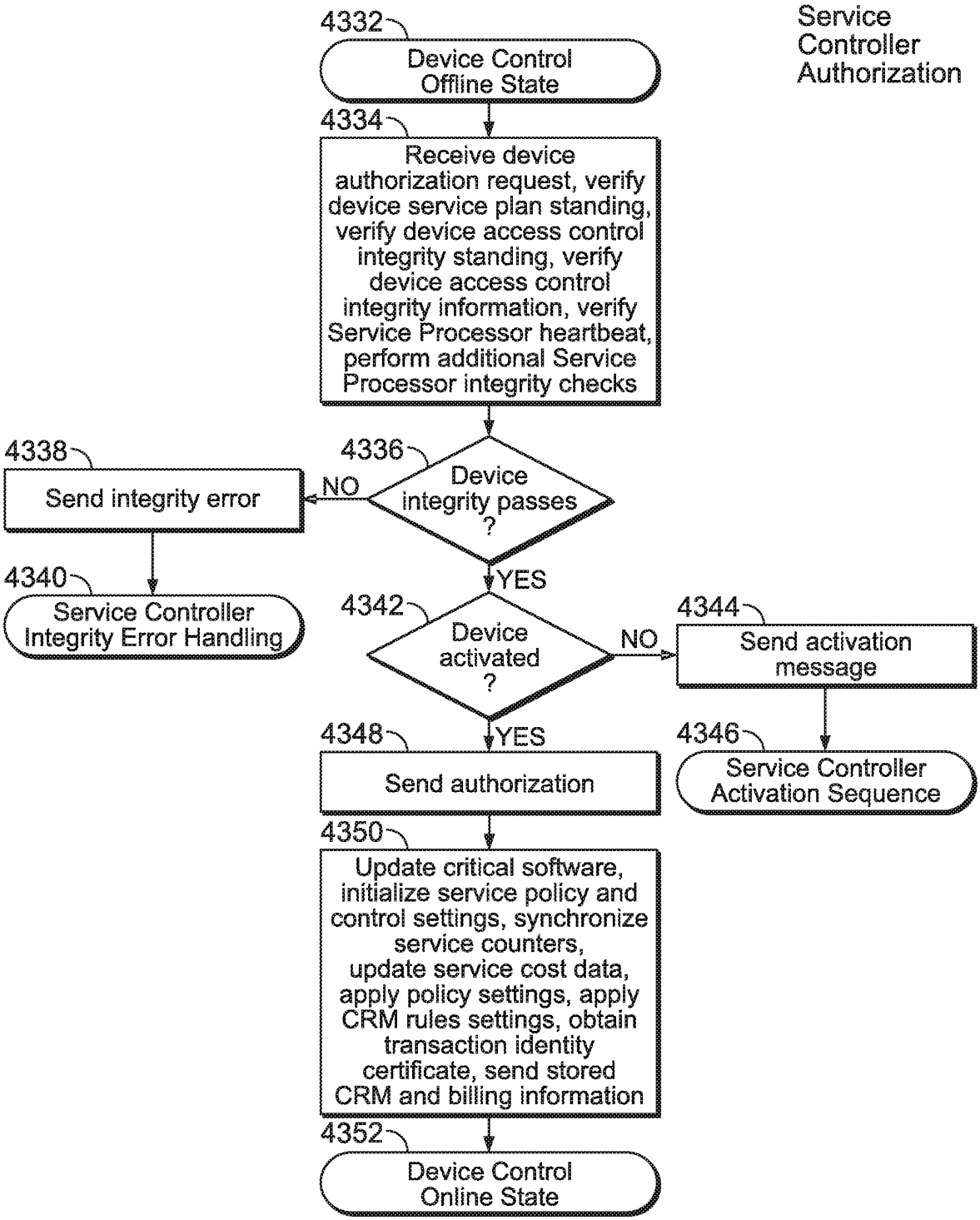

Service Controller Authorization
4332
Device Control Offline State
4334
Receive device authorization request, verify device service plan standing, verify device access control integrity standing, verify device access control integrity information, verify Service Processor heartbeat, perform additional 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

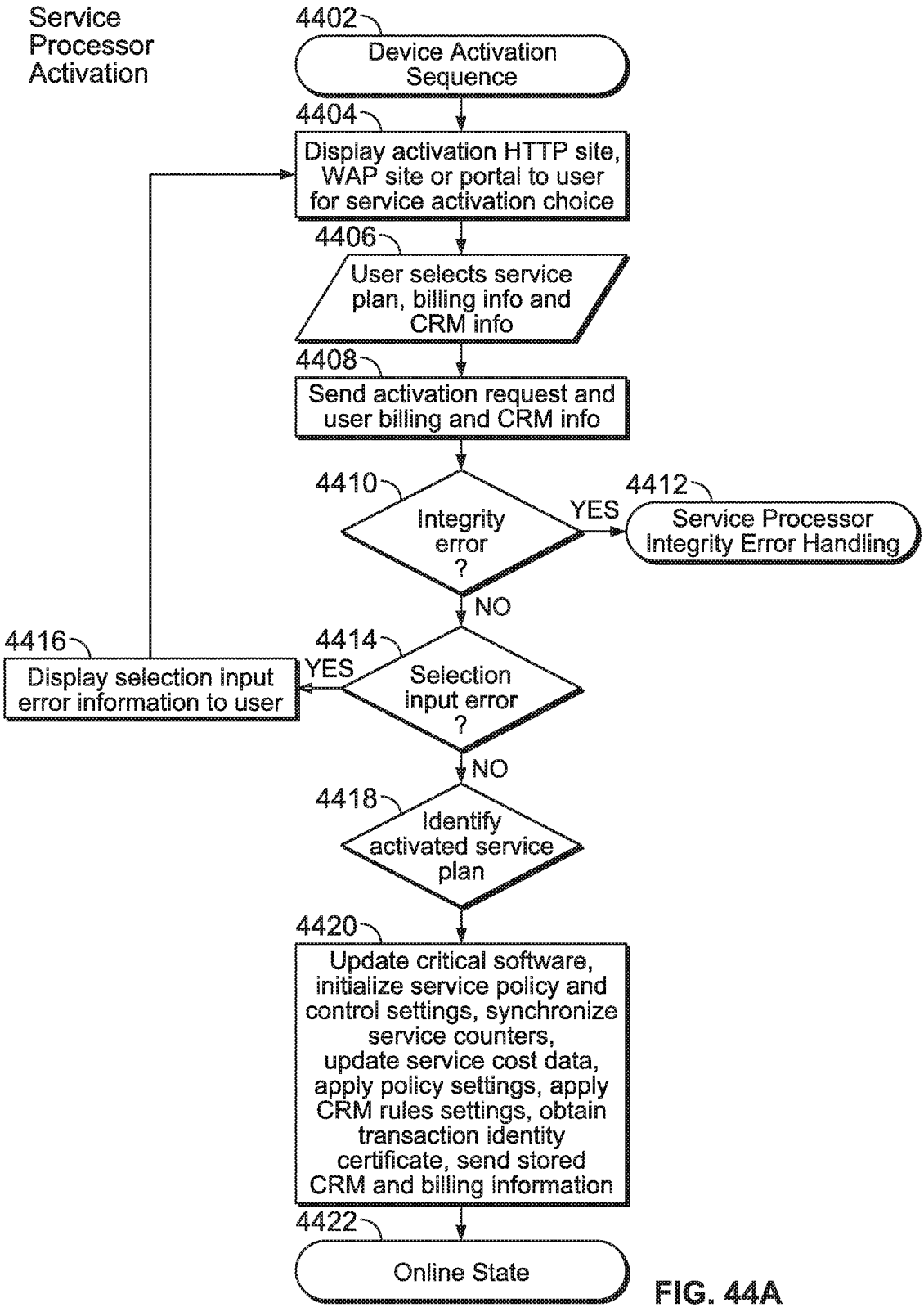

Service Processor Activation
4402
Device Activation Sequence
4404
Display activation HTTP site, WAP site or portal to user for service activation choice
4406
User selects service plan, billing info and CRM info
4408
Send activation request and user billing and CRM info
4410
Integrity error ?
YES
4412
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

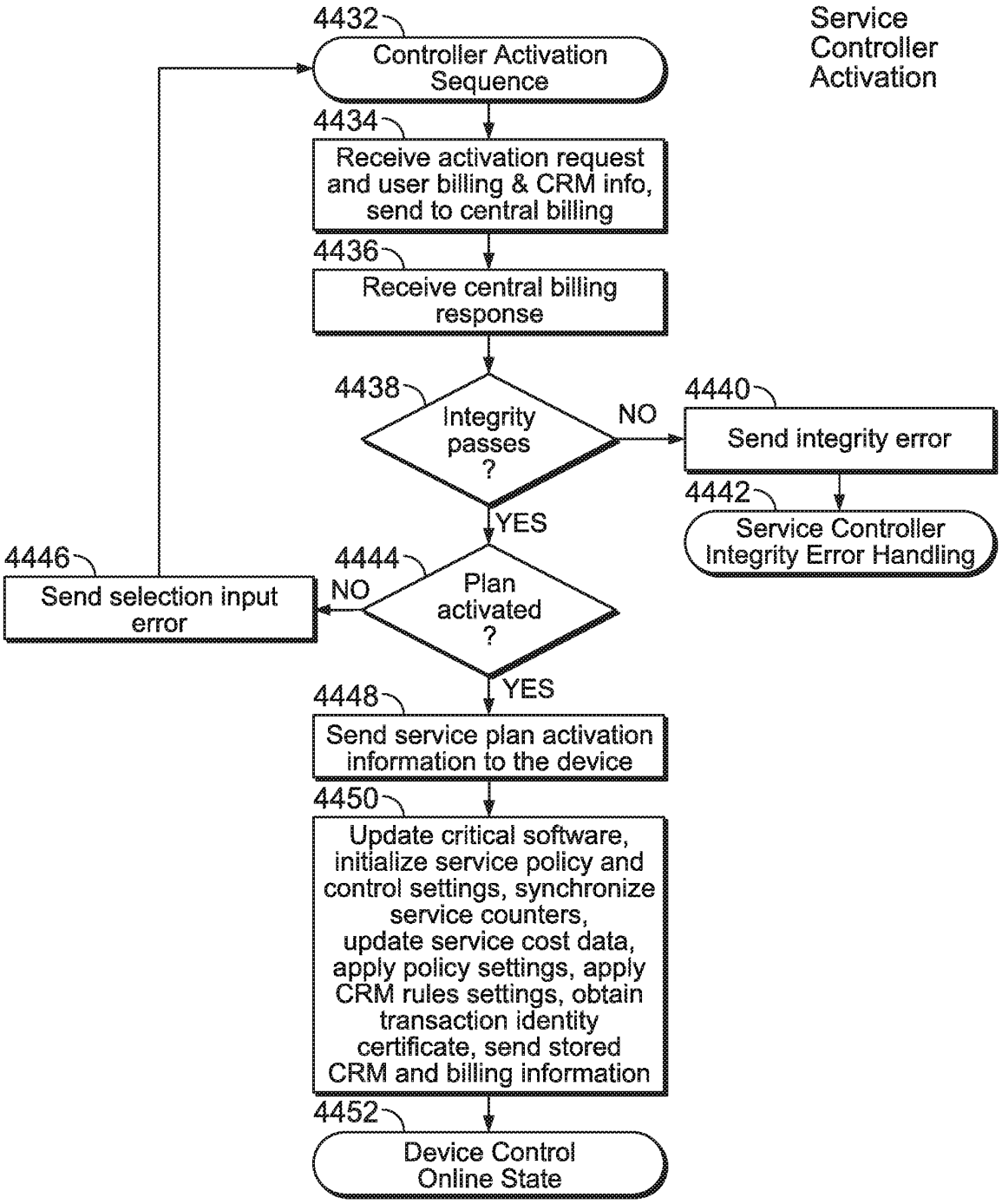

Service Controller Activation
4432
Controller Activation Sequence
4434
Receive activation request and user billing & CRM info, send to central billing
4436
Receive central billing response
4438
Integrity passes ?
NO
4440
Send integrity error
4442
Service Controller Integrity Error Handling
YES
4444
Plan 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

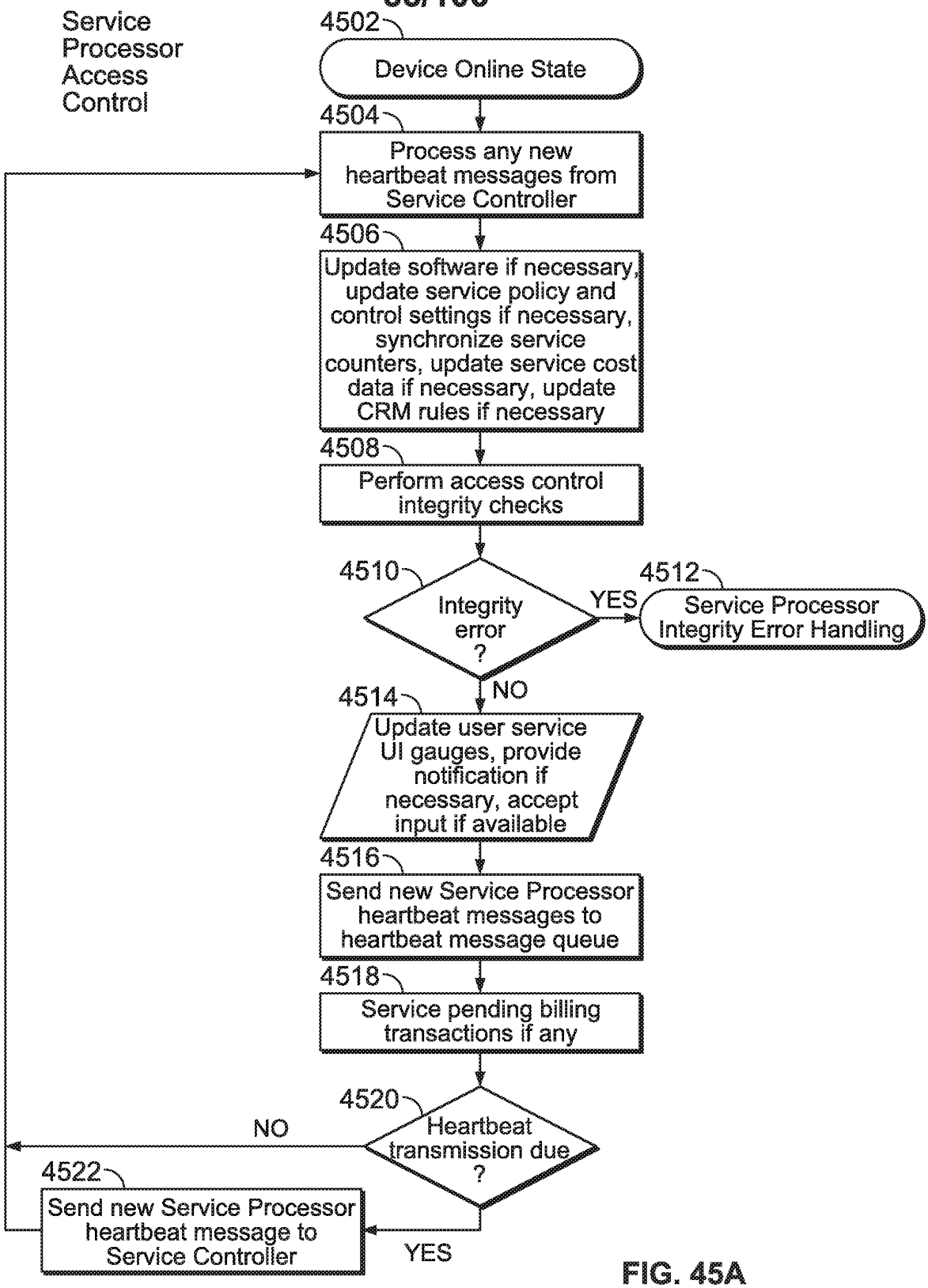

Service Processor Access Control
4502
Device Online State
4504
Process any new heartbeat messages from Service Controller
4506
Update software if necessary, update service policy and control settings if necessary, synchronize service counters, update service cost data if necessary, update CRM rules if 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
4522
Send new Service Processor heartbeat message to Service Controller
YES

FIG. 45A

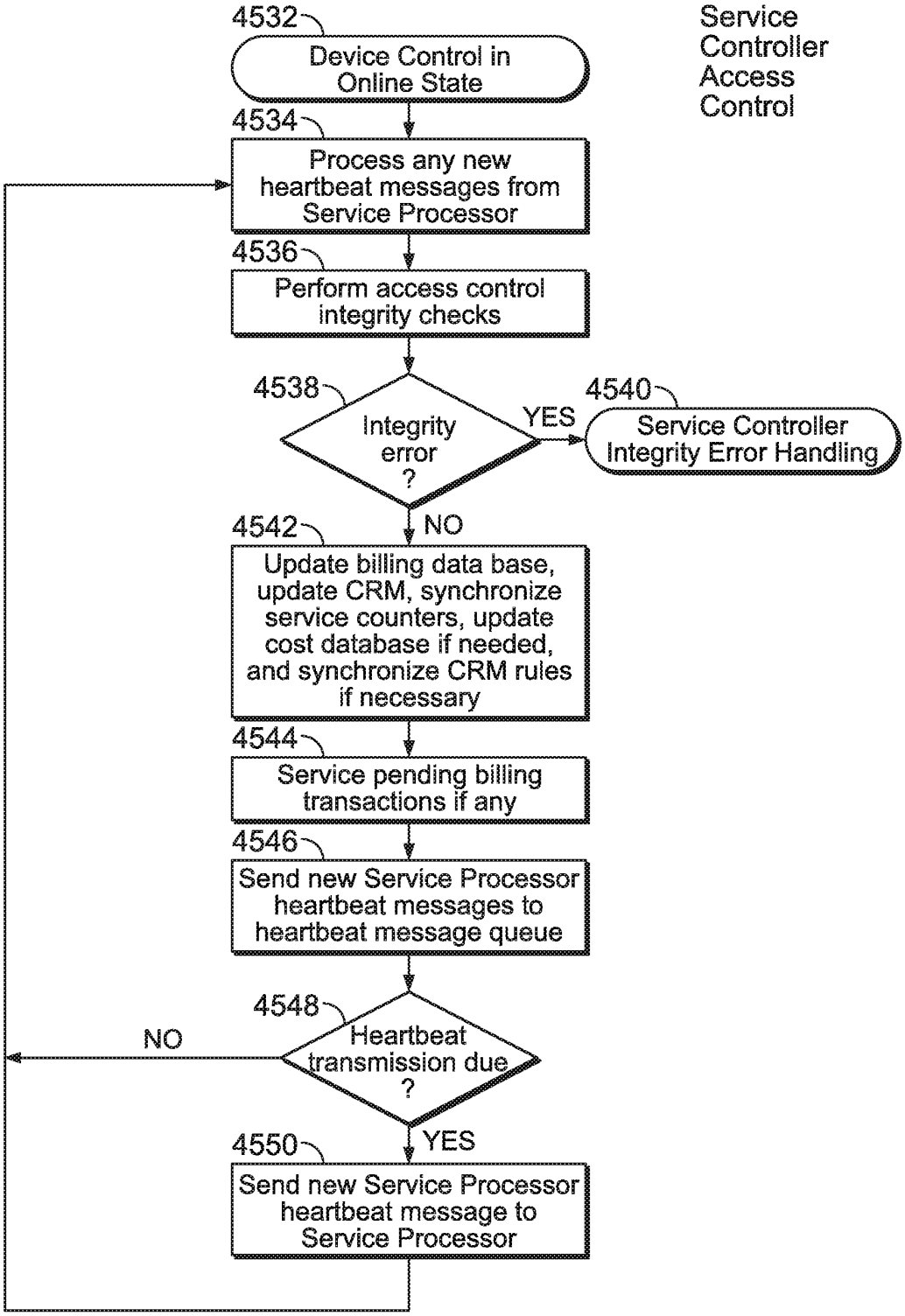

Service Controller Access Control
4532
Device Control in Online State
4534
Process any new heartbeat messages from Service Processor
4536
Perform access control integrity checks
4538
Integrity error ?
YES
4540
Service Controller Integrity Error Handling
NO
4542
Update billing data base, update CRM, synchronize 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

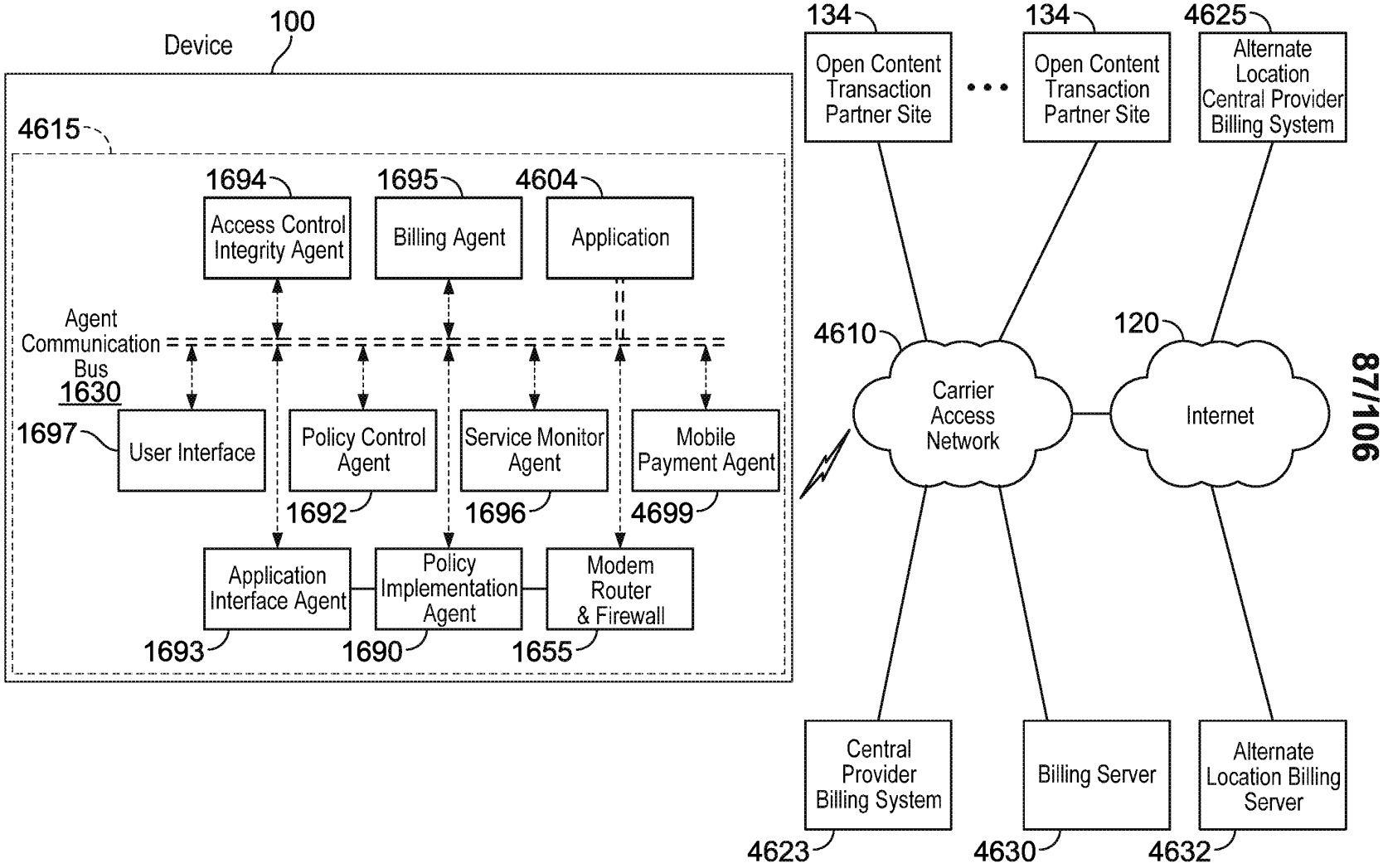

Device
100
4615
1694
Access Control Integrity Agent
1695
Billing Agent
4604
Application
Agent Communication Bus
1630
1697
User Interface
Policy Control Agent
1692
Service Monitor Agent
1696
Mobile Payment Agent
4699
Application Interface Agent
1693
Policy Implementation Agent
1690
Modem Router & Firewall
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

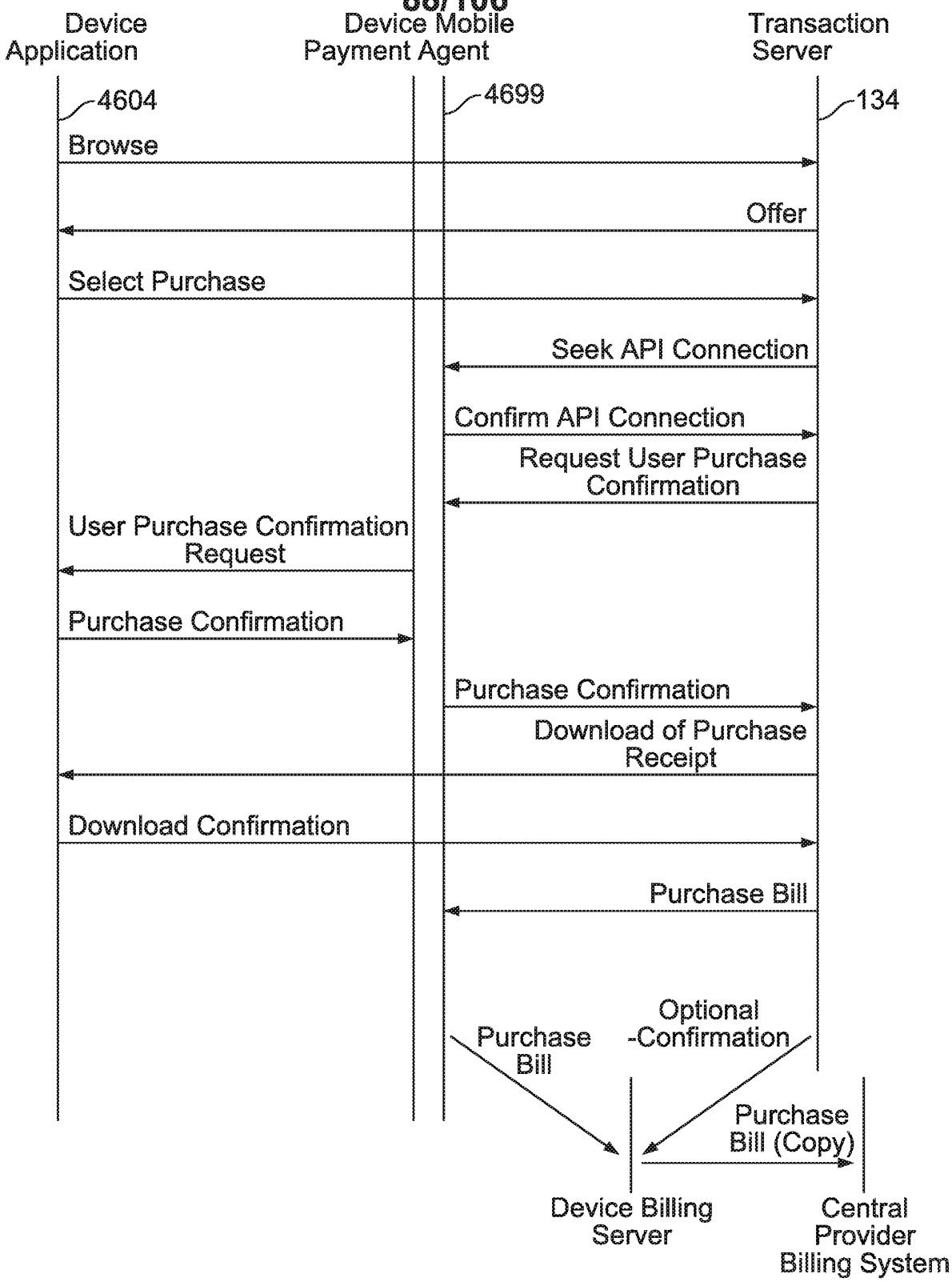

Device Application
Device Mobile Payment Agent
Transaction Server
4604
4699
134
Browse
Offer
Select Purchase
Seek API Connection
Confirm API Connection
Request User Purchase Confirmation
User Purchase Confirmation Request
Purchase Confirmation
Purchase Confirmation
Download of Purchase Receipt
Download Confirmation
Purchase Bill
Optional -Confirmation
Purchase Bill
Purchase Bill (Copy)
Device Billing Server
Central Provider Billing System

FIG. 47A

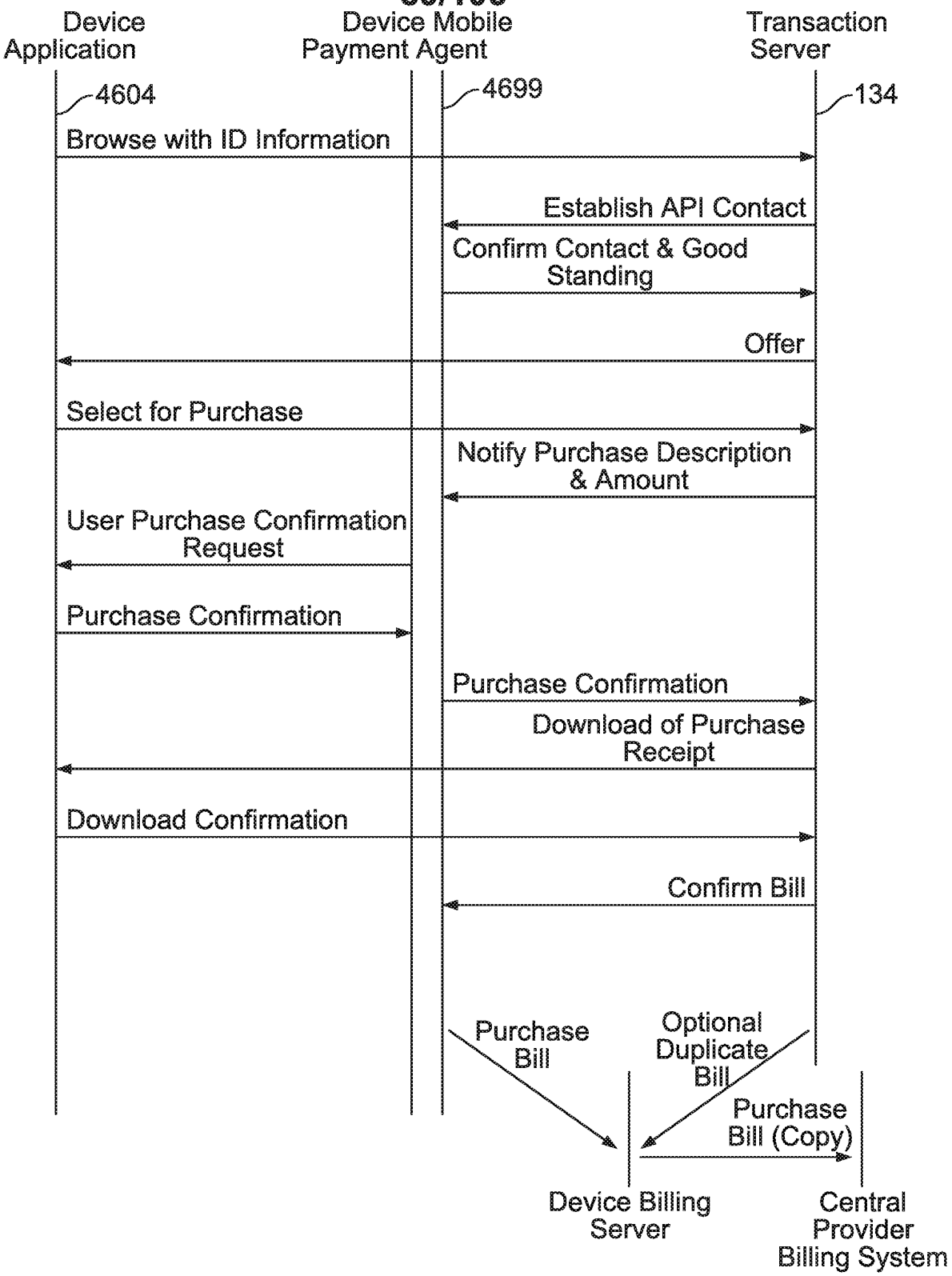

Device Application
Device Mobile Payment Agent
Transaction Server
4604
4699
134
Browse with ID Information
Establish API Contact
Confirm Contact & Good Standing
Offer
Select for Purchase
Notify Purchase Description & Amount
User Purchase Confirmation Request
Purchase Confirmation
Purchase Confirmation
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

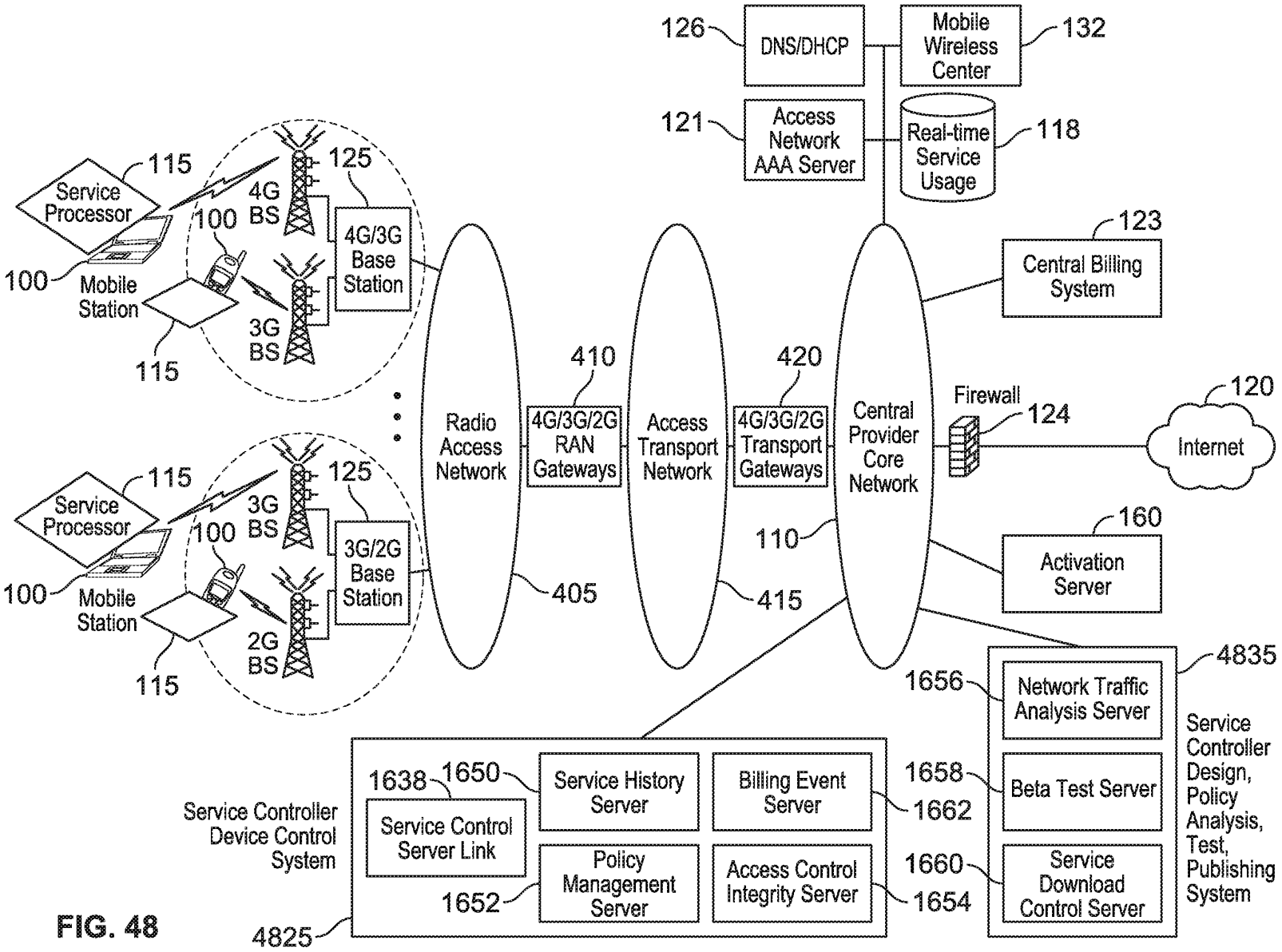

126
DNS/DHCP
Mobile Wireless Center
132
121
Access Network AAA Server
Real-time Service Usage
118
123
Central Billing System
115
Service Processor
100
Mobile Station
4G BS
125
4G/3G Base Station
3G BS
115
410
420
Radio Access Network
4G/3G/2G RAN Gateways
Access Transport Network
4G/3G/2G Transport Gateways
Central Provider Core Network
Firewall
124
120
Internet
90/106
115
Service Processor
100
Mobile Station
3G BS
125
3G/2G Base Station
2G BS
115
110
405
415
160
Activation Server
4835
1656
Network Traffic Analysis Server
Service Controller Design, Policy Analysis, Test, Publishing System
1658
Beta Test Server
1660
Service Download Control Server
1638
1650
Service Control Server Link
Service History Server
Billing Event Server
1662
Service Controller Device Control System
1652
Policy Management Server
Access Control Integrity Server
1654
4825

FIG. 48

1066

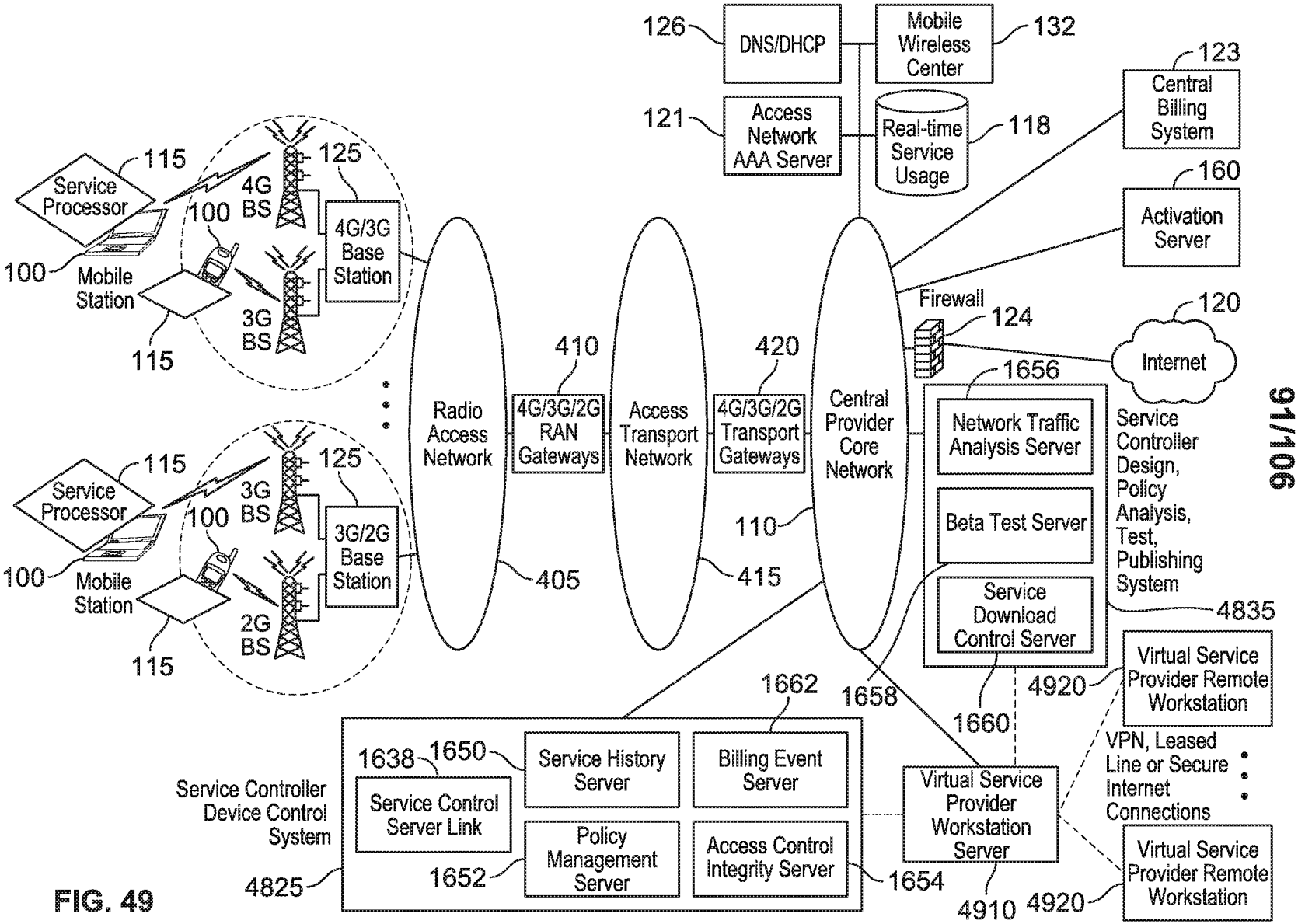


FIG. 49

1067

97/106

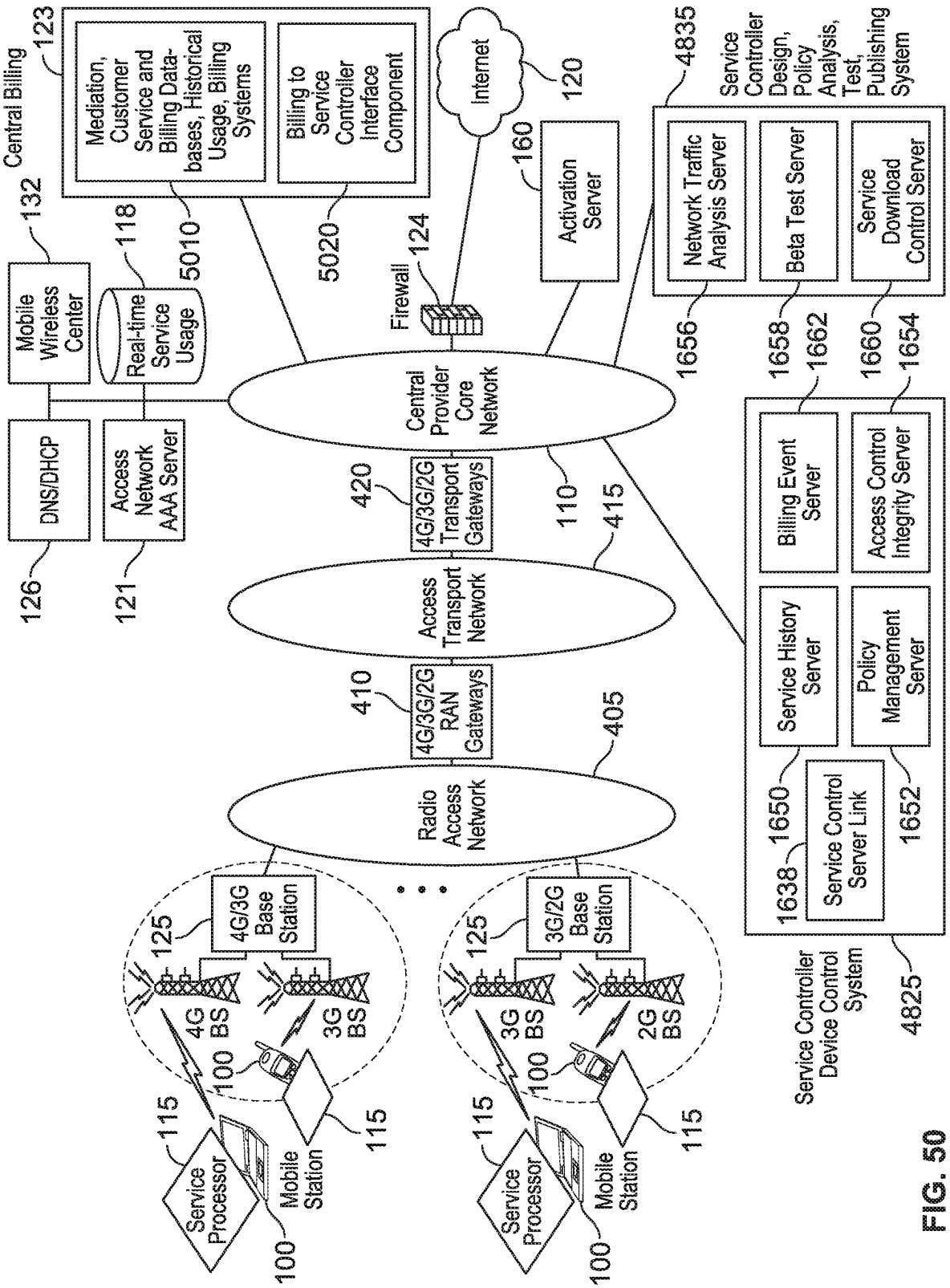

Central Billing
123
Mediation, Customer Service and Billing Data-bases, Historical Usage, Billing Systems
Billing to Service Controller Interface Component
5010
5020
Internet
120
Mobile Wireless Center
132
Real-time Service Usage
118
Firewall
124
Activation Server
160
Service Controller Design, Policy Analysis, Test, Publishing System
4835
Network Traffic Analysis Server
Beta Test Server
Service Download Control Server
1656
1658
1660
1662
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
1652
1638
Service Controller Device Control System
4825
125
4G/3G Base Station
3G/2G Base Station
4G BS
3G BS
3G BS
2G BS
100
115
Service Processor
Mobile Station

FIG. 50

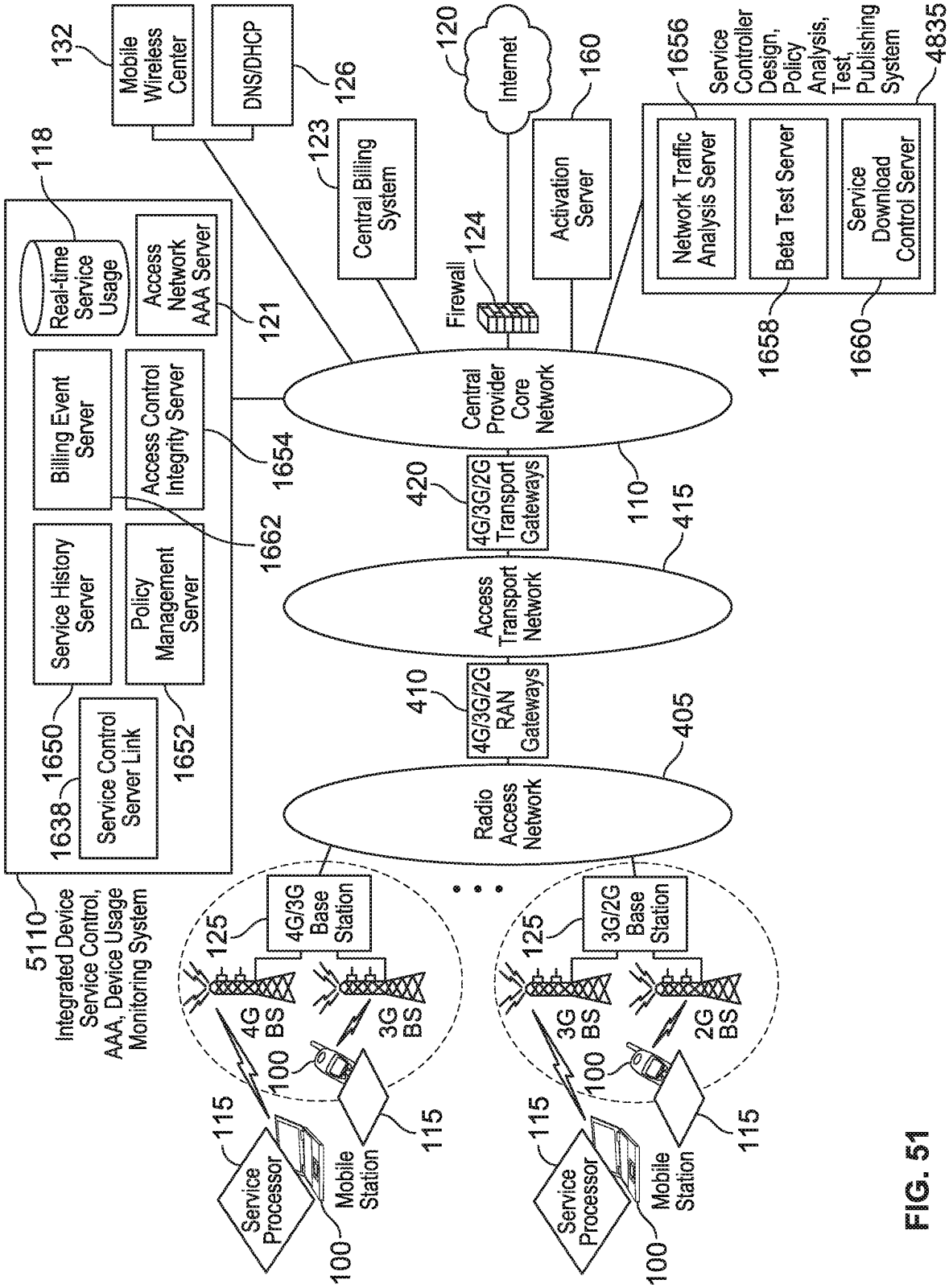

5110
Integrated Device Service Control, AAA, Device Usage Monitoring System
118
Real-time Service Usage
Access Network AAA Server
121
Billing Event Server
Access Control Integrity Server
1654
Service History Server
Policy Management Server
1662
1650
Service Control Server Link
1638
1652
132
Mobile Wireless Center
DNS/DHCP
126
123
Central Billing System
120
Internet
160
Activation Server
Firewall
124
Central Provider Core Network
110
1656
Service Controller Design, Policy Analysis, Test, Publishing System
4835
Network Traffic Analysis Server
Beta Test Server
Service Download Control Server
1658
1660
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
3G/2G Base Station
3G BS
2G BS

FIG. 51

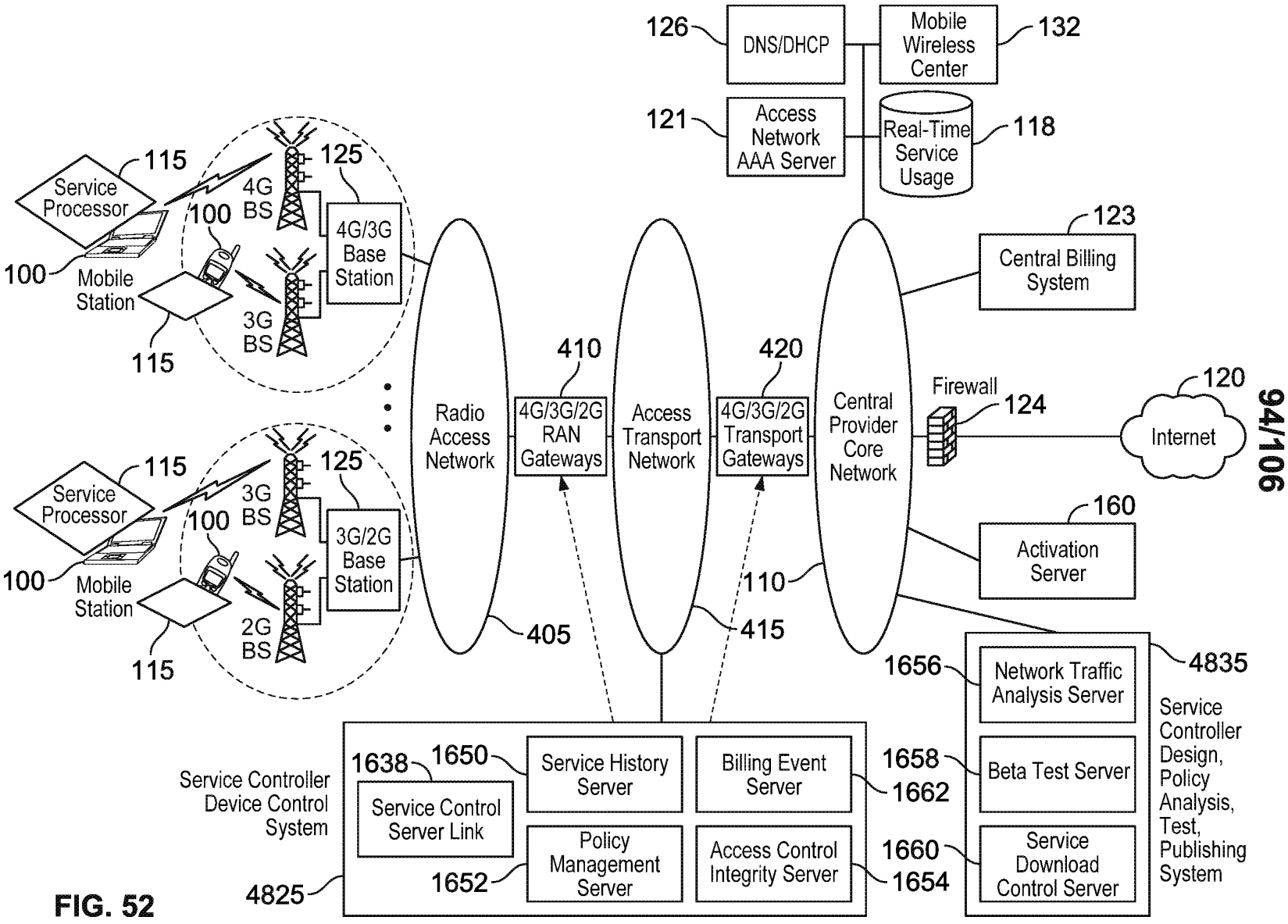

126
DNS/DHCP
Mobile Wireless Center
132
121
Access Network AAA Server
Real-Time Service Usage
118
123
Central Billing System
115
Service Processor
100
Mobile Station
4G BS
125
4G/3G Base Station
3G BS
410
420
Radio Access Network
4G/3G/2G RAN Gateways
Access Transport Network
4G/3G/2G Transport Gateways
Central Provider Core Network
Firewall
124
120
Internet
94/106
160
Activation Server
110
405
415
3G BS
3G/2G Base Station
2G BS
1656
Network Traffic Analysis Server
4835
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
1070

FIG. 52

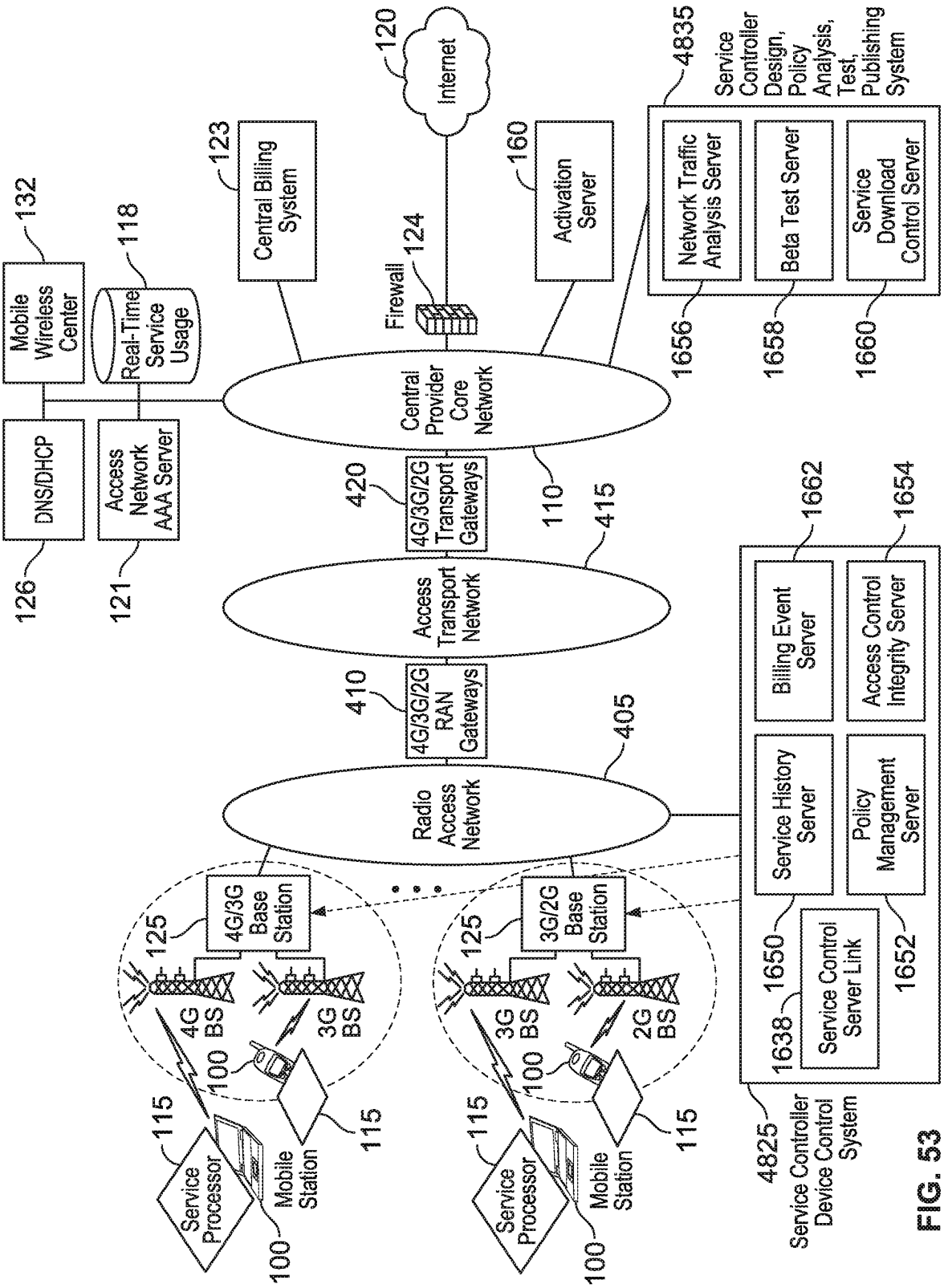

Mobile Wireless Center
132
Real-Time Service Usage
118
Central Billing System
123
Internet
120
Service Controller Design, Policy Analysis, Test, Publishing System
4835
Activation Server
160
Firewall
124
Network Traffic Analysis Server
Beta Test Server
Service Download Control Server
1656
1658
1660
DNS/DHCP
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
1650
1652
Service Control Server Link
1638
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. 53

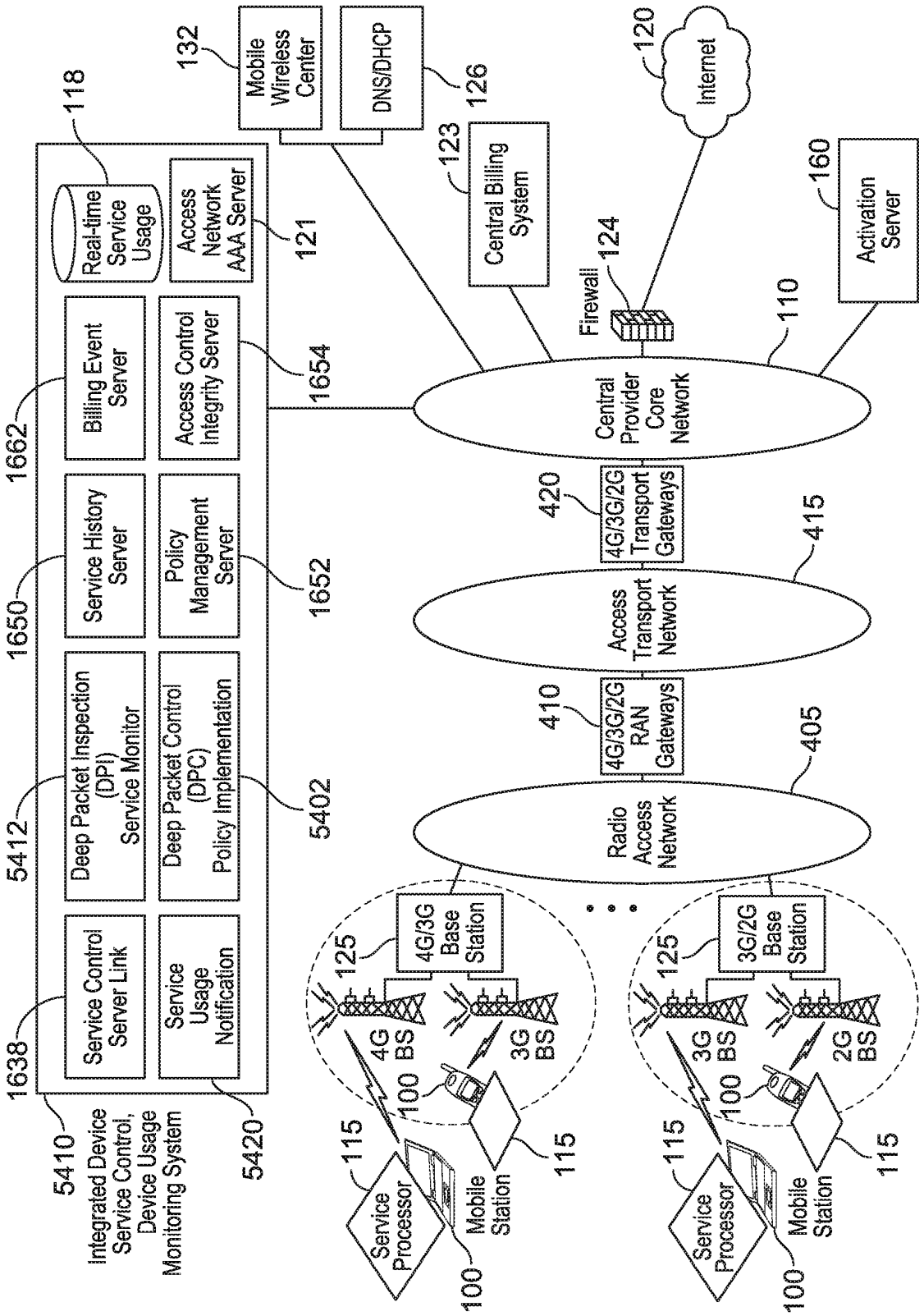

5410
Integrated Device Service Control, Device Usage Monitoring System
1638
Service Control Server Link
5412
Deep Packet Inspection (DPI) Service Monitor
1650
Service History Server
1662
Billing Event Server
118
Real-time Service Usage
132
Mobile Wireless Center
5420
Service Usage Notification
5402
Deep Packet Control (DPC) Policy Implementation
1652
Policy Management Server
1654
Access Control Integrity Server
121
Access Network AAA Server
126
DNS/DHCP
123
Central Billing System
120
Internet
124
Firewall
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
115
Service Processor
Mobile Station
125
3G/2G Base Station
3G BS
2G BS
100
115
Service Processor
Mobile Station

FIG. 54

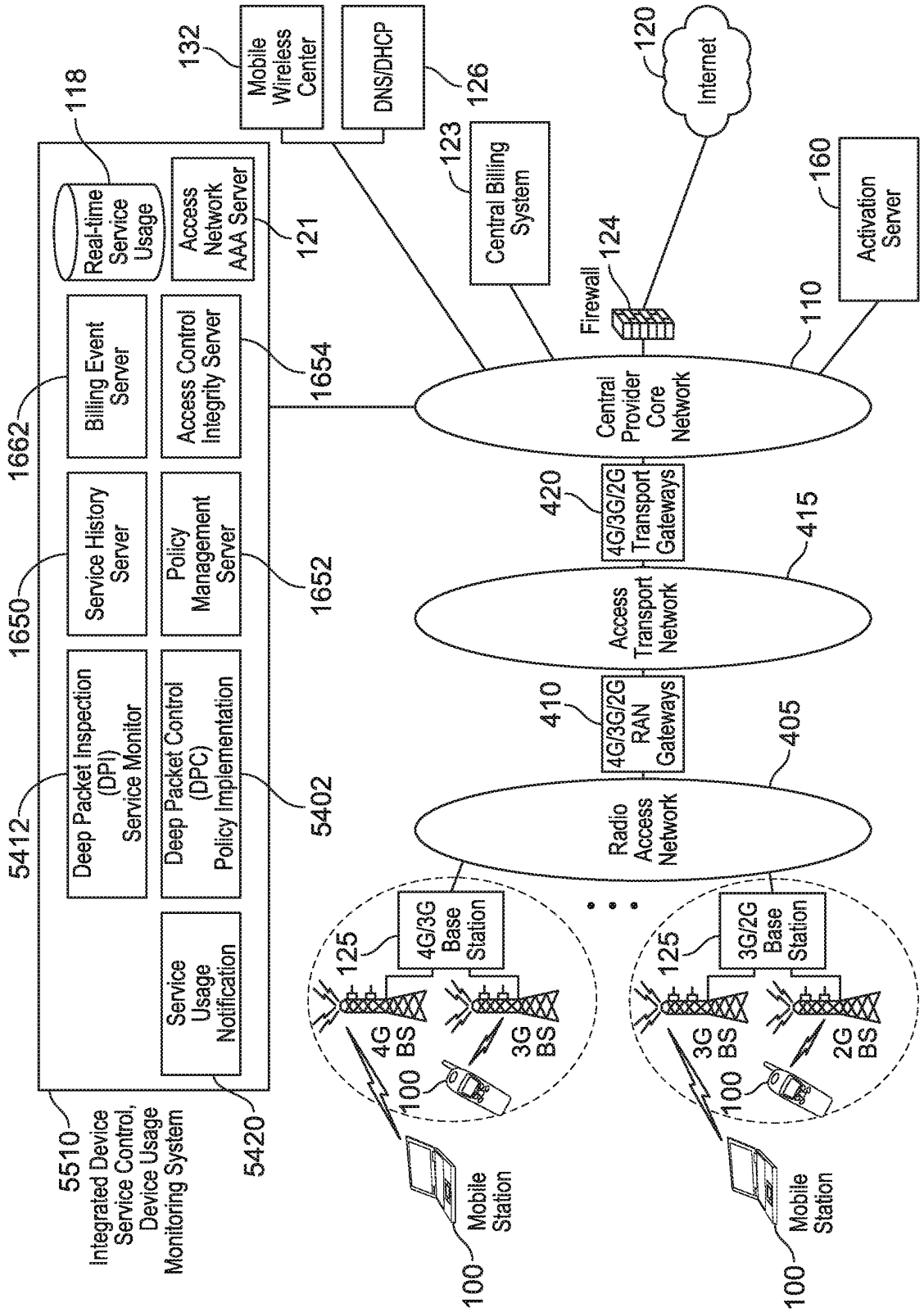

5510
Integrated Device Service Control, Device Usage Monitoring System
5420
5412
Deep Packet Inspection (DPI) Service Monitor
Service Usage Notification
1650
Service History Server
5402
Deep Packet Control (DPC) Policy Implementation
1652
Policy Management Server
1662
Billing Event Server
1654
Access Control Integrity Server
118
Real-time Service Usage
121
Access Network AAA Server
132
Mobile Wireless Center
126
DNS/DHCP
123
Central Billing System
124
Firewall
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
Mobile Station
125
3G/2G Base Station
3G BS
2G BS
100
Mobile Station

FIG. 55

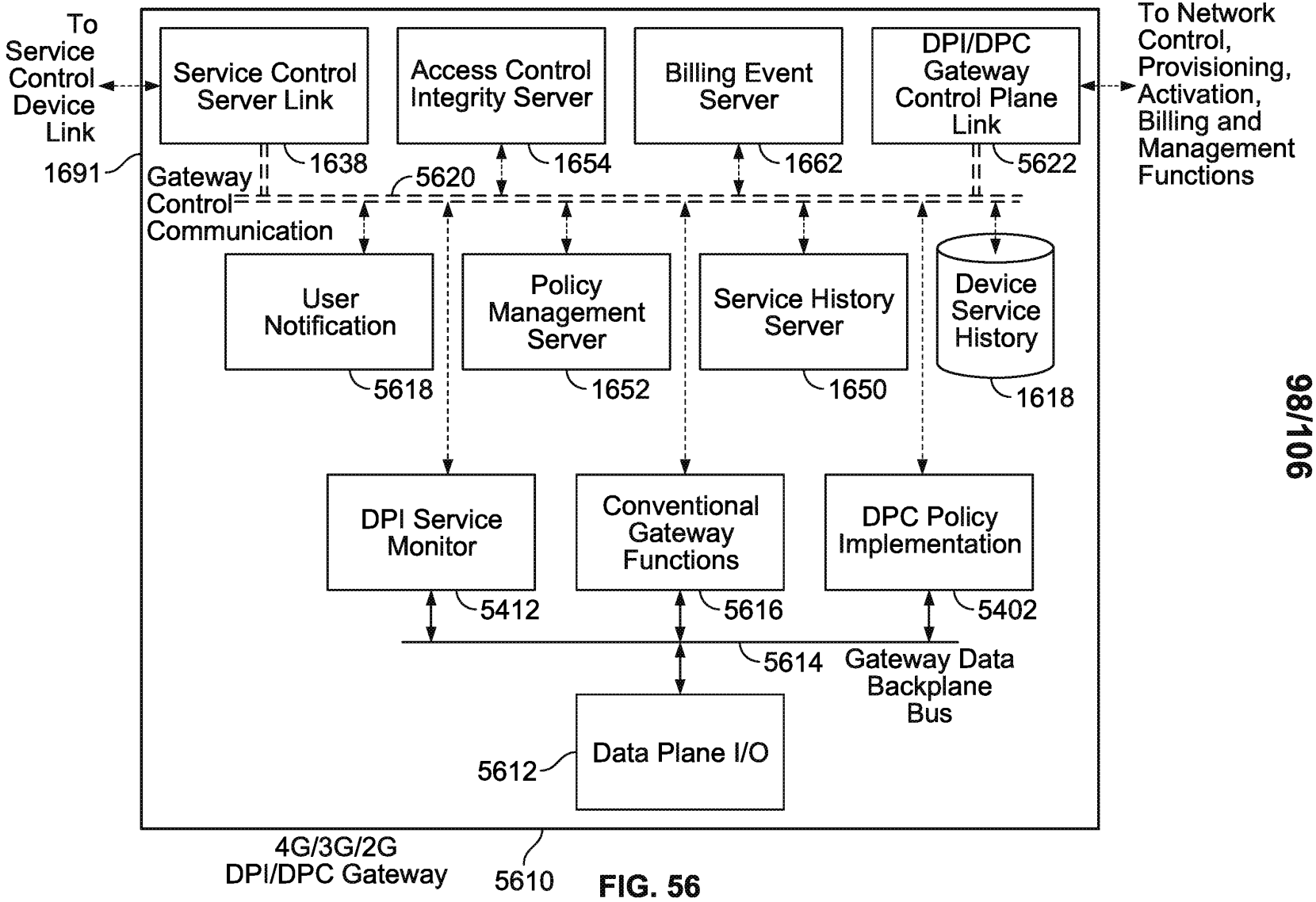


FIG. 56

98/106

1074

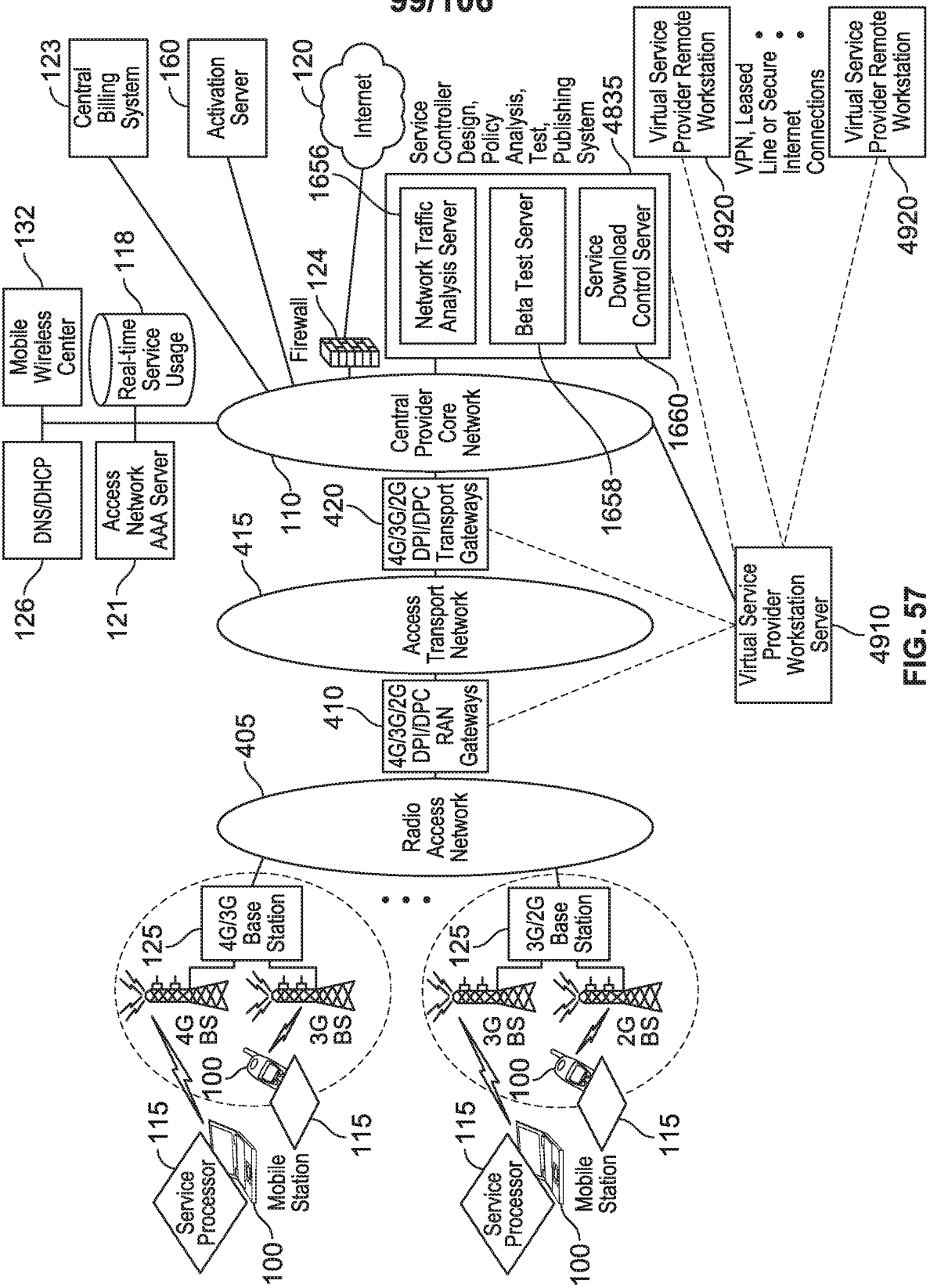

Central Billing System
123
Activation Server
160
Internet
120
Service Controller Design, Policy Analysis, Test, Publishing System
4835
Virtual Service Provider Remote Workstation
4920
VPN, Leased Line or Secure Internet Connections
Mobile Wireless Center
132
Real-time Service Usage
118
Firewall
124
1656
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
3G/2G Base Station
125
4G BS
3G BS
3G BS
2G BS
100
115
Service Processor
Mobile Station

FIG. 57

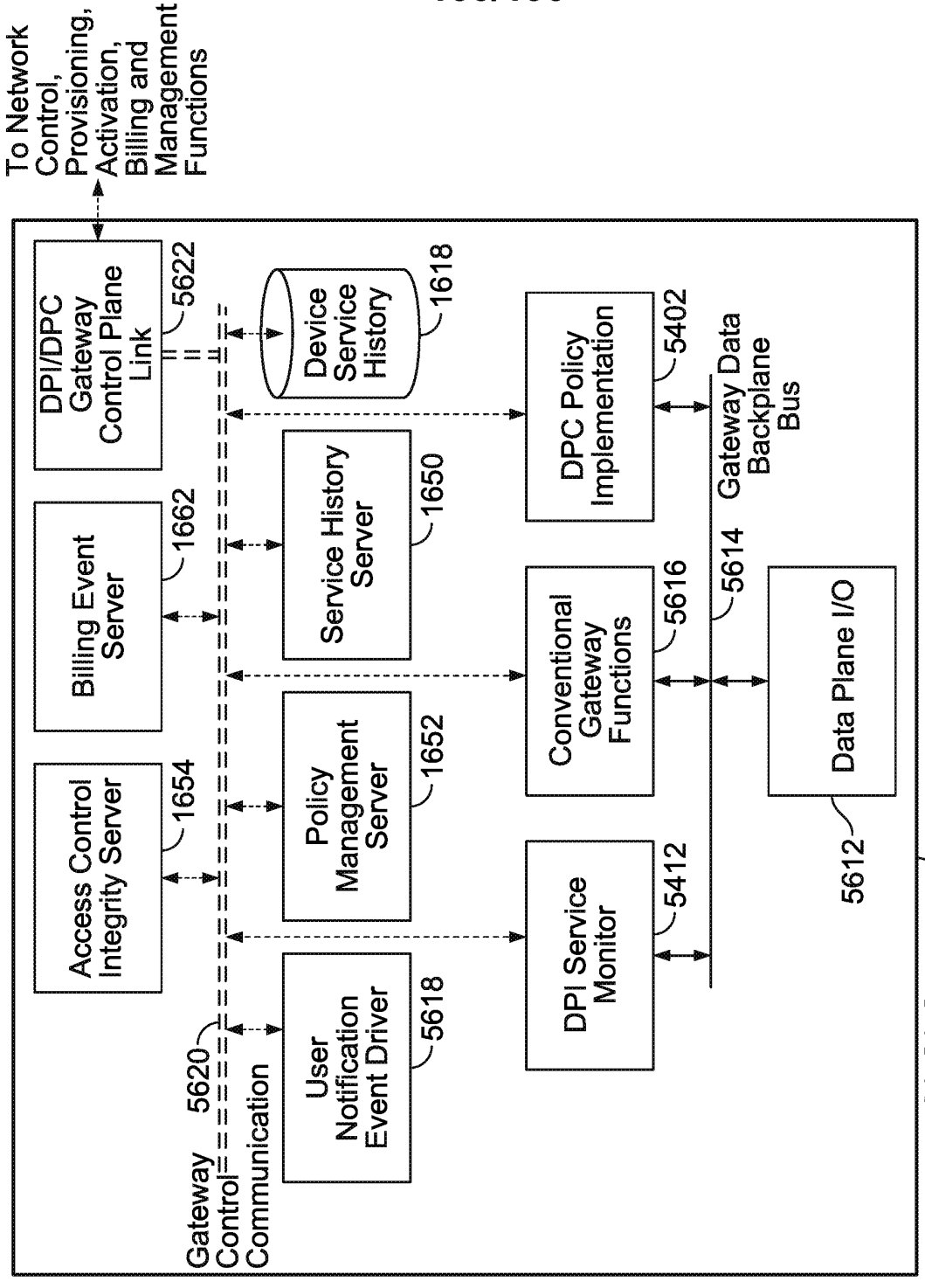

To Network Control, Provisioning, Activation, Billing and Management Functions
DPI/DPC Gateway Control Plane Link
5622
Device Service History
1618
Billing Event Server
1662
Service History Server
1650
DPC Policy Implementation
5402
Gateway Data Backplane Bus
Access Control Integrity Server
1654
Policy 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
Virtual Service Provider Remote Workstation
VPN, Leased Line or Secure Internet Connections
4920
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
125
4G/3G Base Station
4G BS
3G BS
100
Mobile Station
100
125
3G/2G Base Station
3G BS
2G BS
100
Mobile Station
100

FIG. 59

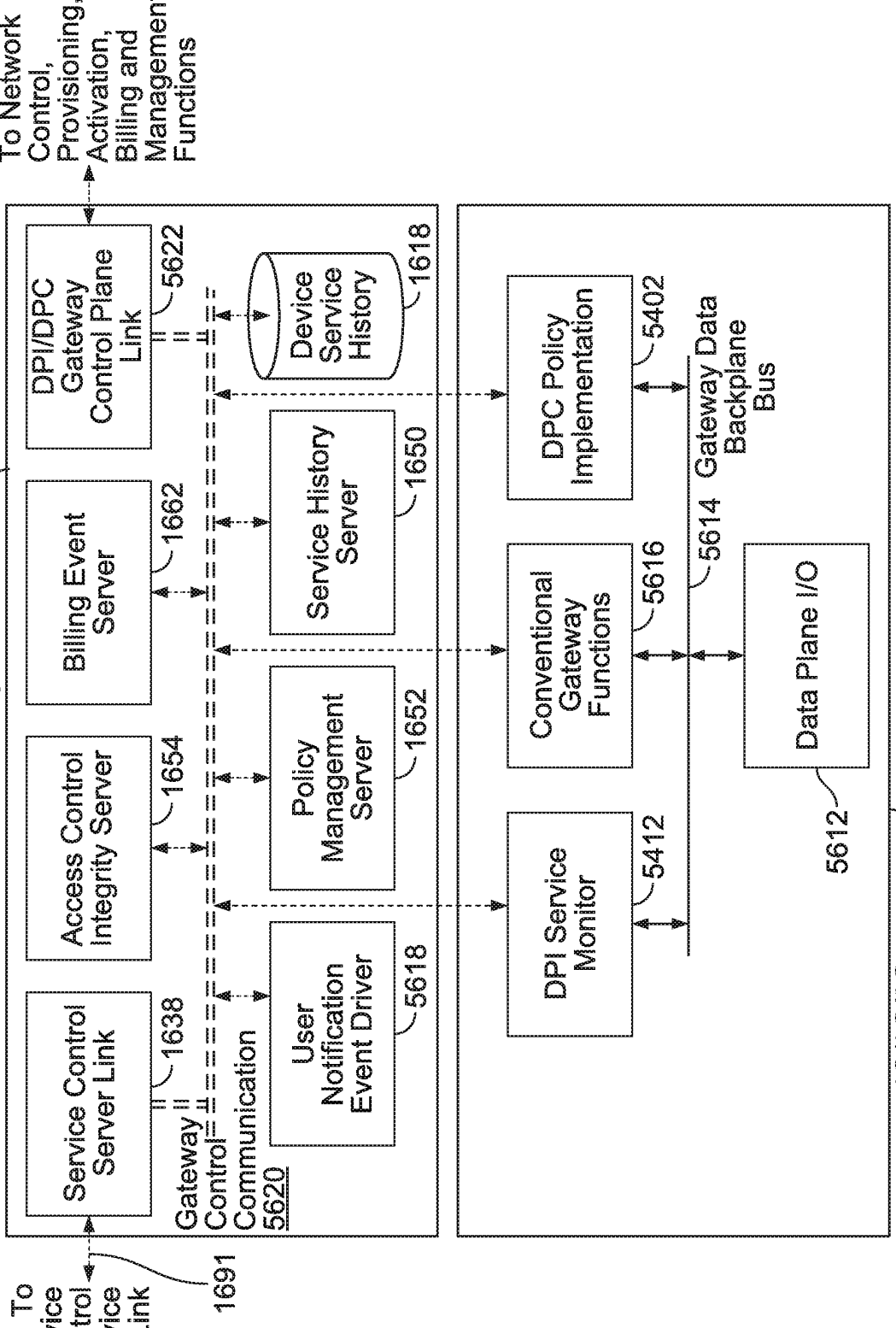

To Network Control, Provisioning, Activation, Billing and Management Functions
Service Controller Device Control System
6025
Service Control Server Link
1638
Access Control Integrity Server
1654
Billing Event Server
1662
DPI/DPC Gateway Control Plane Link
5622
Device Service History
1618
Gateway Control Communication 5620
User Notification Event Driver
5618
Policy Management Server
1652
Service History Server
1650
DPC Policy Implementation
5402
Gateway Data Backplane Bus
5614
Conventional Gateway Functions
5616
DPI Service Monitor
5412
Data Plane I/O
5612
4G/3G/2G DPI/DPC Gateway
6010
To Service Control Device Link
1691

FIG. 60

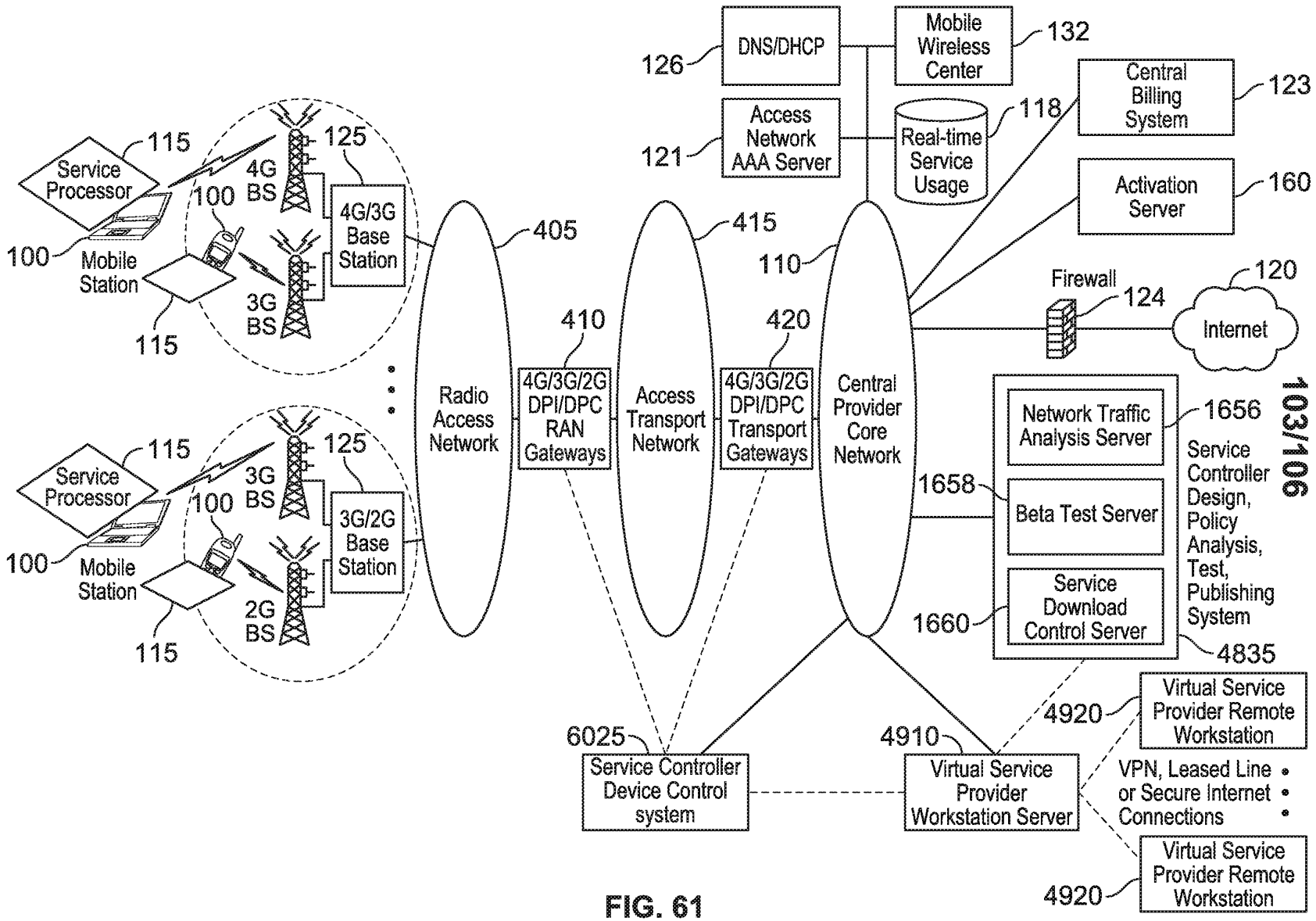

Service Processor
115
100
Mobile Station
4G BS
125
4G/3G Base Station
3G BS
Service Processor
3G BS
3G/2G Base Station
2G BS
Radio Access Network
405
4G/3G/2G DPI/DPC RAN Gateways
410
Access Transport Network
415
4G/3G/2G DPI/DPC Transport Gateways
420
Central Provider Core Network
110
DNS/DHCP
126
Mobile 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

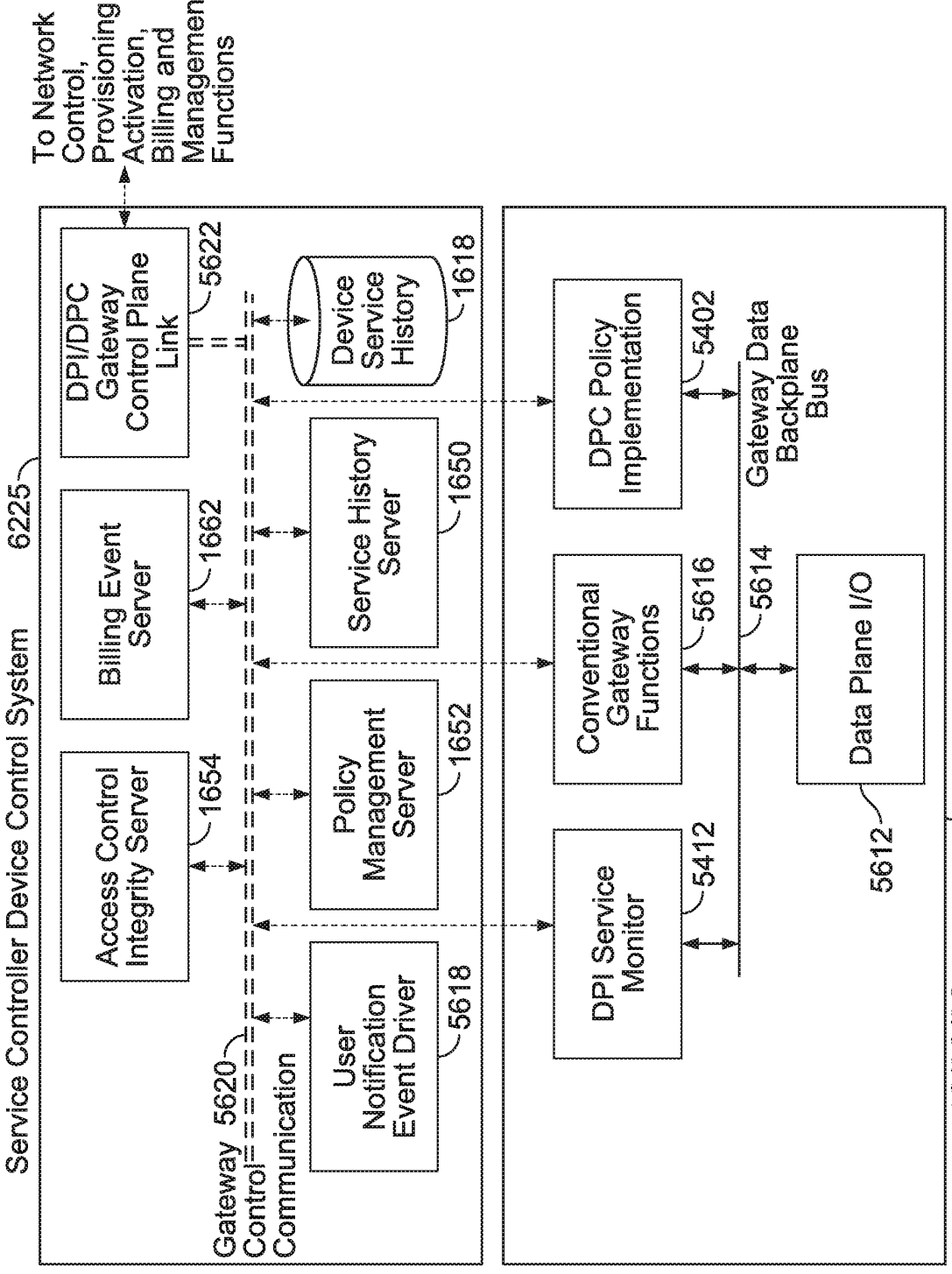

To Network Control, Provisioning, Activation, Billing and Management Functions
Service Controller Device Control System
6225
Access Control Integrity Server
1654
Billing Event Server
1662
DPI/DPC Gateway Control Plane Link
5622
Device Service History
1618
Service History Server
1650
Policy Management Server
1652
User Notification Event Driver
5618
Gateway Control Communication
5620
DPC Policy Implementation
5402
Gateway Data Backplane Bus
Conventional Gateway Functions
5616
5614
DPI Service Monitor
5412
Data Plane I/O
5612
4G/3G/2G DPI/DPC Gateway
6210

FIG. 62

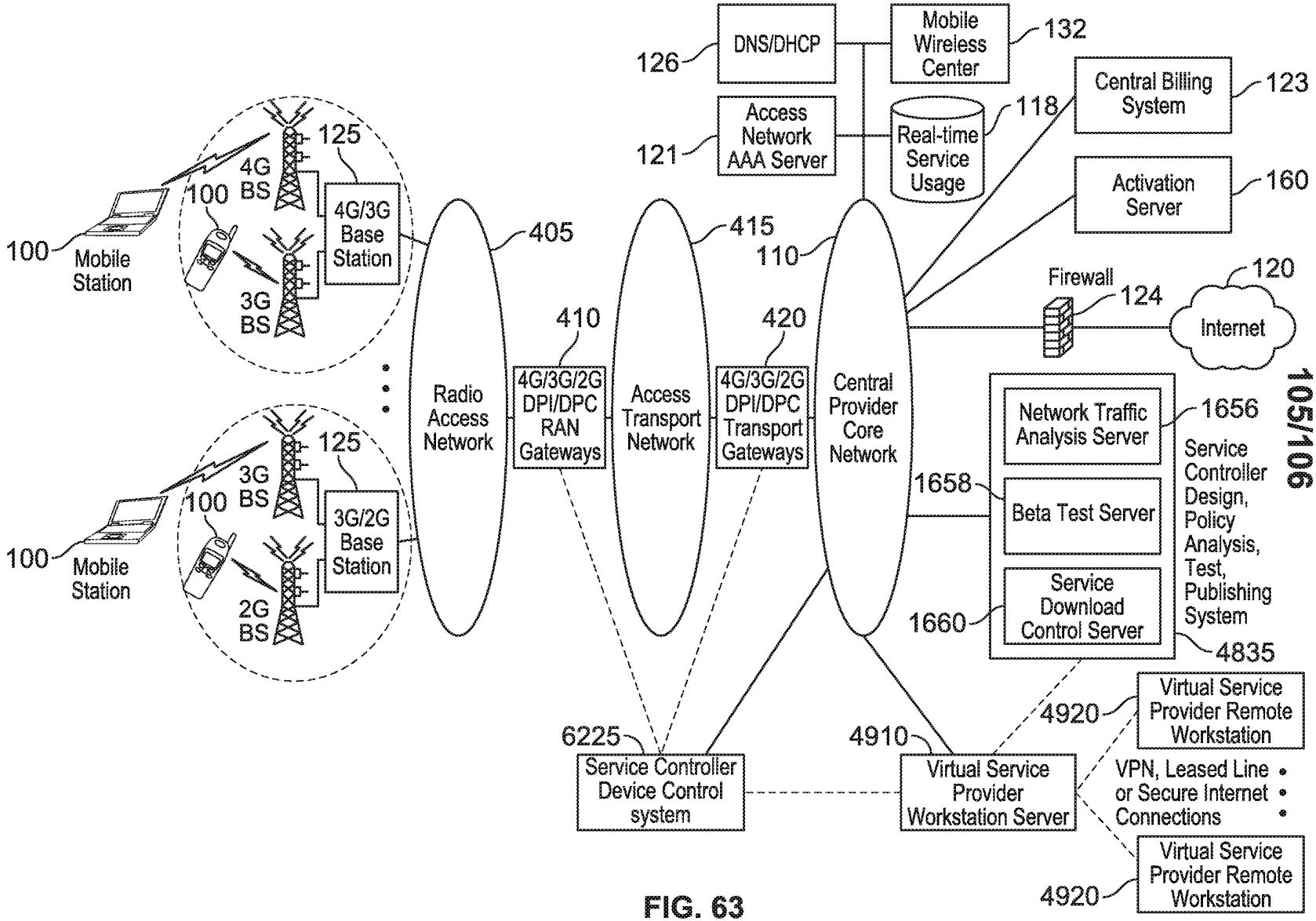

100
Mobile Station
100
Mobile Station
4G BS
3G BS
125
4G/3G Base Station
3G BS
2G BS
125
3G/2G Base Station
Radio Access Network
405
4G/3G/2G DPI/DPC RAN Gateways
410
Access Transport Network
415
4G/3G/2G DPI/DPC Transport Gateways
420
Central Provider Core Network
110
DNS/DHCP
126
Access Network AAA Server
121
Mobile Wireless Center
132
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
105/106
Service Controller Device Control system
6225
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. 63

1081

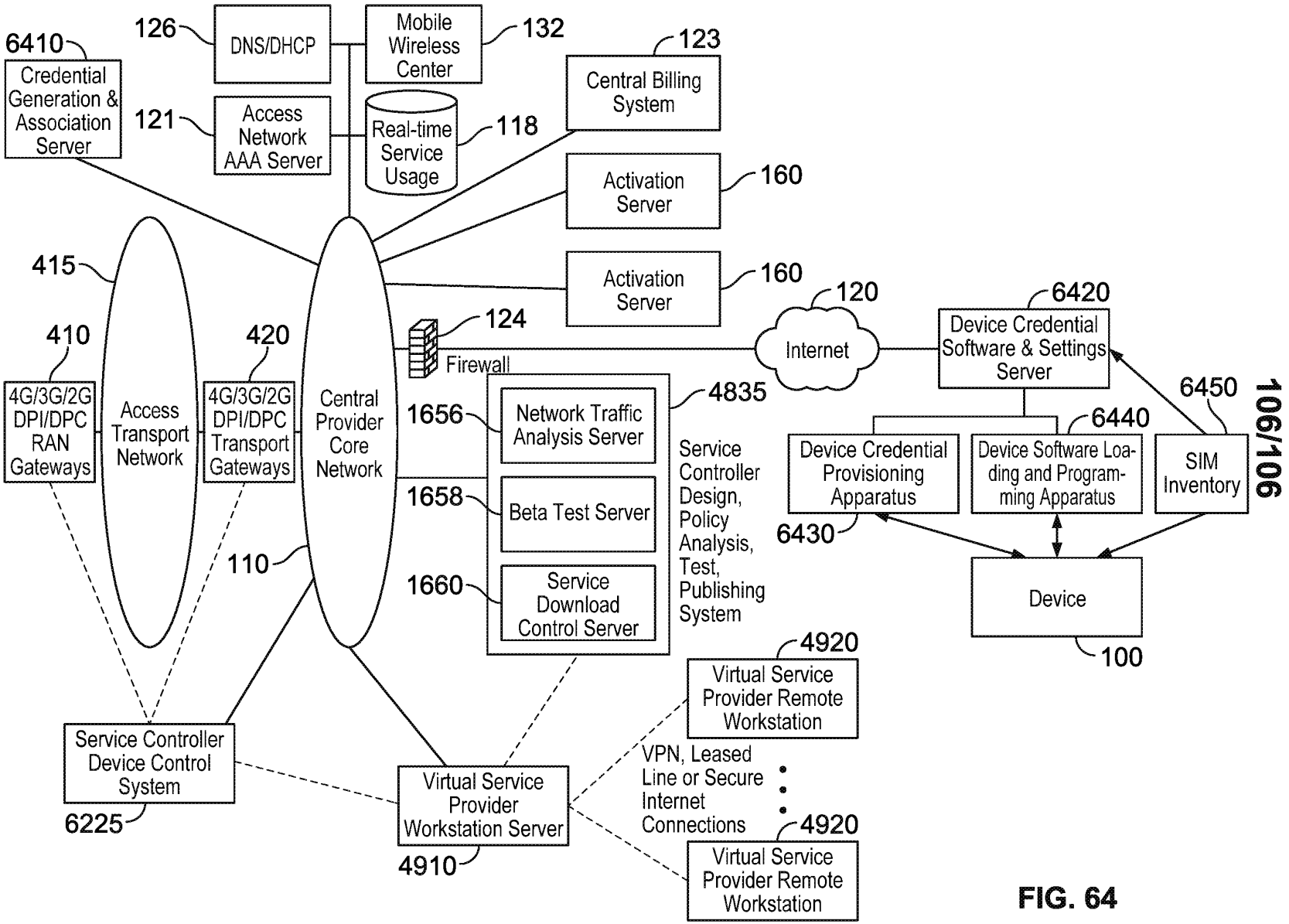

6410
Credential Generation & Association Server
126
DNS/DHCP
Mobile Wireless Center
132
123
Central Billing System
121
Access Network AAA Server
Real-time Service Usage
118
Activation Server
160
415
Activation Server
160
120
6420
410
420
124
Internet
Device Credential Software & Settings Server
Firewall
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
6440
106/106
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

1082