Doc Code: TRACK1.REQ
Document Description: TrackOne Request

PTO/AIA/424 (04-14)

CERTIFICATION AND REQUEST FOR PRIORITIZED EXAMINATION UNDER 37 CFR 1.102(e) (Page 1 of 1)

First Named Inventor:	Raleigh	Nonprovisional Application Number (if known):	RALEP007C11C3C2C2
Title of Invention:	Automated Device Provisioning and Activation		

APPLICANT HEREBY CERTIFIES THE FOLLOWING AND REQUESTS PRIORITIZED EXAMINATION FOR THE ABOVE-IDENTIFIED APPLICATION.

1. The processing fee set forth in 37 CFR 1.17(i)(1) and the prioritized examination fee set forth in 37 CFR 1.17(c) have been filed with the request. The publication fee requirement is met because that fee, set forth in 37 CFR 1.18(d), is currently $0. The basic filing fee, search fee, and examination fee are filed with the request or have been already been paid. I understand that any required excess claims fees or application size fee must be paid for the application.

2. I understand that the application may not contain, or be amended to contain, more than four independent claims, more than thirty total claims, or any multiple dependent claims, and that any request for an extension of time will cause an outstanding Track I request to be dismissed.

3. The applicable box is checked below:

I. ☑ Original Application (Track One) - Prioritized Examination under § 1.102(e)(1)

i. (a) The application is an original nonprovisional utility application filed under 35 U.S.C. 111(a). This certification and request is being filed with the utility application via EFS-Web.

---OR---

(b) The application is an original nonprovisional plant application filed under 35 U.S.C. 111(a). This certification and request is being filed with the plant application in paper.

ii. An executed inventor's oath or declaration under 37 CFR 1.63 or 37 CFR 1.64 for each inventor, **or** the application data sheet meeting the conditions specified in 37 CFR 1.53(f)(3)(i) is filed with the application.

II. ☐ Request for Continued Examination - Prioritized Examination under § 1.102(e)(2)

i. A request for continued examination has been filed with, or prior to, this form.
ii. If the application is a utility application, this certification and request is being filed via EFS-Web.
iii. The application is an original nonprovisional utility application filed under 35 U.S.C. 111(a), or is a national stage entry under 35 U.S.C. 371.
iv. This certification and request is being filed prior to the mailing of a first Office action responsive to the request for continued examination.
v. No prior request for continued examination has been granted prioritized examination status under 37 CFR 1.102(e)(2).

Signature /James E. Harris/	Date 2016-07-22
Name (Print/Typed) James E. Harris	Practitioner Registration Number 40013

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

☐ *Total of _____ forms are submitted.

AMAZON-1002
IPR2026-00361

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/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	RALEP007C11C3C2C2
	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 i	US

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

☐ **An Address is being provided for the correspondence Information of this application.**

Customer Number	106963		
Email Address	patent@headwaterllc.com	Add Email	Remove Email

Application Information:

Title of the Invention	Automated Device Provisioning and Activation		
Attorney Docket Number	RALEP007C11C3C2C2	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	RALEP007C11C3C2C2
	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)
thisapplication	Continuation of	14979233	2015-12-22

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	RALEP007C11C3C2C2
	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)
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	RALEP007C11C3C2C2
	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	RALEP007C11C3C2C2
	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	RALEP007C11C3C2C2
	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 Partners I 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	RALEP007C11C3C2C2
	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)	2016-07-22
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	RALEP007C11C3C2C2
	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.

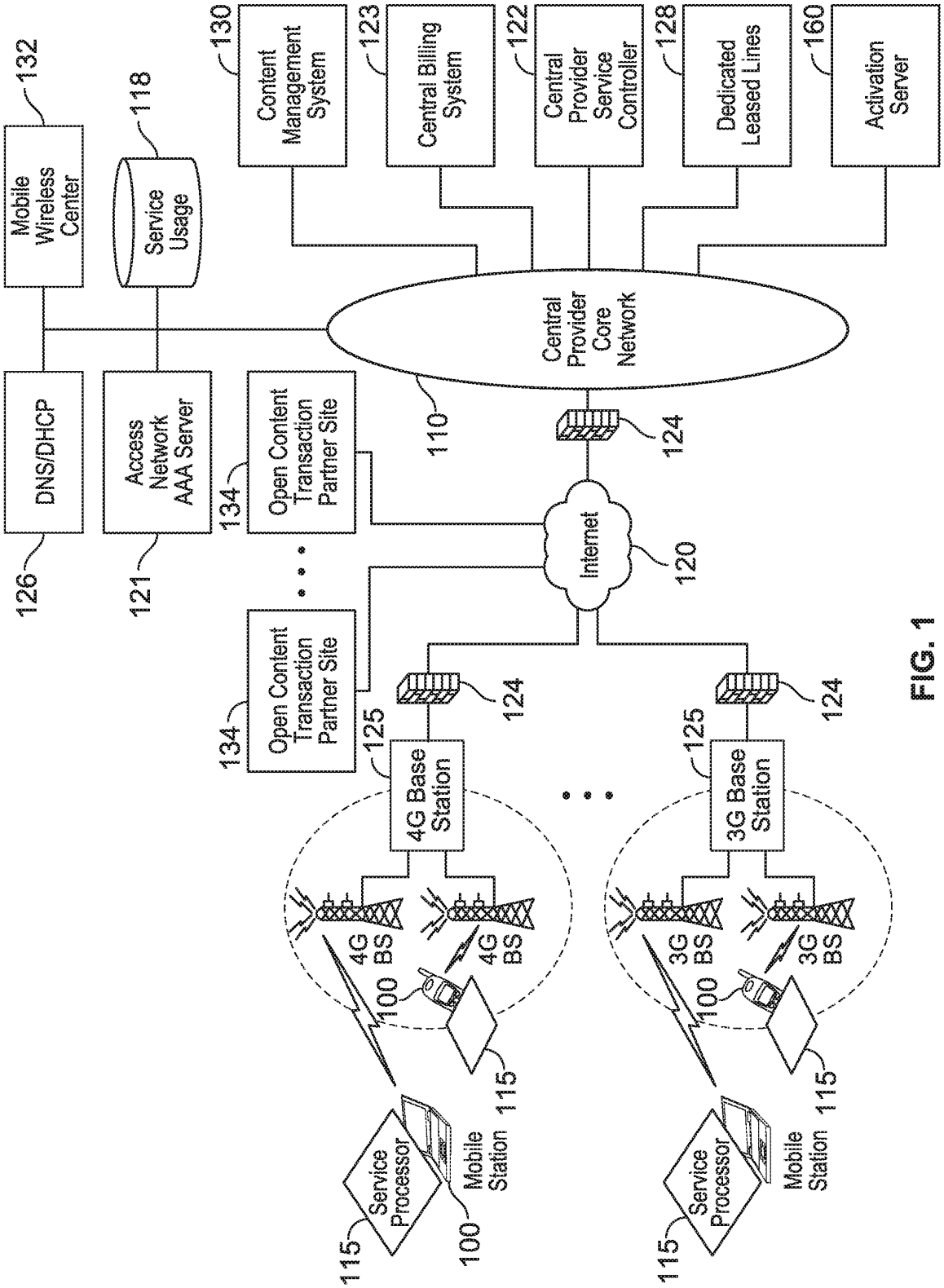

Mobile Wireless Center
132
Service Usage
118
Content Management System
130
Central Billing System
123
Central Provider Service Controller
122
Dedicated Leased Lines
128
Activation Server
160
DNS/DHCP
126
Access Network AAA Server
121
Open Content Transaction Partner Site
134
Central Provider Core Network
110
124
Internet
120
4G Base Station
125
3G Base Station
4G BS
3G BS
100
115
Service Processor
Mobile Station

FIG. 1

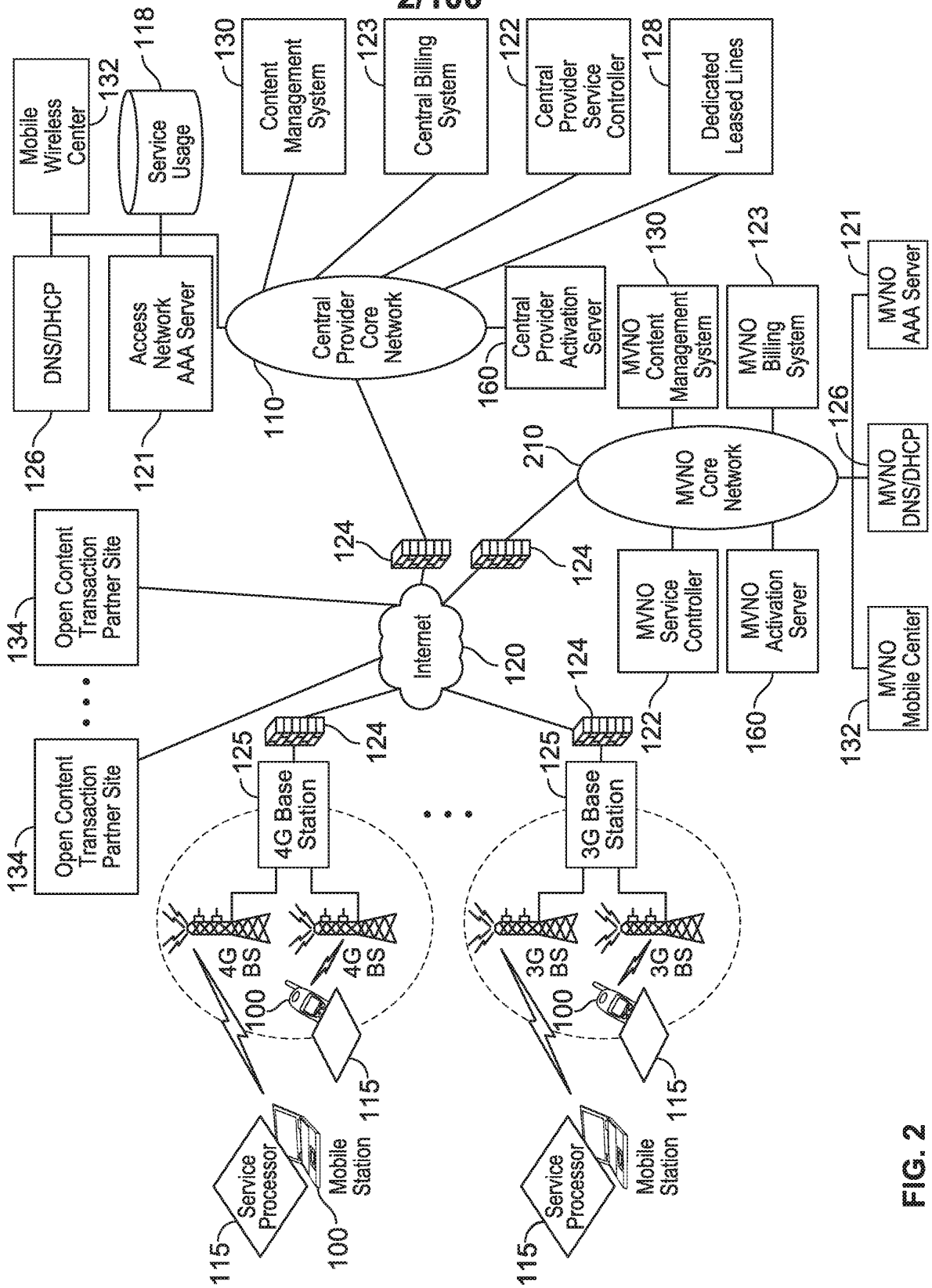

Mobile Wireless Center
132
Service Usage
118
Content Management System
130
Central Billing System
123
Central Provider Service Controller
122
Dedicated Leased Lines
128
DNS/DHCP
126
Access Network AAA Server
121
Central Provider Core Network
110
Central Provider Activation Server
160
MVNO Content Management 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

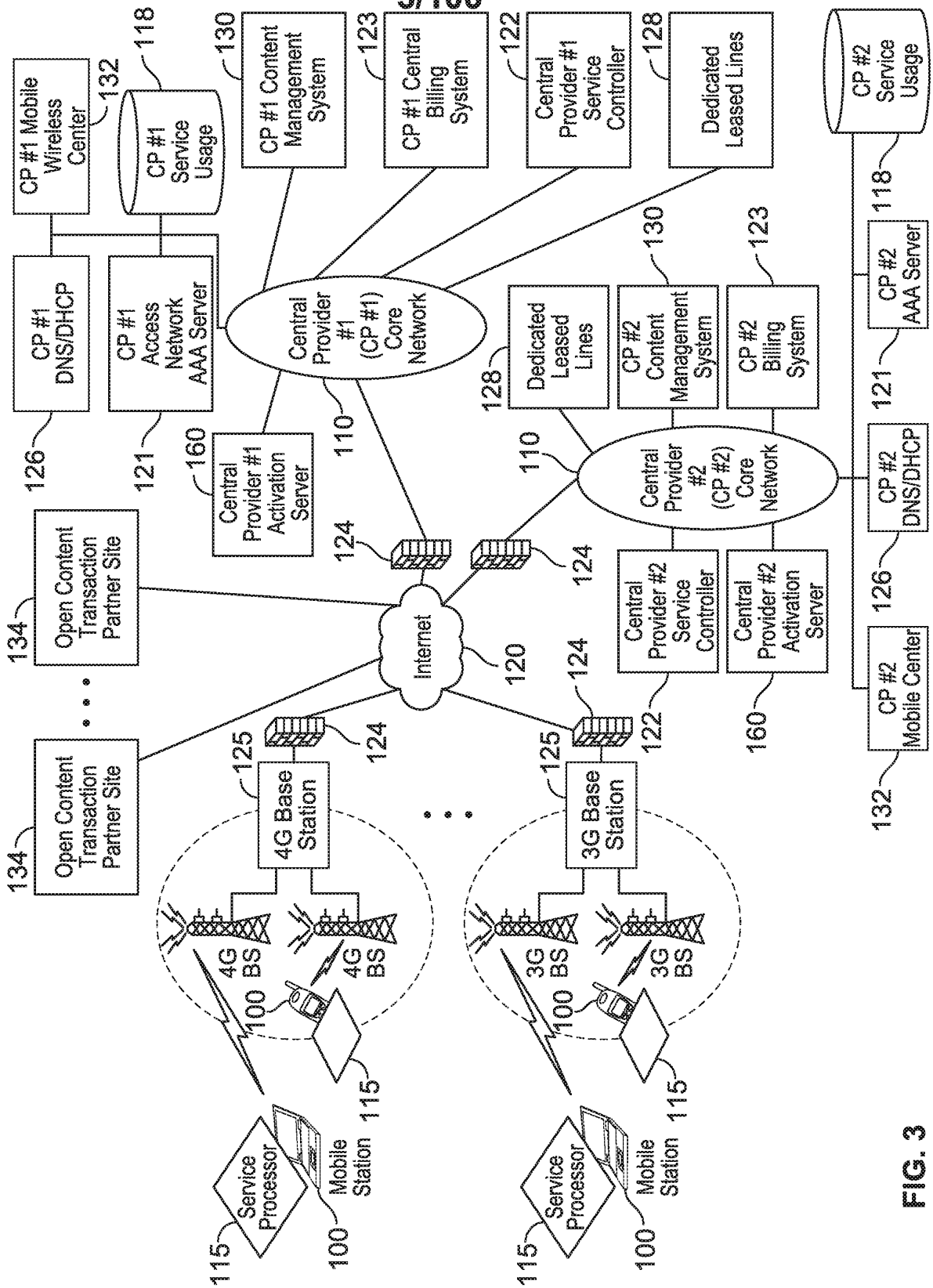

CP #1 Mobile Wireless Center
132
CP #1 Service Usage
118
CP #1 Content Management System
130
CP #1 Central Billing System
123
Central Provider #1 Service Controller
122
Dedicated Leased Lines
128
CP #2 Service Usage
CP #1 DNS/DHCP
126
CP #1 Access Network AAA Server
121
Central Provider #1 (CP #1) Core Network
110
Central Provider #1 Activation Server
160
Dedicated Leased Lines
128
CP #2 Content Management System
130
CP #2 Billing System
123
CP #2 AAA Server
121
118
Central Provider #2 (CP #2) Core Network
110
CP #2 DNS/DHCP
126
Open Content Transaction Partner Site
134
Internet
120
124
Central Provider #2 Service Controller
122
Central Provider #2 Activation Server
160
CP #2 Mobile Center
132
4G Base Station
125
3G Base Station
125
4G BS
3G BS
100
115
Service Processor
Mobile Station

FIG. 3

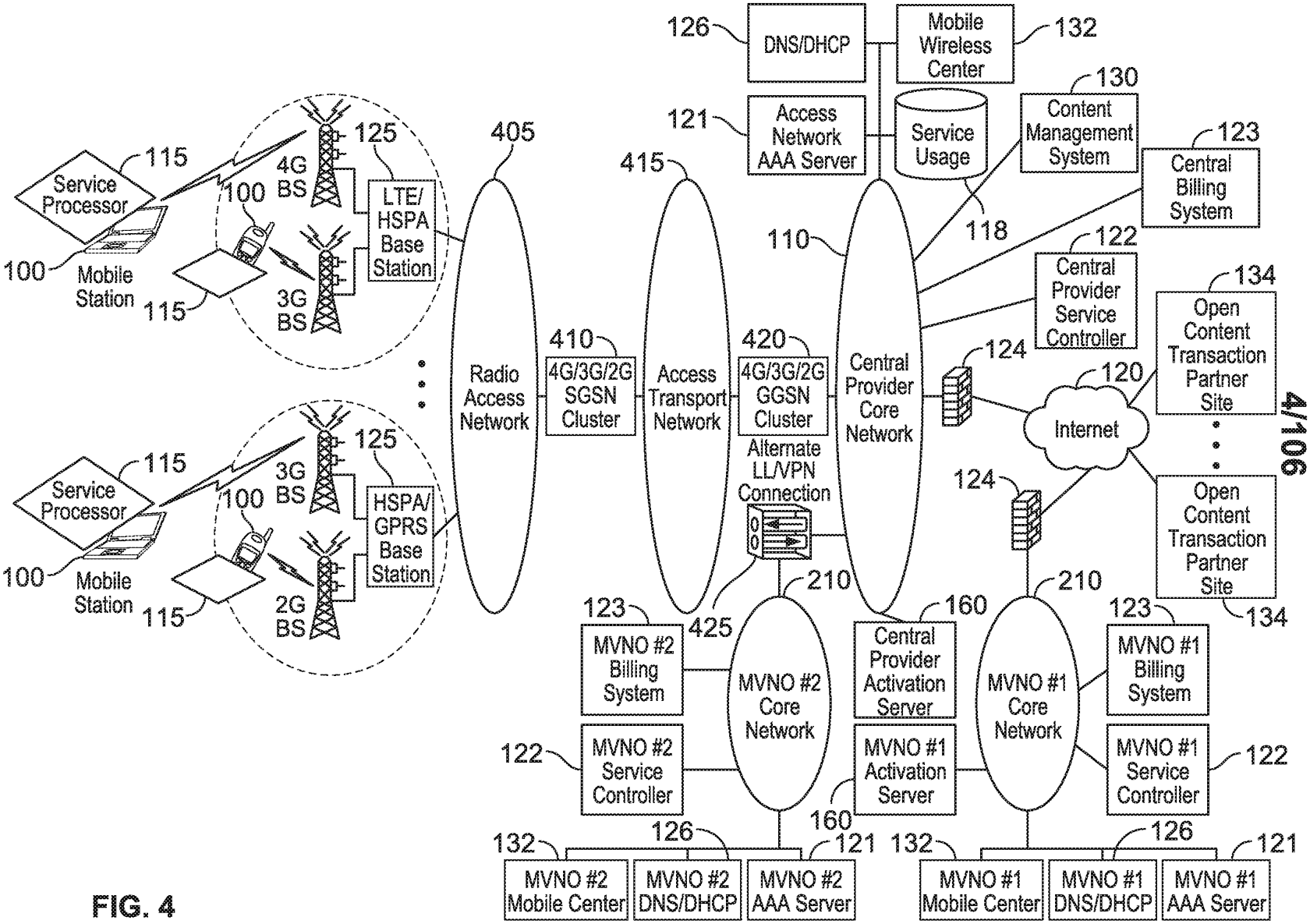

126
DNS/DHCP
Mobile Wireless Center
132
130
Content Management System
121
Access Network AAA Server
Service Usage
123
Central Billing System
118
405
415
110
122
Central Provider Service Controller
134
Open Content Transaction Partner Site
115
Service Processor
100
Mobile Station
4G BS
125
LTE/ HSPA Base Station
3G BS
Radio Access Network
410
4G/3G/2G SGSN Cluster
Access Transport Network
420
4G/3G/2G GGSN Cluster
Central Provider Core Network
124
120
Internet
3G BS
HSPA/ GPRS Base Station
2G BS
Alternate LL/VPN Connection
425
210
160
MVNO #2 Billing System
MVNO #2 Core Network
Central Provider Activation Server
MVNO #1 Core Network
MVNO #1 Billing System
MVNO #2 Service Controller
MVNO #1 Activation Server
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

FIG. 4

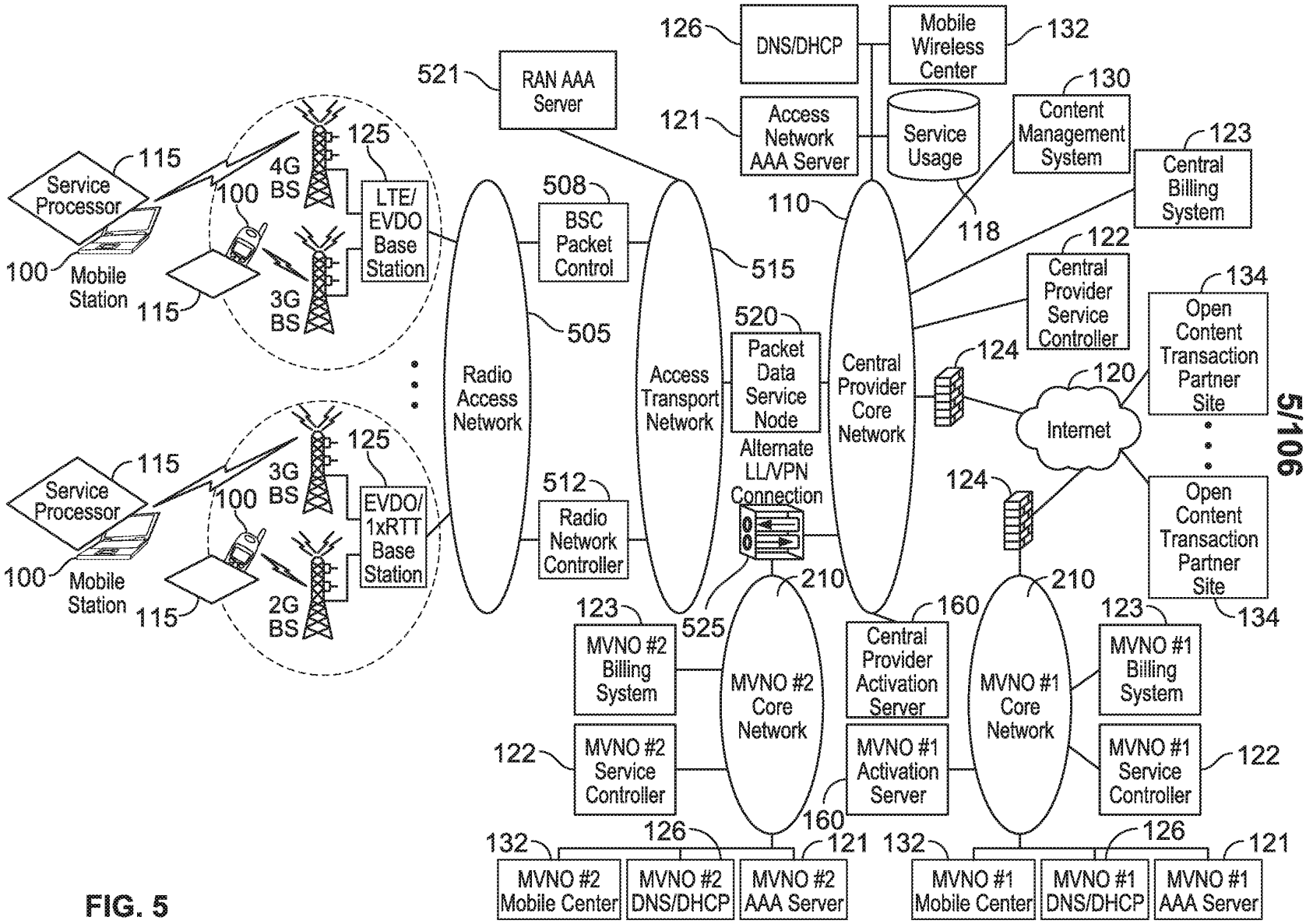

126
DNS/DHCP
Mobile Wireless Center
132
521
RAN AAA Server
121
Access Network AAA Server
Service Usage
130
Content Management System
123
Central Billing System
118
110
122
Central Provider Service Controller
134
Open Content Transaction Partner Site
508
BSC Packet Control
515
520
Packet Data Service Node
Alternate LL/VPN Connection
124
120
Internet
Central Provider Core Network
Access Transport Network
Radio Access Network
505
125
LTE/ EVDO Base Station
4G BS
3G BS
100
Service Processor
Mobile Station
115
512
Radio Network Controller
EVDO/ 1xRTT Base Station
2G BS
525
210
160
MVNO #2 Billing System
MVNO #2 Core Network
Central Provider Activation Server
MVNO #1 Core Network
MVNO #1 Billing System
MVNO #2 Service Controller
MVNO #1 Activation Server
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

FIG. 5

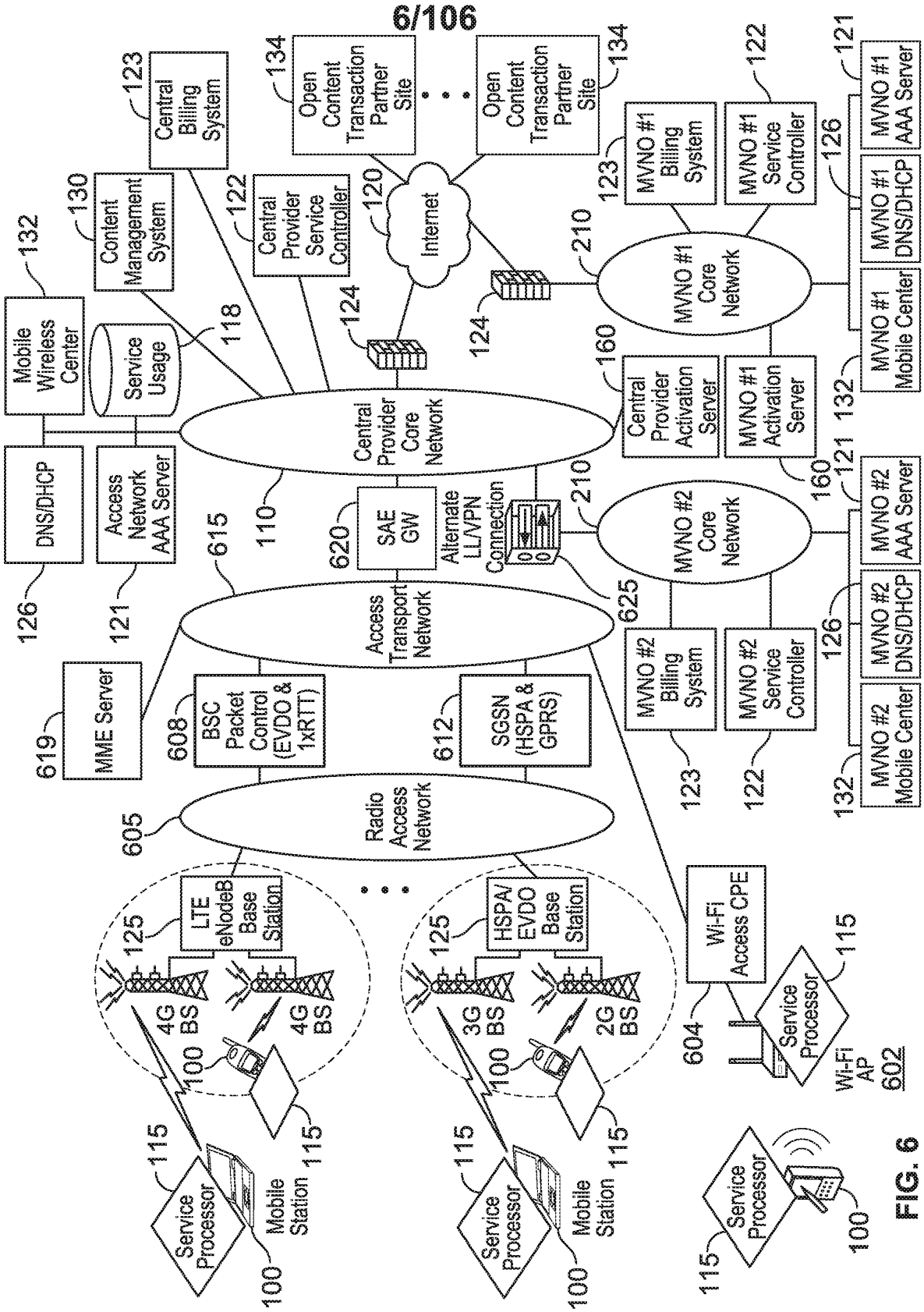

Mobile Wireless Center
132
DNS/DHCP
126
Access Network AAA Server
121
Service Usage
118
Content Management System
130
Central Billing System
123
Central Provider Service Controller
122
Open Content Transaction Partner Site
134
Internet
120
Central Provider Core Network
110
MME Server
619
BSC Packet Control (EVDO & 1xRTT)
608
SGSN (HSPA & GPRS)
612
Radio Access Network
605
Access Transport Network
615
SAE GW
620
Alternate LL/VPN Connection
625
Central Provider Activation Server
160
MVNO #1 Billing System
123
MVNO #1 Service Controller
122
MVNO #1 Core Network
210
MVNO #1 Mobile Center
132
MVNO #1 DNS/DHCP
126
MVNO #1 AAA Server
121
MVNO #1 Activation Server
160
MVNO #2 Billing System
123
MVNO #2 Service Controller
122
MVNO #2 Core Network
210
MVNO #2 Mobile Center
132
MVNO #2 DNS/DHCP
126
MVNO #2 AAA Server
121
LTE eNodeB Base Station
125
HSPA/ EVDO Base Station
125
4G BS
3G BS
2G BS
Wi-Fi Access CPE
604
Service Processor
115
Wi-Fi AP
602
Mobile Station
100

FIG. 6

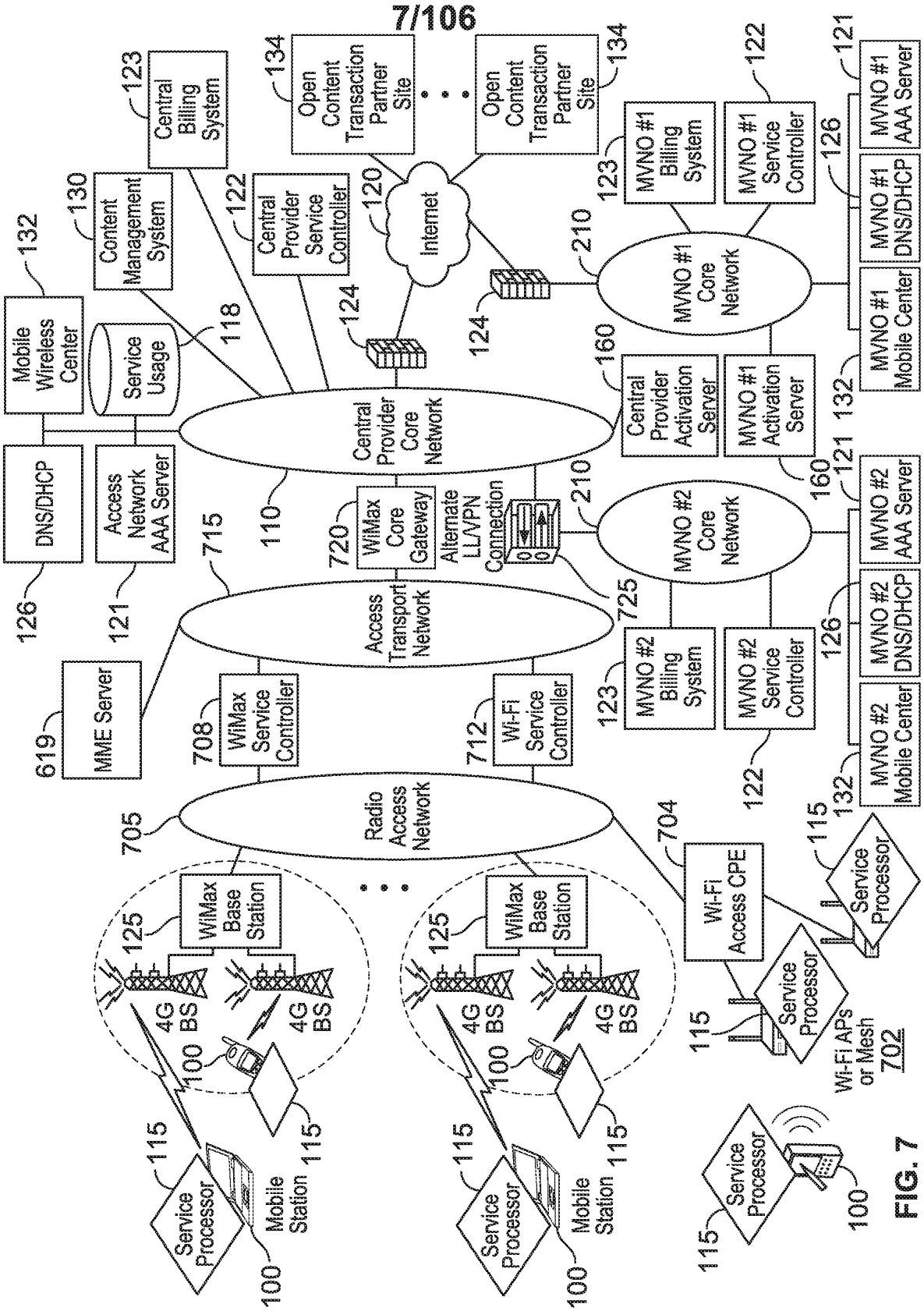

Mobile Station
Service Processor
WiMax Base Station
4G BS
Radio Access Network
Access Transport Network
Central Provider Core Network
MVNO #1 Core Network
MVNO #2 Core Network
Internet
Wi-Fi Access CPE
Wi-Fi APs or Mesh
MME Server
WiMax Service Controller
Wi-Fi Service Controller
WiMax Core Gateway
Alternate LL/VPN Connection
Access Network AAA Server
DNS/DHCP
Mobile Wireless Center
Service Usage
Content Management System
Central Billing System
Central Provider Service Controller
Open Content Transaction Partner Site
Central Provider Activation Server
MVNO #1 Activation Server
MVNO #2 Activation Server
MVNO #1 Billing System
MVNO #2 Billing System
MVNO #1 Service Controller
MVNO #2 Service Controller
MVNO #1 Mobile Center
MVNO #2 Mobile Center
MVNO #1 DNS/DHCP
MVNO #2 DNS/DHCP
MVNO #1 AAA Server
MVNO #2 AAA Server
100
110
115
118
120
121
122
123
124
125
126
130
132
134
160
210
619
702
704
705
708
712
715
720
725

FIG. 7

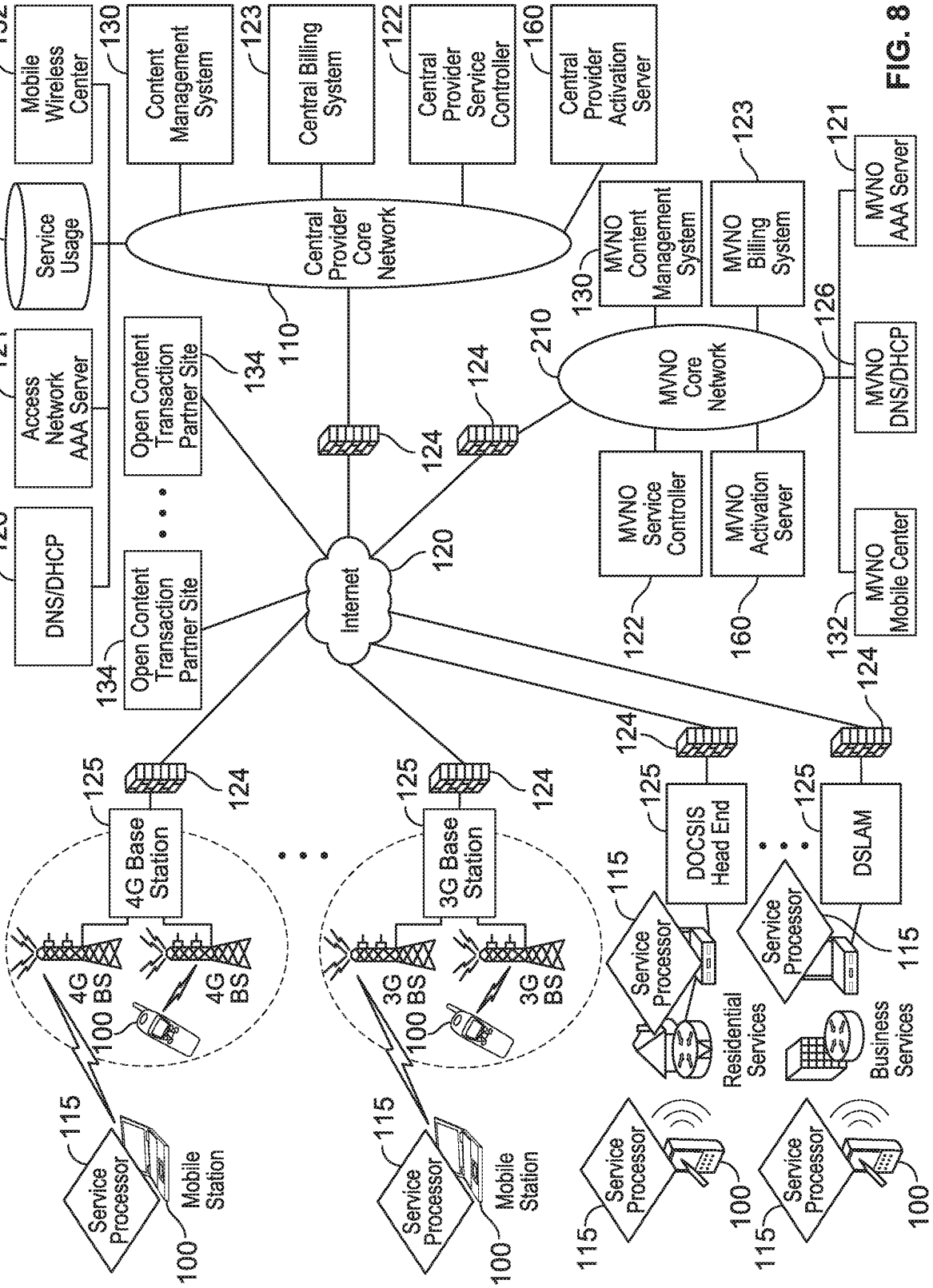

Mobile Wireless Center
132
Content Management System
130
Central Billing System
123
Central Provider Service Controller
122
Central Provider Activation Server
160
Service Usage
118
Central Provider Core Network
110
Access Network AAA Server
121
Open Content Transaction Partner Site
134
DNS/DHCP
126
Internet
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
4G Base Station
3G Base Station
DOCSIS Head End
DSLAM
125
124
4G BS
3G BS
100 BS
Service Processor
115
Mobile Station
100
Residential Services
Business Services

FIG. 8

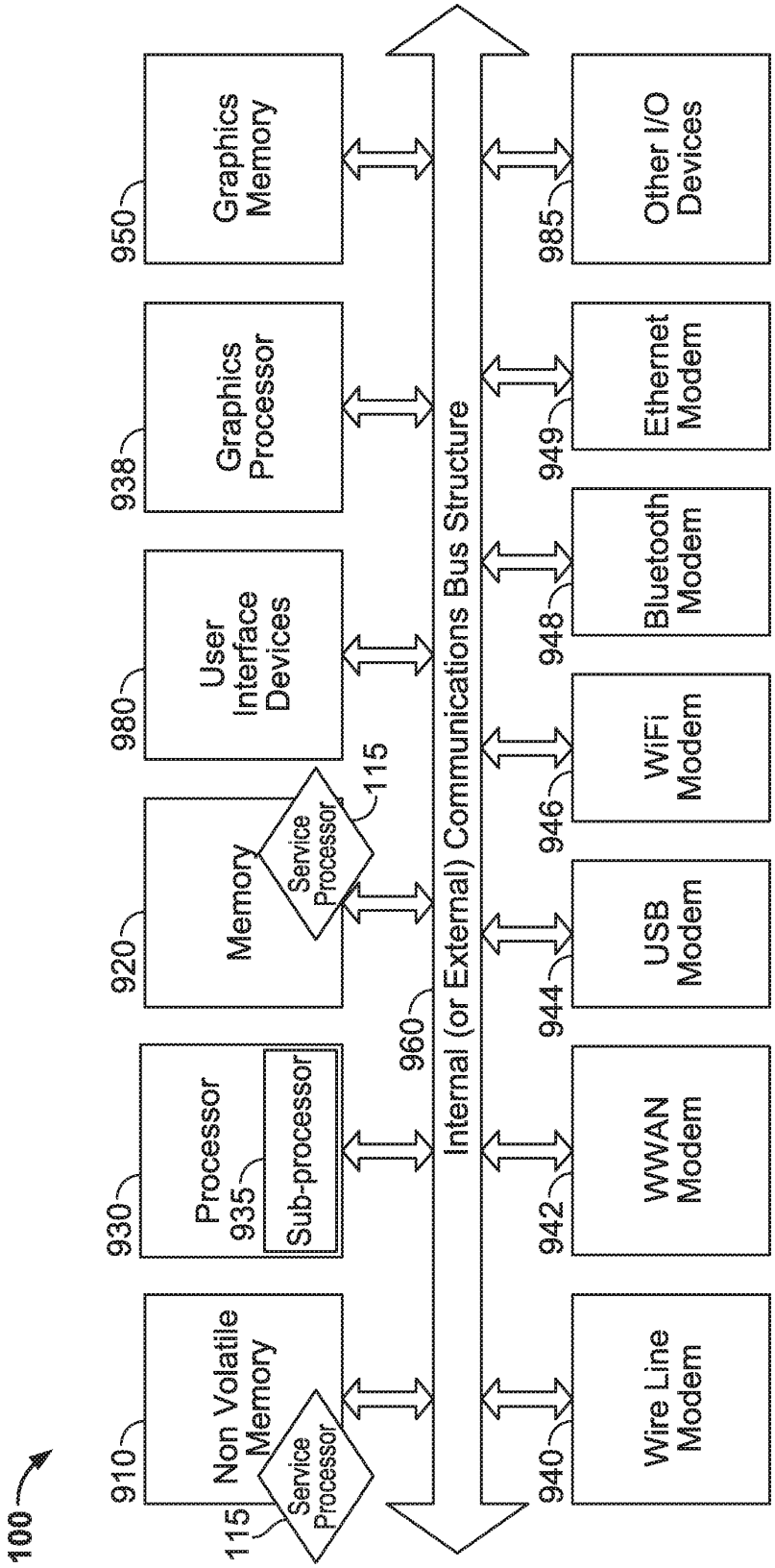

100
910
Non Volatile Memory
115
Service Processor
930
Processor
935
Sub-processor
920
Memory
Service Processor
115
980
User Interface Devices
938
Graphics Processor
950
Graphics Memory
960
Internal (or External) Communications Bus Structure
940
Wire Line Modem
942
WWAN Modem
944
USB Modem
946
WiFi Modem
948
Bluetooth Modem
949
Ethernet Modem
985
Other I/O Devices

FIG. 9

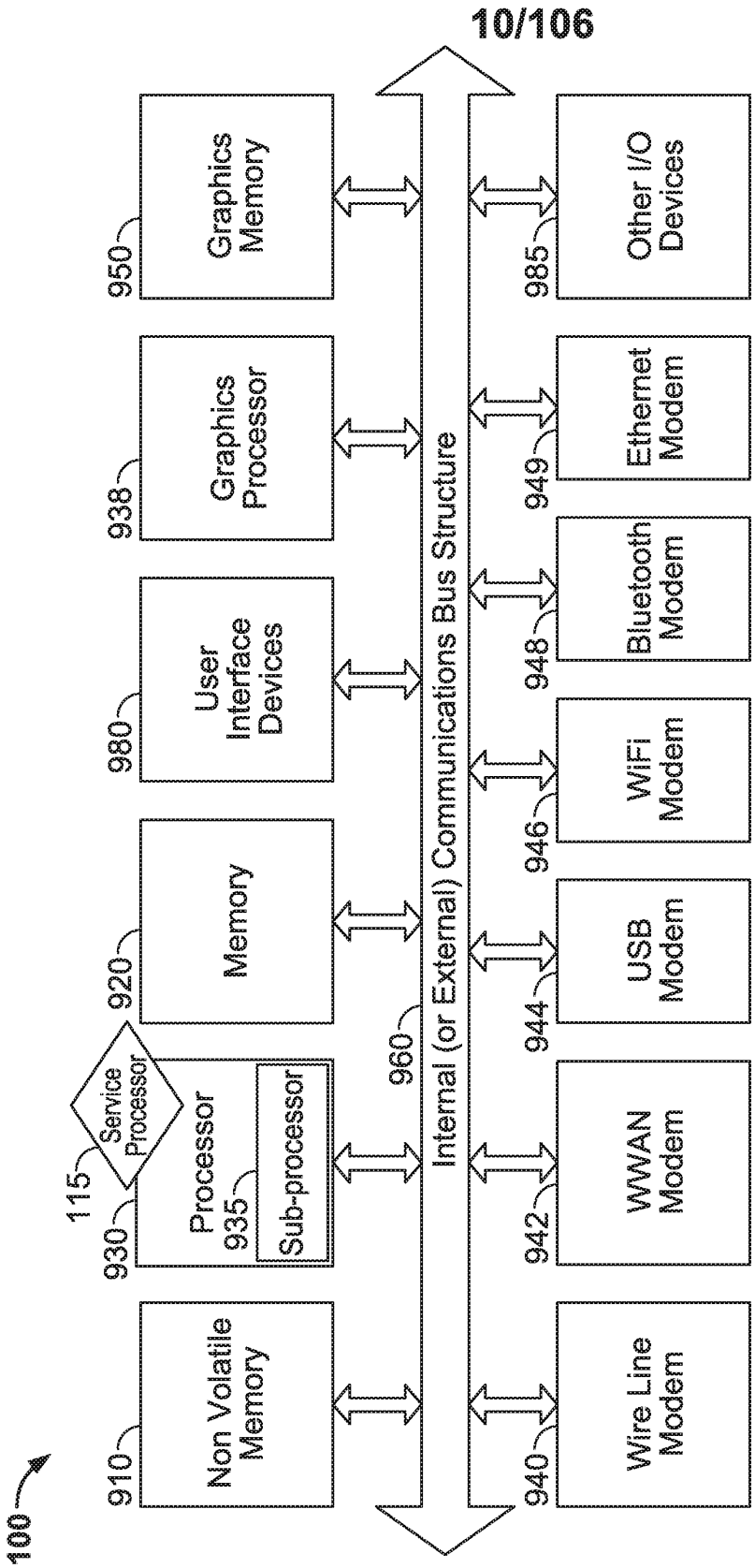

100
910
Non Volatile Memory
930
Processor
935
Sub-processor
115
Service Processor
920
Memory
980
User Interface Devices
938
Graphics Processor
950
Graphics Memory
960
Internal (or External) Communications Bus Structure
940
Wire Line Modem
942
WWAN Modem
944
USB Modem
946
WiFi Modem
948
Bluetooth Modem
949
Ethernet Modem
985
Other I/O Devices

FIG. 10

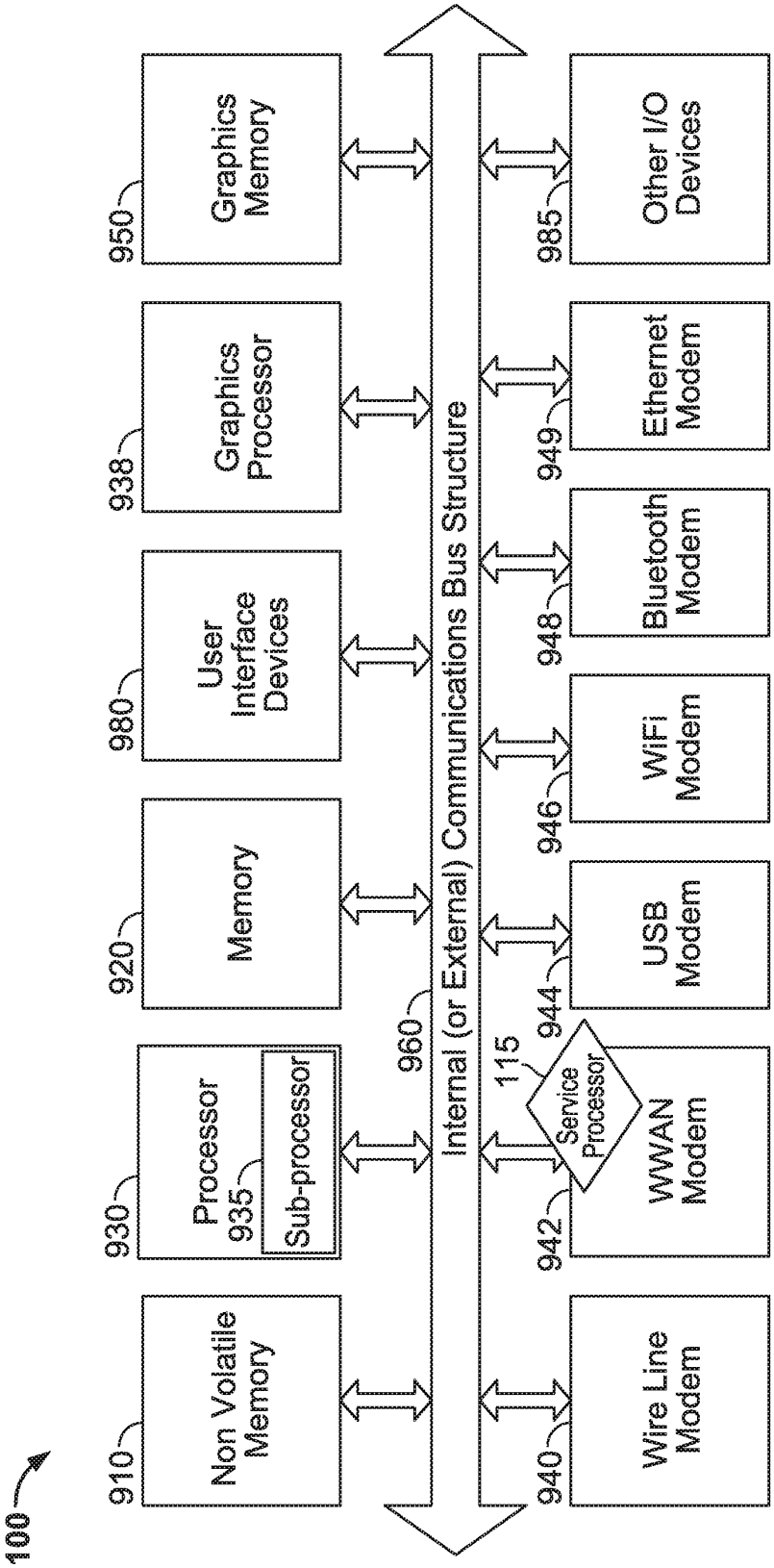

100
910
Non Volatile Memory
930
Processor
935
Sub-processor
920
Memory
980
User Interface Devices
938
Graphics Processor
950
Graphics Memory
960
Internal (or External) Communications Bus Structure
940
Wire Line Modem
942
WWAN Modem
115
Service Processor
944
USB Modem
946
WiFi Modem
948
Bluetooth Modem
949
Ethernet Modem
985
Other I/O Devices

FIG. 11

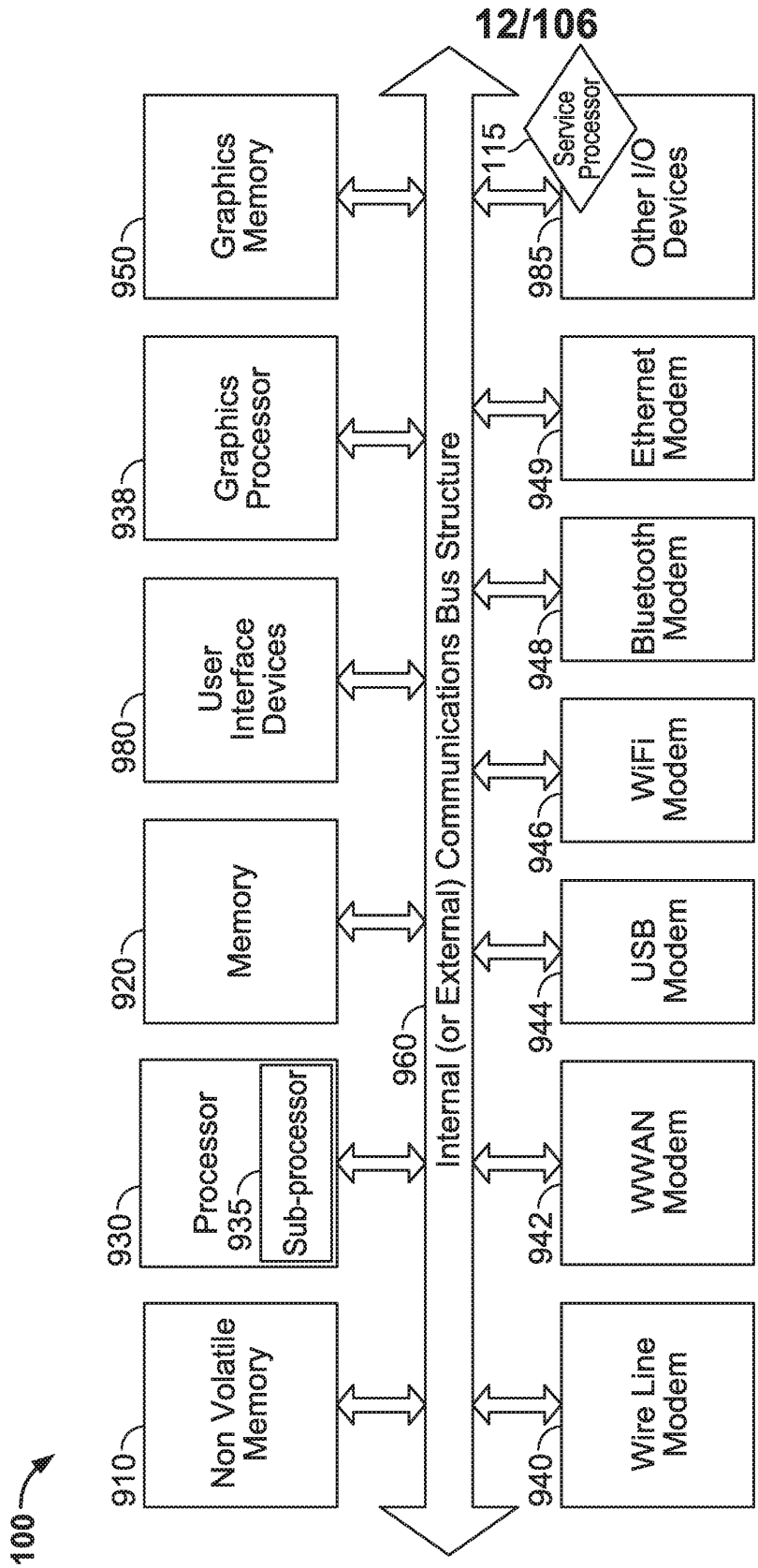

100
910
Non Volatile Memory
930
Processor
935
Sub-processor
920
Memory
980
User Interface Devices
938
Graphics Processor
950
Graphics Memory
940
Wire Line Modem
942
WWAN Modem
944
USB Modem
946
WiFi Modem
948
Bluetooth Modem
949
Ethernet Modem
985
Other I/O Devices
115
Service Processor
960
Internal (or External) Communications Bus Structure

FIG. 12

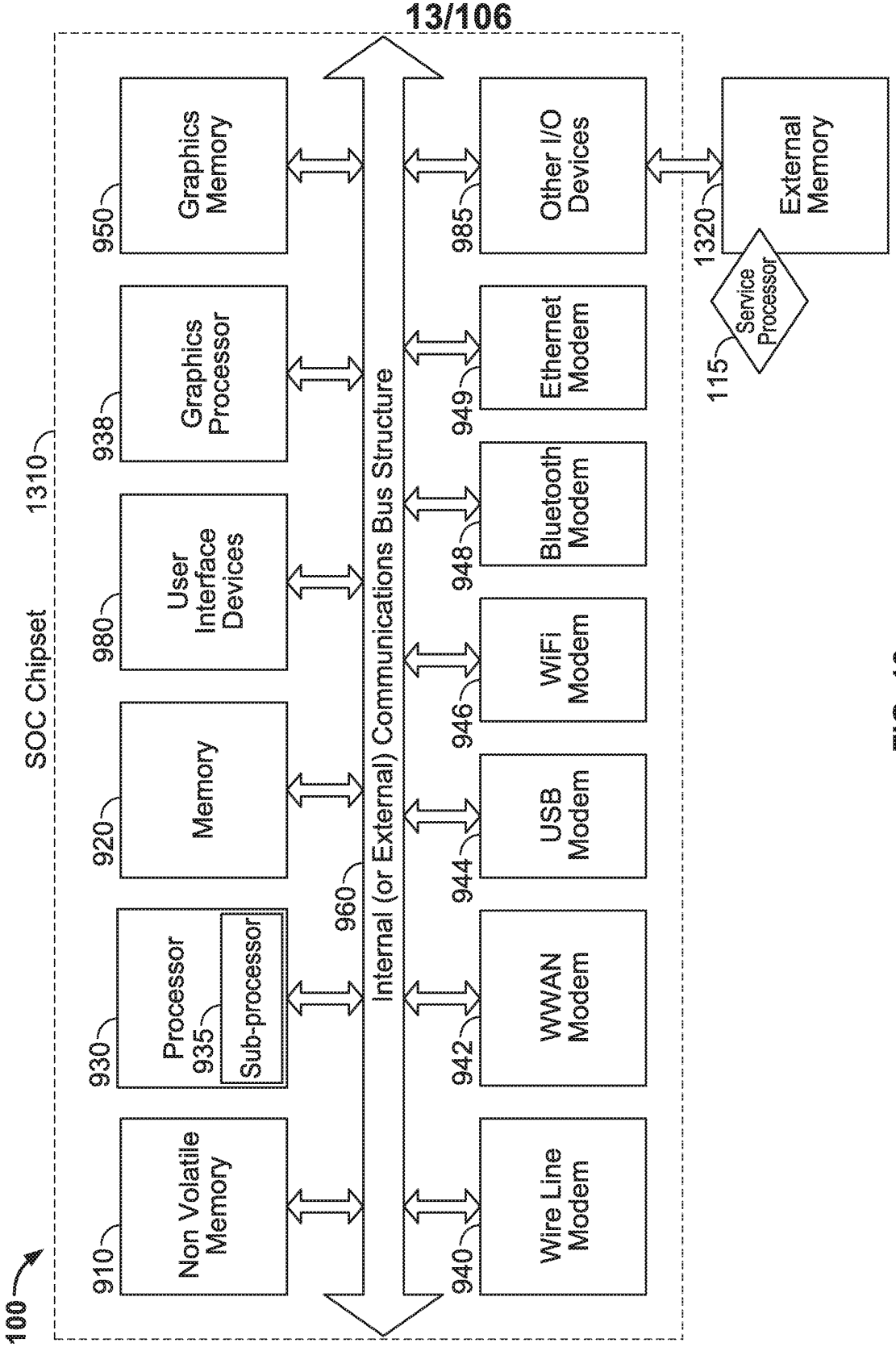

100
SOC Chipset
1310
910
Non Volatile Memory
930
Processor
935
Sub-processor
920
Memory
980
User Interface Devices
938
Graphics Processor
950
Graphics Memory
960
Internal (or External) Communications Bus Structure
940
Wire Line Modem
942
WWAN Modem
944
USB Modem
946
WiFi Modem
948
Bluetooth Modem
949
Ethernet Modem
985
Other I/O Devices
1320
External Memory
115
Service Processor

FIG. 13

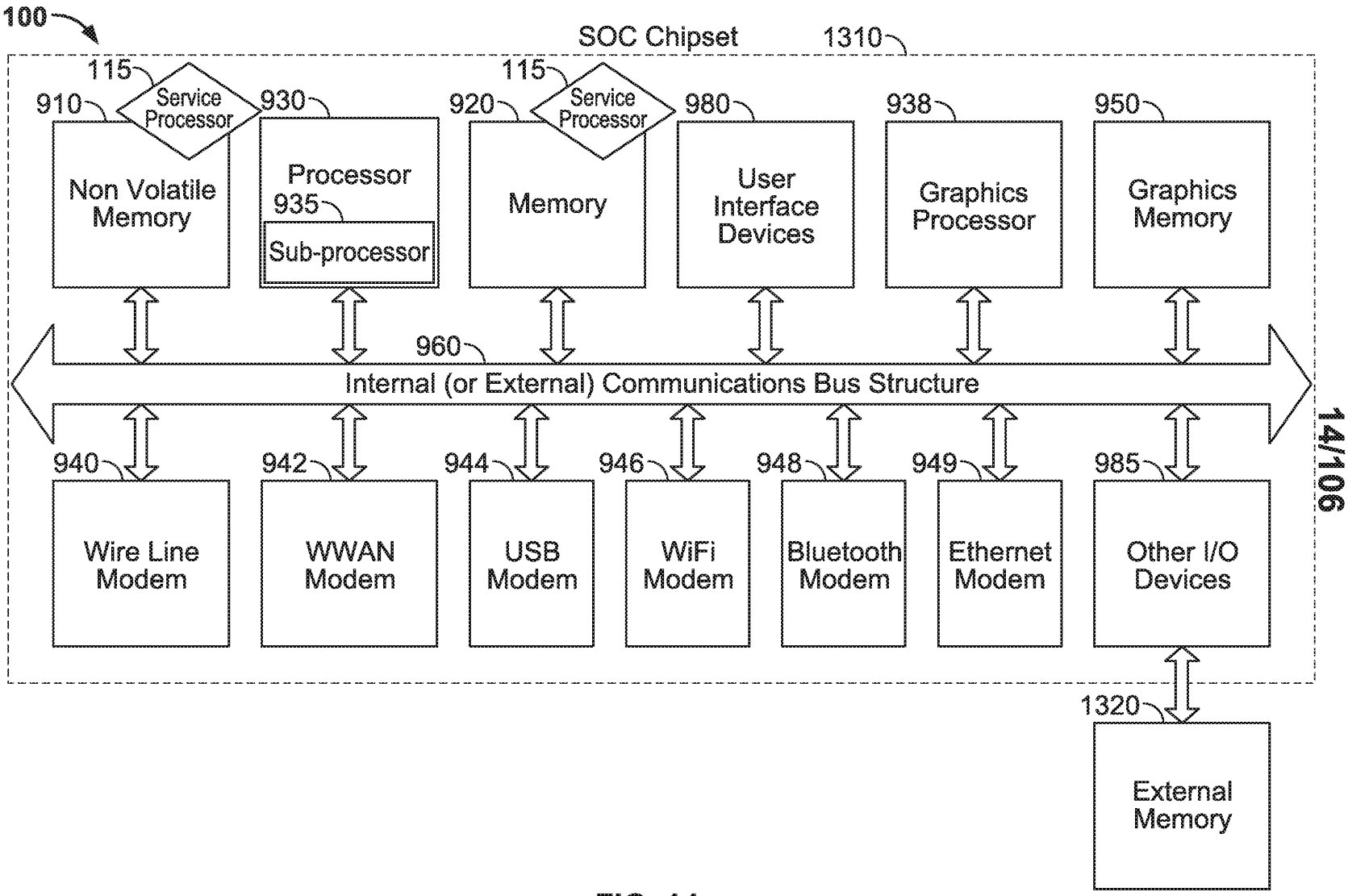


FIG. 14

EX1002 - Page 25

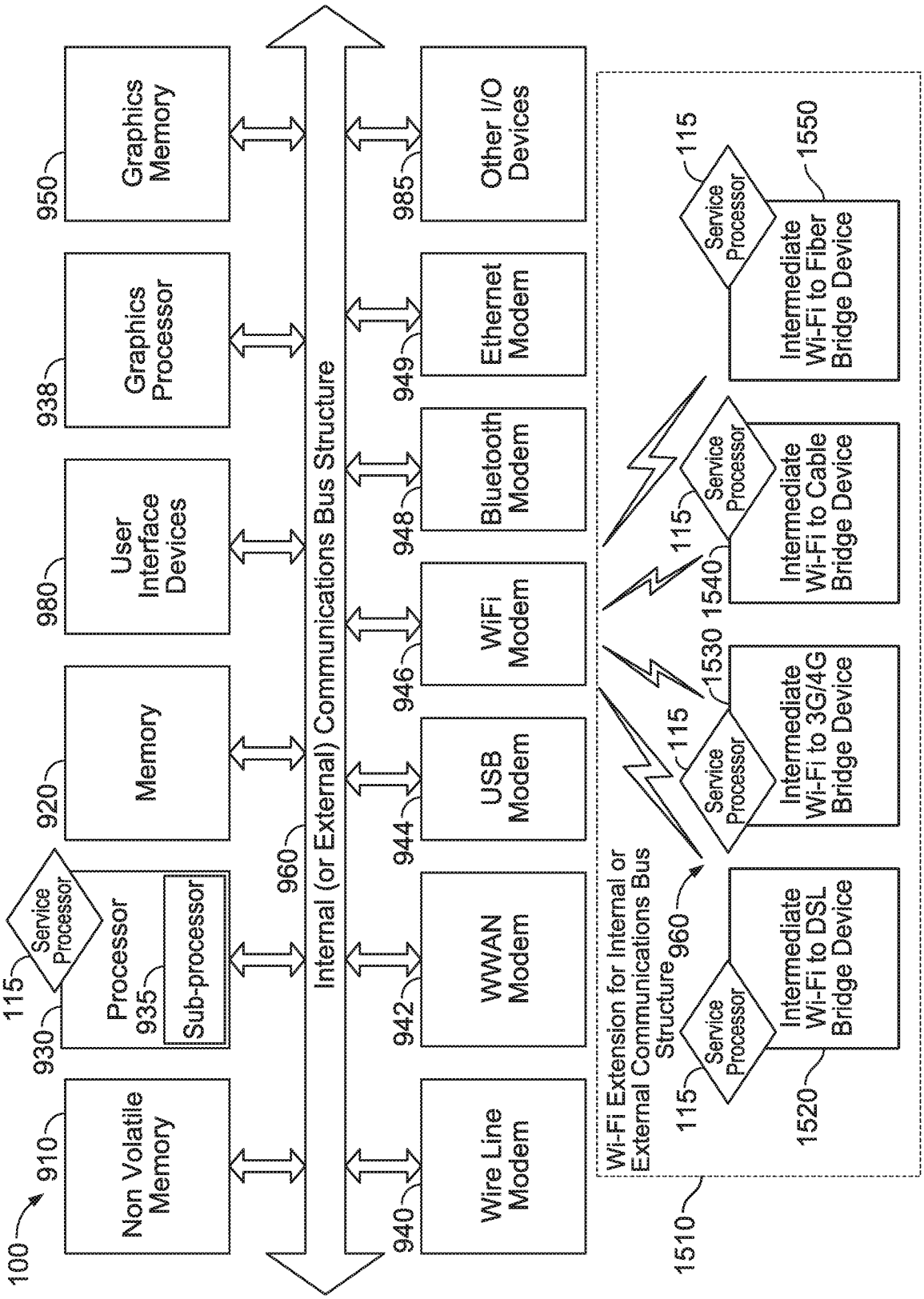

100
Non Volatile Memory
910
Processor
935
Sub-processor
930
Service Processor
115
Memory
920
Graphics Processor
938
Graphics Memory
950
User Interface Devices
980
Internal (or External) Communications Bus Structure
960
Wire Line Modem
940
WWAN Modem
942
USB Modem
944
WiFi Modem
946
Bluetooth Modem
948
Ethernet Modem
949
Other I/O Devices
985
Wi-Fi Extension for Internal or External Communications Bus Structure
1510
Intermediate Wi-Fi to DSL Bridge Device
1520
Intermediate Wi-Fi to 3G/4G Bridge Device
1530
Intermediate Wi-Fi to Cable Bridge Device
1540
Intermediate Wi-Fi to Fiber Bridge Device
1550

FIG. 15A

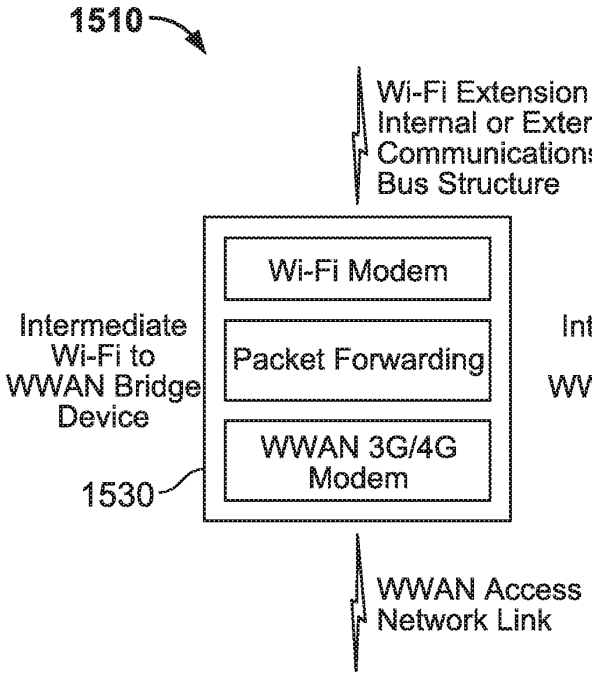


FIG. 15B

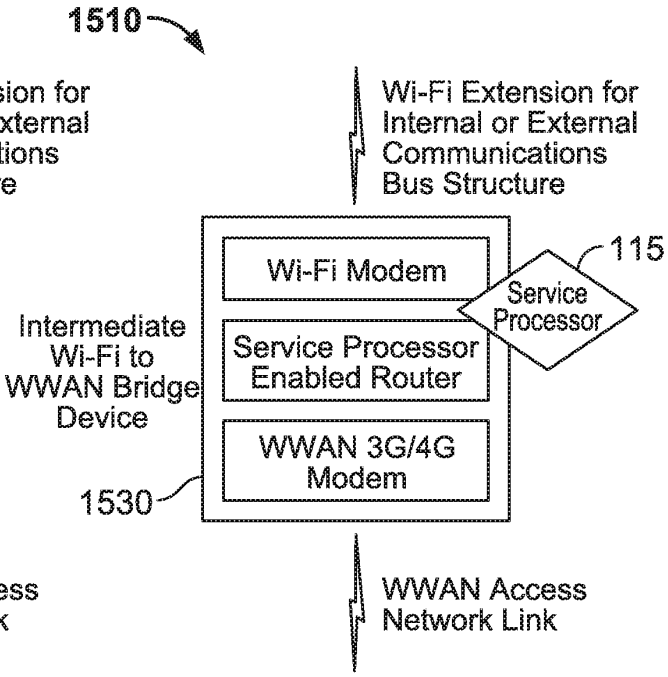


FIG. 15C

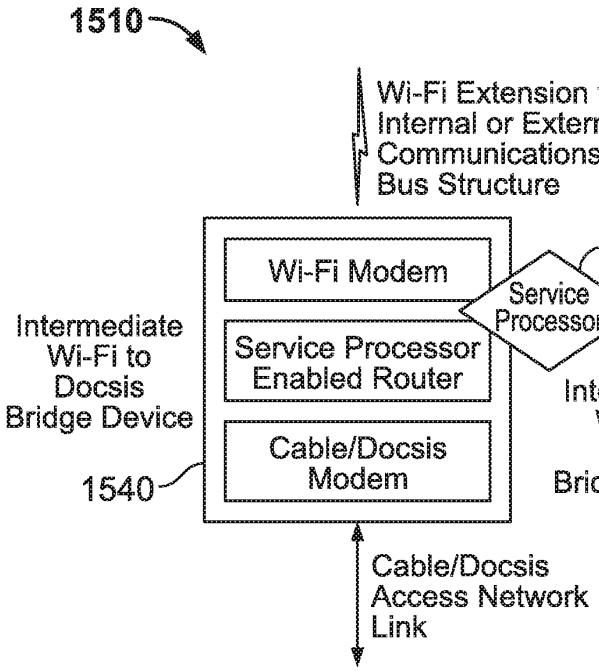


FIG. 15D

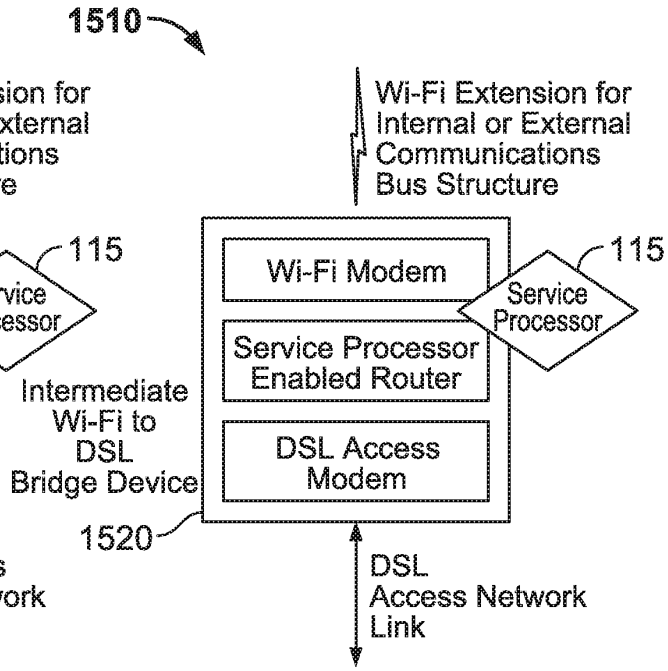


FIG. 15E

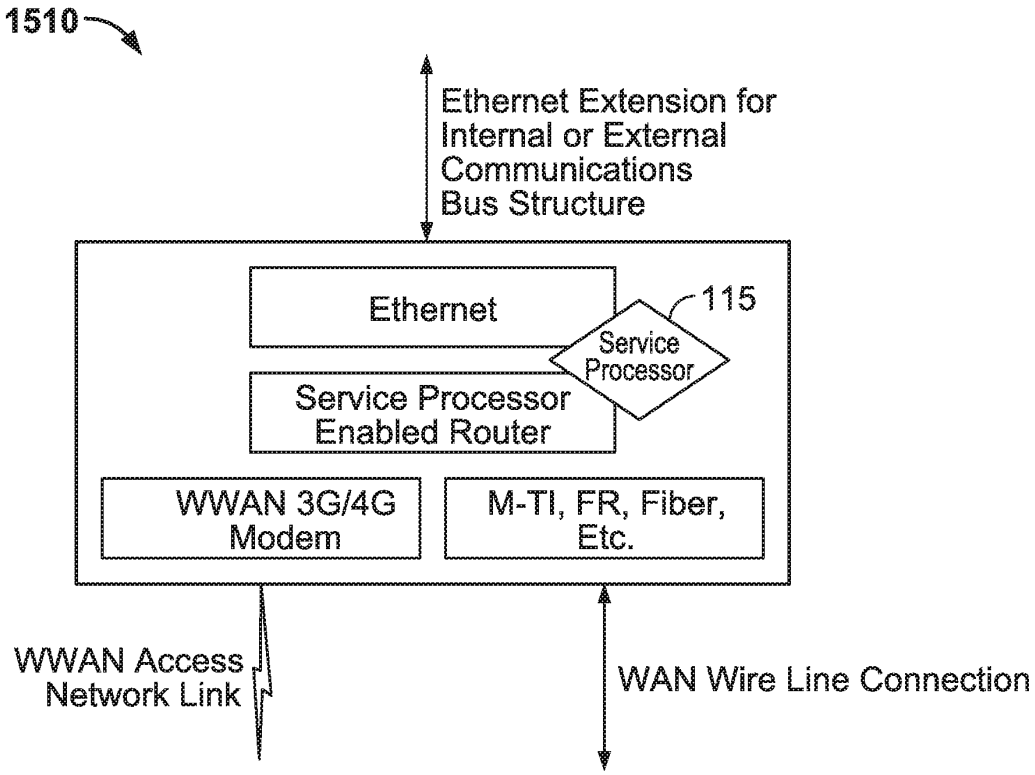

1510
Ethernet Extension for Internal or External Communications Bus Structure
Ethernet
115
Service Processor
Service Processor Enabled Router
WWAN 3G/4G Modem
M-TI, FR, Fiber, Etc.
WWAN Access Network Link
WAN Wire Line Connection

FIG. 15F

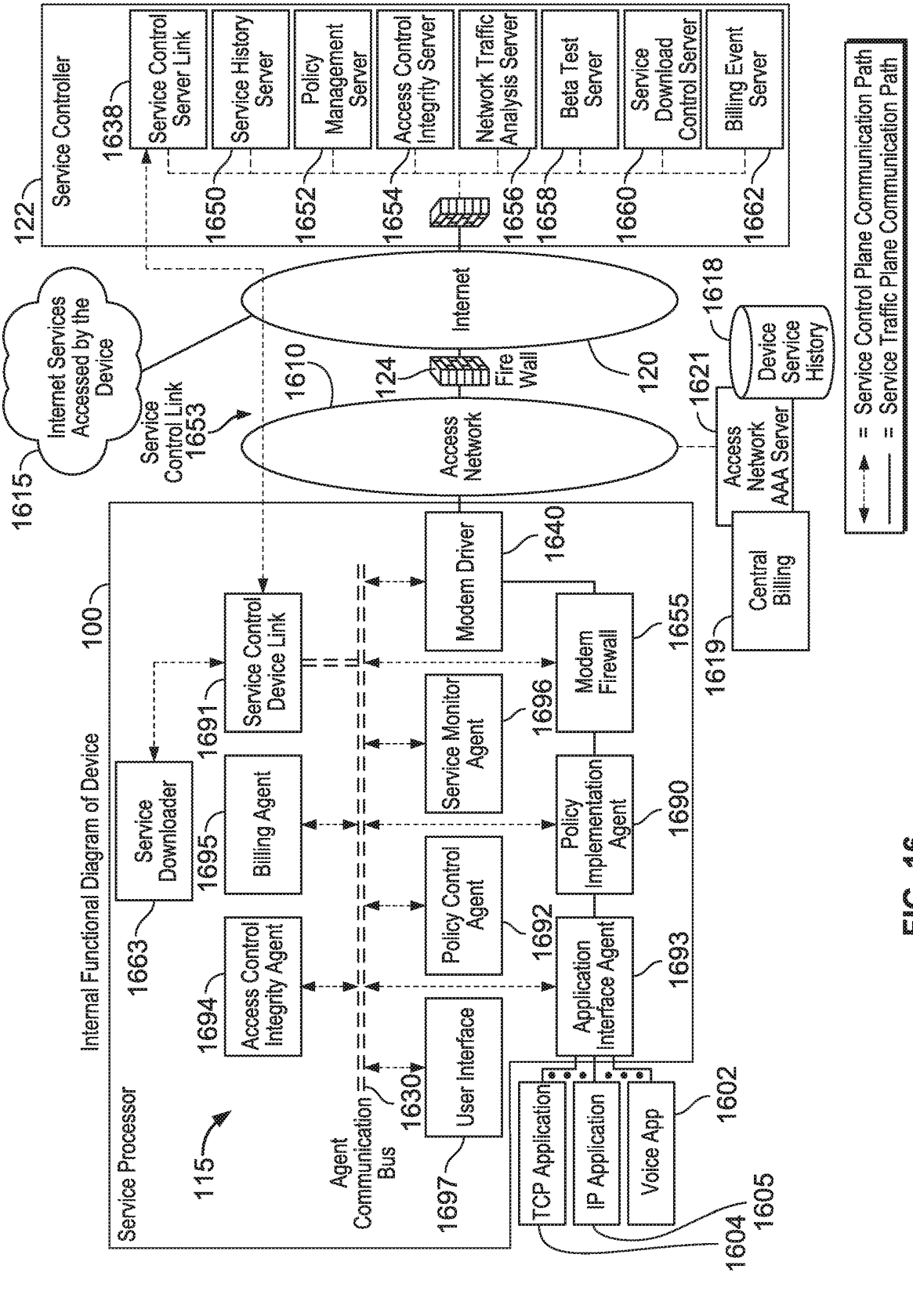

Service Controller
122
Service Control Server Link
1638
Service History Server
Policy Management Server
Access Control Integrity Server
Network Traffic Analysis Server
Beta Test Server
Service Download Control Server
Billing Event Server
1650
1652
1654
1656
1658
1660
1662
Internet Services Accessed by the Device
1615
Service Control Link
1653
1610
Internet
120
124
Fire Wall
Access Network
1621
Access Network AAA Server
1618
Device Service History
1619
Central Billing
= Service Control Plane Communication Path
= Service Traffic Plane Communication Path
Internal Functional Diagram of Device
100
Service Processor
115
Service Downloader
1663
Service Control Device Link
1691
Modem Driver
1640
Billing Agent
1695
Service Monitor Agent
1696
Modem Firewall
1655
Access Control Integrity Agent
1694
Policy Control Agent
1692
Policy Implementation Agent
1690
Application Interface Agent
1693
User Interface
1697
Agent Communication Bus
1630
TCP Application
IP Application
Voice App
1602
1604
1605

FIG. 16

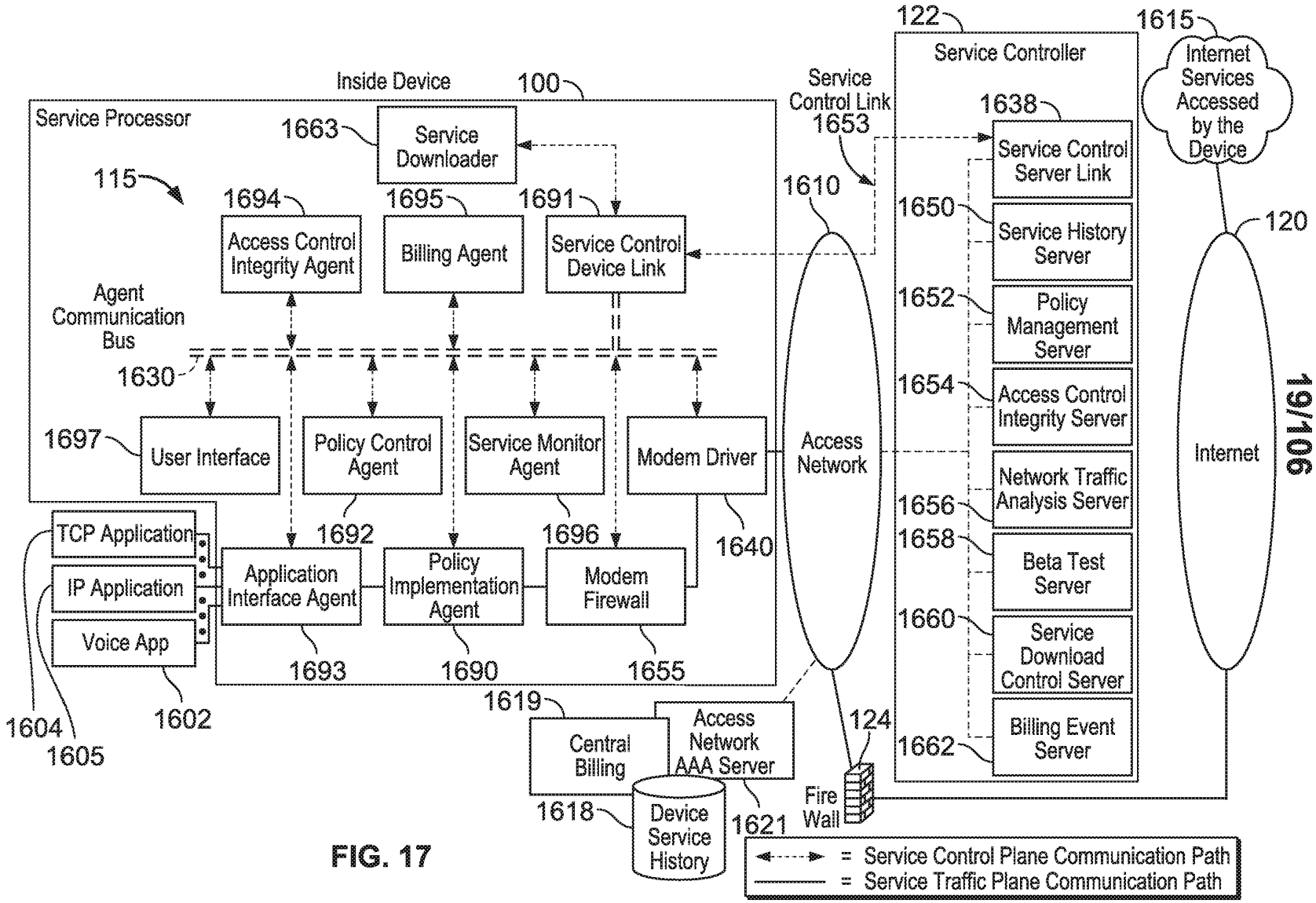

Inside Device
100
Service Processor
115
1663
Service Downloader
1694
Access Control Integrity Agent
1695
Billing Agent
1691
Service Control Device Link
Agent Communication Bus
1630
1697
User Interface
Policy Control Agent
Service Monitor Agent
Modem Driver
1692
1696
1640
TCP Application
IP Application
Voice App
Application Interface Agent
Policy Implementation Agent
Modem Firewall
1693
1690
1655
1604
1605
1602
1619
Central Billing
Access Network AAA Server
1618
Device Service History
1621
Service Control Link
1653
1610
Access Network
124
Fire Wall
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
1615
Internet Services Accessed by the Device
120
Internet
19/106
= Service Control Plane Communication Path
= Service Traffic Plane Communication Path

FIG. 17

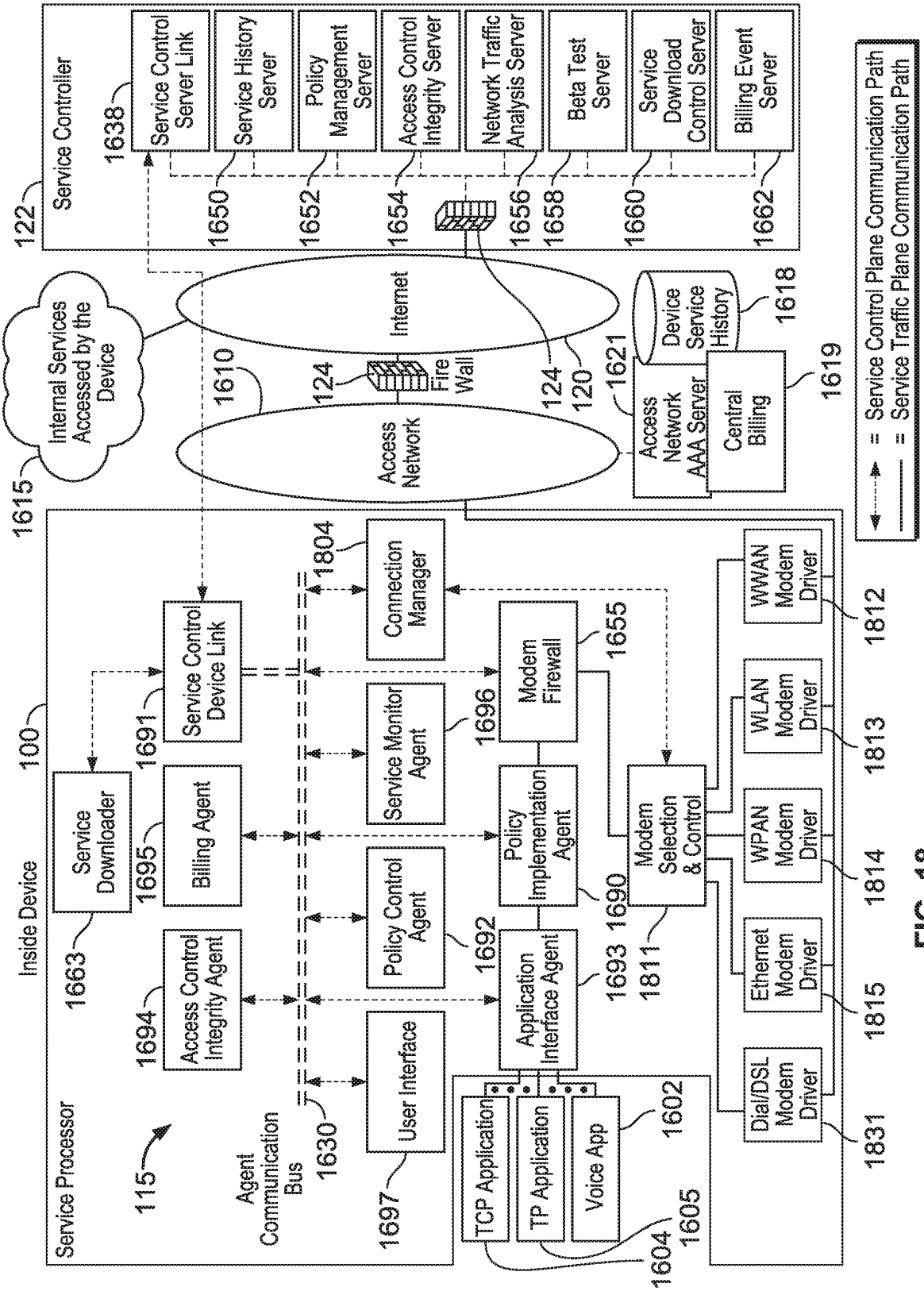

Service Controller
122
Service Control Server Link
1638
Service History Server
Policy Management Server
Access Control Integrity Server
Network Traffic Analysis Server
Beta Test Server
Service Download Control Server
Billing Event Server
1650
1652
1654
1656
1658
1660
1662
Internet
Internal Services Accessed 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
Agent Communication Bus
1630
Service Downloader
1663
Billing Agent
1695
Service Control Device Link
1691
Connection Manager
1804
Service Monitor Agent
1696
Modem Firewall
1655
Access Control Integrity Agent
1694
Policy Control Agent
1692
Policy Implementation Agent
1690
Modem Selection & Control
1811
Application Interface Agent
1693
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

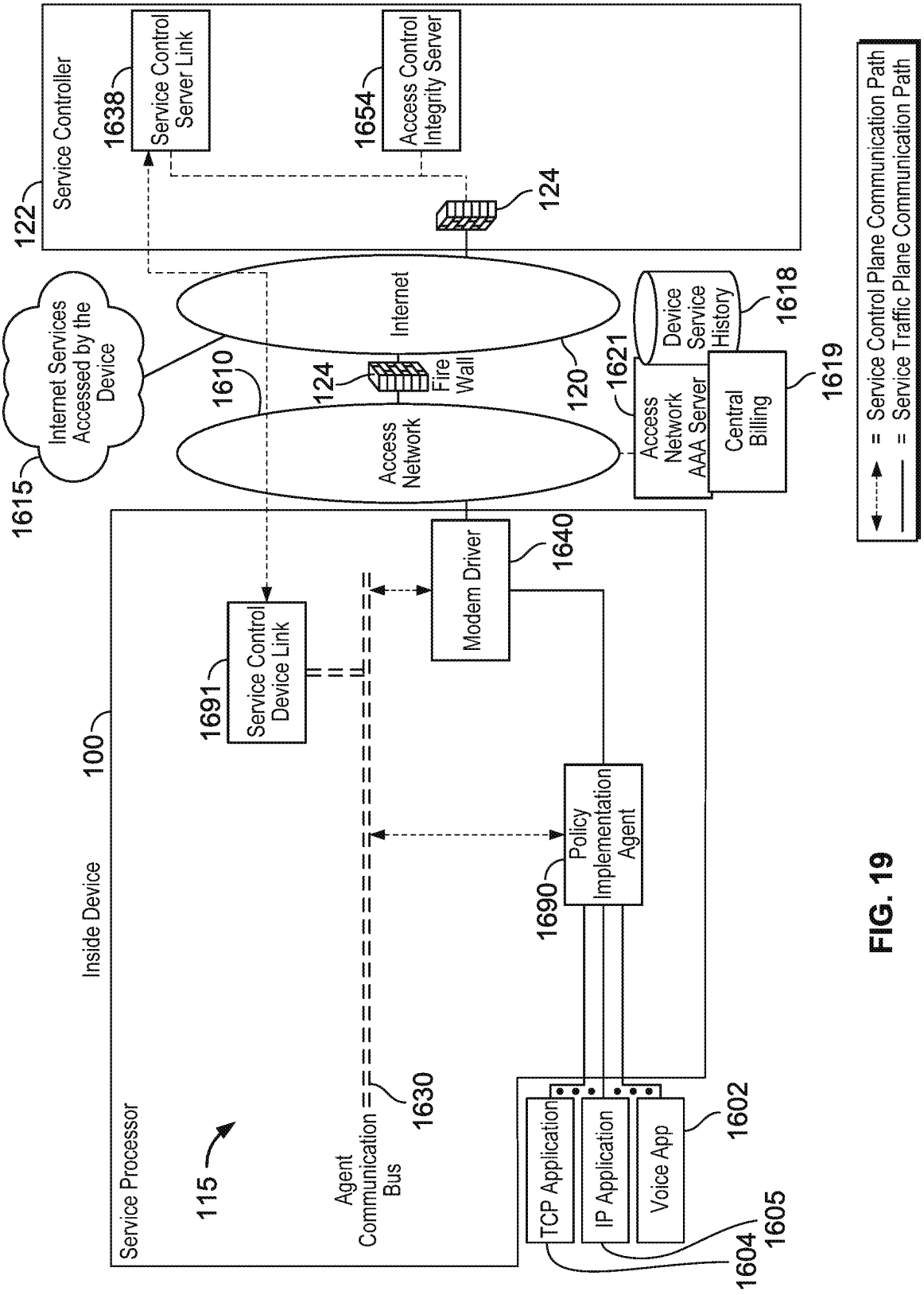

Service Controller
122
Service Control Server Link
1638
Access Control Integrity Server
1654
124
Internet
Internet Services Accessed by the Device
1615
1610
124
Fire Wall
120
1621
Device Service History
1618
Access Network
Access Network AAA Server
Central Billing
1619
Inside Device
100
Service Processor
115
Modem Driver
1640
Service Control Device Link
1691
Policy Implementation Agent
1690
Agent Communication Bus
1630
TCP Application
IP Application
Voice App
1602
1604
1605
= Service Control Plane Communication Path
= Service Traffic Plane Communication Path

FIG. 19

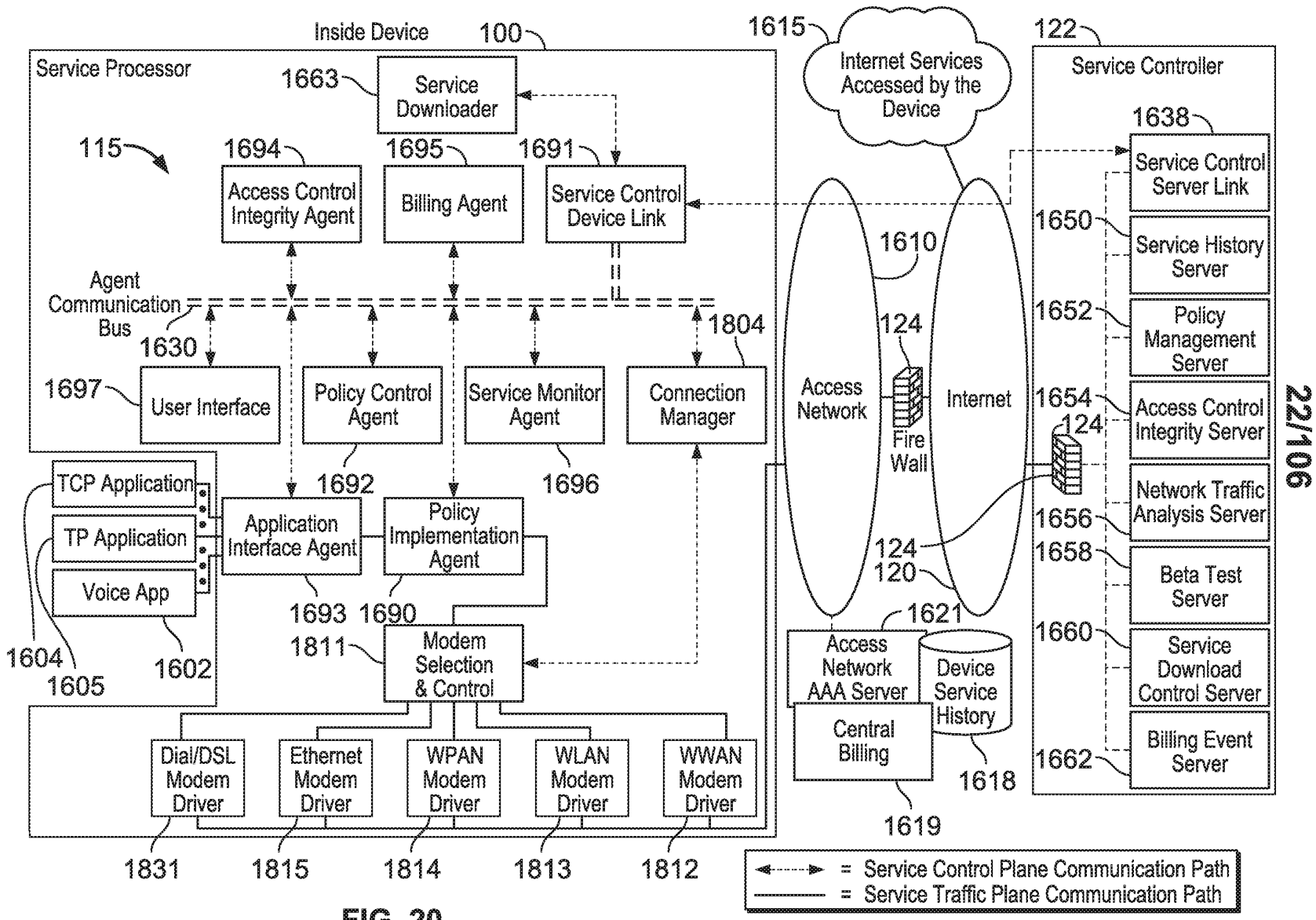

Inside Device
100
Service Processor
1663
Service Downloader
115
1694
Access Control Integrity Agent
1695
Billing Agent
1691
Service Control Device Link
Agent Communication Bus
1630
1804
1697
User Interface
Policy Control Agent
Service Monitor Agent
Connection Manager
1692
1696
TCP Application
TP Application
Voice App
Application Interface Agent
Policy Implementation Agent
1693
1690
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
120
1621
Access Network AAA Server
Device Service History
Central Billing
1618
1619
122
Service Controller
1638
Service Control Server Link
1650
Service History Server
1652
Policy Management Server
1654
Access Control Integrity Server
124
Network Traffic Analysis Server
1656
1658
Beta Test Server
1660
Service Download Control Server
Billing Event Server
1662
= Service Control Plane Communication Path
= Service Traffic Plane Communication Path

FIG. 20

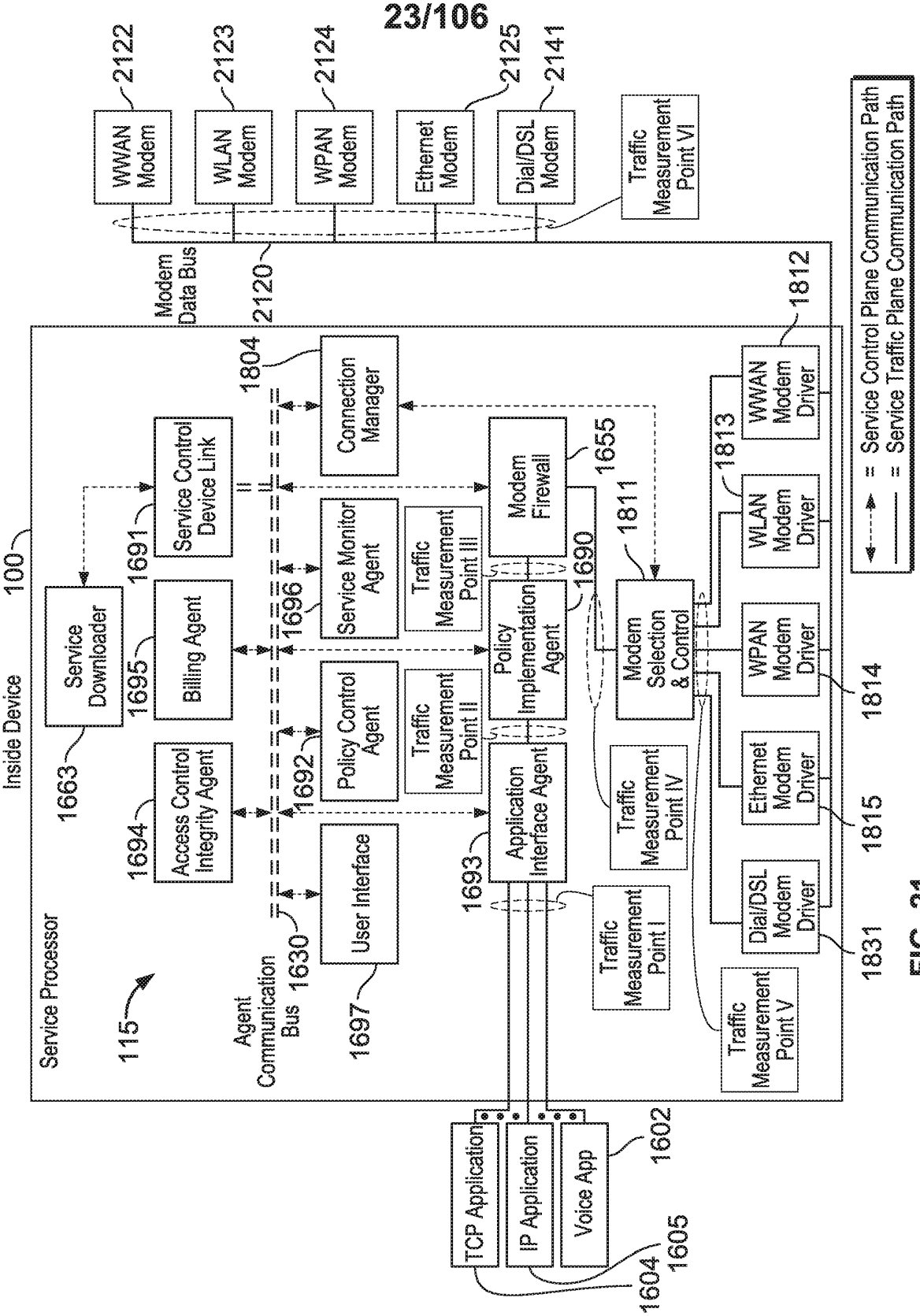

Inside Device
100
Service Processor
115
Service Downloader
1663
Billing Agent
1695
Service Control Device Link
1691
Connection Manager
1804
Access Control Integrity Agent
1694
Policy Control Agent
1692
Service Monitor Agent
1696
Traffic Measurement Point III
Modem Firewall
1655
Traffic Measurement Point II
Policy Implementation Agent
1690
Application Interface Agent
1693
Modem Selection & Control
1811
User Interface
1697
Agent Communication Bus
1630
Traffic Measurement Point I
Traffic Measurement Point IV
Traffic Measurement Point V
Dial/DSL Modem Driver
1831
Ethernet Modem Driver
1815
WPAN Modem Driver
1814
WLAN Modem Driver
1813
WWAN Modem Driver
1812
Modem Data Bus
2120
WWAN Modem
2122
WLAN Modem
2123
WPAN Modem
2124
Ethernet Modem
2125
Dial/DSL Modem
2141
Traffic Measurement Point VI
TCP Application
IP Application
Voice App
1602
1604
1605
= Service Control Plane Communication Path
= Service Traffic Plane Communication Path

FIG. 21

Service Processor 115 Embodiment	Partial Summary of Embodiment Functions
Service Control Device Link 1691	Device side control plane link for connecting Service Processor 115 to Service Controller. In some embodiments, also serves as the link for the agent heartbeat function.
Access Control Integrity Agent 1694	Collects device information on service policy, service usage, agent configuration and agent behavior. Cross checks this information to identify integrity breaches in the service policy implementation and control system. Initiates action when a service policy violation or a system integrity breach is suspected. In some embodiments, verifies configuration of other agents or performs challenge-response sequence testing. In some embodiments, monitors software loading activity, protected memory access or communication with Service Processor agents to detect unauthorized changes to Service Processor software or configuration.
Policy Control Agent 1692	Takes policy instructions from the network and sets instantaneous device service policy. In some embodiments, performs a policy control function to adapt instantaneous service policies to achieve a service usage objective.
Policy Implementation Agent 1690	Implements traffic control and QOS policy rules for device. In some embodiments provides the functions of access control and/or firewall function or perform traffic inspection and characterization. In some embodiments packet inspection is aided by literal or virtual application layer tagging while in other embodiments packet inspection is performed completely in the Policy Implementation Agent 1690.
Service Monitor Agent 1696	Records and reports device service usage. In some embodiments, assists in communicating application tagging of traffic flows through the networking stack policy implementation. In some embodiments, maintains a history and provides reports or summary reports of which networks in addition to the networks controlled by the Service Controller that the device has connected to. In some embodiments, this network activity summary may include a summary of the networks accessed, activity vs. time per connection, traffic vs. time per connection.
Application Interface Agent 1693	Rich feature interface for device application programs. In some embodiments, identifies application level traffic, reports service usage or tags traffic for service QOS control. In some embodiments, interacts with applications or programs applications to arrange application settings such as email file transfer options or browser headers. In some embodiments, intercepts certain application traffic to modify traffic application layer parameters such as email file transfer options or browser headers. In some embodiments implements certain aspects of traffic control or other service policies. In some embodiments, provides the functions of traffic control, access control and/or firewall.
Modem Firewall 1655	Blocks or passes traffic based on service policies and traffic attributes. In some embodiments, assists in traffic flow tagging. In some embodiments provides the functions of traffic control and/or access control.
Billing Agent 1695	Detects and reports billing events. In some embodiments interacts with the User Interface Agent 1697 to provide the user with service plan options, accept service plan selections, provide notification on service usage levels, provide options on service usage control policy, accept choices on service usage policy, provide transaction options or accept transaction choices. In some embodiments, interacts with Transaction Servers 134 to conduct ecommerce transactions with central billing.

FIG. 22A

EX1002 - Page 35

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.

FIG. 22B

EX1002 - Page 36

Service Controller 122 Element	Partial Summary of Embodiment Functions
Service Control Server Link 1638	Network side control plane link for connecting Service Controller 122 Service Processor 115 device agents. In some embodiments, also serves as the link for the agent heartbeat function.
Access Control Integrity Server 1654	Collects device information on service policy, service usage, agent configuration and agent behavior. Cross checks this information to identify integrity breaches in the service policy implementation and control system. Initiates action when a service policy violation or a system integrity breach is suspected.
Policy Management Server 1652	Transmits policies to the Service Processor 115.
Access Network AAA Server 1621	Provides access control and authorization functions for the device access layer. Records and reports device network service usage.
Service History Server 1650	Collects and records service usage reports from the Access Network AAA Server 121 and the Service Monitor Agent 1696. In some embodiments, maintains a history of which networks in addition to the networks controlled by the Service Controller that the device has connected to. In some embodiments, this network activity summary may include a summary of the networks accessed, activity vs. time per connection, traffic vs. time per connection. In some embodiments, this activity summary is further analyzed or reported to estimate the type of service plan associated with the traffic activity for the purpose of bill sharing reconciliation.
Central Provider Billing System 1619	Provides mediation function for central provider billing events. Accepts service plan changes. In some embodiments, provides updates on device service usage, service plan limits or service policies.
Billing Event Server 1662	In some embodiments, collects billing events, provides service plan information to the Service Processor 115, provides service usage updates to the Service Processor 115, serves as interface between device and central Provider Billing System 123, or provides trusted third party function for certain ecommerce billing transactions.
Network Traffic Analysis Server 1656	Collects service usage history for devices or groups of devices and analyses the service usage. In some embodiments, presents service usage statistics in various formats to identify improvements in network service quality or service profitability. In other embodiments, estimates the service quality or service usage for the network under variable settings on potential service policy. In other embodiments, identifies actual or potential service behaviors by one or more devices that are causing problems for overall network service quality or service cost.
Beta Test Server 1658	Publishes candidate service plan policy setting to one or more devices. In some embodiments, provides summary reports of network service usage or user feedback information for one or more candidate service plan policy setting. In some embodiments, provides a means to compare the beta test results for different candidate service plan policy settings or select the optimum candidates for further setting optimization.
Service Download Control Server 1660	Provides a download function to install or update service software elements on the device.
Transaction Server 134	Provides an electronic commerce offering and transaction platform to the device.

FIG. 23

EX1002 - Page 37

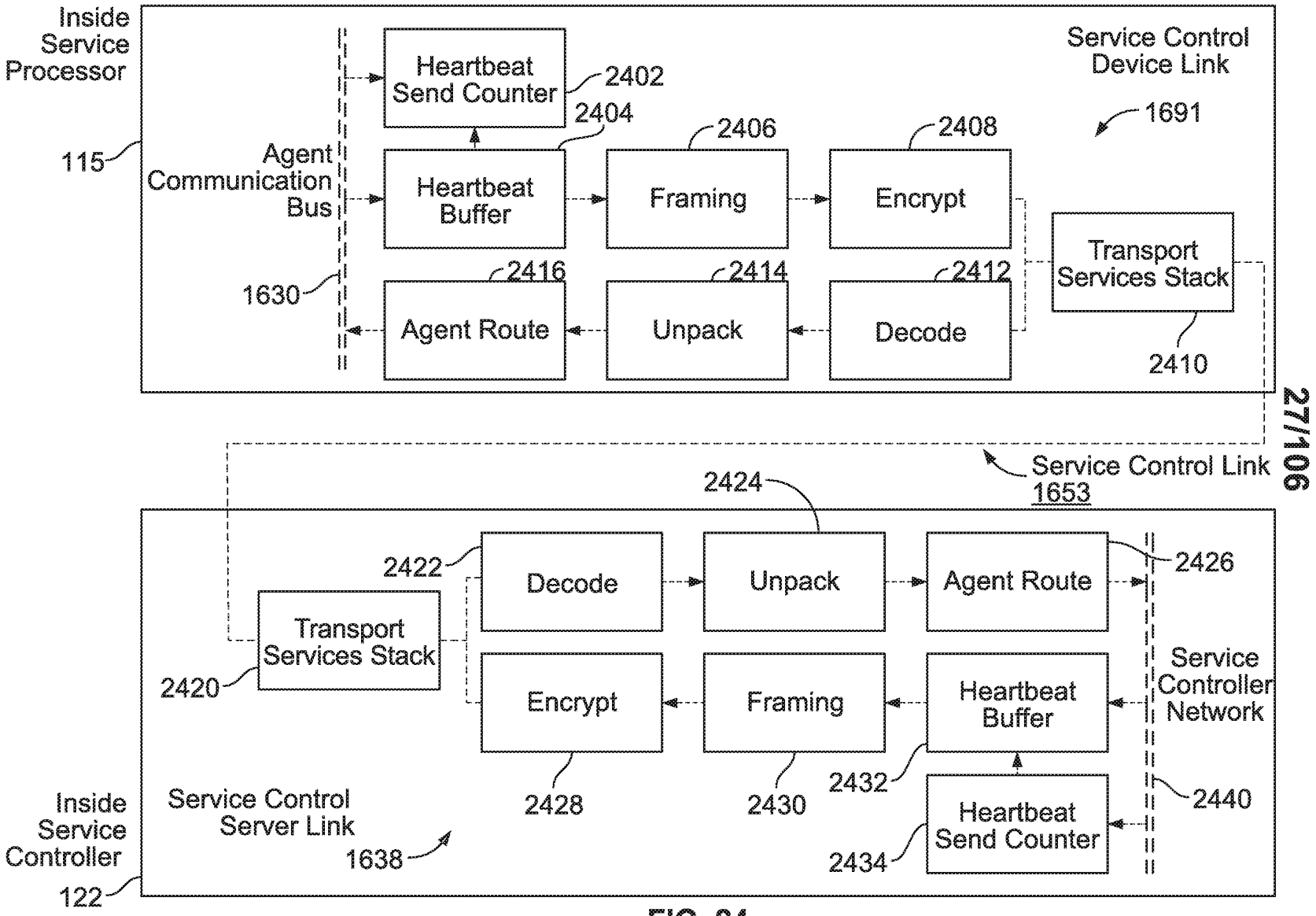


FIG. 24

EX1002 - Page 38

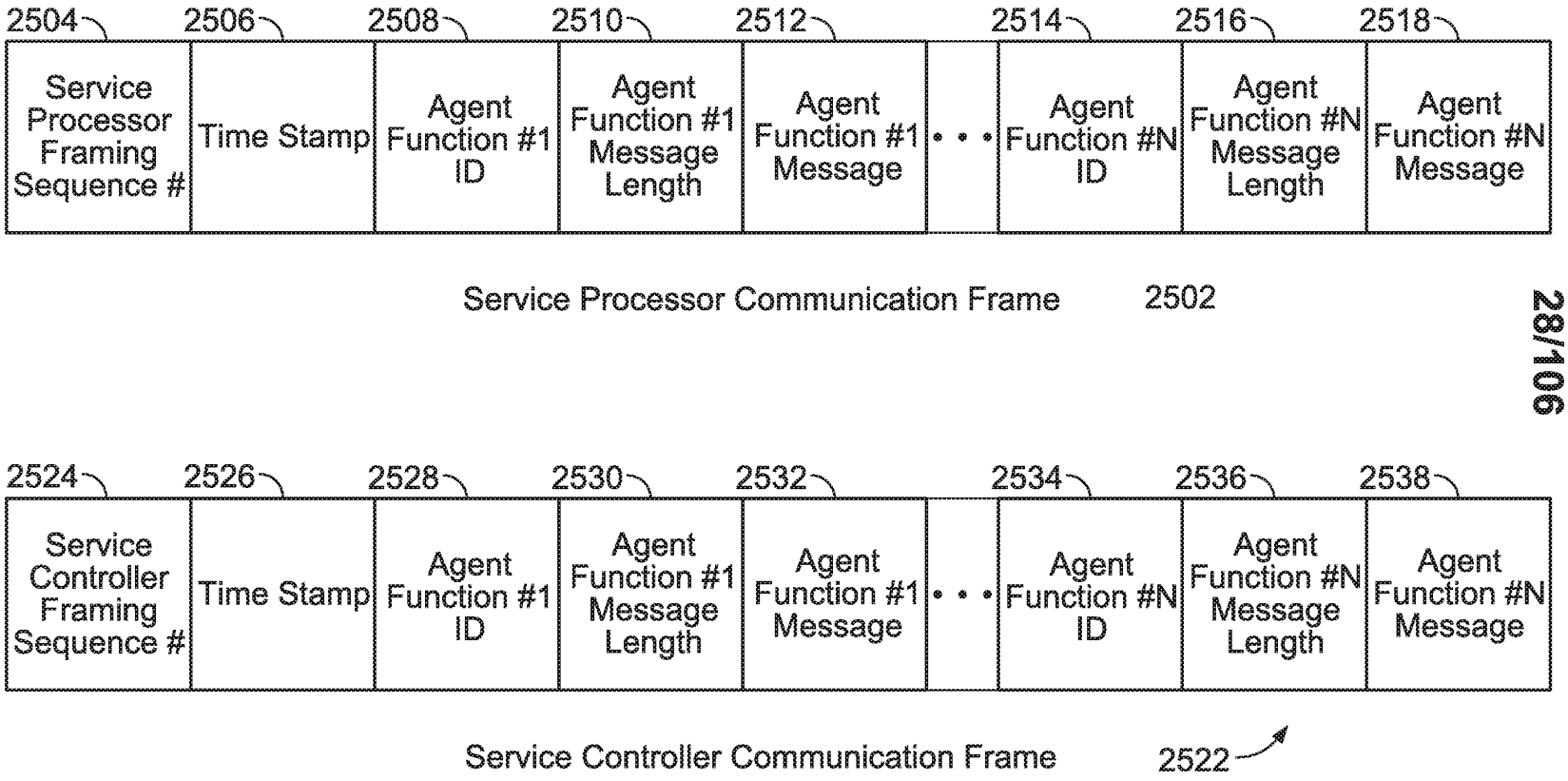


FIG. 25

EX1002 - Page 39

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

EX1002 - Page 40

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.

FIG. 26B

EX1002 - Page 41

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.

FIG. 26D

EX1002 - Page 43

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.

FIG. 26E

	events using a service usage to cost look up data base stored locally on the device or available from a network function. In some embodiments, service cost estimation is done entirely in the network and the result is pushed out to the device UI. In other embodiments service cost estimation is done in the device based on local usage estimates and a local usage to cost lookup table.	
Available network information and roaming information	Device receives available network or available roaming service provider information from a network function. The available network or roaming service information may include the potential network service or roaming service a device or user may choose to select, or the network service or roaming service the user has already selected. In some embodiments this information includes service cost information to aid the device or the user in determining the potential or actual costs of service usage while using the available network or roaming network. In some embodiments the service cost information is used to help the user in selecting the available network provider or roaming service provider. In some embodiments the available network cost information or roaming cost information is combined with a measure of expected or possible service usage to estimate how much a typical usage scenario may cost. In some embodiments, the available network information or roaming information is used to help the user estimate the present available network or roaming service charges for services used to date. In some embodiments service usage is recorded and sent to a network function that estimates the current service cost. In other embodiments the service cost is estimated locally on the device based on a service usage estimate and a service usage to cost look up function. In other	In some embodiments available network information or roaming information is requested by the device. In other embodiments, the information is periodically updated by the Service Controller or other network function that contains the information.

FIG. 26F

EX1002 - Page 45

	embodiments, the service cost is derived by querying the available network or roaming network billing system.	
System messages and responses	In some embodiments the heartbeat function may be used as a secure control channel to display a system messages or screen that is generated by a network function or server to the end user and possibly report user inputs to the UI message or screen. Examples include, ….. etc.	System messages are generated by the Service Controller and transmitted as needed in some embodiments. In other embodiments, some system messages are generated in response to user input or requests. In other embodiments, system messages are generated on a regular time table or in accordance with a certain amount of service usage.
UI screen messages and responses	In some embodiments the heartbeat function may be used as a secure control channel to display user interface message or screen that is generated by a network function or serve to the end user and possibly report user inputs to the UI message or screen. Examples include service usage UI, service choice UI, upgrade UI, transaction UI, marketing UI, billing UI, user identify confirmation UI, user service warning UI, user potential service tamper response request UI, etc.	UI screen messages are generated by the Service Controller and transmitted as needed in some embodiments. In other embodiments some user UI messages are generated in response to user input or requests. In other embodiments, UI messages are generated on a regular time table or in accordance with a certain amount of service usage.
Local agent check-in history	Logs and reports agent check-ins or self-reports that are made to a local agent integrity verification function.	In some embodiments a report is made during every heartbeat transmission. In other embodiments the report is generated by a request from the Service Controller. In other embodiments the report is generated by timing determined by the device. In some embodiments the report is generated when there is a verification error of some kind that is identified.
Software install report	Logs and reports one or more aspects of software installs that have occurred on the device.	In some embodiments a report is made during every heartbeat transmission. In other embodiments the report is generated by a request from the Service Controller. In other embodiments the report is generated by timing determined by the device. In some embodiments the report is generated when there is a verification error of some kind that is identified. In some

FIG. 26G

		embodiments, the report is generated when new SW is installed.
Test billing event	In some embodiments the Service Controller or other network function may send or cause a test billing event wherein the device triggers a local billing sequence for the purpose of verifying that the billing sequence is properly logged, conducted and reported. The billing sequence can be related to a service usage event or sequence, a transaction event or sequence, or any other event or sequence that should result in a billing event.	In some embodiments, the test billing event timing is determined by the Service Controller or other network function. In others it is generated by the device or on a regular schedule.
Test service event	In some embodiments the service Controller or other network function may send or cause a service usage event wherein the device triggers a local service usage event or sequence for the purpose of verifying that the service usage event or sequence is properly logged and reported.	In some embodiments, the test service usage event timing is determined by the Service Controller or other network function. In others it is generated by the device or on a regular schedule.

FIG. 26H

Service Policy Implementation Verification Technique Embodiments	Example Error Trigger Criteria Embodiments	Example Error Response Embodiments
Verify service usage measure in network is consistent with expected service behavior	Network service usage measure is in conflict with expected service usage. Examples: traffic usage outside limits, address access outside limits, data rate outside limits, traffic shaping rules not being followed.	In some embodiments the severity of the error and/or the persistence of the error and/or the existence of the other errors are used to determine the appropriate response or action. In some embodiments, reset service policies and see if errors persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/ response to determine agent integrity. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service inspection process, or usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.

FIG. 27A

EX1002 - Page 48

Verify service usage measure at device is consistent with expected service behavior	Device service usage measure is in conflict with expected service usage. Examples: traffic usage too high, address access outside limits, email accessed against policy.	Same as above.
Verify service usage measure in network is consistent with service usage measure at device	Device service usage measure varies significantly from network service usage measure	Same as above.
Verify service usage measure at one point in device is consistent with service usage measure at a second point in device	Service usage measure at one point in device stack that is inconsistent with another point indicates error or potential parasitic usage	Same as above. In some embodiments, the differences in service measures on the device may be used to evaluate the nature of the service usage policy implementation problem.
Verify that service policies in effect are as intended	Service policy setting queries result in settings that are different than intended	In some embodiments, reset service policies and see if error persist. If this does not clear the error, or if this is not the error correction method employed, then perform one or more of the following actions: In some embodiments, perform agent query/response to determine agent integrity.In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition

FIG. 27B

EX1002 - Page 49

		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

EX1002 - Page 50

		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

FIG. 27D

EX1002 - Page 51

		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

EX1002 - Page 52

		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

EX1002 - Page 53

		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

EX1002 - Page 54

		agent integrity. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a service usage test to determine if the device is properly reporting service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis
Verify device reports billing events reported from transaction servers.	Transaction server receipts do not correspond with billing events from device.	In some embodiments, perform checks to determine if transaction server receipts are valid. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. If this does not clear the error, or if these are not the error correction methods employed, then perform one or more of the following actions: In some embodiments the severity of the error and/or the persistence of the error and/or the existence of other errors are used to determine the appropriate response or action. In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, a user query or warning is sent to

FIG. 27H

EX1002 - Page 55

		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

EX1002 - Page 56

		Controller, send the UI an error message instructing the user how to proceed. In some embodiments, configure the Service Processor for the ambient service intended for that device. In some embodiments, download the appropriate Service Processor agent software that is appropriate for that device.
Verify proper operation of Service Processor agents	Check input to output relationship on Policy Implementation agent, Firewall agent. Check billing event reports to verify events are being recorded. Check application and traffic inspection tagging system correctly tagging traffic. Verify Service Processor heartbeat reports proper agent integrity self-checks, cross-checks and query/response sequences with Service Controller.	In some embodiments the severity of the error and/or the persistence of the error and/or the existence of other errors are used to determine the appropriate response or action. In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.

FIG. 27J

EX1002 - Page 57

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

FIG. 27L

EX1002 - Page 59

		user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.
Verify Service Processor code configuration with agent self diagnosis checks	One or more of the agents indicates an error after running a self-check.	Run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh other agents and see if problem persists. If this does not clear the error, or if this is not the error correction method employed, then perform one or more of the following actions: In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the

FIG. 27M

EX1002 - Page 60

		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

FIG. 27N

EX1002 - Page 61

		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

EX1002 - Page 62

		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.

FIG. 27P

EX1002 - Page 63

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.

FIG. 28A

EX1002 - Page 64

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.

FIG. 28B

EX1002 - Page 65

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

EX1002 - Page 66

		error message to human interface for troubleshooting. Identify the entity that may have gained access to the Service Processor if possible and eradicate.
Obfuscated agent code	Code check, agent query-response, agent self check or other agent configuration check discovers error in code obfuscation	Same as above.
Unique agent identification numbers and signatures	Agent is discovered to have an incorrect ID. or fails signature	Same as above.
Secure agent communication bus	Agent communication bus monitoring discovers unauthorized communication or other unauthorized access to one or more agents is discovered	Same as above.
Agent level message encryption	Agent is found to be communicating without the required level of agent communication encryption	Same as above.
Service control link message level encryption	Unauthorized communication traffic is discovered on service control link	In some embodiments repair any compromised agents with dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code. In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting. Identify the entity that may have gained access to the Service Processor if possible and eradicate.
Service control link transport layer encryption	Unauthorized communication traffic is discovered on service control link	Same as above.
Agent communication access permissions	Unauthorized communication is discovered with one or more agents	Same as above.

FIG. 28D

EX1002 - Page 67

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.

FIG. 28E

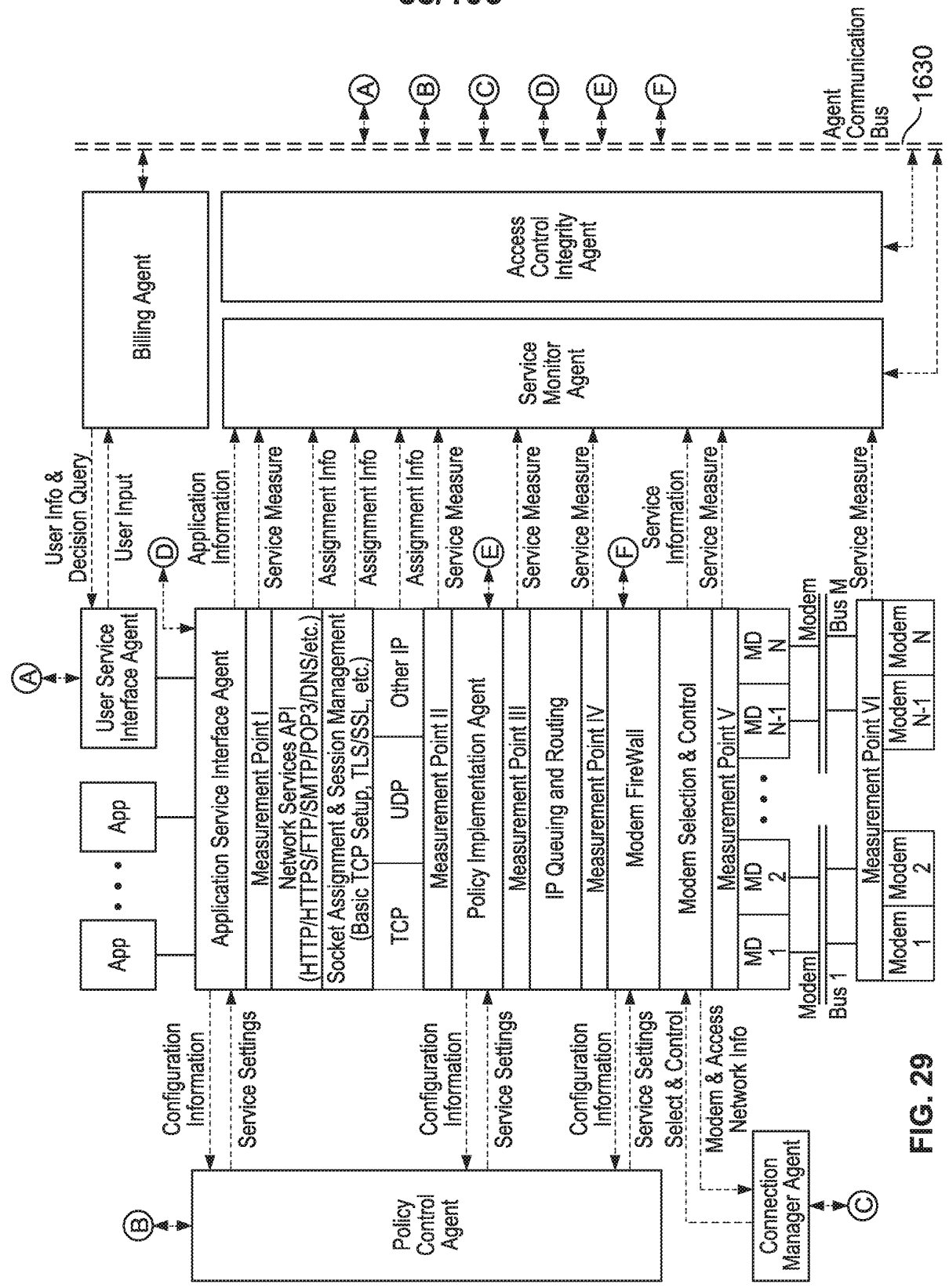

Billing Agent
Access Control Integrity Agent
Service Monitor Agent
User Info & Decision Query
User Input
Application Information
Service Measure
Assignment Info
Service Information
Agent Communication Bus
1630
A
B
C
D
E
F
App
App
User Service Interface Agent
Application Service Interface Agent
Measurement 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

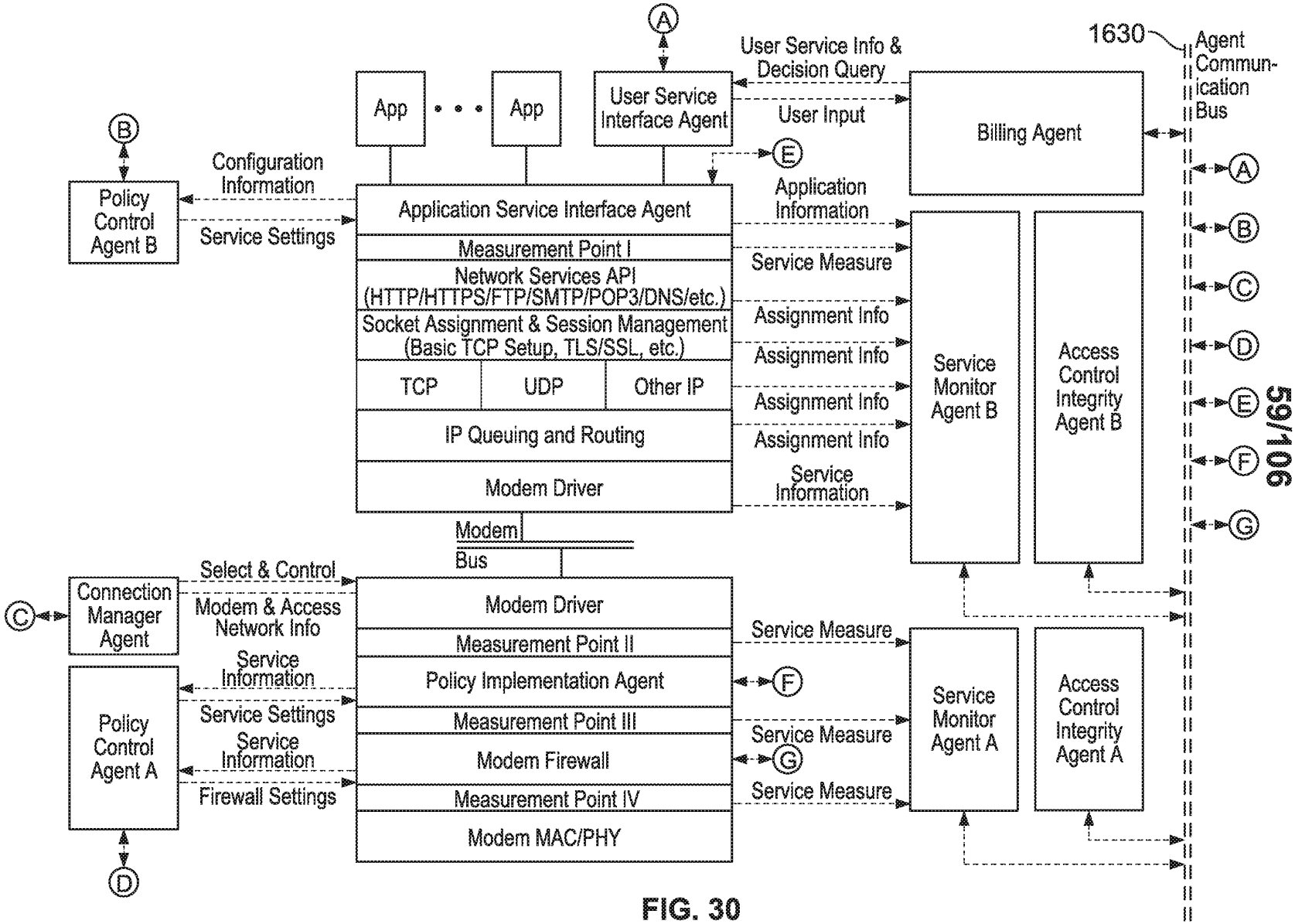

A
1630
Agent Communication Bus
User Service Info & Decision Query
User Input
App
App
User Service Interface Agent
Billing Agent
B
Configuration Information
Service Settings
Policy Control Agent B
E
Application Information
Application Service Interface Agent
Measurement Point I
Service Measure
Network Services API (HTTP/HTTPS/FTP/SMTP/POP3/DNS/etc.)
Assignment Info
Socket Assignment & Session Management (Basic TCP Setup, TLS/SSL, etc.)
Assignment Info
TCP
UDP
Other IP
Assignment Info
IP Queuing and Routing
Assignment Info
Modem Driver
Service Information
Service Monitor Agent B
Access Control Integrity Agent B
Modem Bus
Select & Control
Modem & Access Network Info
C
Connection Manager Agent
Modem Driver
Measurement Point II
Service Measure
Service Information
Service Settings
Policy Implementation Agent
F
Measurement Point III
Service Measure
Service Information
Firewall Settings
Policy Control Agent A
Modem Firewall
G
Measurement Point IV
Service Measure
Modem MAC/PHY
Service Monitor Agent A
Access Control Integrity Agent A
D
59/106

FIG. 30

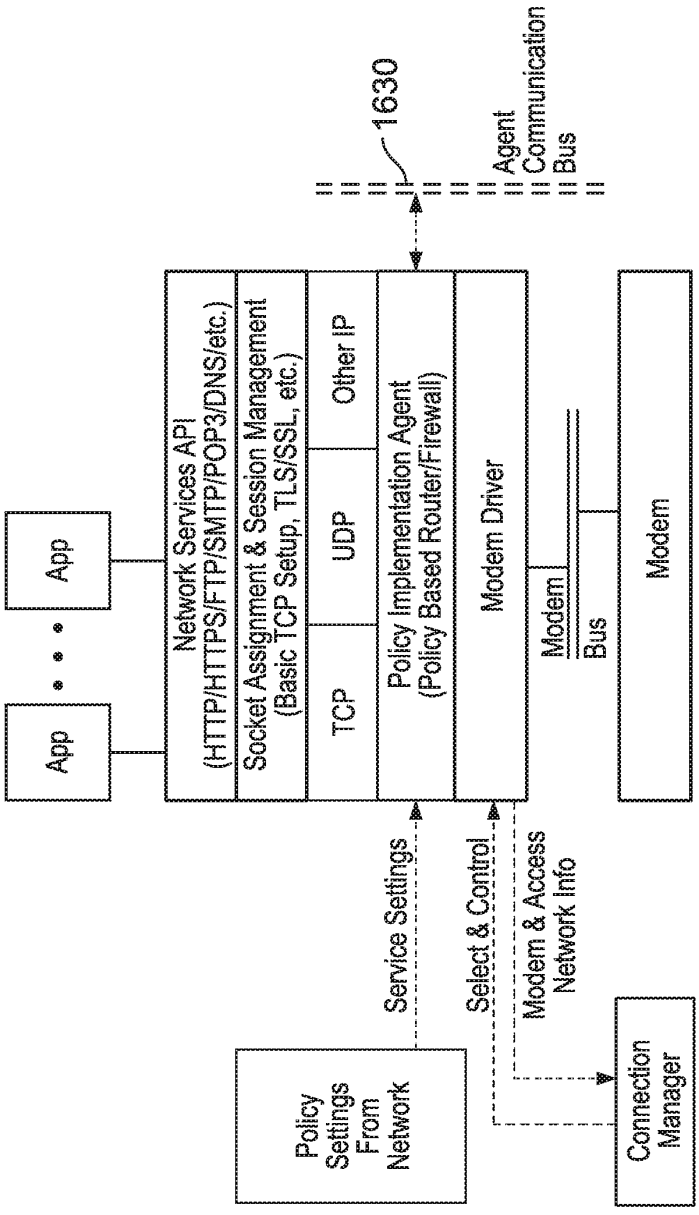

App
App
Network Services API
(HTTP/HTTPS/FTP/SMTP/POP3/DNS/etc.)
Socket Assignment & Session Management
(Basic TCP Setup, TLS/SSL, etc.)
TCP
UDP
Other IP
Policy Implementation Agent
(Policy Based Router/Firewall)
Modem Driver
Modem
Bus
Modem
1630
Agent
Communication
Bus
Service Settings
Select & Control
Modem & Access
Network Info
Policy
Settings
From
Network
Connection
Manager

FIG. 31

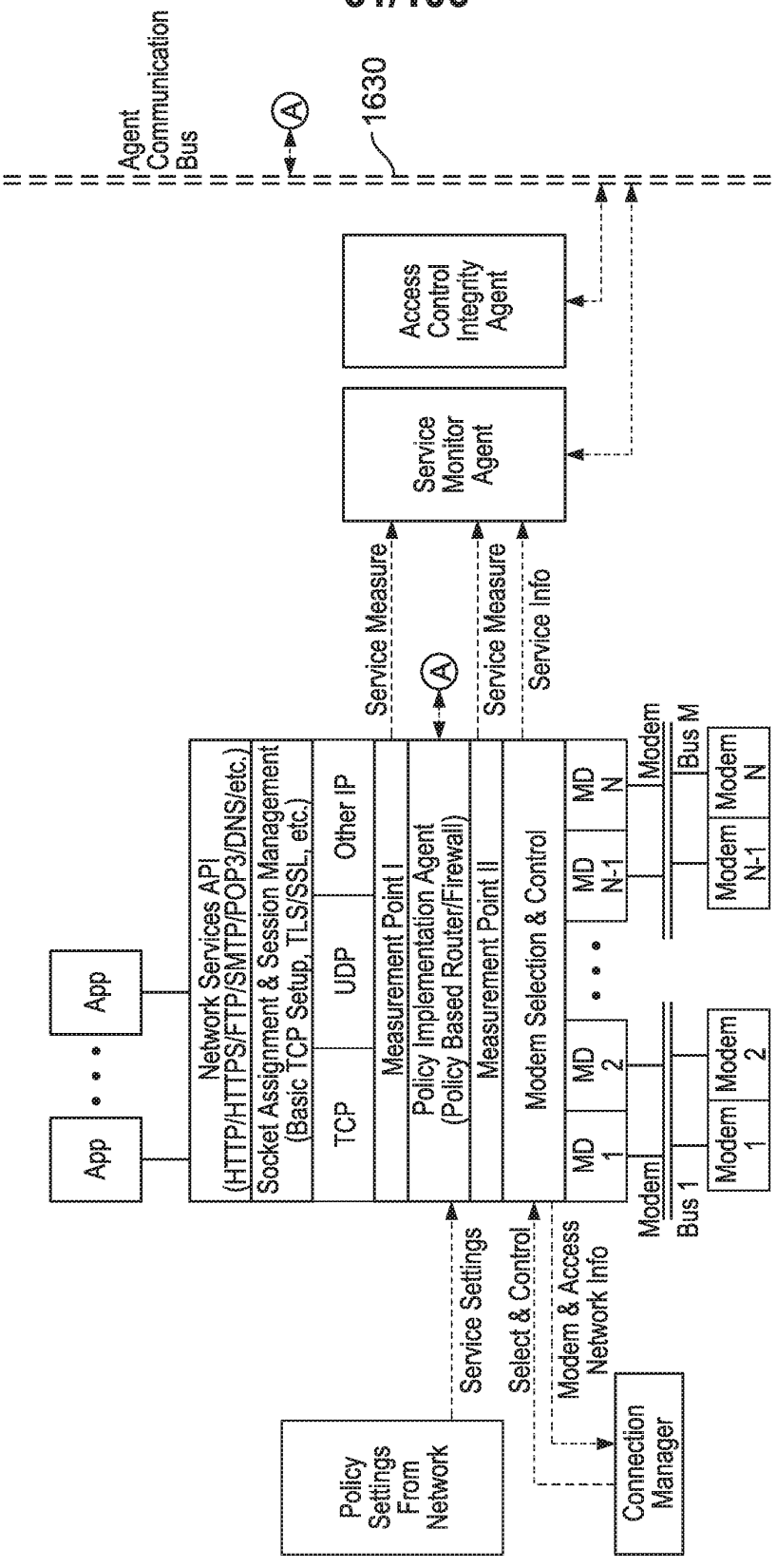

Agent Communication Bus
1630
A
Access Control Integrity Agent
Service Monitor Agent
Service Measure
Service Measure
Service Info
A
App
App
Network Services API (HTTP/HTTPS/FTP/SMTP/POP3/DNS/etc.)
Socket Assignment & Session Management (Basic TCP Setup, TLS/SSL, etc.)
TCP
UDP
Other IP
Measurement Point I
Policy Implementation Agent (Policy Based Router/Firewall)
Measurement Point II
Modem Selection & Control
MD 1
MD 2
MD N-1
MD N
Modem
Bus 1
Modem 1
Modem 2
Modem
Bus M
Modem N-1
Modem N
Service Settings
Select & Control
Modem & Access Network Info
Policy Settings From Network
Connection Manager

FIG. 32

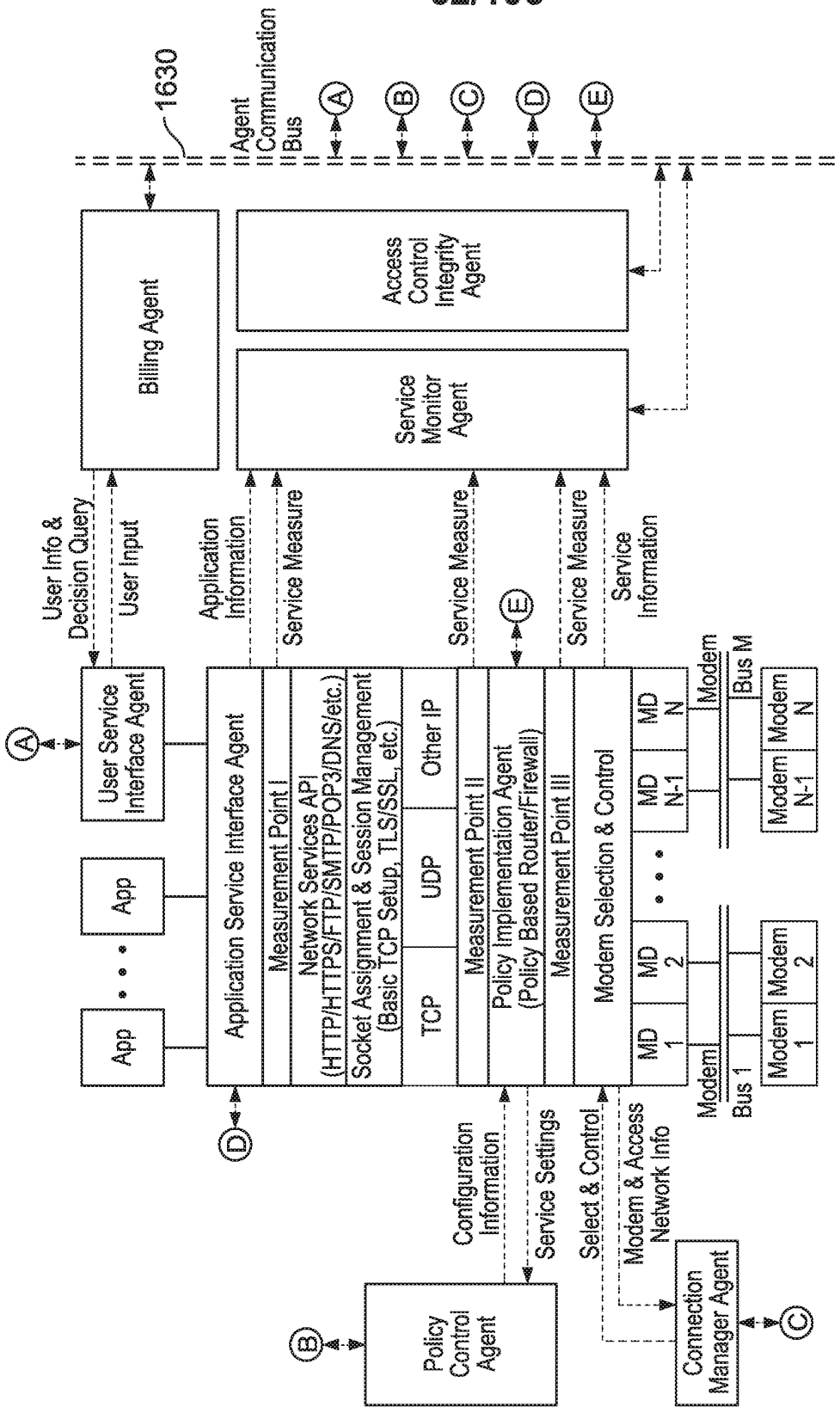

1630
Agent Communication Bus
A
B
C
D
E
Billing Agent
Access Control Integrity Agent
Service Monitor Agent
User Info & Decision Query
User Input
Application Information
Service Measure
Service Measure
Service Measure
Service Information
User Service Interface Agent
App
App
Application Service Interface Agent
Measurement Point I
Network Services API (HTTP/HTTPS/FTP/SMTP/POP3/DNS/etc.)
Socket Assignment & Session Management (Basic TCP Setup, TLS/SSL, etc.)
TCP
UDP
Other IP
Measurement Point II
Policy Implementation Agent (Policy Based Router/Firewall)
Measurement Point III
Modem Selection & Control
MD 1
MD 2
MD N-1
MD N
Modem
Bus 1
Bus M
Modem 1
Modem 2
Modem N-1
Modem N
Configuration Information
Service Settings
Select & Control
Modem & Access Network Info
Policy Control Agent
Connection Manager Agent

FIG. 33

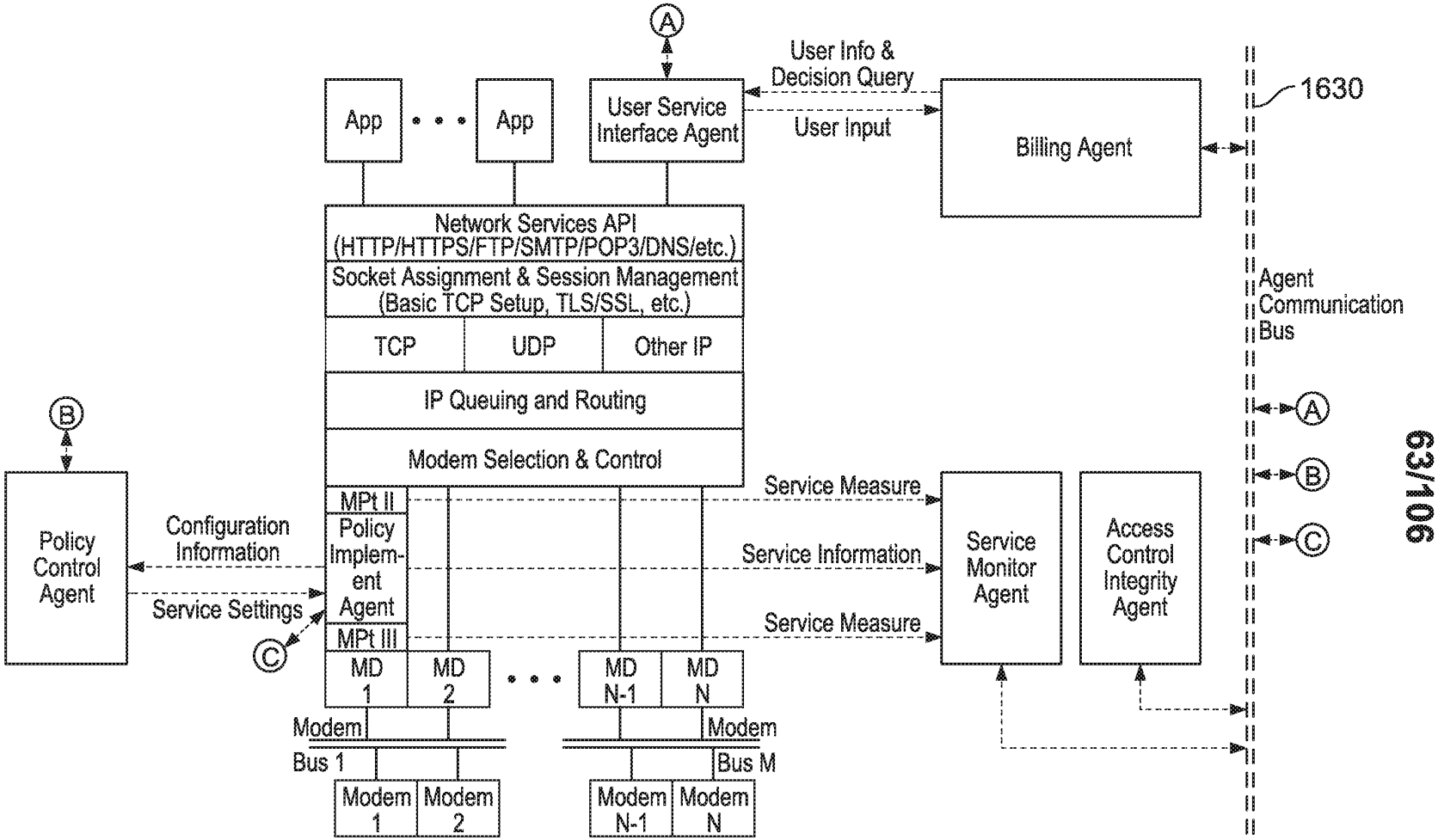

A
User Info &
Decision Query
User Input
App
App
User Service
Interface Agent
Billing Agent
1630
Network Services API
(HTTP/HTTPS/FTP/SMTP/POP3/DNS/etc.)
Socket Assignment & Session Management
(Basic TCP Setup, TLS/SSL, etc.)
TCP
UDP
Other IP
IP Queuing and Routing
Modem Selection & Control
Agent
Communication
Bus
B
C
Policy
Control
Agent
Configuration
Information
Service Settings
MPt II
Policy
Implem-
ent
Agent
MPt III
Service Measure
Service Information
Service Measure
Service
Monitor
Agent
Access
Control
Integrity
Agent
MD
1
MD
2
MD
N-1
MD
N
Modem
Bus 1
Modem
Bus M
Modem
1
Modem
2
Modem
N-1
Modem
N
63/106

FIG. 34

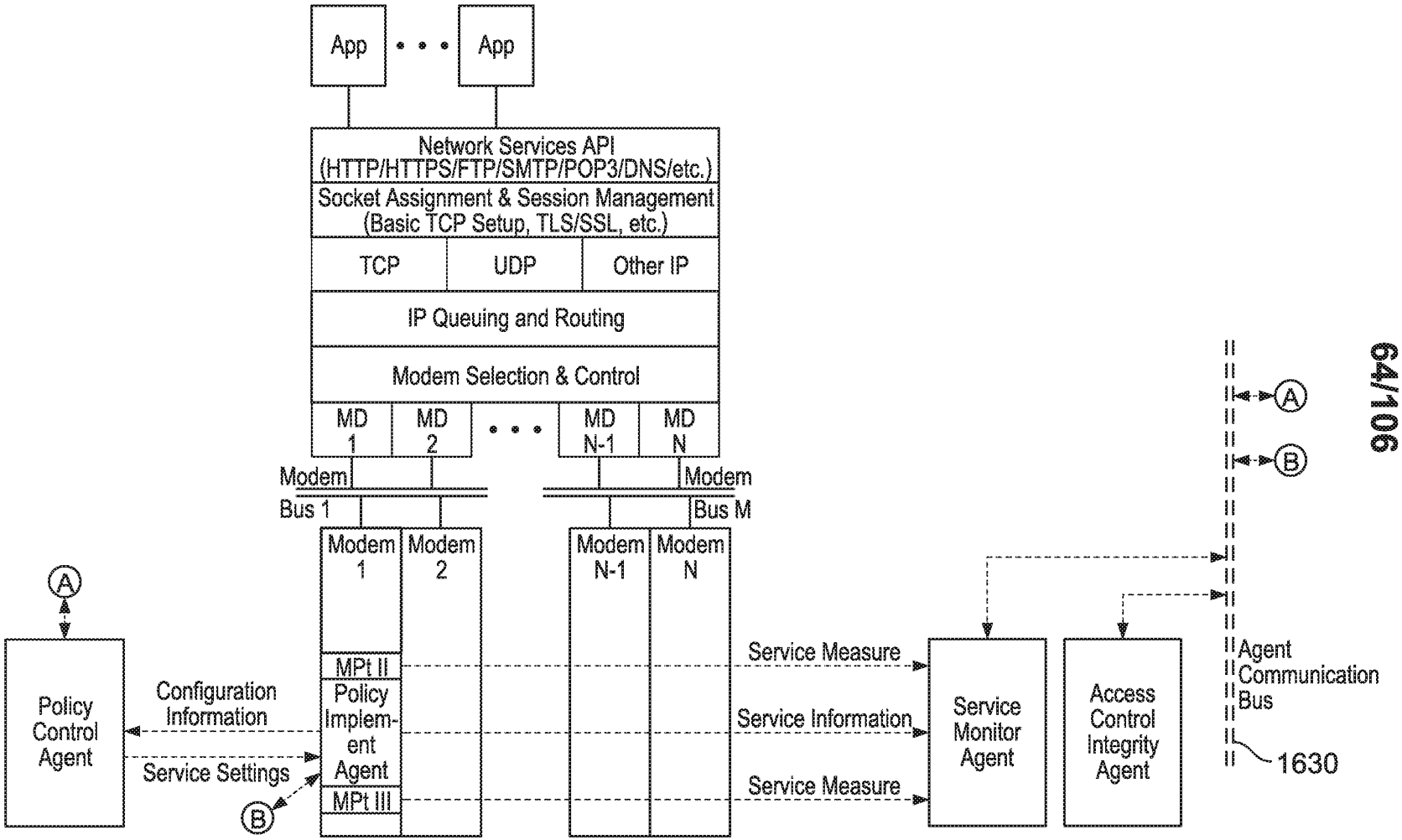


FIG. 35

EX1002 - Page 75

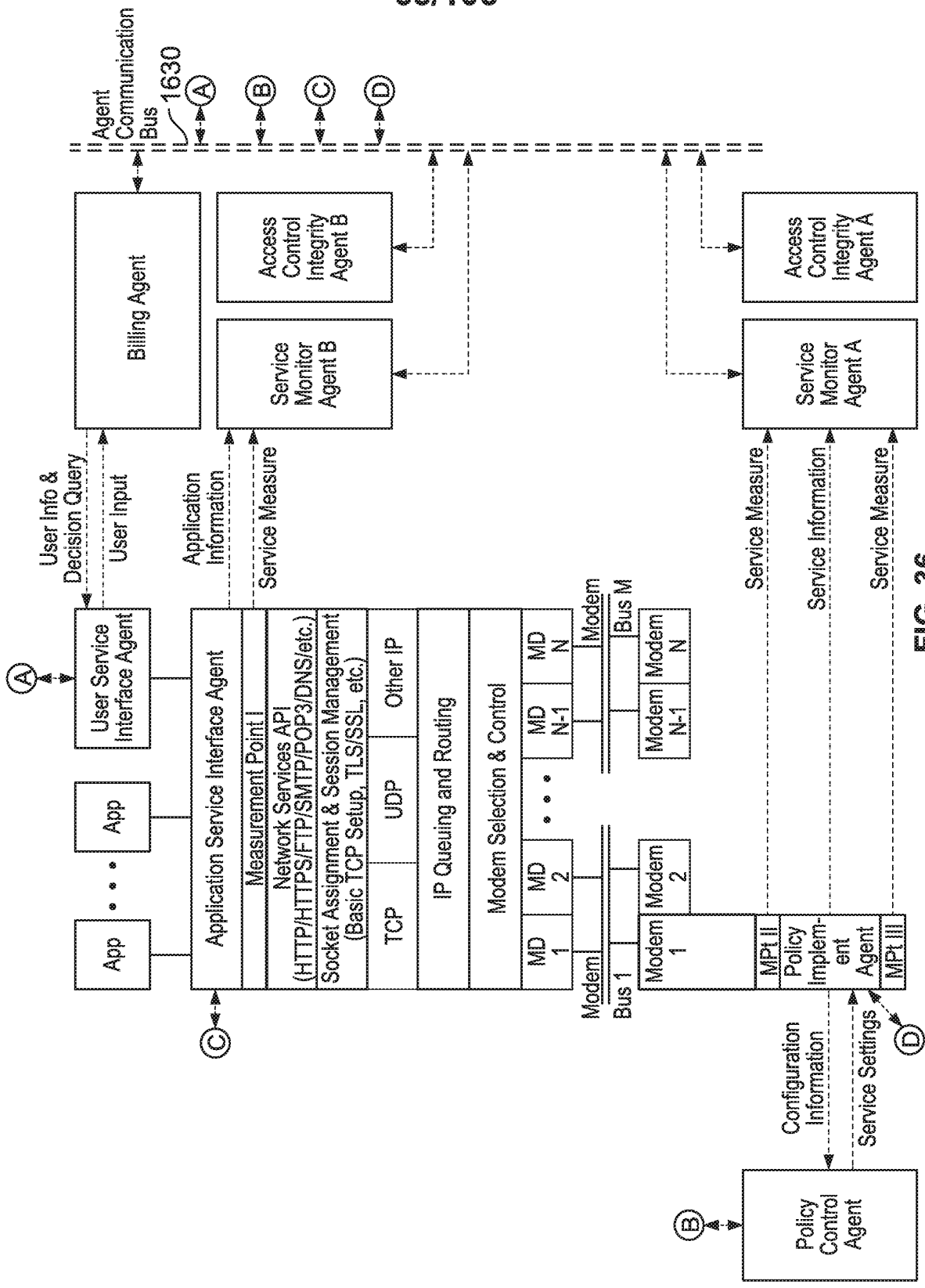

Agent Communication Bus
1630
A
B
C
D
Billing Agent
Access Control Integrity Agent B
Service Monitor Agent B
Access Control Integrity Agent A
Service Monitor Agent A
User Info & Decision Query
User Input
Application Information
Service Measure
Service Measure
Service Information
Service Measure
User Service Interface Agent
App
App
Application Service Interface Agent
Measurement Point I
Network Services API (HTTP/HTTPS/FTP/SMTP/POP3/DNS/etc.)
Socket Assignment & Session Management (Basic TCP Setup, TLS/SSL, etc.)
TCP
UDP
Other IP
IP Queuing and Routing
Modem Selection & Control
MD 1
MD 2
MD N-1
MD N
Modem Bus 1
Modem Bus M
Modem 1
Modem 2
Modem N-1
Modem N
MPt II
Policy Implem-ent Agent
MPt III
Configuration Information
Service Settings
Policy Control Agent

FIG. 36

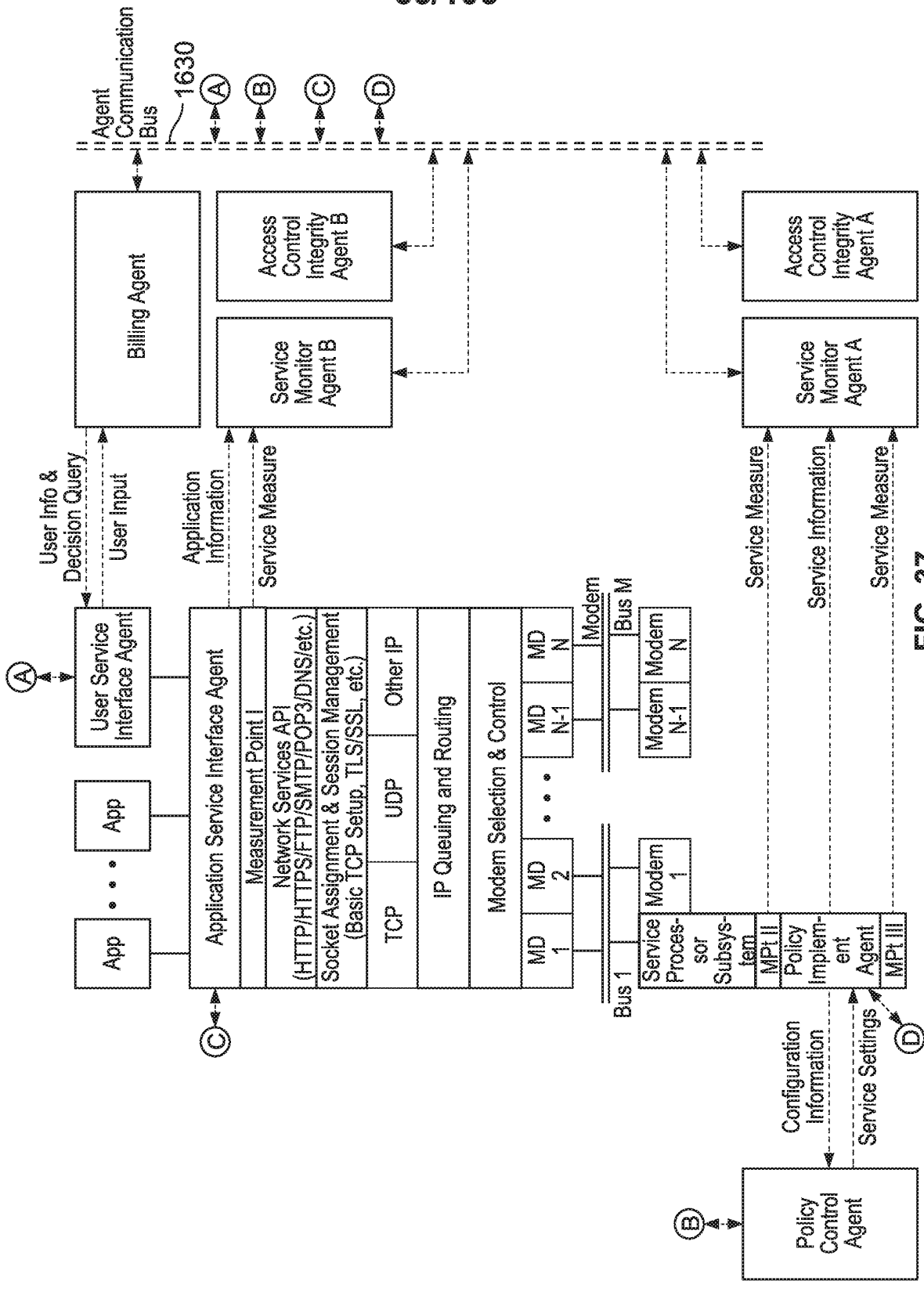

Agent Communication Bus
1630
A
B
C
D
Billing Agent
Access Control Integrity Agent B
Service Monitor Agent B
Access Control Integrity Agent A
Service Monitor Agent A
User Info & Decision Query
User Input
Application Information
Service Measure
Service Measure
Service Information
Service Measure
User Service Interface Agent
App
App
Application Service Interface Agent
Measurement Point I
Network Services API (HTTP/HTTPS/FTP/SMTP/POP3/DNS/etc.)
Socket Assignment & Session Management (Basic TCP Setup, TLS/SSL, etc.)
TCP
UDP
Other IP
IP Queuing and Routing
Modem Selection & Control
MD 1
MD 2
MD N-1
MD N
Modem
Bus 1
Bus M
Service Processor Subsystem
Modem 1
Modem N-1
Modem N
MPt II
Policy Implement Agent
MPt III
Configuration Information
Service Settings
Policy Control Agent

FIG. 37

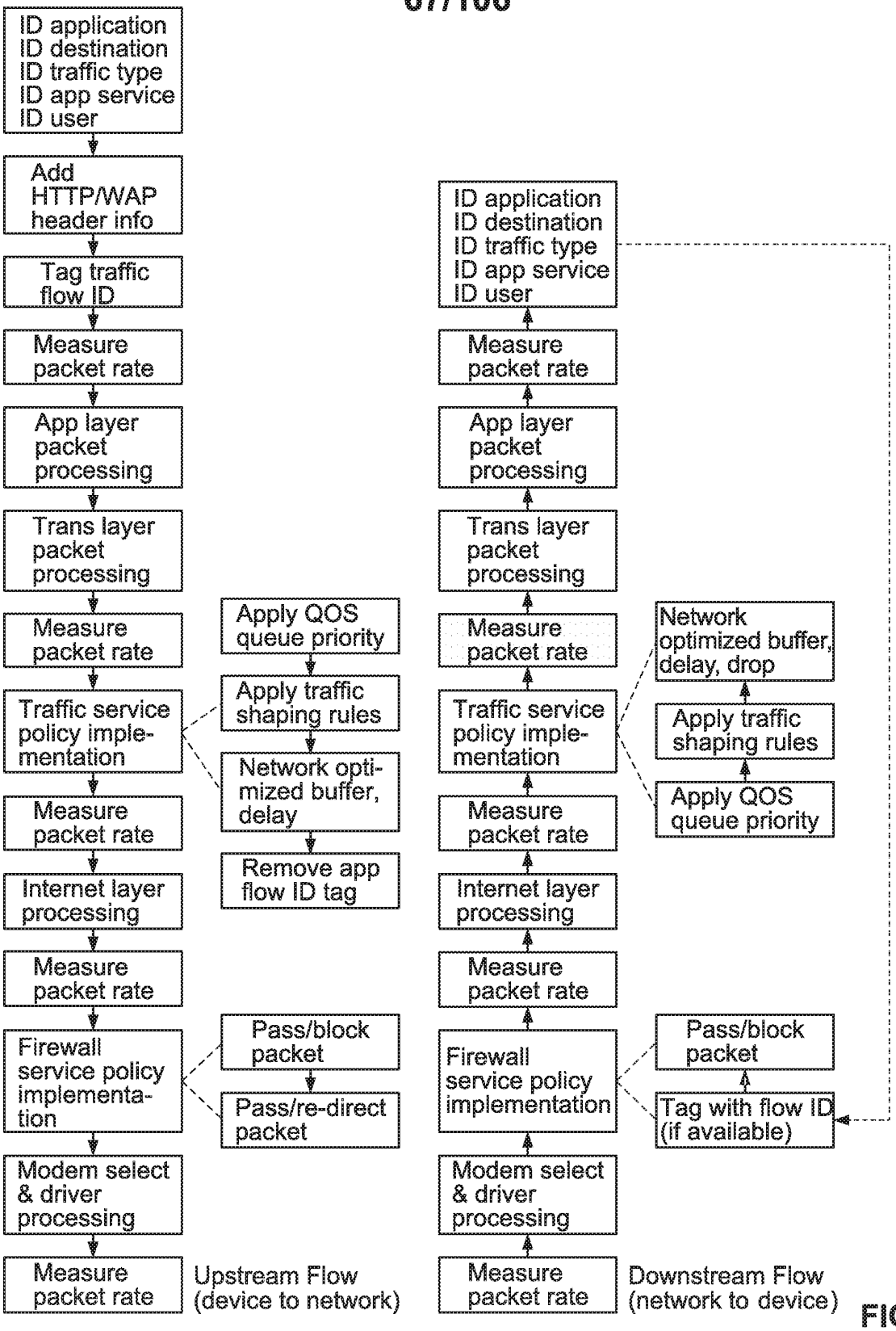

ID application
ID destination
ID traffic type
ID app service
ID user
Add HTTP/WAP header info
Tag traffic flow ID
Measure packet rate
App layer packet processing
Trans layer packet processing
Measure packet rate
Traffic service policy imple-mentation
Apply QOS queue priority
Apply traffic shaping rules
Network opti-mized buffer, delay
Remove app flow ID tag
Measure packet rate
Internet layer processing
Measure packet rate
Firewall service policy implementa-tion
Pass/block packet
Pass/re-direct packet
Modem select & driver processing
Measure packet rate
Upstream Flow (device to network)
ID application
ID destination
ID traffic type
ID app service
ID user
Measure packet rate
App layer packet processing
Trans layer packet processing
Measure packet rate
Traffic service policy imple-mentation
Network optimized buffer, delay, drop
Apply traffic shaping rules
Apply QOS queue priority
Measure packet rate
Internet layer processing
Measure packet rate
Firewall service policy implementation
Pass/block packet
Tag with flow ID (if available)
Modem select & driver processing
Measure packet rate
Downstream Flow (network to device)

FIG. 38

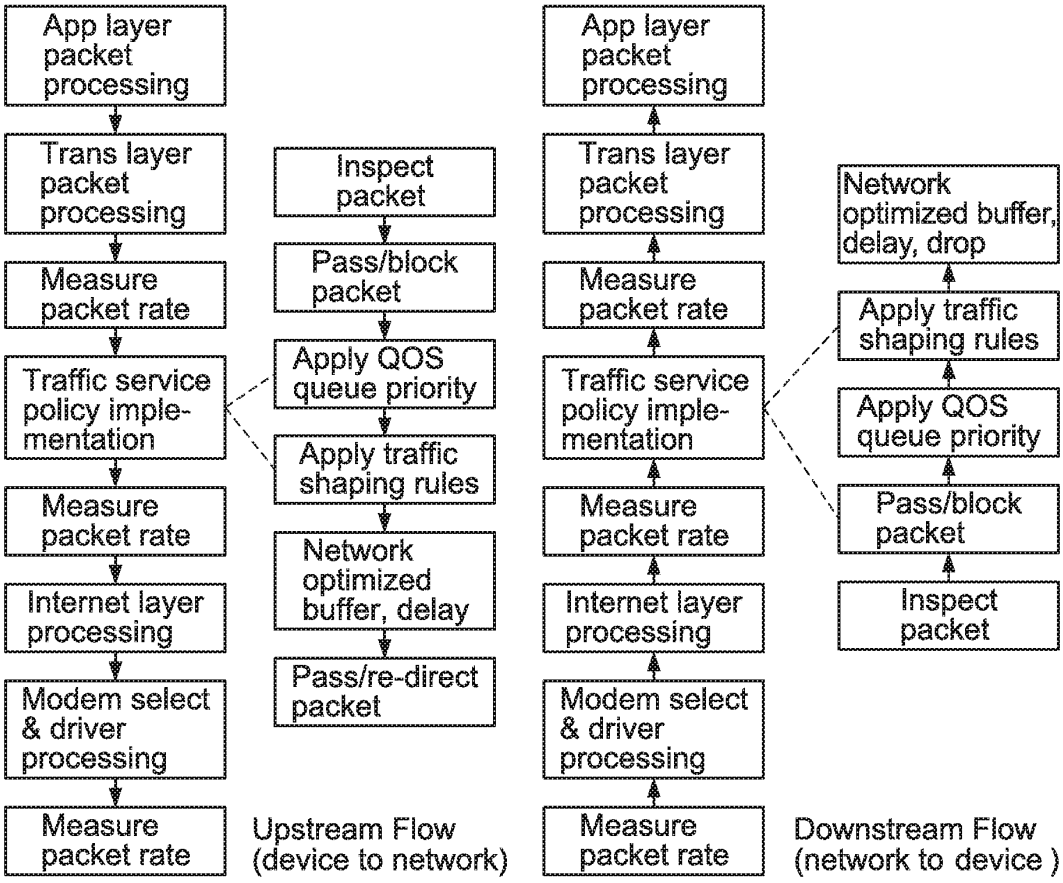

App layer packet processing
Trans layer packet processing
Measure packet rate
Traffic service policy imple-mentation
Measure packet rate
Internet layer processing
Modem select & driver processing
Measure packet rate
Upstream Flow (device to network)
Inspect packet
Pass/block packet
Apply QOS queue priority
Apply traffic shaping rules
Network optimized buffer, delay
Pass/re-direct packet
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
Inspect packet

FIG. 39

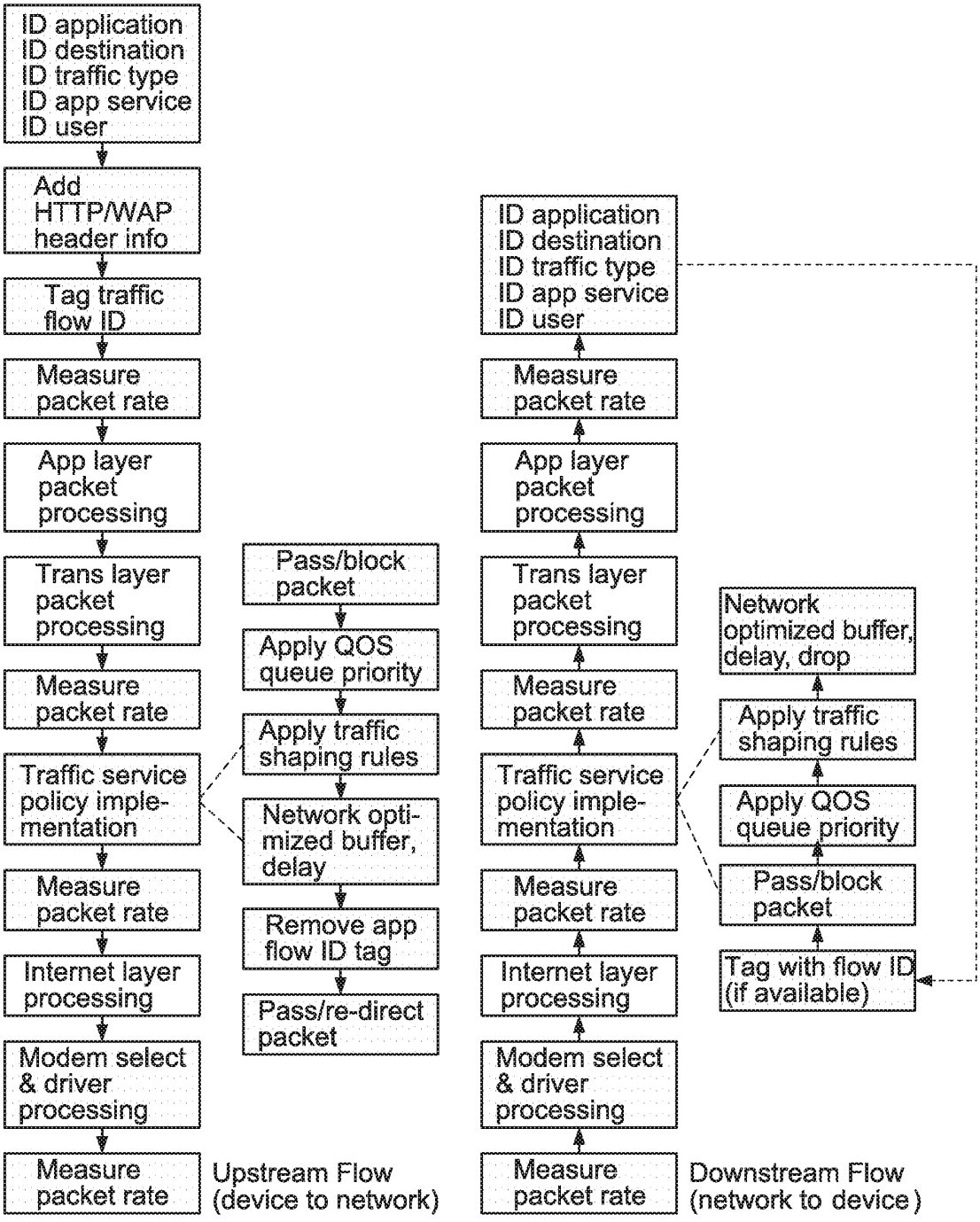

ID application
ID destination
ID traffic type
ID app service
ID user
Add HTTP/WAP header info
Tag traffic flow ID
Measure packet rate
App layer packet processing
Trans layer packet processing
Measure packet rate
Traffic service policy imple-mentation
Measure packet rate
Internet layer processing
Modem select & driver processing
Measure packet rate
Upstream Flow (device to network)
Pass/block packet
Apply QOS queue priority
Apply traffic shaping rules
Network opti-mized buffer, delay
Remove app flow ID tag
Pass/re-direct packet
ID application
ID destination
ID traffic type
ID app service
ID user
Measure packet rate
App layer packet processing
Trans layer packet processing
Measure packet rate
Traffic service policy imple-mentation
Measure packet rate
Internet layer processing
Modem select & driver processing
Measure packet rate
Downstream Flow (network to device)
Network optimized buffer, delay, drop
Apply traffic shaping rules
Apply QOS queue priority
Pass/block packet
Tag with flow ID (if available)

FIG. 40

Example Device CRM Data Collection and Reporting Classification	Partial Description	Example Sensitivity Level Classification	Example Authorization Level to Include in Report
Basic non-specific service usage parameters	User sensitive information is filtered from this report which is used for purposes such as service control, service control integrity monitoring or network traffic analysis.	Low	None
Service billing events or service plan selection events	Documents user selection process from service plan selection or billing options.	Low	Customer authorization with basic service agreement or enterprise agreement
Transaction billing events	Documents user selection process from service plan selection or billing options.	Low	Customer authorization with central billing agreement or enterprise agreement
Device location – customer location based service assist	Reports customer location for the purpose of assisting with location based services such as directions, yellow pages, shopping and social networking.	High	Customer authorization with basic service agreement or enterprise agreement
Device location – device or people tracking	Reports customer location for the purpose of providing tracking services for the device or the user.	High	Customer authorization with separate device tracking service agreement or enterprise agreement
Transaction associated information	Reports customer information such as networking activity, location, advertising usage, shopping behavior that is associated with a commerce transaction or happens around the same time as the transaction.	High	Customer authorization – potential service discount or upgrade or enterprise agreement
URL history	Reports customer web surfing history.	High	Customer authorization – potential service discount or upgrade or enterprise agreement
Served and visited advertisement history	Reports the advertisements served to the user or which advertisements the user responded to. This information may be used to determine customer preferences or for a revenue sharing relationship with the advertisers.	Medium	Customer authorization – potential service discount, perk or upgrade or enterprise agreement
911 Service usage and location trace log	This log contains all information pertinent to emergency service personnel responding to a 911 call or other emergency situation. In some embodiments this information is password protected and generally not available to the service provider unless it happens to also be contained in reports authorized by the consumer as in the examples above.	Very High	Available only for 911 support or enterprise agreement

FIG. 41

EX1002 - Page 81

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.

FIG. 42A

EX1002 - Page 82

Analyze traffic	Provides capability resident on the device to analyze device or user traffic statistics to determine how to implement adaptive policy control or how best to assist the user with notification messages. In some embodiments it is important to perform traffic analysis locally on the device to reduce network chatter with the Control Processor or to maintain user CRM privacy levels by not sharing sensitive raw traffic usage history needed to determine implementation of less sensitive service control policies. Typical but non-exhaustive examples of command usage are analyzing traffic usage statistics or patterns to determine compliance with service plan limits; analyzing traffic usage statistics or patterns to determine likely future compliance with service plan limits; analyzing traffic statistics or patterns to categorize usage according to network address identifiers, applications, content types, network types or central providers; analyzing traffic demand vs. usage statistics or patterns to determine if user may be better served with another service plan; analyzing traffic statistics or patterns to identify potential tamper threats. This command may be implemented in instantaneous policy implementation mode or adaptive policy control mode, but adaptive application of the analysis results is typically associated with adaptive policy control mode.	Authorization to analyze traffic for local device service policy control purposes or 911 service typically may be provided for in the basic service contract. Authorization to transmit a complete or filtered version of the traffic analysis to the Service Controller typically may be provided under user selected options in the service plan contract.
Successive limitation	Provides capability to begin with one limit on access or data rate according to a set of defined service usage trigger criteria, to further limit access or data rate according to said criteria, and then to successively remove limits according to said criteria. In some embodiments this function provides for service usage that starts at a given level for one or more service aspects, but as said service aspect exhibits usage that potentially threatens an overage on service plan limits then the level of service for said service aspect is reduced successively until the threat of service plan overage is reduced or eliminated. In some embodiments, the limits on service level for said service aspect are eventually removed either all at once or successively over a specified time period or set of time periods so that the limits on service level for said service aspect are eventually removed if the service aspect is used less vigorously for a period of time. In this type of embodiment the projection for future service usage by a given service aspect is assisted by the analyze traffic statistics function. As a more specific example, the service aspect may be a URL address that is popular with the user and demands a high service consumption, and the data rate allowed to that URL may start at a relatively high level when the user first begins to surf and as long as the surfing session is finished quickly there is never a reduction in service level, but if the user surfs for a longer time so that service usage begins to threaten plan limit overage, the data rate allowed to that URL is successively reduced the longer the surfing session occurs. Continuing this	Authorization to limit data rate for all traffic or a subset of traffic typically may be provided in the options the user specifies for how to limit potential or actual service plan usage or cost overages. For example, one user may choose to have no limits and be notified when service usage is over or about to go over, while another user may choose to allow traffic control sufficient to keep service usage under the service plan limit without any notification.

FIG. 42B

	example embodiment, if the URL is not visited for a defined period of time then the data rate limitation may be removed in steps over multiple pre-defined time periods, or may be removed all at once back to the initial data rate established in the service policy for that URL. Other specific embodiment examples include email download or upload data rate; download or upload rates for certain types of file transfers; or download or upload rates for a given network access technology or central provider. This command is associated with adaptive policy control mode for the Service Processor. In more advanced adaptive embodiments, the policy control system first identifies those service aspects that are consuming a large percentage of the service usage and then begins to successively limit service level only for these highest usage service aspects so that all other service aspects that are not responsible for potential service plan limit overage continue to receive relatively high service levels. In another embodiment, some high usage service aspects may be exempt or partially exempt from limitations in service level, as for example a service aspect that is associated with a secondary source of service or transaction payment or that may be separately accounted for in the service plan usage reporting.	
Limit email file transfers	Sets and enforces limits on email downloads. In some embodiments this can include use of the successively limit functionality. In some embodiments, this is accomplished by identifying specific email downloads or uploads and controlling traffic for those traffic flows. In other embodiments, this includes interacting with the email application to set download or upload file settings. This functionality may be implemented in instantaneous policy implementation mode or adaptive policy control mode, with the more advanced functionality such as successive limitation on email file transfers being implemented in the adaptive policy control mode.	Authorization to limit data rate for all traffic or a subset of traffic typically may be provided in the options the user specifies for how to limit potential or actual service plan usage or cost overages. For example, one user may choose to have no limits and be notified when service usage is over or about to go over, while another user may choose to allow traffic control sufficient to keep service usage under the service plan limit without any notification.
Seek to manage below service limit	Implements adaptive policy control in an attempt to manage service usage to reduce service plan limit overages. In some embodiments there are successive limits on service level for overall traffic, or for the highest usage service aspects, with the successive limits being lowered until average service usage is projected to be below service plan limits. The algorithms that may be applied to achieve this adaptive service level limitation are quite varied and only a few are given here. In one embodiment, the service usage for the service plan period is projected using the analyze traffic functionality, and overall device data rate is successively limited until service usage is projected to be below the service plan limit. In another	Same as above.

FIG. 42C

EX1002 - Page 84

	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

EX1002 - Page 85

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.

FIG. 42E

EX1002 - Page 86

Limit access likely to cause overage and notify	Uses the project service usage functionality to determine if the service usage is projected to go beyond the service plan limit, if the service usage is projected to go over the service limit, notifies the user that limits are being applied to keep service usage or cost under the service limit, applies limits to various aspects of service usage to bring down usage so that projections are within service limits. In one embodiment, the seek to manage below service limit functionality is used.	Authorization to limit data rate for all traffic or a subset of traffic typically may be provided in the options the user specifies for how to limit potential or actual service plan usage or cost overages. For example, one user may choose to have no limits and be notified when service usage is over or about to go over, while another user may choose to allow traffic control sufficient to keep service usage under the service plan limit without any notification.
Require acknowledgm-ent of notification	Requires the user to acknowledge a notification of potential service or cost overage or a notification of an option to limit the service overage or cost of service overage.	Provided for in the basic service agreement.
Log or report acknowledgm-ent of notification	In some embodiments, the user acknowledgment of notification is stored, or sent to the Service Controller, or stored and later sent to the service Controller.	Same as above.
Notify user of service plan options prior to running over service usage limit	Notifies the user of options to extend the service plan limit before reaching the service plan limit. In some embodiments, accepts user input on which service plan extension option if any the user wishes to accept. In some embodiments, notifies the billing system when the user has accepted a service plan extension option.	Same as above.
Notify user of service plan options after running over service usage limit	Notifies the user of options to extend the service plan limit after reaching the service plan limit. In some embodiments, accepts user input on which service plan extension option if any the user wishes to accept. In some embodiments, notifies the billing system when the user has accepted a service plan extension option.	Same as above.
Time of day variations	Each of the functionalities for traffic control, service cost, service limits may be modified with a time of day variation so that the values used are different for different times of day.	Same as above.

FIG. 42F

EX1002 - Page 87

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.

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

EX1002 - Page 89

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.

FIG. 42I

EX1002 - Page 90

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.

FIG. 42J

Service Processor Authorization

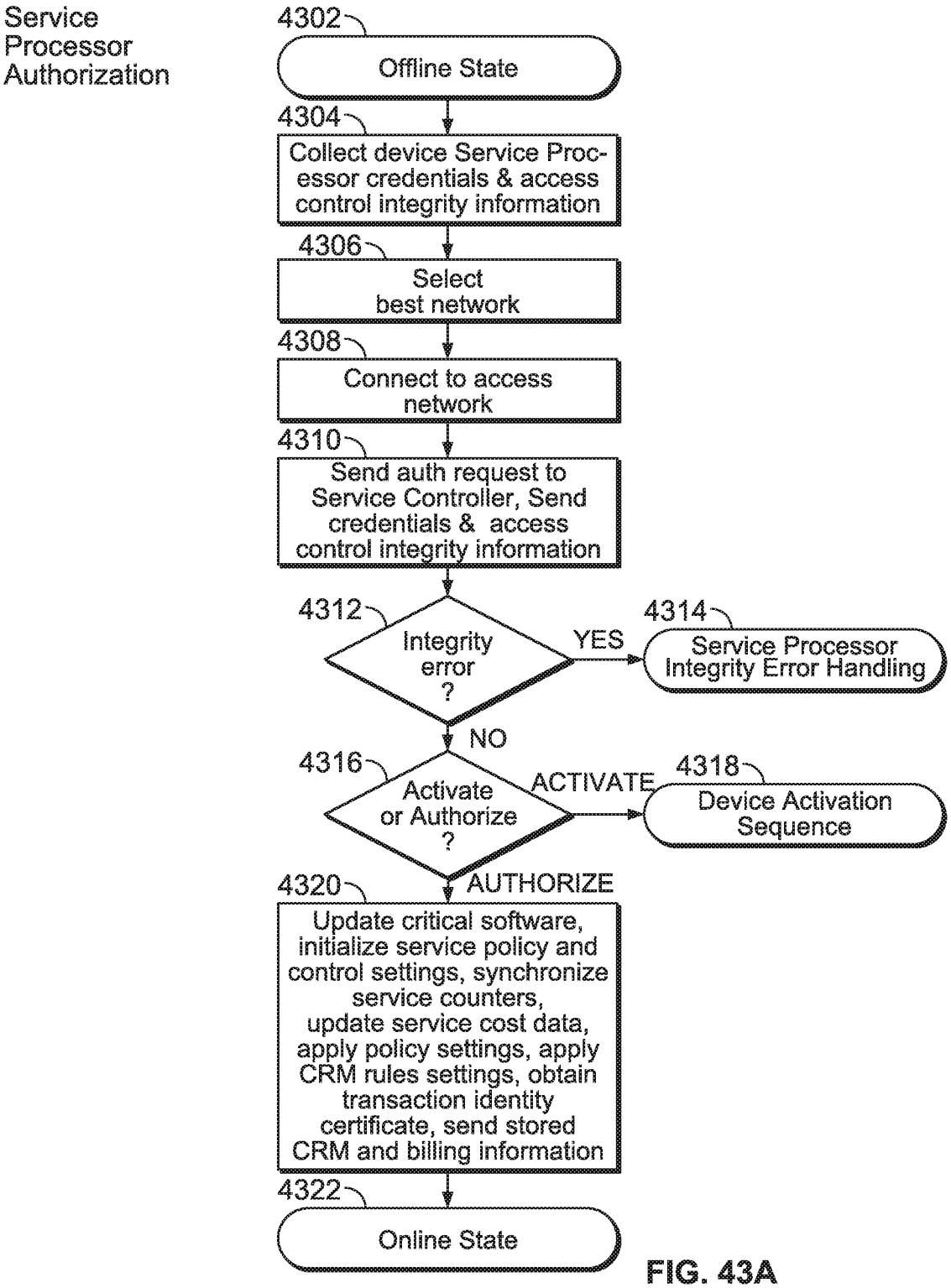


FIG. 43A

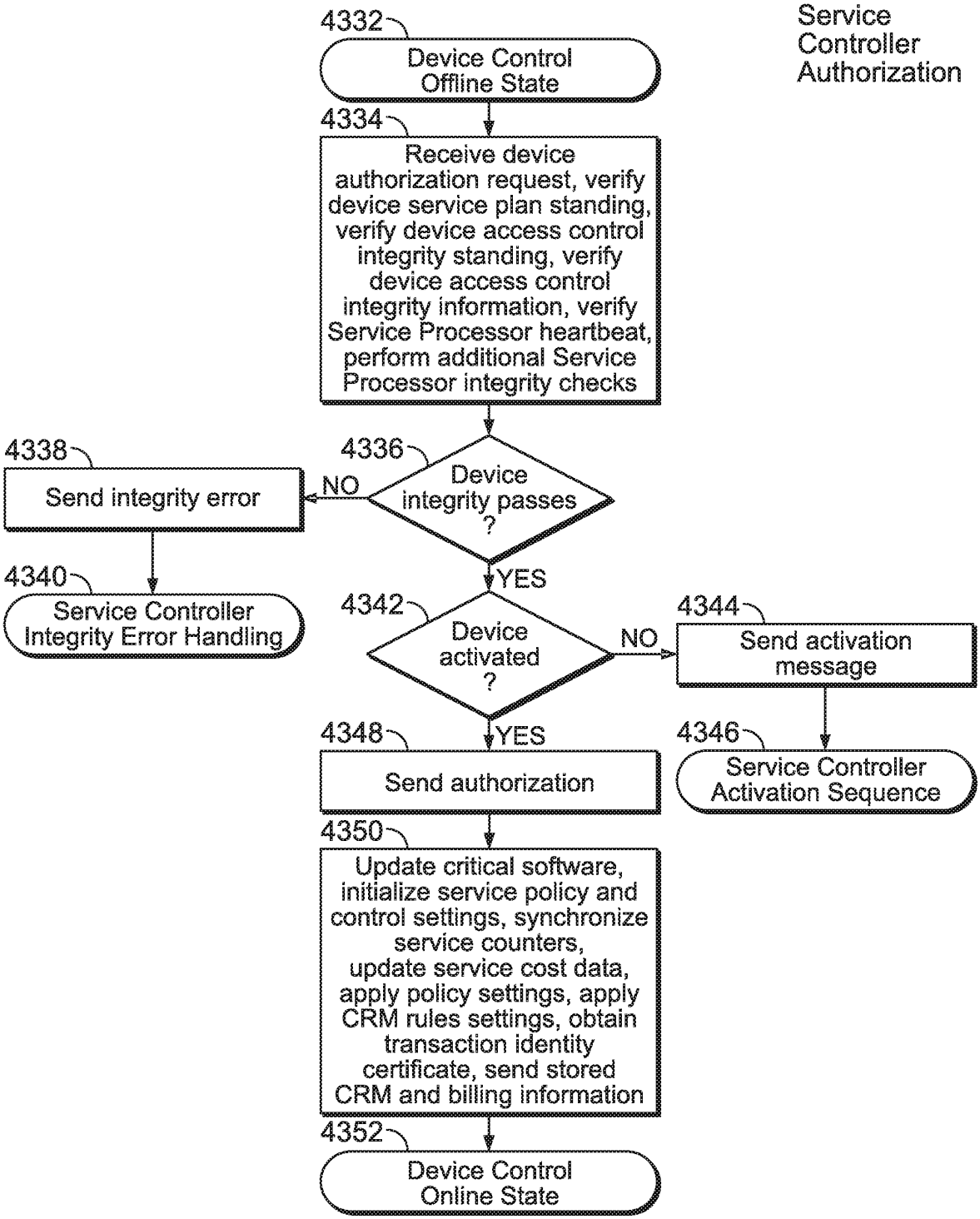

Service Controller Authorization
4332
Device Control Offline State
4334
Receive device authorization request, verify device service plan standing, verify device access control integrity standing, verify device access control integrity information, verify Service Processor heartbeat, perform additional Service Processor integrity checks
4336
Device integrity passes ?
NO
4338
Send integrity error
4340
Service Controller Integrity Error Handling
YES
4342
Device activated ?
NO
4344
Send activation message
4346
Service Controller Activation Sequence
YES
4348
Send authorization
4350
Update critical software, initialize service policy and control settings, synchronize service counters, update service cost data, apply policy settings, apply CRM rules settings, obtain transaction identity certificate, send stored CRM and billing information
4352
Device Control Online State

FIG. 43B

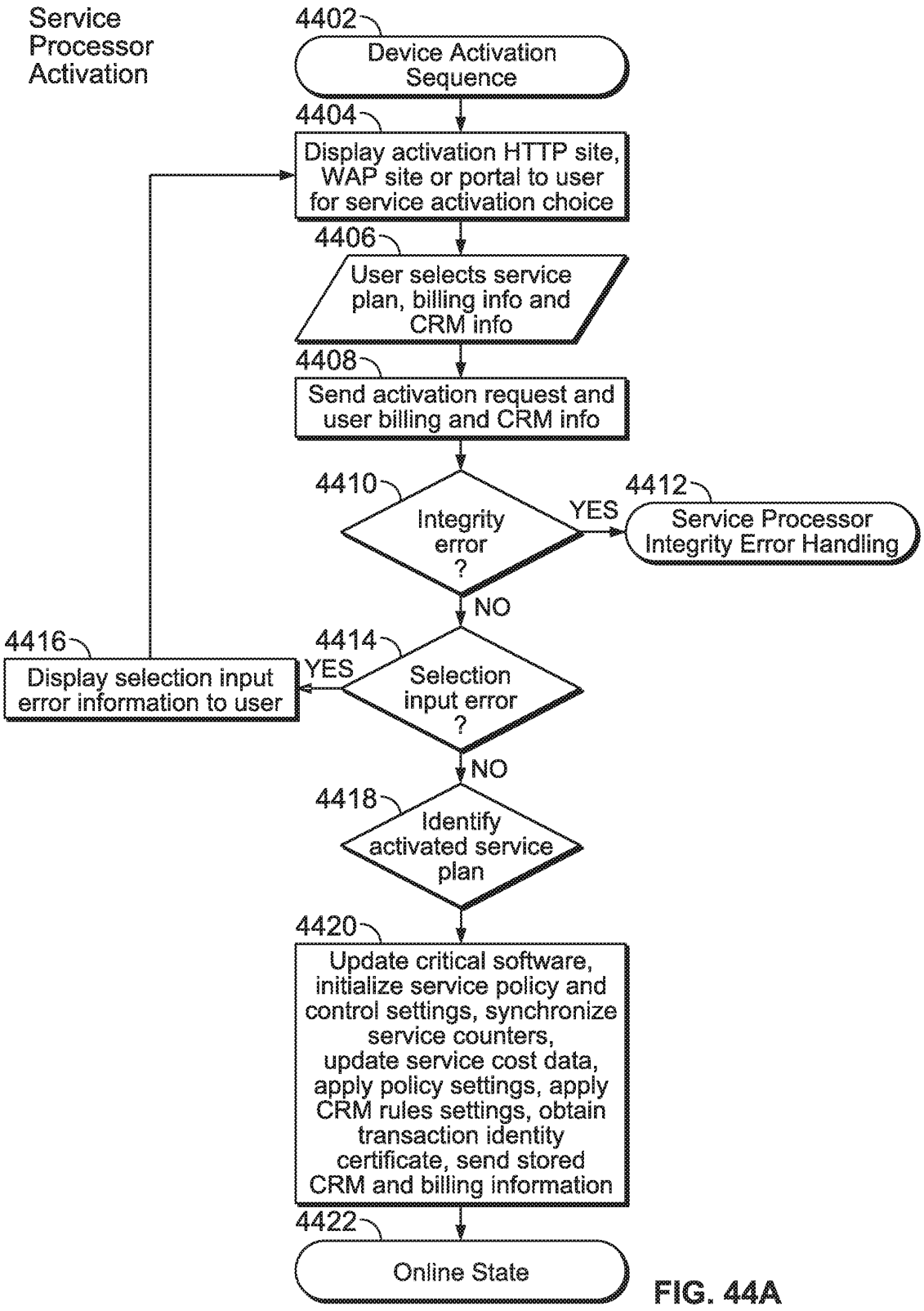

Service Processor Activation
4402
Device Activation Sequence
4404
Display activation HTTP site, WAP site or portal to user for service activation choice
4406
User selects service plan, billing info and CRM info
4408
Send activation request and user billing and CRM info
4410
Integrity error ?
YES
4412
Service Processor Integrity Error Handling
NO
4414
Selection input error ?
YES
4416
Display selection input error information to user
NO
4418
Identify activated service plan
4420
Update critical software, initialize service policy and control settings, synchronize service counters, update service cost data, apply policy settings, apply CRM rules settings, obtain transaction identity certificate, send stored CRM and billing information
4422
Online State

FIG. 44A

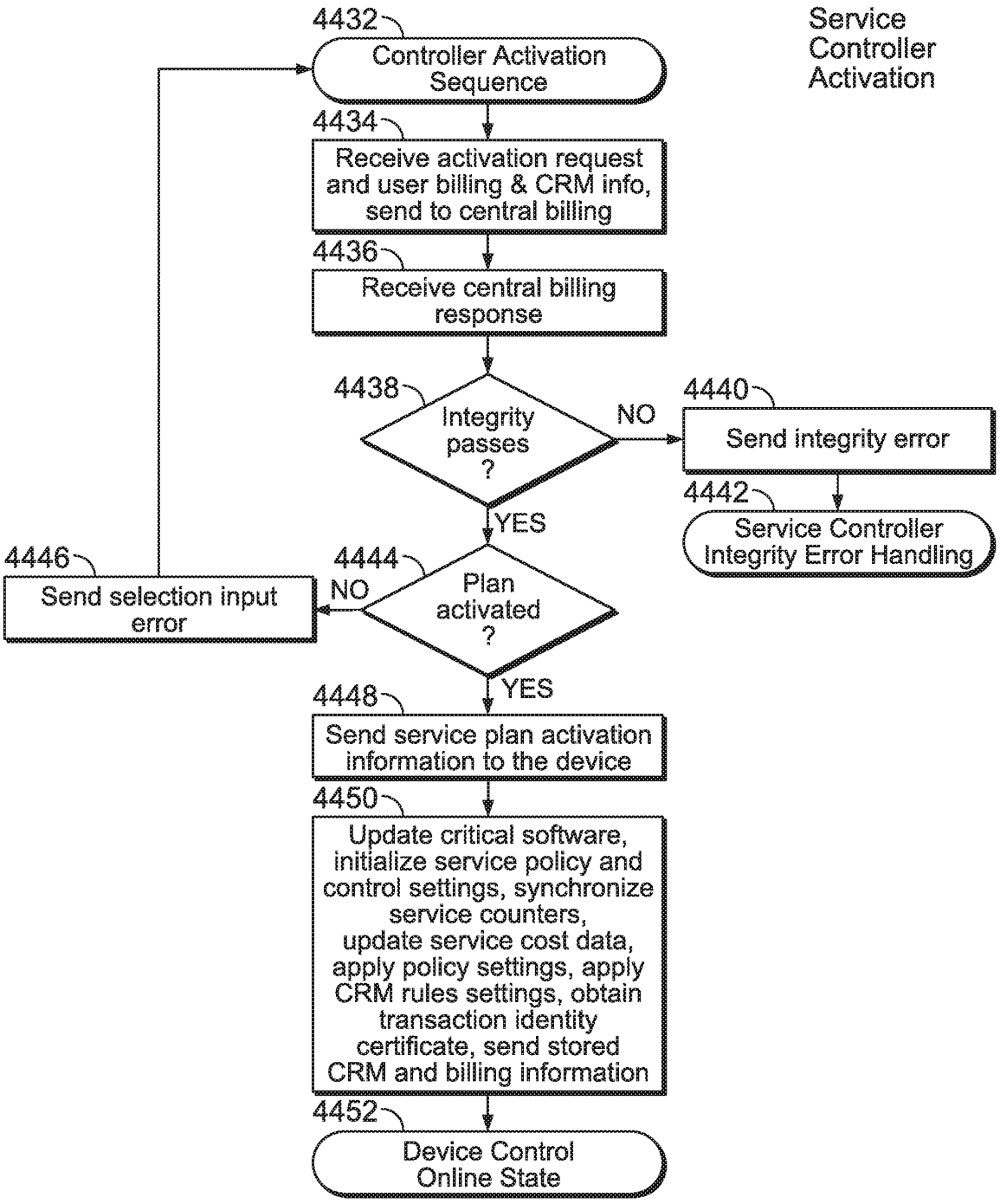

Service Controller Activation
4432
Controller Activation Sequence
4434
Receive activation request and user billing & CRM info, send to central billing
4436
Receive central billing response
4438
Integrity passes ?
NO
4440
Send integrity error
4442
Service Controller Integrity Error Handling
YES
4444
Plan activated ?
NO
4446
Send selection input error
YES
4448
Send service plan activation information to the device
4450
Update critical software, initialize service policy and control settings, synchronize service counters, update service cost data, apply policy settings, apply CRM rules settings, obtain transaction identity certificate, send stored CRM and billing information
4452
Device Control Online State

FIG. 44B

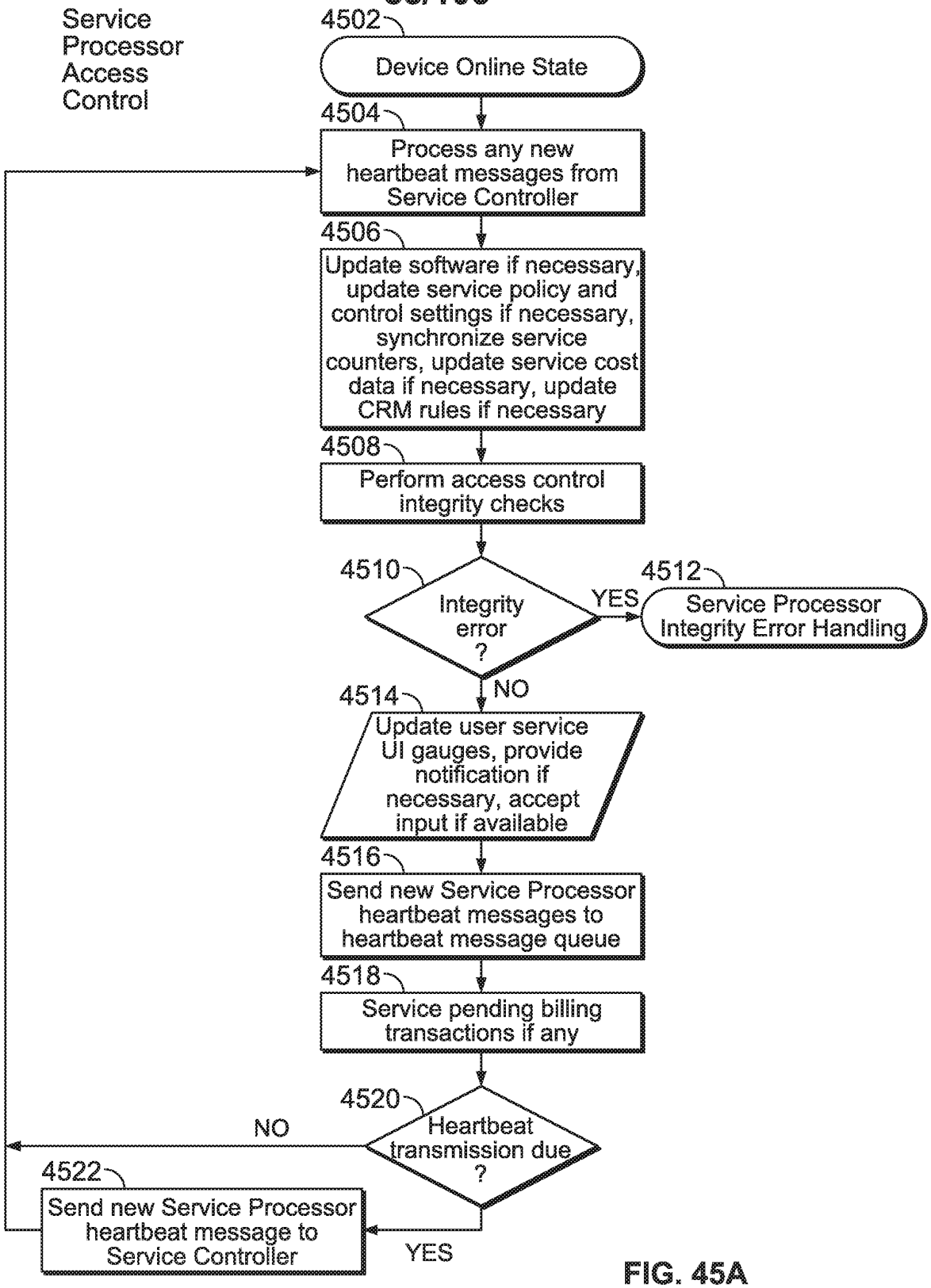

Service Processor Access Control
4502
Device Online State
4504
Process any new heartbeat messages from Service Controller
4506
Update software if necessary, update service policy and control settings if necessary, synchronize service counters, update service cost data if necessary, update CRM rules if necessary
4508
Perform access control integrity checks
4510
Integrity error ?
YES
4512
Service Processor Integrity Error Handling
NO
4514
Update user service UI gauges, provide notification if necessary, accept input if available
4516
Send new Service Processor heartbeat messages to heartbeat message queue
4518
Service pending billing transactions if any
4520
Heartbeat transmission due ?
NO
YES
4522
Send new Service Processor heartbeat message to Service Controller

FIG. 45A

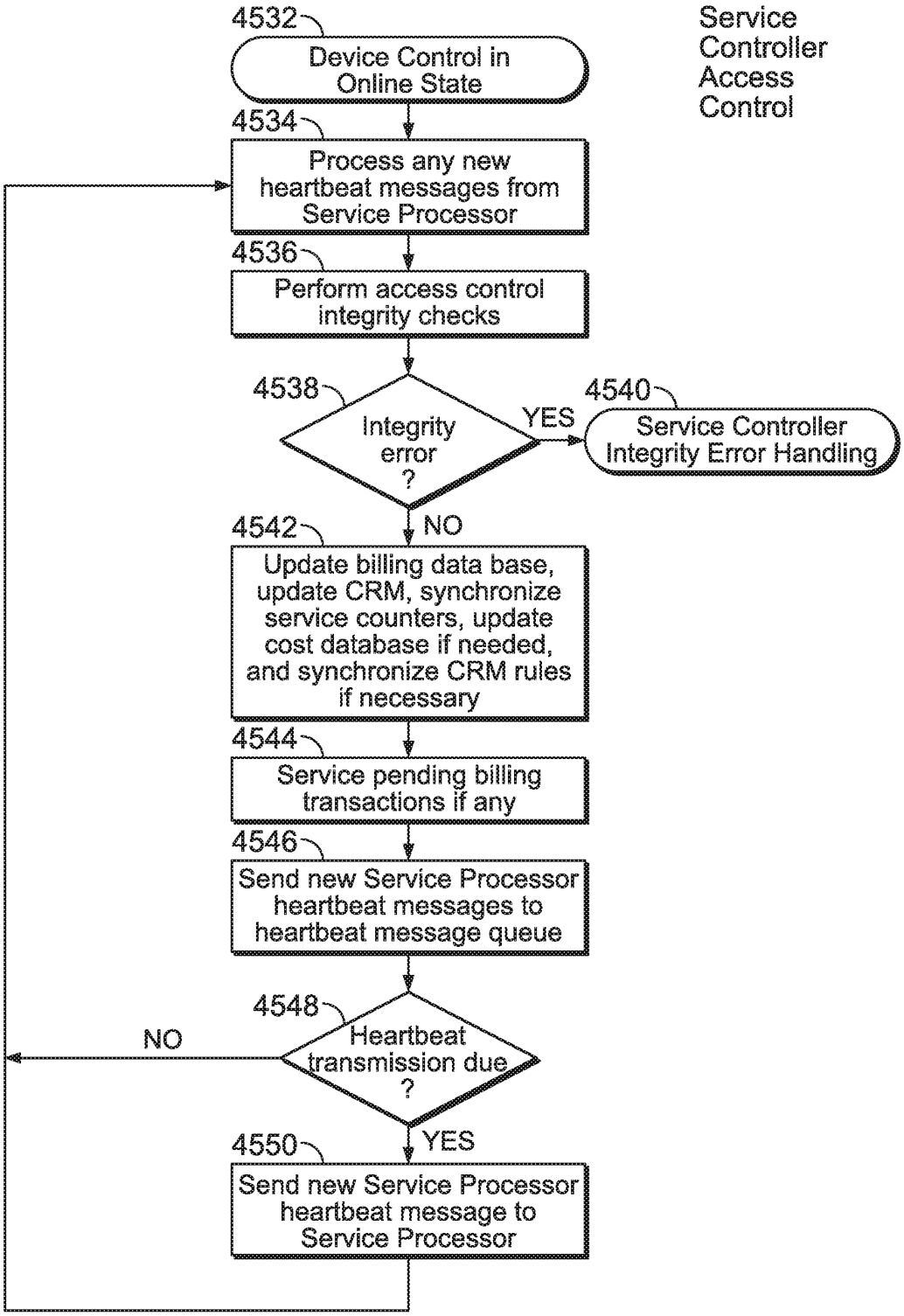

Service Controller Access Control
4532
Device Control in Online State
4534
Process any new heartbeat messages from Service Processor
4536
Perform access control integrity checks
4538
Integrity error ?
YES
4540
Service Controller Integrity Error Handling
NO
4542
Update billing data base, update CRM, synchronize service counters, update cost database if needed, and synchronize CRM rules if necessary
4544
Service pending billing transactions if any
4546
Send new Service Processor heartbeat messages to heartbeat message queue
4548
Heartbeat transmission due ?
NO
YES
4550
Send new Service Processor heartbeat message to Service Processor

FIG. 45B

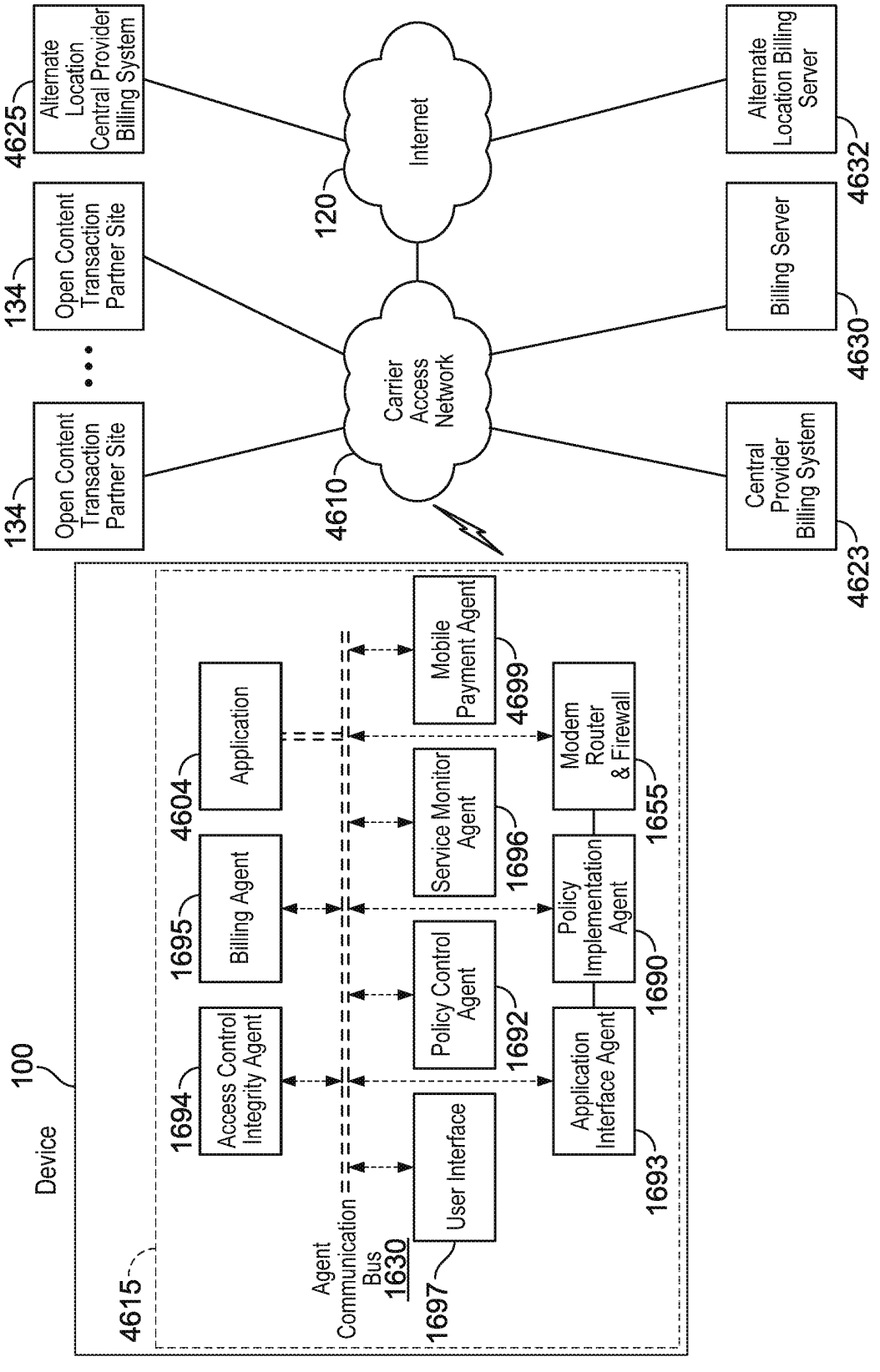

Alternate Location Central Provider Billing System
4625
Open Content Transaction Partner Site
134
Open Content Transaction Partner Site
134
Internet
120
Carrier Access Network
4610
Alternate Location Billing Server
4632
Billing Server
4630
Central Provider Billing System
4623
Device
100
4615
Agent Communication Bus
1630
User Interface
1697
Access Control Integrity Agent
1694
Billing Agent
1695
Application
4604
Policy Control Agent
1692
Service Monitor Agent
1696
Mobile Payment Agent
4699
Application Interface Agent
1693
Policy Implementation Agent
1690
Modem Router & Firewall
1655

FIG. 46

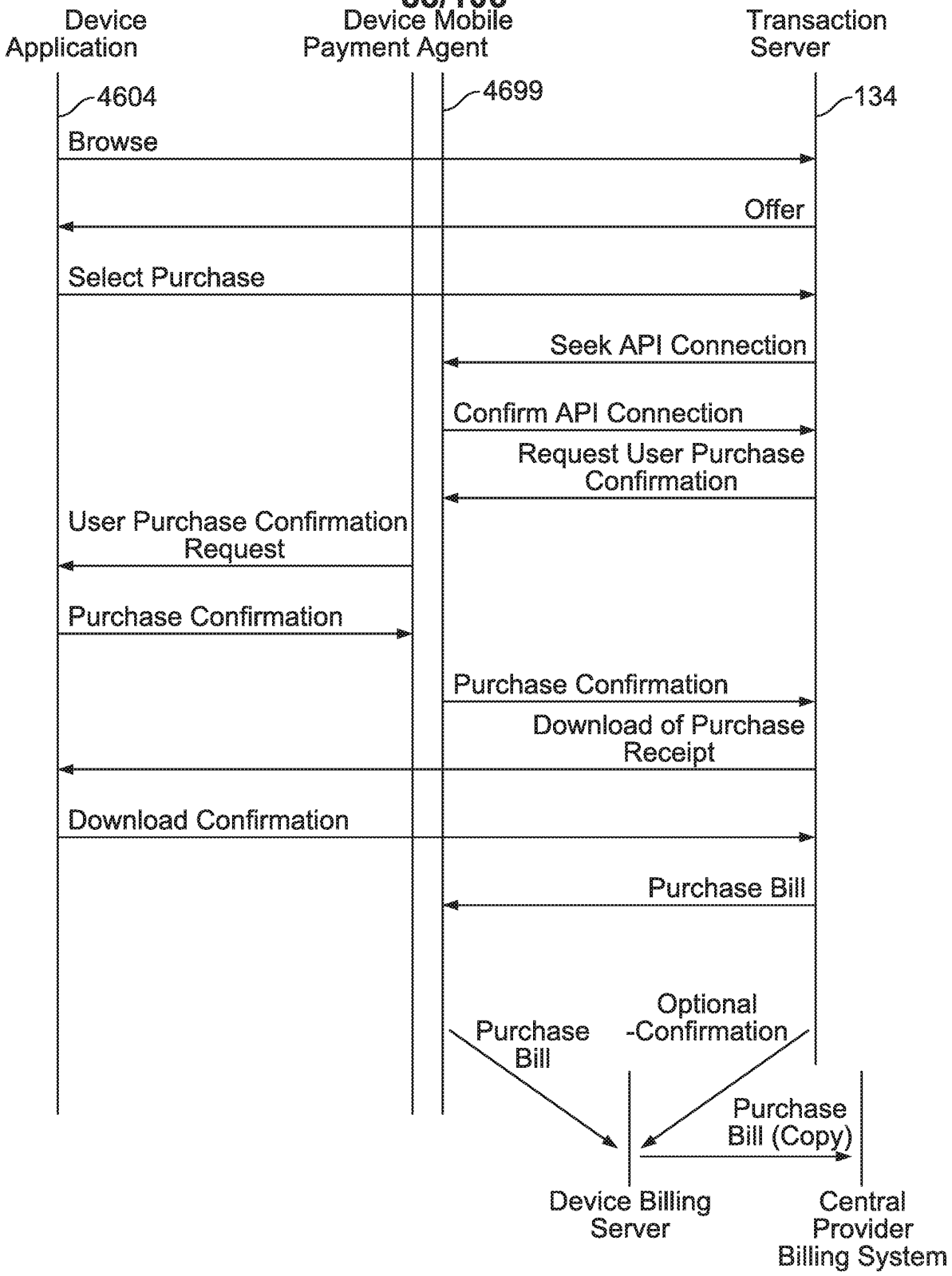

Device Application
Device Mobile Payment Agent
Transaction Server
4604
4699
134
Browse
Offer
Select Purchase
Seek API Connection
Confirm API Connection
Request User Purchase Confirmation
User Purchase Confirmation Request
Purchase Confirmation
Purchase Confirmation
Download of Purchase Receipt
Download Confirmation
Purchase Bill
Optional -Confirmation
Purchase Bill
Purchase Bill (Copy)
Device Billing Server
Central Provider Billing System

FIG. 47A

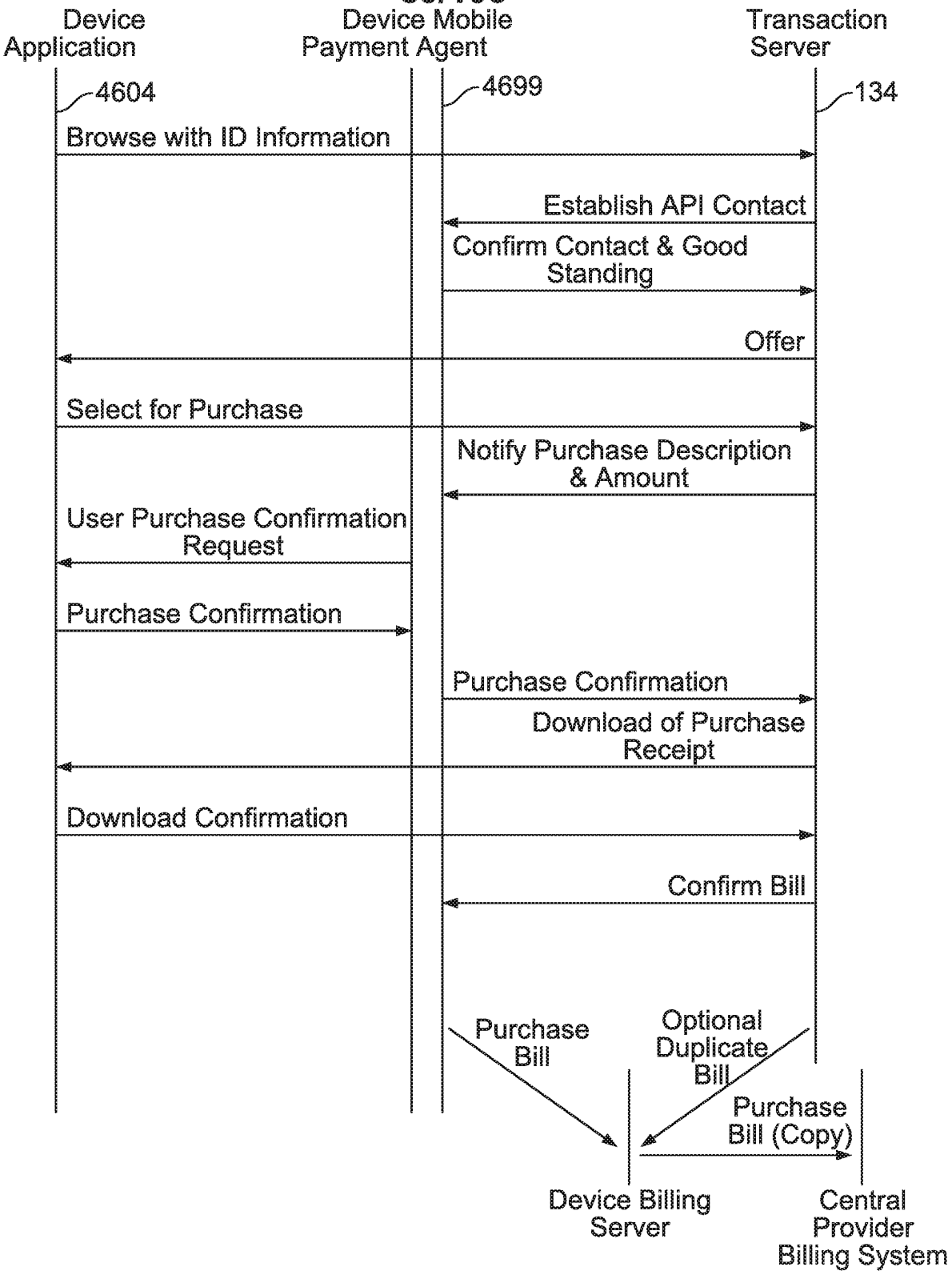

Device Application
Device Mobile Payment Agent
Transaction Server
4604
4699
134
Browse with ID Information
Establish API Contact
Confirm Contact & Good Standing
Offer
Select for Purchase
Notify Purchase Description & Amount
User Purchase Confirmation Request
Purchase Confirmation
Purchase Confirmation
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

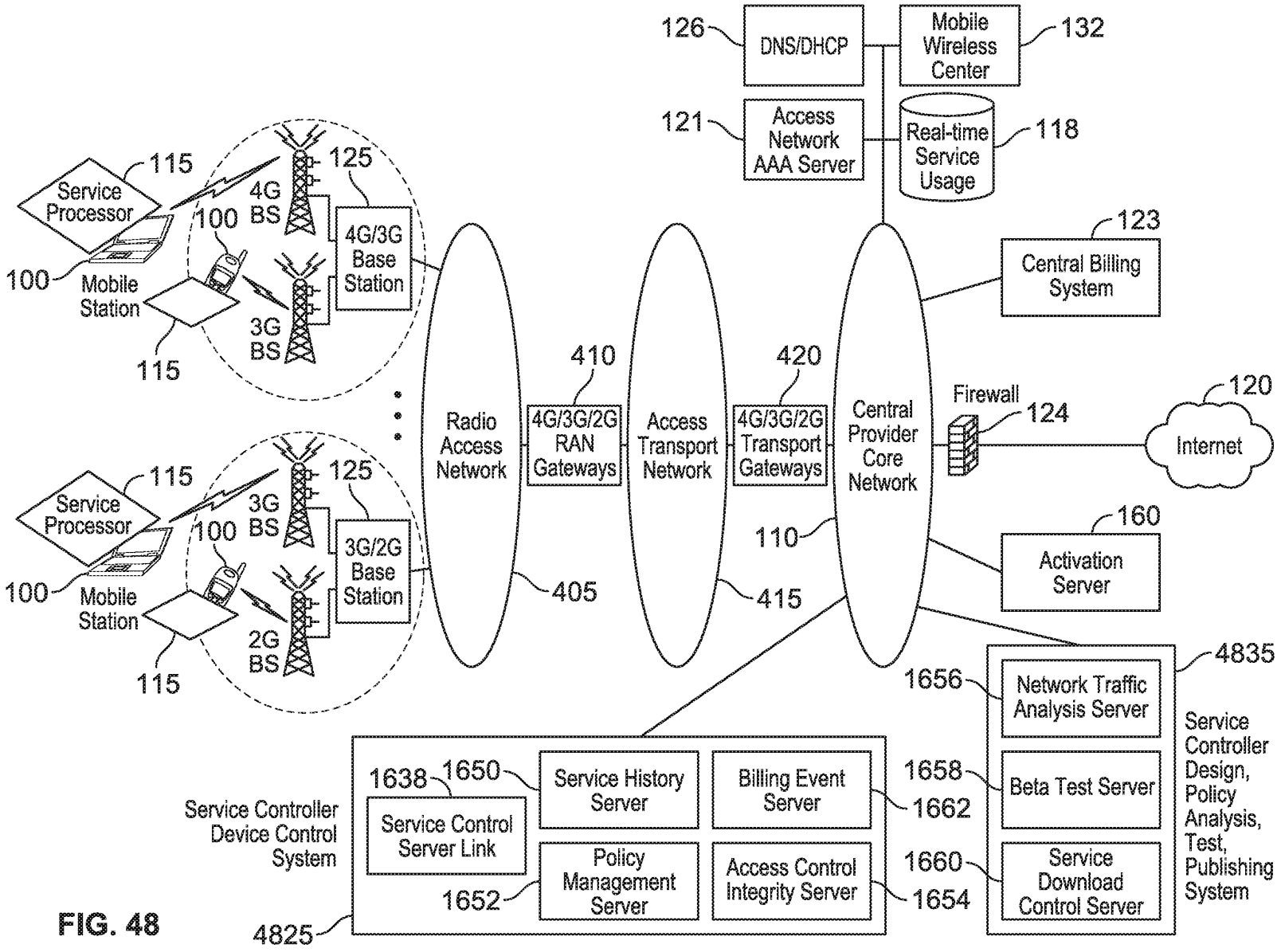

126
DNS/DHCP
Mobile Wireless Center
132
121
Access Network AAA Server
Real-time Service Usage
118
123
Central Billing System
115
Service Processor
100
Mobile Station
4G BS
125
4G/3G Base Station
3G BS
410
420
Radio Access Network
4G/3G/2G RAN Gateways
Access Transport Network
4G/3G/2G Transport Gateways
Central Provider Core Network
Firewall
124
120
Internet
90/106
3G BS
3G/2G Base Station
2G BS
110
160
Activation Server
405
415
4835
1656
Network Traffic Analysis Server
Service Controller Design, Policy Analysis, Test, Publishing System
1658
Beta Test Server
1660
Service Download Control Server
1638
1650
Service History Server
Billing Event Server
1662
Service Control Server Link
Policy Management Server
Access Control Integrity Server
1652
1654
Service Controller Device Control System
4825

FIG. 48

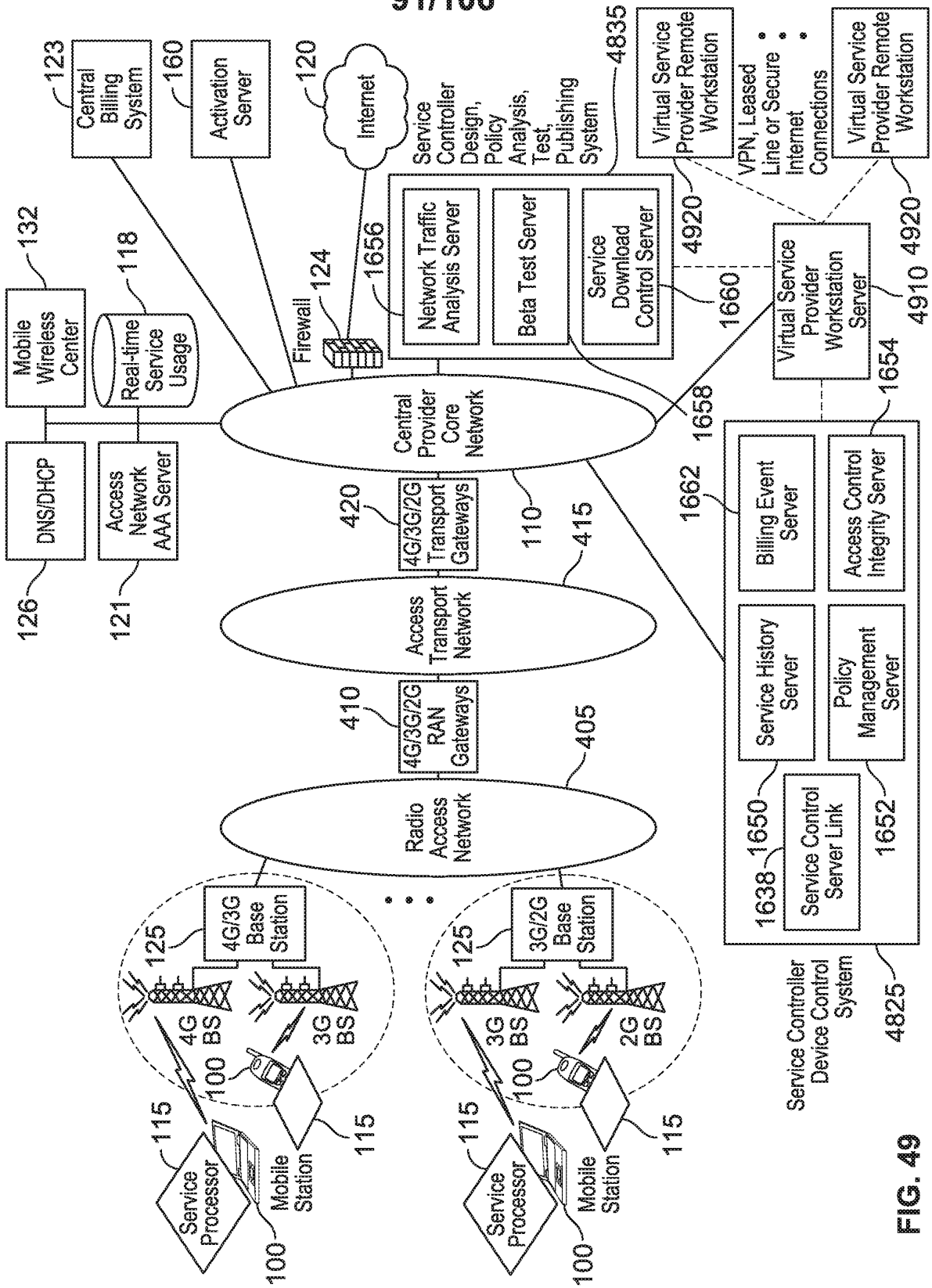

Central Billing System
123
Activation Server
160
Internet
120
Service Controller Design, Policy Analysis, Test, Publishing System
4835
Virtual Service Provider Remote Workstation
Mobile Wireless Center
132
Real-time Service Usage
118
Firewall
124
1656
Network Traffic Analysis Server
Beta Test Server
Service Download Control Server
4920
1660
VPN, Leased Line or Secure Internet Connections
Virtual Service Provider Workstation Server
4910
4920
Central Provider Core Network
1658
1654
DNS/DHCP
126
Access Network AAA Server
121
420
4G/3G/2G Transport Gateways
110
415
Billing Event Server
1662
Access Control Integrity Server
Access Transport Network
410
4G/3G/2G RAN Gateways
405
Service History Server
Policy Management Server
1650
1652
1638
Service Control Server Link
Radio Access Network
125
4G/3G Base Station
3G/2G Base Station
4G BS
3G BS
3G BS
2G BS
100
115
Service Processor
Mobile Station
Service Controller Device Control System
4825

FIG. 49

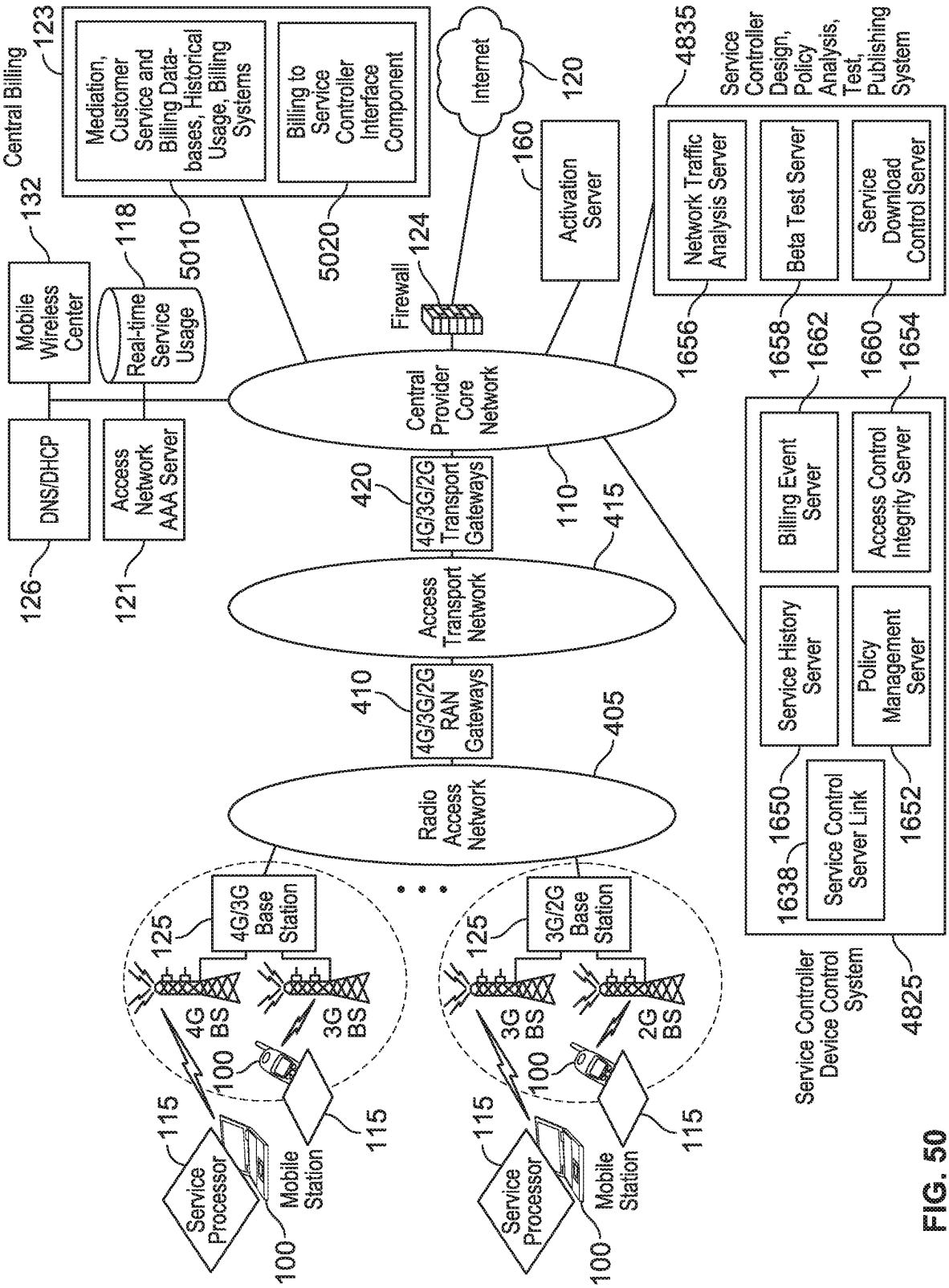

Central Billing
123
Mediation, Customer Service and Billing Data-bases, Historical Usage, Billing Systems
Billing to Service Controller Interface Component
5010
5020
Internet
120
Mobile Wireless Center
132
Real-time Service Usage
118
Firewall
124
Activation Server
160
Service Controller Design, Policy 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
4G BS
3G BS
3G/2G Base Station
3G BS
2G BS
100
115
Service Processor
Mobile Station

FIG. 50

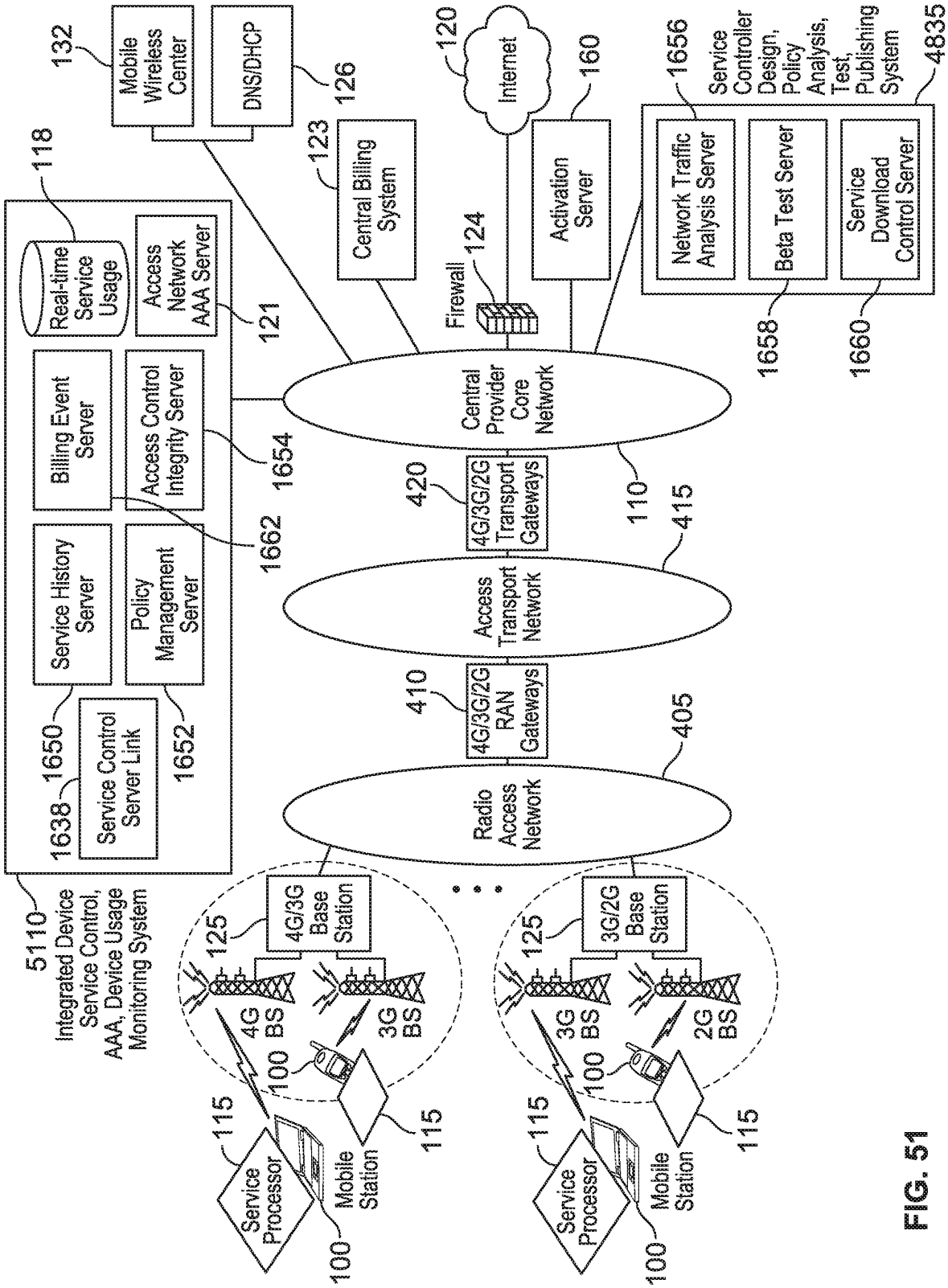

5110
Integrated Device Service Control, AAA, Device Usage Monitoring System
118
Real-time Service Usage
Service History Server
Billing Event Server
Service Control Server Link
Policy Management Server
Access Control Integrity Server
Access Network AAA Server
1638
1650
1652
1662
1654
121
132
Mobile Wireless Center
DNS/DHCP
126
123
Central Billing System
120
Internet
160
Activation Server
124
Firewall
1656
Service Controller Design, Policy Analysis, Test, Publishing System
4835
Network Traffic Analysis Server
Beta Test Server
Service Download Control Server
1658
1660
Central Provider Core Network
110
420
4G/3G/2G Transport Gateways
415
Access Transport Network
410
4G/3G/2G RAN Gateways
405
Radio Access Network
125
4G/3G Base Station
3G/2G Base Station
4G BS
3G BS
3G BS
2G BS
100
115
Service Processor
Mobile Station

FIG. 51

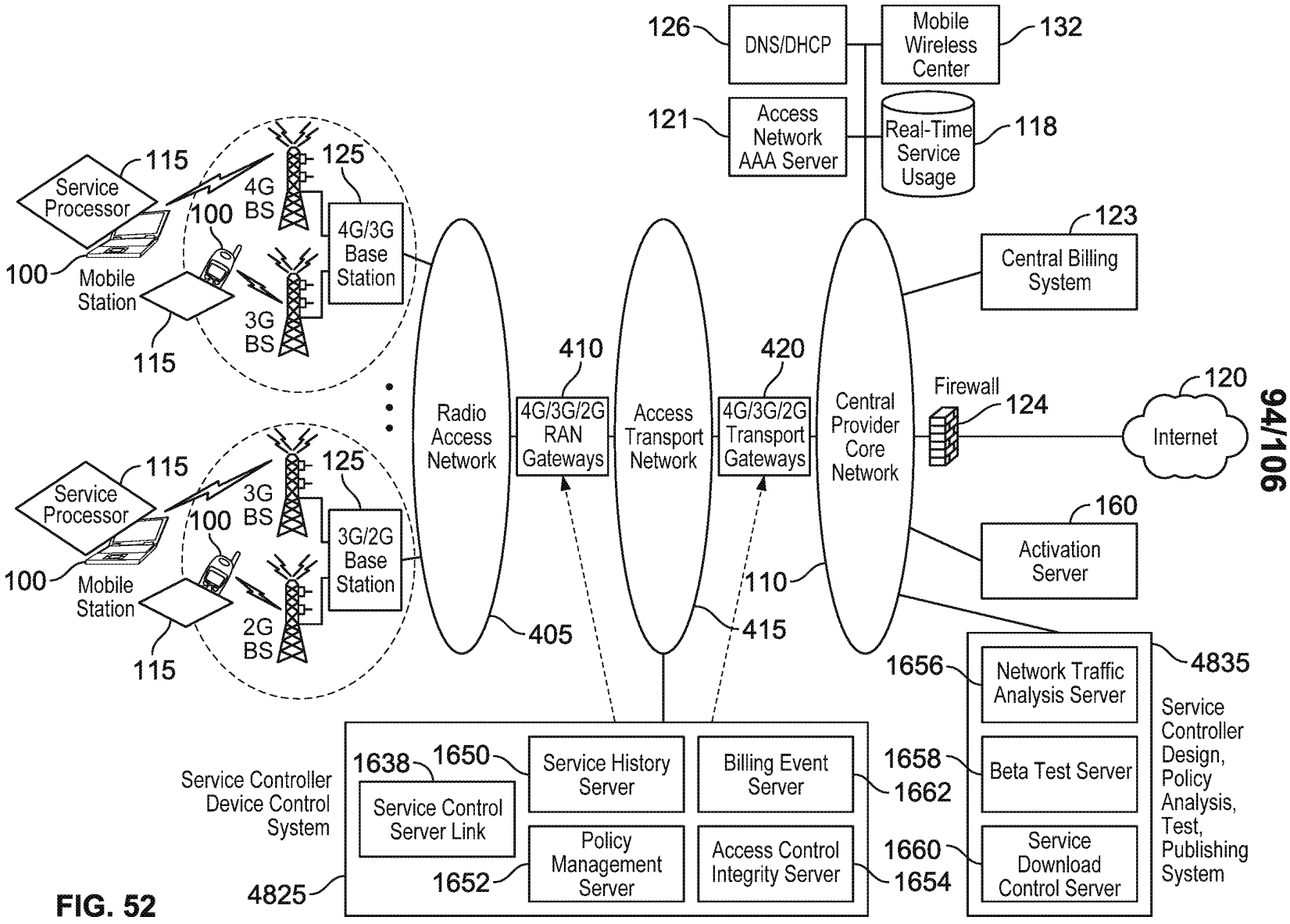

126
DNS/DHCP
Mobile Wireless Center
132
121
Access Network AAA Server
Real-Time Service Usage
118
123
Central Billing System
115
Service Processor
100
Mobile Station
4G BS
125
4G/3G Base Station
3G BS
410
420
Radio Access Network
4G/3G/2G RAN Gateways
Access Transport Network
4G/3G/2G Transport Gateways
Central Provider Core Network
Firewall
124
120
Internet
94/106
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 Controller Device Control System
Service Control Server Link
Service History Server
Billing Event Server
Policy Management Server
Access Control Integrity Server
1652
4825

FIG. 52

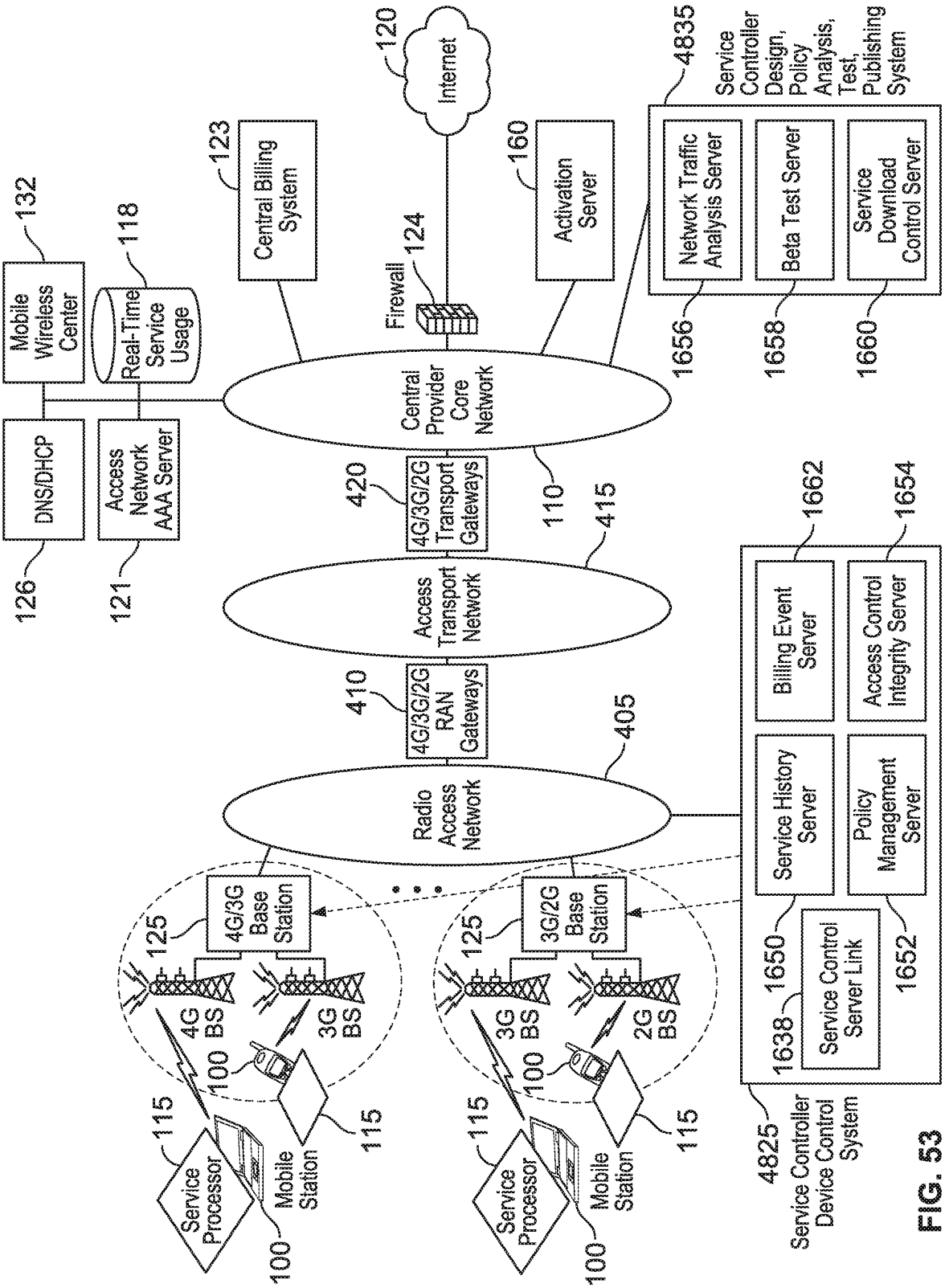

Mobile Wireless Center
132
Real-Time Service Usage
118
Central Billing System
123
Internet
120
Service Controller Design, Policy Analysis, Test, Publishing System
4835
Activation Server
160
Firewall
124
Network Traffic Analysis Server
Beta Test Server
Service Download Control Server
1656
1658
1660
DNS/DHCP
126
Access Network AAA Server
121
Central Provider Core Network
110
420
4G/3G/2G Transport Gateways
Access Transport Network
415
410
4G/3G/2G RAN Gateways
405
Radio Access Network
1662
Billing Event Server
1654
Access Control Integrity Server
Service History Server
Policy Management Server
1650
1652
1638
Service Control Server Link
4825
Service Controller Device Control System
125
4G/3G Base Station
3G/2G Base Station
4G BS
3G BS
3G BS
2G BS
100
115
Service Processor
Mobile Station

FIG. 53

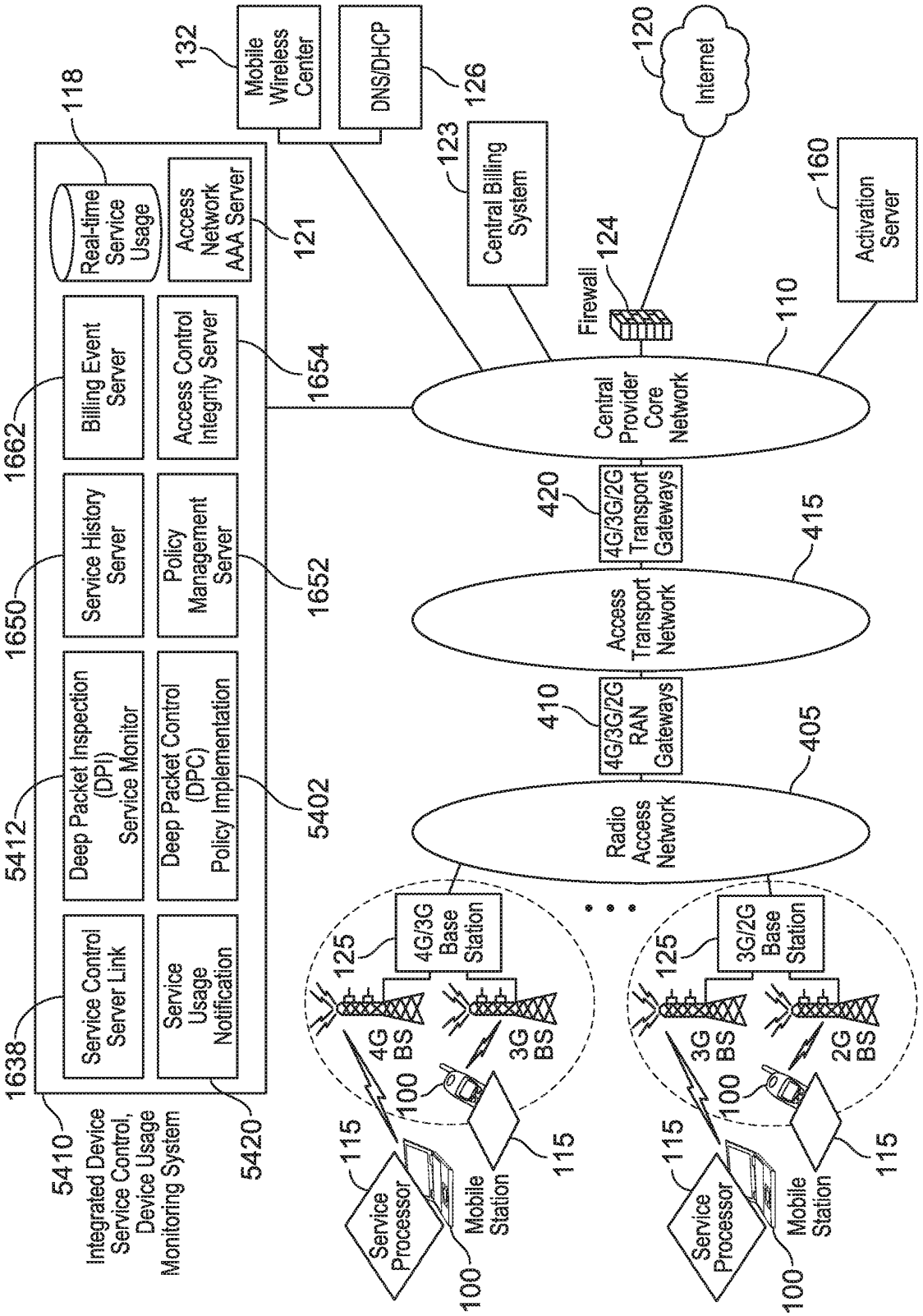

5410
Integrated Device Service Control, Device Usage Monitoring System
1638
Service Control Server Link
5412
Deep Packet Inspection (DPI) Service Monitor
1650
Service History Server
1662
Billing Event Server
5420
Service Usage Notification
5402
Deep Packet Control (DPC) Policy Implementation
1652
Policy Management 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
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

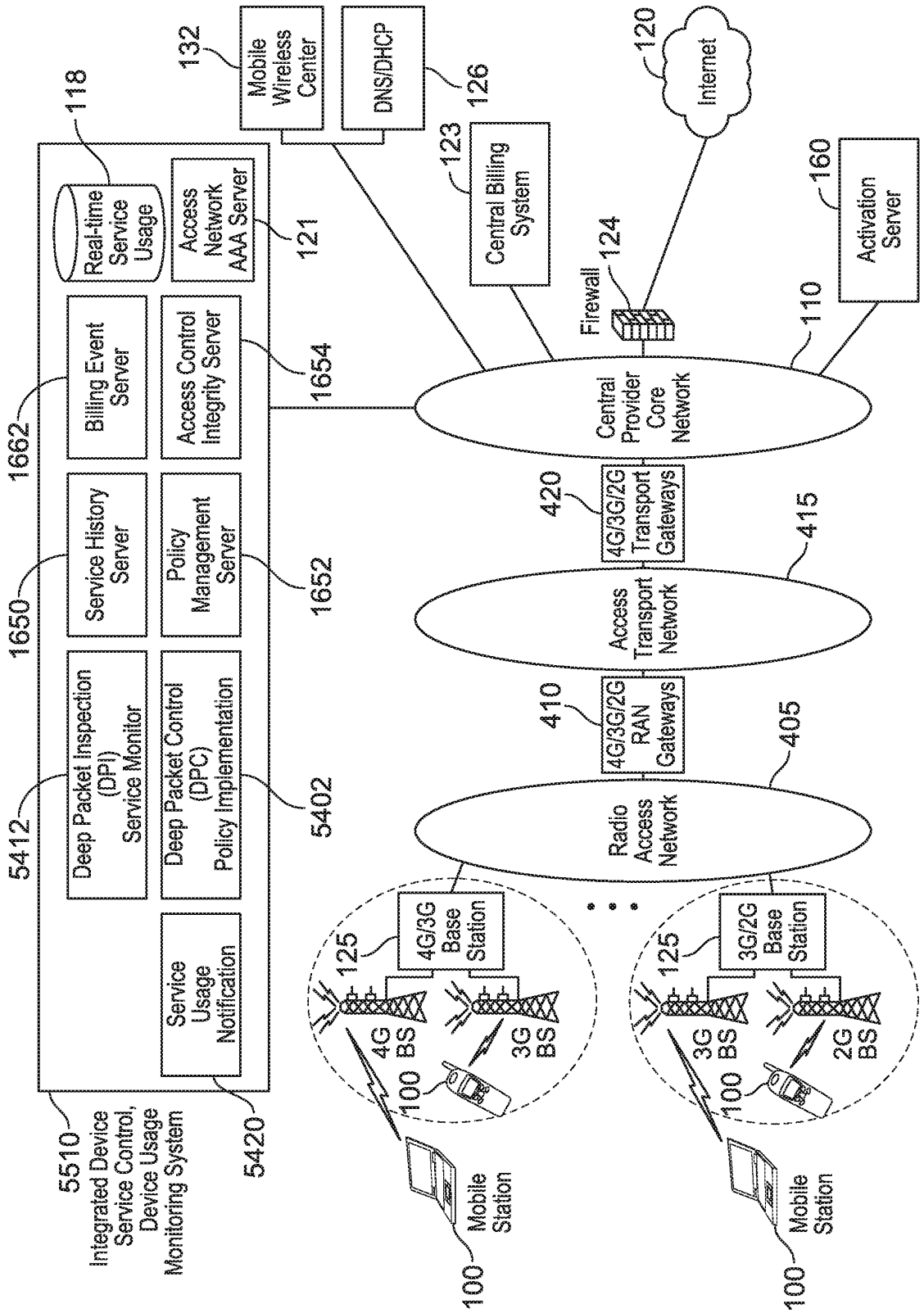

5510
Integrated Device Service Control, Device Usage Monitoring System
5420
5412
Deep Packet Inspection (DPI) Service Monitor
1650
Service History Server
1662
Billing Event Server
5402
Deep Packet Control (DPC) Policy Implementation
1652
Policy Management Server
1654
Access Control Integrity Server
Service Usage Notification
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

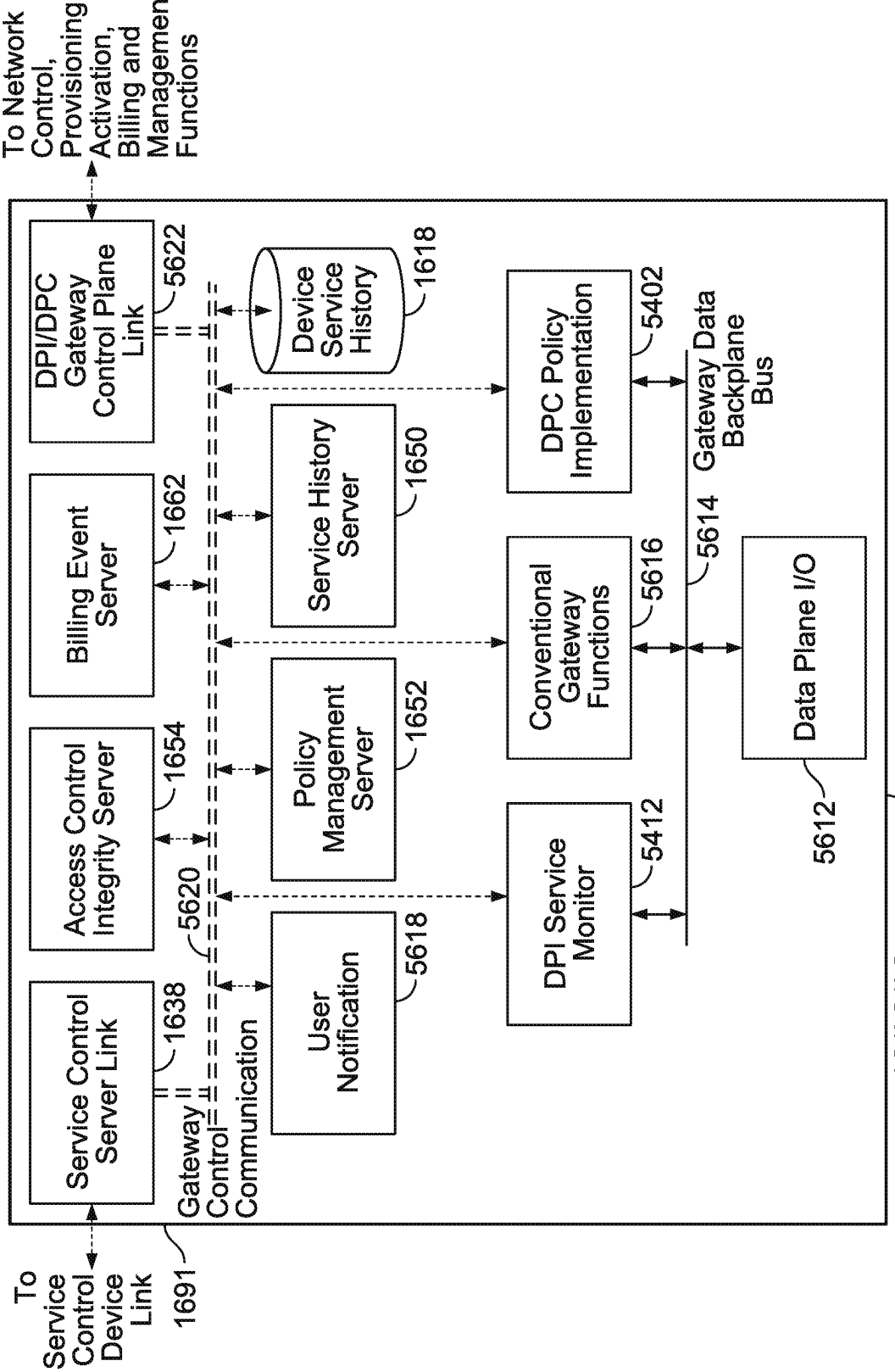

To Network Control, Provisioning, Activation, Billing and Management Functions
DPI/DPC Gateway Control Plane Link
5622
Device Service History
1618
Billing Event Server
1662
Service History Server
1650
DPC Policy Implementation
5402
Gateway Data Backplane Bus
5614
Access Control Integrity Server
1654
Policy Management Server
1652
Conventional Gateway Functions
5616
Service Control Server Link
1638
User Notification
5618
DPI Service Monitor
5412
Data Plane I/O
5612
Gateway Control Communication
5620
4G/3G/2G DPI/DPC Gateway
5610
To Service Control Device Link
1691

FIG. 56

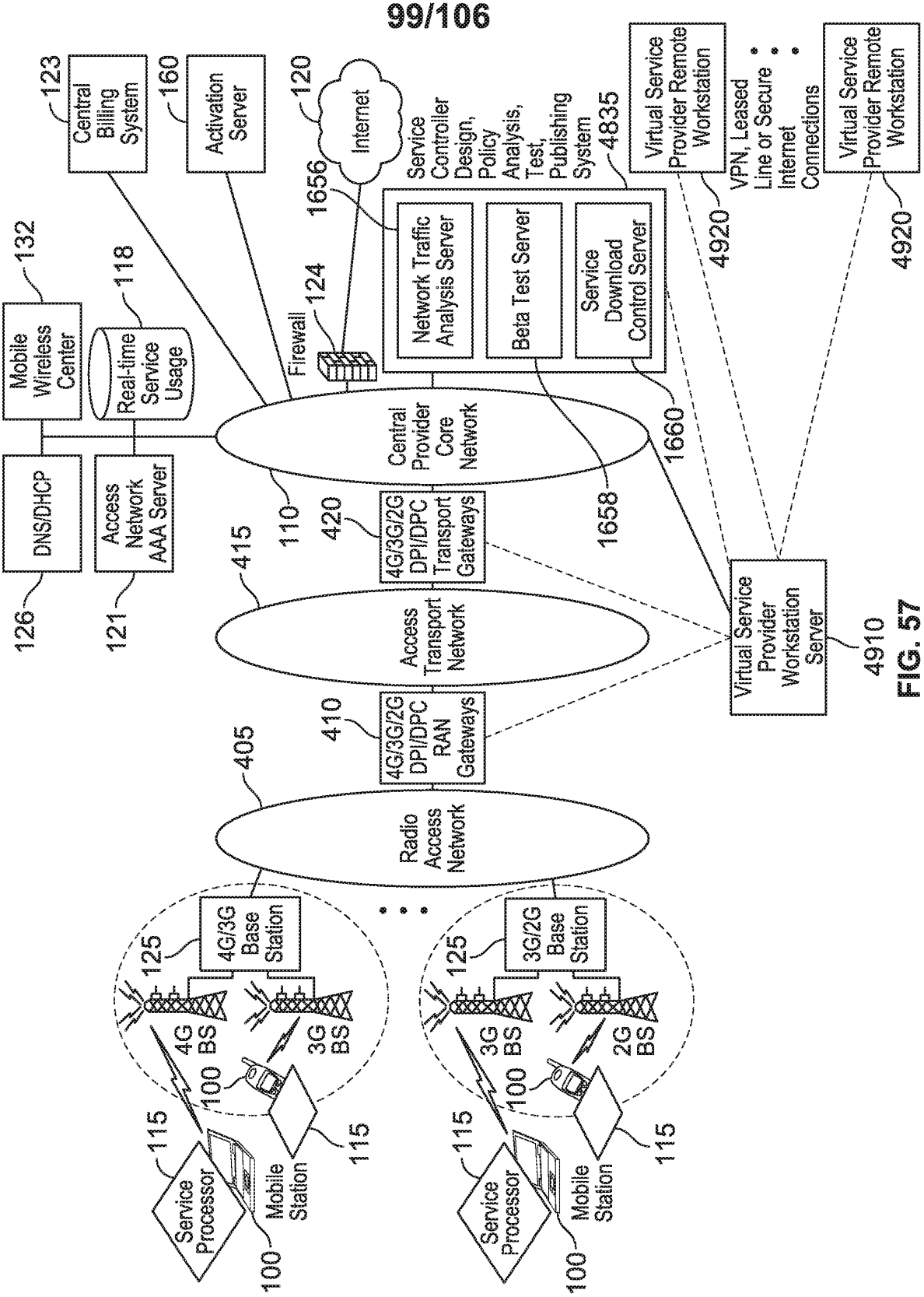

Central Billing System
123
Activation Server
160
Internet
120
Service Controller Design, Policy Analysis, Test, Publishing System
4835
Virtual Service Provider Remote Workstation
VPN, Leased Line or Secure Internet Connections
4920
Mobile Wireless Center
132
Real-time Service Usage
118
Firewall
124
1656
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
415
420
4G/3G/2G DPI/DPC Transport Gateways
Access Transport Network
410
4G/3G/2G DPI/DPC RAN Gateways
405
Radio Access Network
Virtual Service Provider Workstation Server
4910
4G/3G Base Station
125
4G BS
3G BS
100
115
Service Processor
Mobile Station
3G/2G Base Station
3G BS
2G BS

FIG. 57

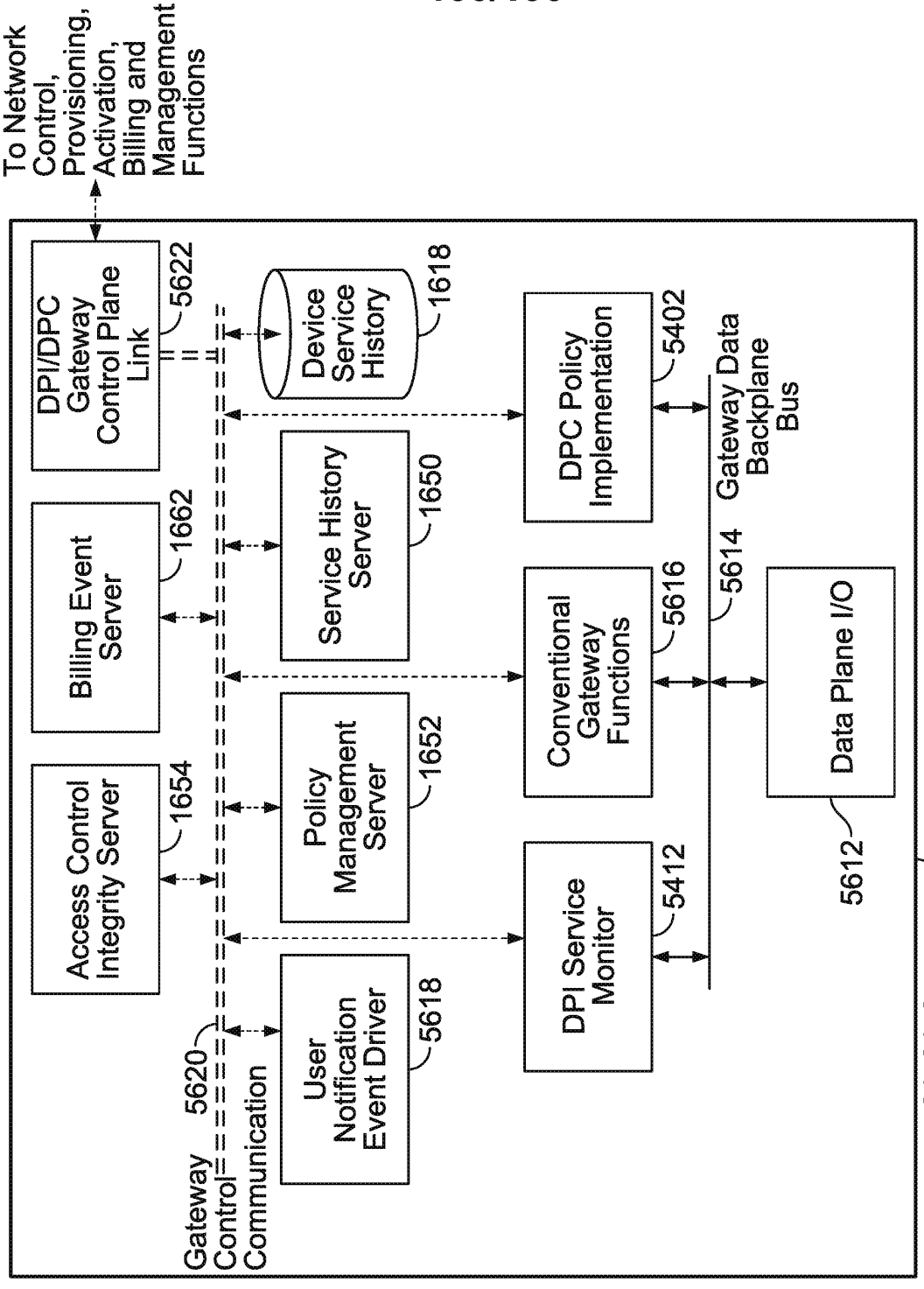

To Network Control, Provisioning, Activation, Billing and Management Functions
DPI/DPC Gateway Control Plane Link
5622
Device Service History
1618
Billing Event Server
1662
Service History Server
1650
DPC Policy Implementation
5402
Gateway Data Backplane Bus
Access Control Integrity Server
1654
Policy Management Server
1652
Conventional Gateway Functions
5616
5614
Data Plane I/O
User Notification Event Driver
5618
DPI Service Monitor
5412
5612
Gateway Control Communication
5620
4G/3G/2G DPI/DPC Gateway
5810

FIG. 58

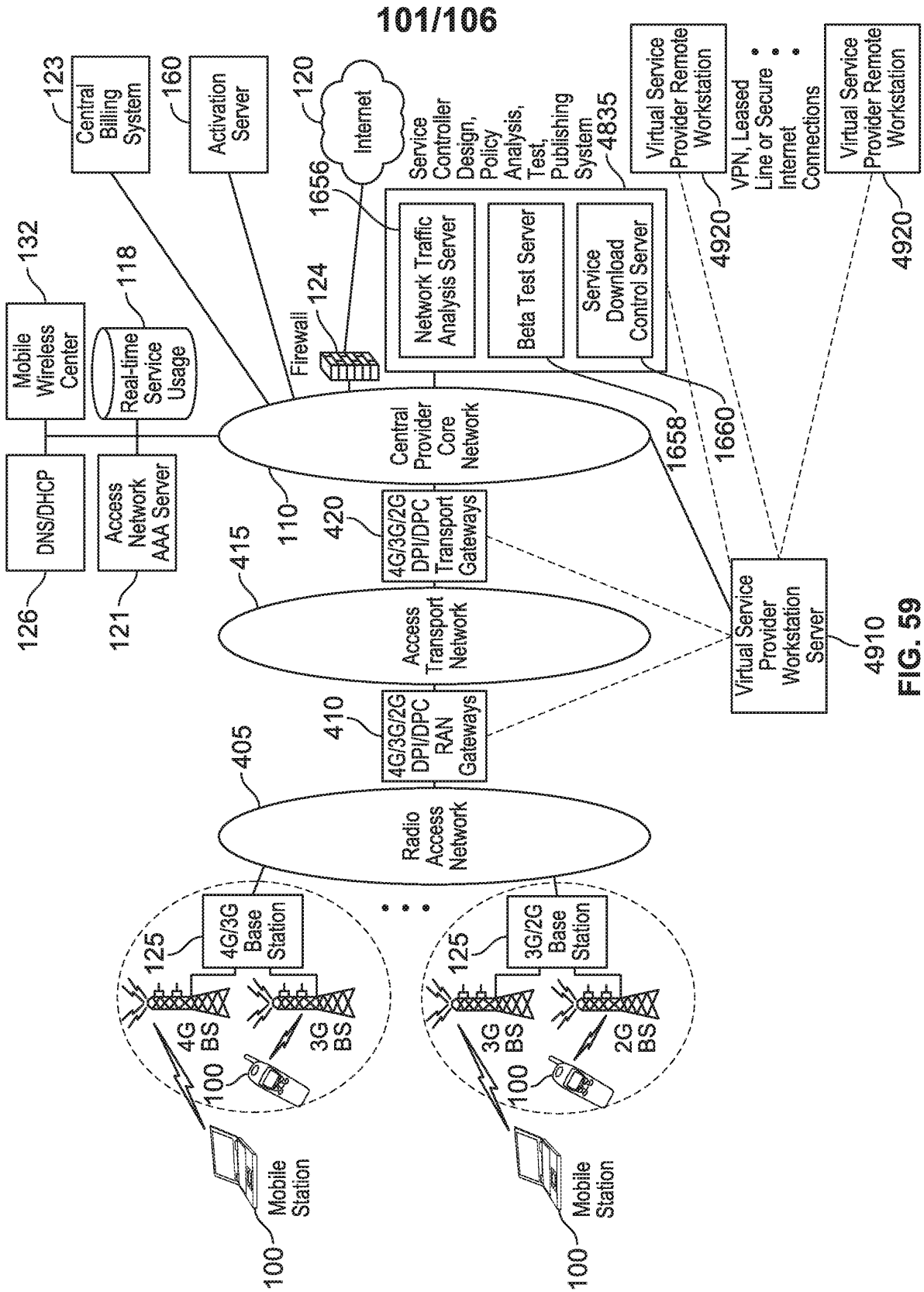

101/106
Central Billing System
123
Activation Server
160
Internet
120
Service Controller Design, Policy Analysis, Test, Publishing System
4835
Virtual Service Provider Remote Workstation
VPN, Leased Line or Secure Internet Connections
Virtual Service Provider Remote Workstation
4920
4920
1656
Network Traffic Analysis Server
Beta Test Server
Service Download Control Server
1658
1660
Mobile Wireless Center
132
Real-time Service Usage
118
Firewall
124
Central Provider Core Network
110
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

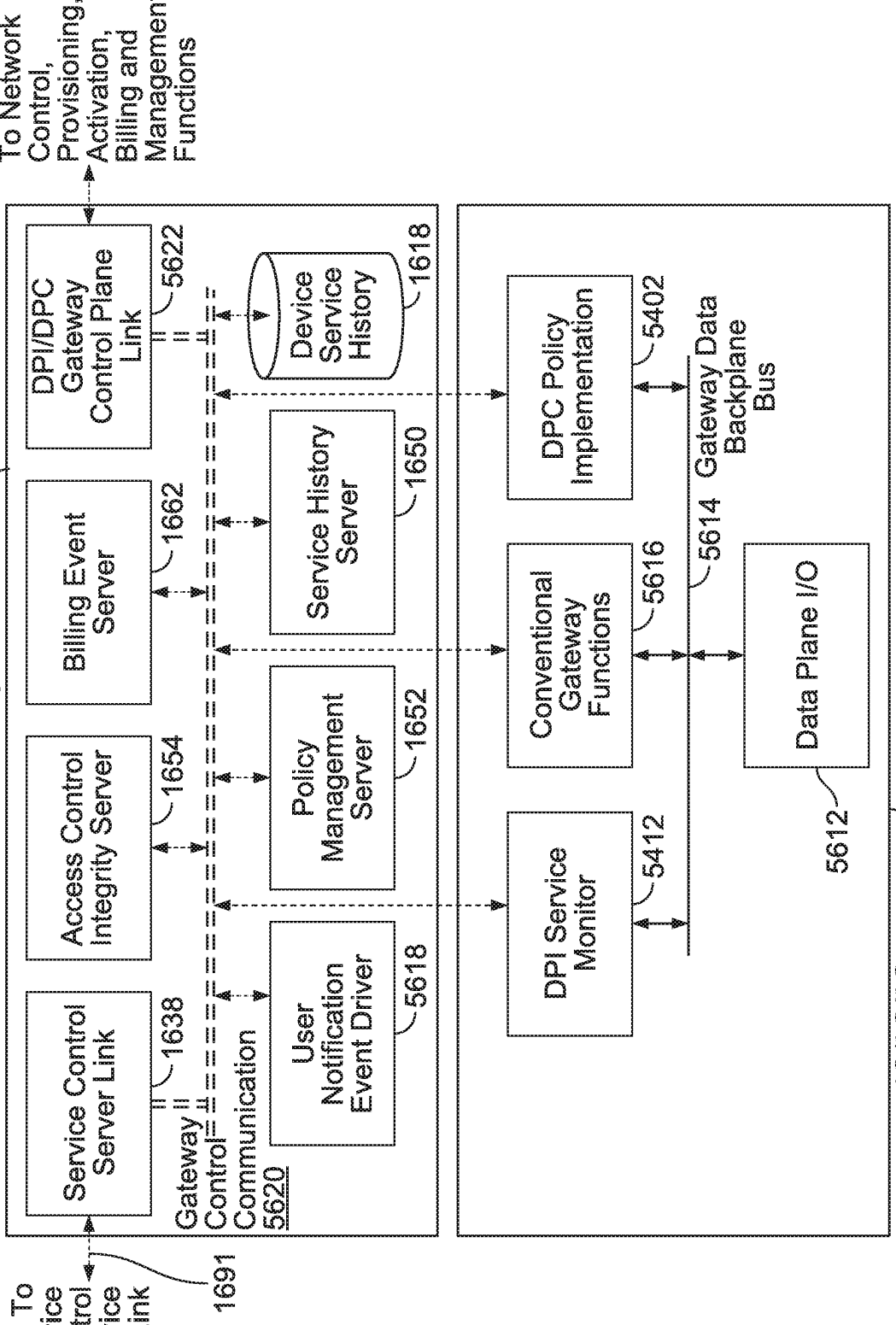

To Network Control, Provisioning, Activation, Billing and Management Functions
Service Controller Device Control System
6025
Service Control Server Link
1638
Access Control Integrity Server
1654
Billing Event Server
1662
DPI/DPC Gateway Control Plane Link
5622
Device Service History
1618
Service History Server
1650
Policy Management Server
1652
User Notification Event Driver
5618
Gateway Control Communication 5620
DPC Policy Implementation
5402
Conventional Gateway Functions
5616
5614 Gateway Data Backplane Bus
DPI Service Monitor
5412
Data Plane I/O
5612
4G/3G/2G DPI/DPC Gateway
6010
To Service Control Device Link
1691

FIG. 60

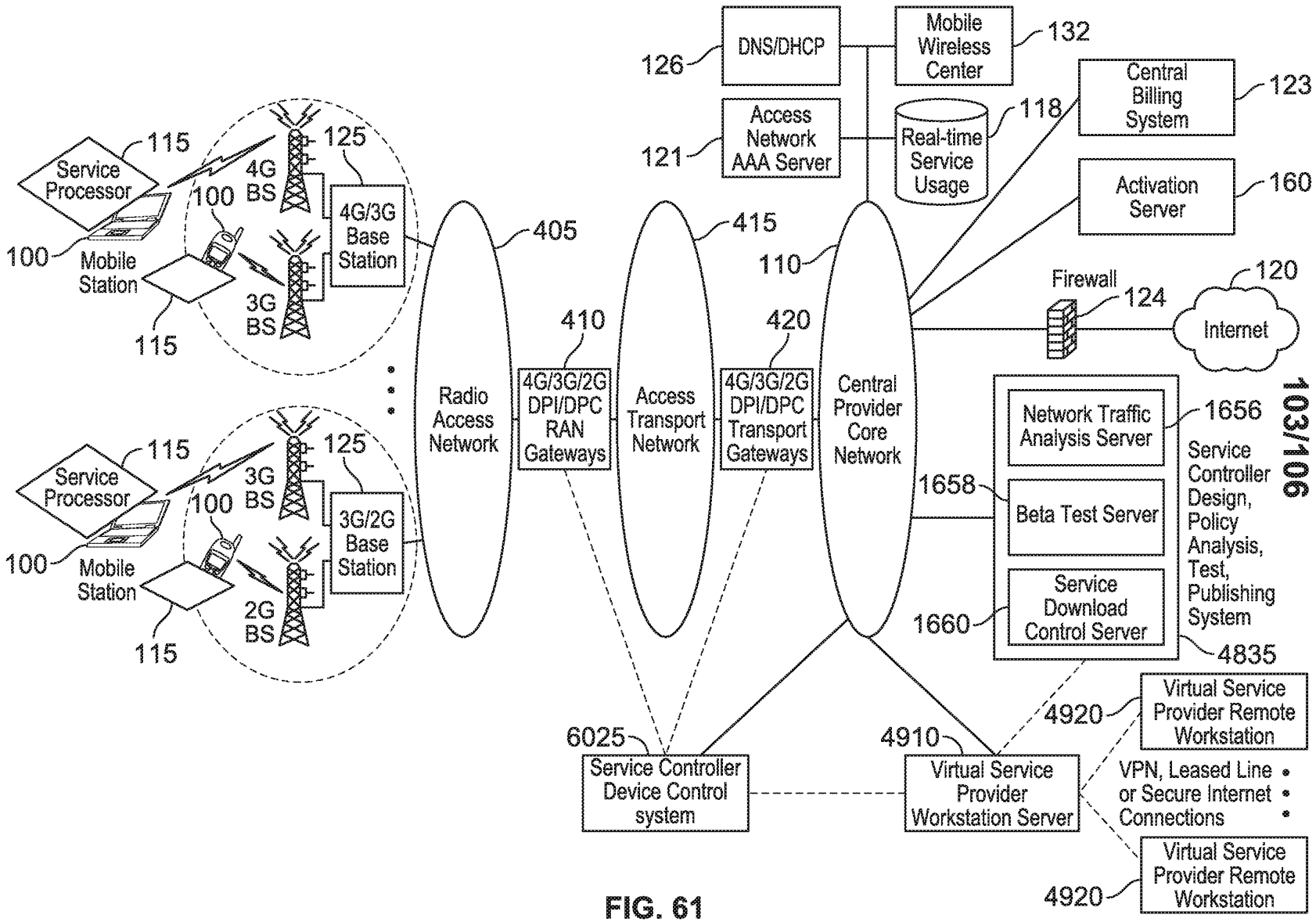

Service Processor
115
100
Mobile Station
4G BS
125
4G/3G Base Station
3G BS
Service Processor
115
100
Mobile Station
3G BS
125
3G/2G Base Station
2G BS
Radio Access Network
405
4G/3G/2G DPI/DPC RAN Gateways
410
Access Transport Network
415
4G/3G/2G DPI/DPC Transport Gateways
420
126
DNS/DHCP
121
Access Network AAA Server
Mobile Wireless Center
132
Real-time Service Usage
118
Central Billing System
123
Activation Server
160
110
Central Provider Core Network
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
6025
Service Controller Device Control system
4910
Virtual Service Provider Workstation Server
4920
Virtual Service Provider Remote Workstation
VPN, Leased Line or Secure Internet Connections
4920
Virtual Service Provider Remote Workstation

FIG. 61

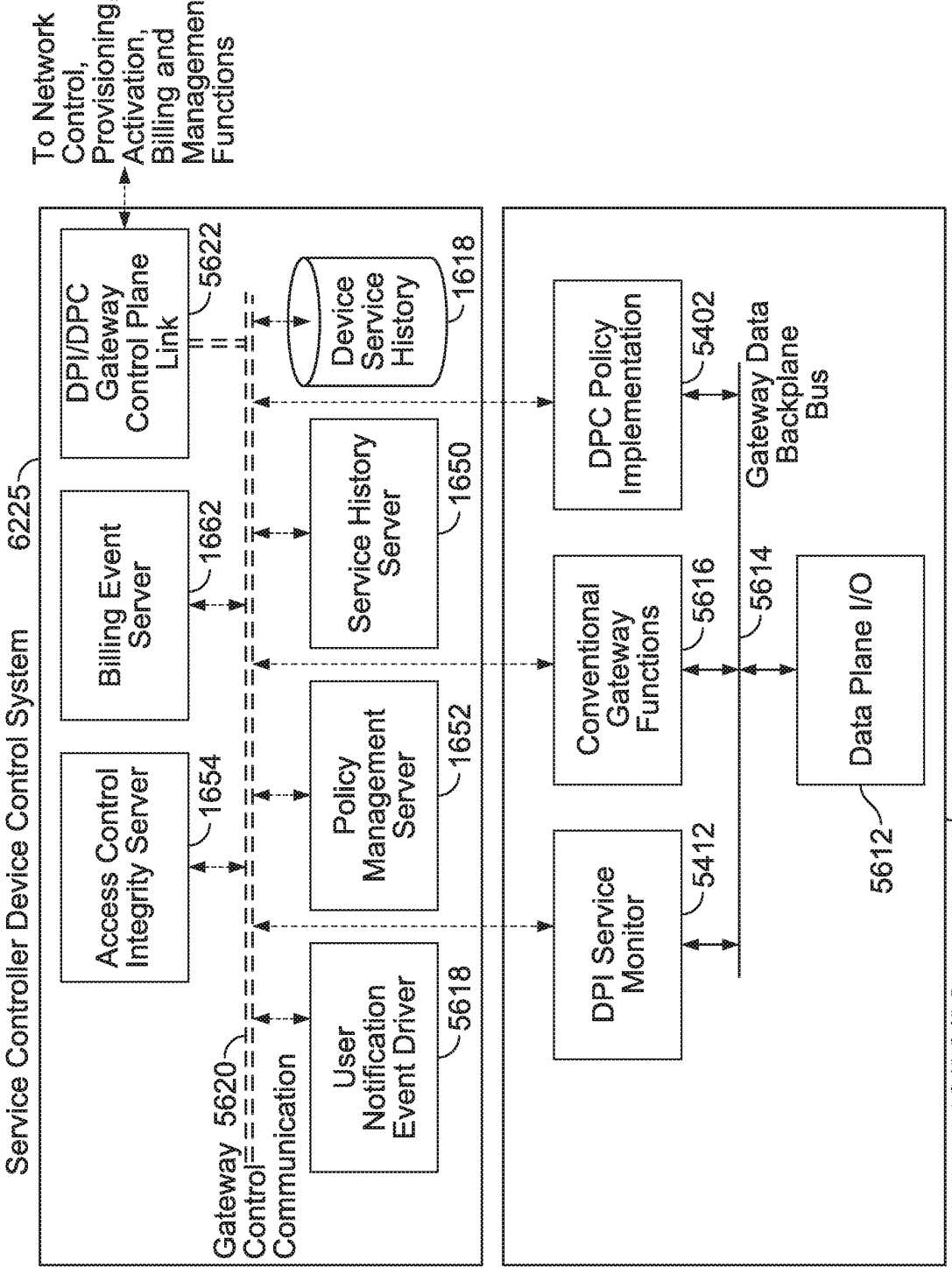

To Network Control, Provisioning, Activation, Billing and Management Functions
Service Controller Device Control System
6225
Access Control Integrity Server
1654
Billing Event Server
1662
Policy Management Server
1652
User Notification Event Driver
5618
Service History Server
1650
DPI/DPC Gateway Control Plane Link
5622
Device Service History
1618
Gateway Control Communication
5620
DPI Service Monitor
5412
Conventional Gateway Functions
5616
DPC Policy Implementation
5402
Gateway Data Backplane Bus
5614
Data Plane I/O
5612
4G/3G/2G DPI/DPC Gateway
6210

FIG. 62

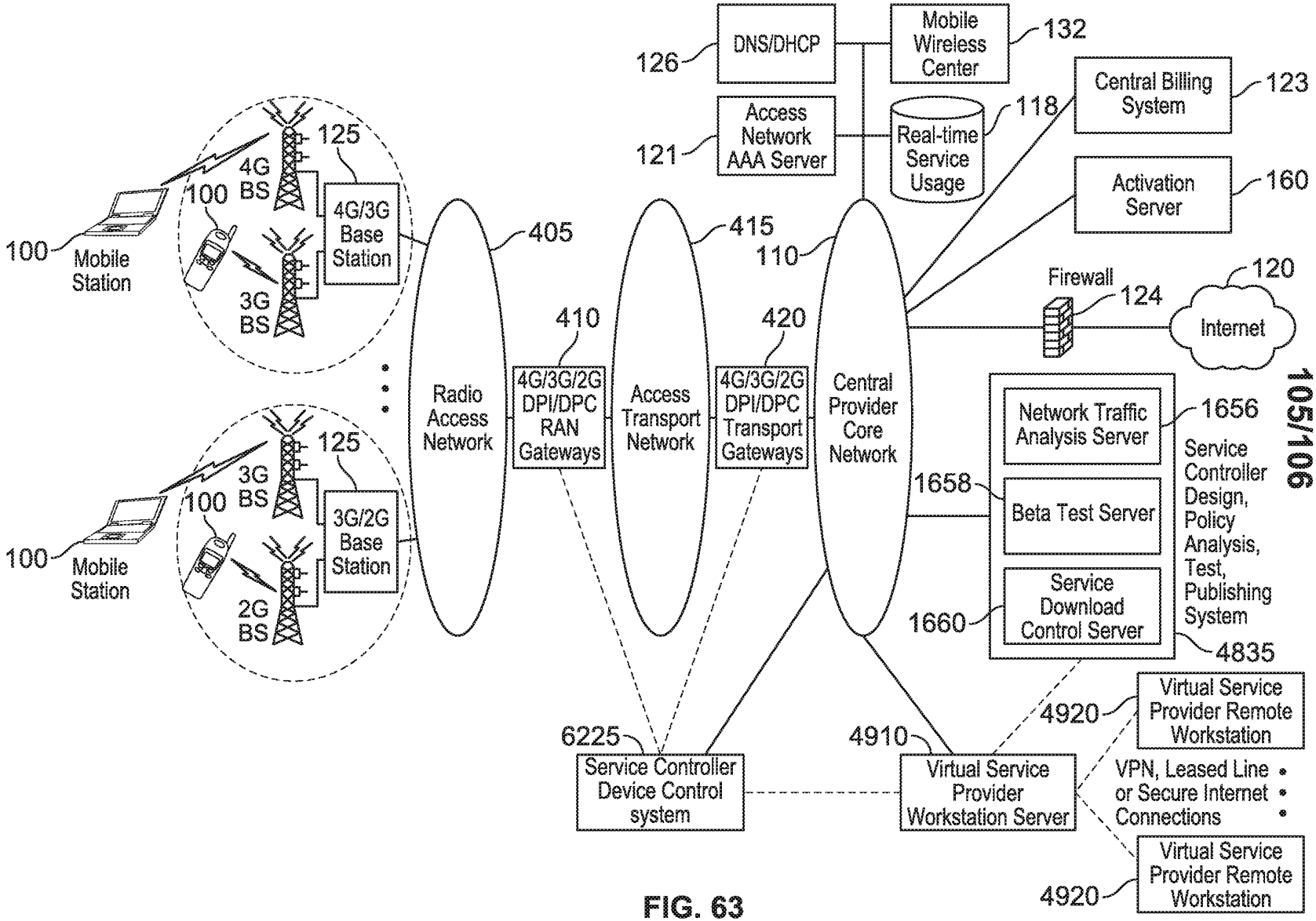


FIG. 63

EX1002 - Page 116

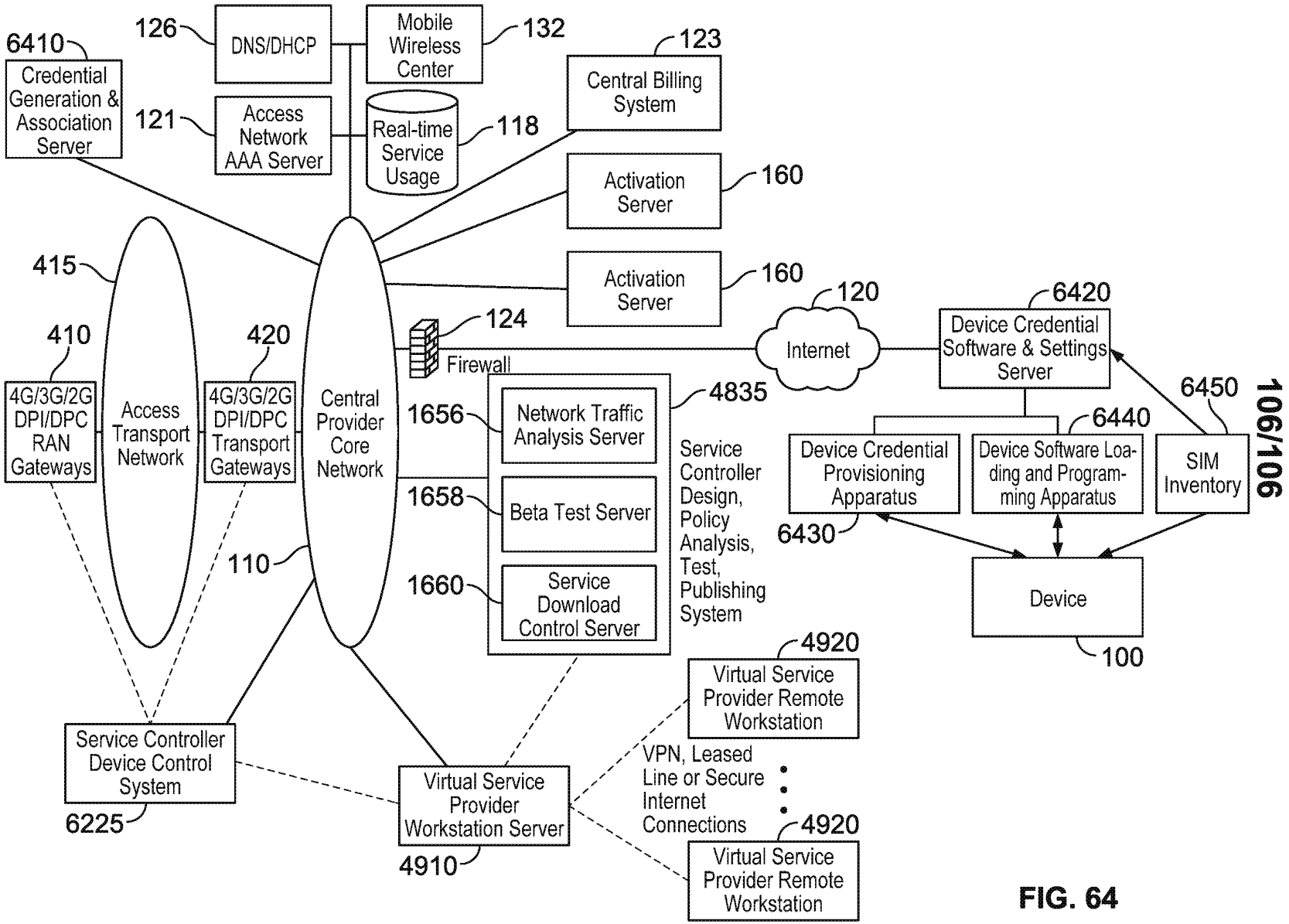

6410
Credential Generation & Association Server
126
DNS/DHCP
Mobile Wireless Center
132
123
Central Billing System
121
Access Network AAA Server
Real-time Service Usage
118
Activation Server
160
Activation Server
160
415
410
420
4G/3G/2G DPI/DPC RAN Gateways
Access Transport Network
4G/3G/2G DPI/DPC Transport Gateways
Central Provider Core Network
124
Firewall
120
Internet
6420
Device Credential Software & Settings Server
6450
106/106
6440
Device Credential Provisioning Apparatus
Device Software Loading and Programming Apparatus
SIM Inventory
6430
Device
100
1656
Network Traffic Analysis Server
4835
1658
Beta Test Server
1660
Service Download Control Server
Service Controller Design, Policy Analysis, Test, Publishing System
110
4920
Virtual Service Provider Remote Workstation
VPN, Leased Line or Secure Internet Connections
Service Controller Device Control System
6225
Virtual Service Provider Workstation Server
4910
4920
Virtual Service Provider Remote Workstation

FIG. 64

PTO/AIA/80 (07-12)
Approved for use through 11/30/2014. OMB 0651-0035
U.S. Patent and Trademark Office; U.S DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO

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

I hereby appoint:

■ Practitioners associated with Customer Number: 106963

OR

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

Name	Registration Number	Name	Registration Number

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

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

■ The address associated with Customer Number: 106963

OR

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

Assignee Name and Address: Headwater Partners I LLC
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	March 10, 2016
Name	David R. Johnson	Telephone	650-517-2782
Title	Chief Executive 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.

PTO/AIA/01 (08-12)
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.

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.

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	Automated Device Provisioning and Activation
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Filer:	James E. Harris/Ann Taylor
Attorney Docket Number:	RALEP007C11C3C2C2

Filed as Small Entity

Filing Fees for Track I Prioritized Examination - Nonprovisional Application 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
Request for Prioritized Examination	2817	1	2000	2000
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($)
Publ. Fee- Early, Voluntary, or Normal	1504	1	0	0
PROCESSING FEE, EXCEPT PROV. APPLS.	2830	1	70	70
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**3600**

Electronic Acknowledgement Receipt	
EFS ID:	26433687
Application Number:	15217538
International Application Number:	
Confirmation Number:	3305
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:	RALEP007C11C3C2C2
Receipt Date:	22-JUL-2016
Filing Date:	
Time Stamp:	16:45:00
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$3600
RAM confirmation Number	3493
Deposit Account	505876
Authorized User	TAYLOR, ANN
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 CFR 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 CFR 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 CFR 1.19 (Document supply fees)

Charge any Additional Fees required under 37 CFR 1.20 (Post Issuance fees)

Charge any Additional Fees required under 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	TrackOne Request	P007C11C3C2C2_TrackOneRequest.pdf	113836 d00ccabef6a1b5cdc2e838cd5fe543e2f9148908	no	2
Warnings:					
Information:					
2	Application Data Sheet	P007C11C3C2C2_ADS.pdf	1823471 bb884876beaafb091b7b8c05762e6378133ae789	no	9
Warnings:					
Information:					
3	Drawings-only black and white line drawings	P007C11C3C2C2_Drawings_Part1.pdf	10373531 e0fc5e83c7051baf9971ec66850158a151bbe2ed	no	54
Warnings:					
Information:					
4	Drawings-only black and white line drawings	P007C11C3C2C2_Drawings_Part2.pdf	8159440 2aa88e3fca51a61630c71981434904942cbd5b67	no	52
Warnings:					
Information:					
5	Power of Attorney	P007C11C3C2C2_POA.pdf	387200 8a625d81e60f9ef081dd94ae772be639675df15d	no	2
Warnings:					
Information:					
6	Oath or Declaration filed	P007C11C3C2C2_RaleighDecl.pdf	104340 45fe2eb014a1714c92385418e355bdfd013a106a	no	1
Warnings:					
Information:					

7		P007C11C3C2C2_Spec.pdf	1095433 4cce501b5b5d13a6b23f2008ca7b0fb332c259ca	yes	242

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Specification	1	240
	Claims	241	241
	Abstract	242	242

Warnings:

Information:

8	Fee Worksheet (SB06)	fee-info.pdf	41911 a02a4efcd87c3a5da02838872b4ba218b0479bfb	no	2

Warnings:

Information:

Total Files Size (in bytes):	22099162

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.:	15/217,538	Art Unit:	
Filed:	July 22, 2016	Conf. No.:	3305
Title:	Automated Device Provisioning and Activation		

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

PRELIMINARY AMENDMENT

Prior to examination on the merits, please amend the above-identified application as follows:

Amendments to the Specification begin on page 2.

Amendments to the Claims begin on page 3.

Remarks begin on page 7.

AMENDMENTS TO THE SPECIFICATION

Please replace the Application Title with the following:

Mobile Device and Method With Secure Network Messaging for Authorized Components

Please replace the Abstract with the following:

A mobile device has an inter-process software communication (IPC) bus that provides secure communication between a device link agent and software component processes. The software processes are allowed to access the bus based on access authorization information from a secure server that identifies those components. The device link object maintains a secure message link to a message link server that receives messages from plural network functions, identified for delivery to respective software components on the mobile device, and conveys them to the device link agent. For the authorized software components, the link agent delivers received messages to the component processes.

AMENDMENTS TO THE CLAIMS

Please amend the claims as follows:

1. (Canceled).

2. (New) A mobile end-user device comprising:

a wireless modem configurable to exchange data via a connection to a wireless network;

an inter-process software communication bus providing secure communication between an executing device link agent and respective executing processes for a plurality of software components, wherein providing secure communication comprises receiving access authorization information from a secure server, and allowing access to the bus only for software components identified by the access authorization information; and

the device link agent, configured to

maintain a secure message link through the wireless network and an Internet network to a message link server, the message link server operating a message service that receives messages over a network from a plurality of network functions,

receive secure messages from the message link server over the secure message link, the received messages identified for delivery to multiple ones of the software components, and including message content received by the message link server from multiple ones of the network functions, and

for software components identified by the access authorization information, route messages identified for delivery to a given one of those software components via the inter-process software communication bus to a software process corresponding to the given software component.

3. (New) The mobile end-user device of claim 2, wherein the software components include a first device component that receives message content in a first format, and a second device component that receives message content in a second format different than the first format.

4. (New) The mobile end-user device of claim 3, further comprising a user interface, wherein the first device component is a user service interface agent, and the first format comprises a notification message, the user service interface agent configured to display the notification message on the user interface.

5. (New) The mobile end-user device of claim 4, the user service interface agent further configured to obtain a user input as a response to the display of the notification message, and deliver the user input to an agent on the device.

6. (New) The mobile end-user device of claim 3, wherein the first device component is a policy control agent, and the first format contains service settings and/or configuration information.

7. (New) The mobile end-user device of claim 2, wherein the received secure messages are encrypted, the device link agent further configured to decrypt the received secure messages prior to delivering those messages to respective software processes.

8. (New) The mobile end-user device of claim 7, 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.

9. (New) The mobile end-user device of claim 2, wherein the device link agent executes in a secure execution environment, and at least one of the software components executes outside of the secure execution environment.

10. (New) The mobile end-user device of claim 2, wherein the device link agent is further configured to receive, from one or more of the authorized software components, upload messages, each of the upload messages identifying a corresponding one of the network functions to which the device respective software component has requested delivery, the device link agent transmitting the upload messages to the network message

server over the secure message link, for delivery by the network message server to the respective identified network elements.

11. (New) The mobile end-user device of claim 10, the device link agent 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.

12. (New) The mobile end-user device of claim 2, wherein at least one of the secure messages received from the network message server comprises multiple identifier/data pairs.

13. (New) The mobile end-user device of claim 2, wherein the access authorization information provided by the secure server for a given one of the software components comprises a signature.

14. (New) The mobile end-user device of claim 13, wherein the given one of the software components is identified by a secure unique identifier.

15. (New) A method of operating a mobile end-user device having a wireless modem to connect to a wireless network, the method comprising:

receiving access authorization information from a secure server;

operating an inter-process software communication bus to provide secure communication between an executing device link agent and respective executing processes for a plurality of software components, the secure communication comprising allowing access to the bus only for software components identified by the access authorization information;

maintaining a secure message link from the device link agent through the wireless network and an Internet network to a message link server, the message link server operating a message service that receives messages over a network from a plurality of network functions;

receiving secure messages at the device link agent from the message link server over the secure message link, the received messages identified for delivery to

multiple ones of the software components, and including message content received by the message link server from multiple ones of the network functions; and

for software components identified by the access authorization information, routing messages identified for delivery to a given one of those software components via the inter-process software communication bus from the device link agent to a software process corresponding to the given software component.

REMARKS

Applicant respectfully requests entry of the amendments provided herein. This preliminary amendment is presented before any office action. Claim 1 has been cancelled, and new claims 2-15 have been added. No new matter has been added. If the Examiner has any questions or needs any additional information, the Examiner is invited to contact the undersigned.

The Commissioner is authorized to charge any fee deficiency or credit any overpayment to Deposit Account 50-5876.

Respectfully submitted,

Date: July 23, 2016 By: /James E. Harris/

James E. Harris
Reg. No. 40013
Patent Counsel
Headwater Partners I 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: July 23, 2016 By: /Ann Taylor/
Ann Taylor

Electronic Acknowledgement Receipt

EFS ID:	26437072
Application Number:	15217538
International Application Number:	
Confirmation Number:	3305
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:	RALEP007C11C3C2C2
Receipt Date:	23-JUL-2016
Filing Date:	
Time Stamp:	11:53:46
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		P007C11C3C2C2_PreliminaryAmendment.pdf	91441 5c17458f837cf1c43f529050266faef4886a5e84	yes	7

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Preliminary Amendment	1	1
	Specification	2	2
	Claims	3	6
	Applicant Arguments/Remarks Made in an Amendment	7	7
Warnings:			
Information:			
	Total Files Size (in bytes):	91441	

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

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

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

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

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 15/217,538	Filing Date 07/22/2016	☐ 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	07/23/2016	(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))	* 14	Minus	** 20	= 0	X $40 =	0
	Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0	X $210 =	0
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	**0**

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

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
/NINA RATANAVONG/

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.

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

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

Application Number	15217538
Filing Date	2016-07-22
First Named Inventor	Raleigh
Art Unit	2447
Examiner Name	not yet assigned
Attorney Docket Number	RALEP007C11C3C2C2

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5577100		1996-11-19	McGREGOR et al.	
	2	5794142		1998-08-11	VANTTILA et al.	
	3	5892900		1999-04-06	GINTER et al.	
	4	5903845		1999-05-11	BUHRMANN et al.	
	5	5933778		1999-08-03	BUHRMANN et al.	
	6	5940472		1999-08-17	NEWMAN et al.	
	7	6047268		2000-04-04	BARTOLI et al.	
	8	6078953		2000-06-20	VAID et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

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

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

FOREIGN PATENT DOCUMENTS Remove

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5
	1	3rd Generation Partnership Project, "Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) Enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) Access," Release 8, Document No. 3GPP TS 23.401, V8.4.0, December 2008	
	2	3rd Generation Partnership Project, "Technical Specification Group Services and System Aspects; Policy and Charging Control Architecture," Release 8, Document No. 3GPP TS 23.203, V8.4.0, December 2008	
	3	ALONISTIOTI et al., "Intelligent Architectures Enabling Flexible Service Provision and Adaptability," 2002	
	4	Amazon Technologies, Inc., "Kindle™ User's Guide," 3rd Edition, Copyright 2004-2009	
	5	CHANDRASEKHAR et al., "Femtocell Networks: A Survey," June 28, 2008	
	6	CHAOUCHI et al., "Policy Based Networking in the Integration Effort of 4G Networks and Services," 2004 IEEE	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

CERTIFICATION STATEMENT

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

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

OR

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

See attached certification statement.

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

☒ None

SIGNATURE

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

Signature	/James E. Harris/	Date (YYYY-MM-DD)	2016-07-25
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.

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

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

Application Number	15217538
Filing Date	2016-07-22
First Named Inventor	Raleigh
Art Unit	2447
Examiner Name	not yet assigned
Attorney Docket Number	RALEP007C11C3C2C2

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	8447980		2013-05-21	Godfrey, James A. et al.	
	2	8429403		2013-04-23	Moret, Eric et al.	
	3	8411587		2013-04-02	Curtis, William et al.	
	4	8396929		2013-03-12	Helfman, Nadav et al.	
	5	8363658		2013-01-29	Delker, Jason R. et al.	
	6	8265004		2012-09-11	Toutonghi, Michael J.	
	7	8233895		2012-07-31	Tysowski, Piotr Konrad	
	8	7685254		2010-03-23	Pandya, Ashish A.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	240	8634425		2014-01-21	Gorti et al.	
	241	8825109		2014-09-02	Montemurro et al.	
	242	9014973		2015-04-21	Ruckart, John	
	243	8977284		2015-03-10	Reed, Mark J.	
	244	8930238		2015-01-06	Coffman et al.	
	245	8880047		2014-11-04	Konicek et al.	
	246	8739035		2014-05-27	Trethewey, Jim	
	247	8571598		2013-07-16	Valavi, John J.	
	248	8489110		2013-07-16	Frank et al.	
	249	8406736		2013-03-26	Das et al.	
	250	8259692		2012-09-04	Bajko, Gabor	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	251	8233433		2012-07-31	Kalhan, Amit	
	252	8155666		2012-04-10	Alizadeh-Shabdiz, Farshid	
	253	8103285		2012-01-24	Kalhan, Amit	
	254	7936736		2011-05-03	Proctor Jr., James Arthur et al.	
	255	7925778		2011-04-12	Wijnands et al.	
	256	7760137		2010-07-20	Martucci et al.	
	257	7684370		2010-03-23	Kezys, Vytautas Robertas	
	258	7084775		2006-08-01	Smith, Michael R.	
	259	6578076		2003-06-10	Putzolu, David Matthew	
	260	7133695		2006-11-07	Beyda, William J.	
	261	7260382		2007-08-21	Lamb et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	262	7685530		2010-03-23	Sherrard et al.	
	263	7937450		2011-05-03	Janik, Craig M.	
	264	8019846		2011-09-13	Roelens et al.	
	265	8050705		2011-11-01	Sicher et al.	
	266	8086791		2011-12-27	Caulkins, Jason	
	267	7627872		2009-12-01	Hebeler et al.	
	268	8532610		2013-09-10	Manning Cassett et al.	
	269	8831561		2014-09-09	Sutaria et al.	
	270	8010082		2011-08-30	Sutaria et al.	
	271	7271765		2007-09-18	Stilp et al.	
	272	7843843		2010-11-30	Papp III et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	273	8495181		2013-07-23	Venkatraman et al.	
	274	9049010		2015-06-02	Jueneman et al.	
	275	8174378		2012-05-08	Richman et al.	
	276	6757717		2004-06-29	Goldstein, Leonid	
	277	7007295		2006-02-28	Rose et al.	
	278	8208788		2012-06-26	Ando et al.	
	279	8326828		2012-12-04	Zhou et al.	
	280	8761711		2014-06-24	Grignani et al.	
	281	7222190		2007-05-22	Klinker, Eric et al.	
	282	8713535		2014-04-29	Malhotra et al.	
	283	5572528		1996-11-05	Shuen, Pauline	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	284	5754953		1998-05-19	Briancon et al.	
	285	6628934		2003-09-30	Rosenberg et al.	
	286	6662014		2003-12-09	Walsh, Patrick Jay	
	287	6901440		2005-05-31	Bimm et al.	
	288	6970692		2005-11-29	Tysor, Arthur James	
	289	7203752		2007-04-10	Rice et al.	
	290	7224968		2007-05-29	Dobson et al.	
	291	7379731		2008-05-27	Natsuno et al.	
	292	7457870		2008-11-25	Lownsbrough et al.	
	293	7515926		2009-04-07	Bu et al.	
	294	7536695		2009-05-19	Alam et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	295	7586871		2009-09-08	Hamilton et al.	
	296	7752330		2010-07-06	Olsen et al.	
	297	7792257		2010-09-07	Vanier et al.	
	298	7801783		2010-09-21	Kende et al.	
	299	7865187		2011-01-04	Ramer et al.	
	300	7933274		2011-04-26	Verma 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	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	1	1538730A	CN		2004-10-20	Zhongxing Communication Co., Ltd.		
	2	101115248A	CN		2008-01-30	Lenovo Beijing Ltd.		
	3	101341764A	CN		2009-01-07	Telefonaktiebolaget LM Ericsson		
	4	2007068288A1	WO		2007-06-21	Telefonaktiebolaget LM Ericsson		
	5	1802839A	CN		2006-07-12	Motorola Inc.		
	6	2004064306A2	WO		2004-07-29	Motorola Inc.		
	7	101123553A	CN		2007-09-11	SouTheast University		
	8	1937511A	CN		2007-03-28	ZTE		
	9	1999027723 A1	WO		1999-06-03	Telefonaktiebolaget LM Ericsson		
	10	2007133844	WO		2007-11-22	Camiant, Inc.		
	11	101183958A	CN		2008-05-21	Huawei Tech. Co. Ltd.		

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	12	1801829A	CN		2006-07-12	Kunda Computer Technology (Kunshan) Co., Ltd.		
	13	1867024A	CN		2006-11-22	Huawei Technologies Co., Ltd.		
	14	101815275A	CN		2010-08-25	Yang, Liu		
	15	1567818A	CN		2005-01-19	Huawei Tech. Co. Ltd.		
	16	2006012610	WO		2006-02-02	Citrix Systems, Inc.		
	17	1508734A	CN		2004-06-30	Chinese Creative Corp.		

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

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5
	1	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	
	2	"The Construction of Intelligent Residential District in Use of Cable Television Network," Shandong Science, Vol. 13, No. 2, June 2000	
	3	"Communication Concepts for Mobile Agent Systems," by Joachim Baumann et al.; Inst. Of Parallel and Distributed High-Performance Systems, Univ. of Stuttgart, Germany, pp. 123-135, 1997	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	4	'End to End QoS Solution for Real-time Multimedia Application;" Computer Engineering and Applications, 2007, 43 (4): 155-159, by Tan Zu-guo, Wang Wen-juan; Information and Science School, Zhanjian Normal College, Zhan jiang, Guangdong 524048, China	
	5	'ASA/PIX: Allow Split Tunneling for VPN Clients on the ASA Configuration Example," Document ID 70917, January 10, 2008	
	6	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	
	7	Kassar et al., "An overview of vertical handover decision strategies in heterogeneous wireless networks," ScienceDirect, University Pierre & Marie Curie, Paris, France, 6/5/2007	
	8	Schiller et al., "Location-Based Services," The Morgan Kaufmann Series in Data Management Systems, 2004	
	9	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	

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	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

CERTIFICATION STATEMENT

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

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

OR

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

See attached certification statement.

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

☒ None

SIGNATURE

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

Signature	/James E. Harris/	Date (YYYY-MM-DD)	2016-07-25
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.

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

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

Application Number	15217538
Filing Date	2016-07-22
First Named Inventor	Raleigh
Art Unit	2447
Examiner Name	not yet assigned
Attorney Docket Number	RALEP007C11C3C2C2

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	8005726		2011-08-23	Bao, Yulin	
	2	8050690		2011-11-01	Neeraj, Chawla	
	3	8086398		2011-12-27	Sanchez et al.	
	4	8107953		2012-01-31	Zimmerman et al.	
	5	8112435		2012-02-07	Epstein et al.	
	6	8195661		2012-06-05	Kalavade, Asawaree	
	7	8200163		2012-06-12	Hoffman, George E.	
	8	8200818		2012-06-12	Freund et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	9	8254880		2012-08-28	Aaltonen et al.	
	10	8270955		2012-09-18	Ramer et al.	
	11	8331223		2012-12-11	Hill et al.	
	12	8358975		2013-01-22	Bahl et al.	
	13	8533775		2013-09-10	Alcorn et al.	
	14	8538394		2013-09-17	Zimmerman et al.	
	15	8538458		2013-09-17	Haney, Richard D.	
	16	8565746		2013-10-22	Hoffman, George E.	
	17	8571501		2013-10-29	Miller et al.	
	18	8644702		2014-02-04	Kalajan, Kevin E.	
	19	8713641		2014-04-29	Pagan et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	20	8730842		2014-05-20	Collins et al.	
	21	8732808		2014-05-20	Sewall et al.	
	22	6445777		2002-09-03	Clark, Curtis	
	23	7039027		2006-05-02	Bridgelall, Raj	
	24	7990049		2011-08-02	Shioya, Shunsuke	
	25	8180886		2012-05-15	Overcash et al.	
	26	8339991		2012-12-25	Biswas et al.	
	27	7149521		2006-12-12	Sundar et al.	
	28	7200112		2007-04-03	Sundar et al.	
	29	7395244		2008-07-01	Kingsford, Bryan	
	30	7411930		2008-08-12	Montojo, Juan et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	31	7508799		2009-03-24	Sumner et al.	
	32	7554983		2009-06-30	Muppala, Suresh	
	33	7564799		2009-07-21	Holland et al.	
	34	7849477		2010-12-07	Cristofalo et al.	
	35	7987496		2011-07-26	Bryce et al.	
	36	8503455		2013-08-06	Heikens, Heico	
	37	RE44412		2013-08-06	Naqvi et al.	
	38	5974439		1999-10-26	Bollella, Gregory	
	39	6882718		2005-04-19	Smith, Benjamin V.	
	40	7058022		2006-06-06	Carolan et al.	
	41	7017189		2006-03-21	DeMello et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	42	7266371		2007-09-04	Amin et al.	
	43	8190122		2012-05-29	Alexander et al.	
	44	9002342		2015-04-07	Tenhunen et al.	
	45	8385964		2013-02-26	Haney, Richard D.	
	46	8504032		2013-08-06	Lott et al.	
	47	7366654		2008-04-29	Moore, Robert C.	
	48	7391724		2008-06-24	Alakoski et al.	
	49	7978686		2011-07-12	Goyal et al.	
	50	8644813		2014-02-04	Gailloux et al.	
	51	6393014		2002-05-21	Daly et al.	
	52	6397259		2002-05-28	Lincke et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	53	7047276		2006-05-16	Liu et al.	
	54	7627767		2009-12-01	Sherman et al.	
	55	7849161		2010-12-07	Koch et al.	
	56	7894431		2011-02-22	Goring et al.	
	57	8073427		2011-12-06	Koch et al.	
	58	8522337		2013-08-27	Adusumilli et al.	
	59	8527662		2013-09-03	Biswas et al.	
	60	8572256		2013-10-29	Babbar, Uppinder Singh	
	61	8966018		2015-02-24	Bugwadia et al.	
	62	7162237		2007-01-09	Silver et al.	
	63	7454191		2008-11-18	Dawson et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	64	7817615		2010-10-19	Breau et al.	
	65	7844034		2010-11-30	Oh et al.	
	66	7899039		2011-03-01	Andreasen et al.	
	67	8104080		2012-01-24	Burns et al.	
	68	8150394		2012-04-03	Bianconi et al.	
	69	8667542		2014-03-04	Bertz et al.	
	70	8793304		2014-07-29	Lu et al.	
	71	8948726		2015-02-03	Smith et al.	
	72	7860088		2010-12-28	Lioy, Marcello	
	73	8407763		2013-03-26	Weller et al.	
	74	8131840		2012-03-06	Denker, Richard E.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	75	7676673		2010-03-09	Weller et al.	
	76	7512128		2009-03-31	DiMambro et al.	
	77	7248570		2007-07-24	Bahl et al.	
	78	7024460		2006-04-04	Koopmas et al.	
	79	6748437		2004-06-08	Mankude et al.	
	80	6735206		2004-05-11	Oki et al.	
	81	6058434		2000-05-02	Wilt et al.	
	82	8032168		2011-10-04	Ikaheimo, Jorma	
	83	7966405		2011-06-21	Sundaresan et al.	
	84	7889384		2011-02-15	Armentrout et al.	
	85	6125391		2000-09-26	Meltzer et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	86	6038540		2000-03-14	Krist et al.	
	87	8504687		2013-08-06	Maffione et al.	
	88	7043225		2006-05-09	Patel et al.	
	89	6725256		2004-04-20	Albal et al.	
	90	6751296		2004-06-15	Albal et al.	
	91	6934751		2005-08-23	Jayapalan et al.	
	92	7174156		2007-02-06	Mangal, Manish	
	93	7636626		2009-12-22	Oesterling et al.	
	94	7720206		2010-05-18	Devolites et al.	
	95	8340678		2012-12-25	Pandey, Vinod	
	96	8005913		2011-08-23	Carlander, Carrie	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	97	6792461		2004-09-14	Hericourt, Olivier	
	98	7027055		2006-04-11	Anderson et al	
	99	8160056		2012-04-17	Van der Merwe et al.	
	100	5633868		1997-05-27	Baldwin et al.	
	101	7680086		2010-03-16	Eglin, Matthew George	
	102	7765294		2010-07-27	Edwards et al.	
	103	7843831		2010-11-30	Morrill et al.	
	104	8131858		2012-03-06	Agulnik et al.	
	105	8223655		2012-07-17	Heinz et al.	
	106	8385199		2013-02-26	Coward et al.	
	107	6061571		2000-05-09	Tamura, Hideo	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	108	6157636		2000-12-05	Voit et al.	
	109	7110753		2006-09-19	Campen, Kenneth Brian	
	110	8523547		2013-09-03	Pekrul, Merton W.	
	111	8875042		2014-10-28	Lejeune et al.	
	112	8315198		2012-11-20	Corneille et al.	
	113	9172553		2015-10-27	Dawes et al.	
	114	7770785		2010-08-10	Jha et al.	
	115	7817983		2010-10-19	Cassett et al.	
	116	8600895		2013-12-03	Felsher, David Paul	
	117	6535855		2003-03-18	Cahill et al.	
	118	6654786		2003-11-25	Fox et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	119	7272660		2007-09-18	Powers et al.	
	120	8065365		2011-11-22	Saxena et al.	
	121	8085808		2011-12-27	Brusca et al.	
	122	8325906		2012-12-04	Fullarton et al.	
	123	8448015		2013-05-21	Gerhart, David	
	124	8675852		2014-03-18	Maes, Stephane H.	
	125	8971912		2015-03-03	Chou et al.	
	126	8151205		2012-04-03	Follmann et al.	
	127	7133386		2006-11-07	Holur et al.	
	128	8744339		2014-06-03	Halfmann et al.	
	129	8811338		2014-08-19	Jin et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	130	8908516		2014-12-09	Tzamaloukas et al.	
	131	9030934		2015-05-12	Shah et al.	
	132	7440433		2008-10-21	Rink et al.	
	133	8191106		2012-05-29	Choyi et al.	
	134	6947985		2005-09-20	Hegli et al.	
	135	8195153		2012-06-05	Frencel et al.	
	136	8505073		2013-08-06	Taglienti et al.	
	137	8995952		2015-03-31	Baker et al.	
	138	8538421		2013-09-17	Brisebois et al.	
	139	8503358		2013-08-06	Hanson et al.	
	140	8271025		2012-09-18	Brisebois et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	141	7661124		2010-02-09	Ramanathan et al.	
	142	6141565		2000-10-31	Feurerstein et al.	
	143	6690918		2004-02-10	Evans et al.	
	144	7657920		2010-02-02	Arseneau et al.	
	145	7724716		2010-05-25	Fadell, Anthony M.	
	146	9325737		2016-04-26	Gutowski et al.	
	147	9344557		2016-05-17	Gruchala et al.	
	148	8731519		2014-05-20	Flynn et al.	
	149	8363799		2013-01-29	Gruchala et al.	
	150	6510152		2003-01-21	Gerszberg et al.	
	151	6542500		2003-04-01	Gerszberg et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	152	6546016		2003-04-08	Gerszberg et al.	
	153	6570974		2003-05-27	Gerszberg et al.	
	154	7082422		2006-07-25	Zirngibl et al.	
	155	7369848		2008-05-06	Jiang, Yue Jun	
	156	7577431		2009-08-18	Jiang, Yue Jun	
	157	7664494		2010-02-16	Jiang, Yue Jun	
	158	7873001		2011-01-18	Silver, Andrew	
	159	8219134		2012-07-10	Maharajh et al.	
	160	8291439		2012-10-16	Jethi et al.	
	161	9367680		2016-06-14	Mahaffey et al.	

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	2688553	CA		2008-12-04	Yoggie Security Systems, Inc.		
	2	1850575	EP		2007-10-31	Research In Motion Limited		

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	Jing et al., "Client-Server Computing in Mobile Environments," GTE Labs. Inc., Purdue University, ACM Computing Surveys, Vol. 31, No. 2, June 1999	
	2	Rivadeneyra et al., "A communication architecture to access data services through GSM," San Sebastian, Spain, 1998	
	3	Loopt User Guide, metroPCS, 7/17/2008	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	4	'Jentro Technologies launches Zenlet platform to accelerate location-based content delivery to mobile devices," The Mobile Internet, Boston, MA, Feb. 2008	
	5	'Ads and movies on the run," the Gold Coast Bulletin, Southport, Qld, Jan. 29, 2008	
	6	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	
	7	Kim, "Free wireless a high-wire act; MetroFi needs to draw enough ads to make service add profits," San Francisco Chronicle, Aug. 21, 2006	
	8	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	
	9	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	
	10	Sabat, "The evolving mobile wireless value chain and market structure," Nov. 2002	
	11	Nuzman et al., "A compund model for TCP connection arrivals for LAN and WAN applications," Oct. 22, 2002	
	12	Kuntze et al., "Trustworthy content push," Fraunhofer-Institute for Secure Information Technology SIT; Germany; WCNC 2007 proceedings, IEEE	
	13	Blackberry Mobile Data System, version 4.1, Technical Overview, 2006	
	14	Client Guide for Symantec Endpoint Protection and Symantec Network Access Control, 2007	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	15	Ehnert, "Small application to monitor IP trafic on a Blackberry - 1.01.03 ", March 27, 2008; http://www.ehnert.net/MiniMoni/	
	16	NetLimiter Lite 4.0.19.0; http://www.heise.de/download/netlimiter-lite-3617703.html from vol. 14/2007	
	17	Muntermann et al., "Potentiale und Sicherheitsanforderungen mobiler Finanzinformationsdienste und deren Systeminfrastrukturen," Chair of Mobile Commerce & Multilateral Security, Goethe Univ. Frankfurt, 2004	
	18	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	
	19	Fujitsu, "Server Push Technology Survey and Bidirectional Communication in HTTP Browser," January 9, 2008 (JP)	
	20	Windows7 Power Management, published April 2009	
	21	Open Mobile Alliance (OMA), Push Architecture, Candidate Version 2.2; Oct. 2, 2007; OMA-AD-Push-V2_2-20071002-C	

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	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

CERTIFICATION STATEMENT

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

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

OR

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

See attached certification statement.

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

☒ None

SIGNATURE

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

Signature	/James E. Harris/	Date (YYYY-MM-DD)	2016-07-25
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.

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

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

Application Number	15217538
Filing Date	2016-07-22
First Named Inventor	Raleigh
Art Unit	2447
Examiner Name	not yet assigned
Attorney Docket Number	RALEP007C11C3C2C2

U.S.PATENTS Remove

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

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20020022472		2002-02-21	WATLER et al.	
	2	20020120540		2002-08-29	KENDE et al.	
	3	20020131404		2002-09-19	MEHTA et al.	
	4	20020138601		2002-09-26	PIPONIUS et al.	
	5	20020176377		2002-11-28	HAMILTON, Thomas E.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

FOREIGN PATENT DOCUMENTS Remove

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

EFS Web 2.1.17

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	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	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

CERTIFICATION STATEMENT

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

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

OR

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

See attached certification statement.

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

☒ None

SIGNATURE

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

Signature	/James E. Harris/	Date (YYYY-MM-DD)	2016-07-25
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.

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

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

Application Number	15217538
Filing Date	2016-07-22
First Named Inventor	Raleigh
Art Unit	2447
Examiner Name	not yet assigned
Attorney Docket Number	RALEP007C11C3C2C2

U.S.PATENTS Remove

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

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20100030890		2010-02-04	Dutta, Satadip et al.	
	2	20080025230		2008-01-31	Patel, Alpesh et al.	
	3	20040170191		2004-09-02	Guo, Zihua et al.	
	4	20020188732		2002-12-12	Buckman, Charles R. et al.	
	5	20080034419		2008-02-07	Mullick, Amarnath et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	39	20080080457		2008-04-03	Cole, Terry L.	
	40	20090049518		2009-02-19	Roman et al.	
	41	20100248719		2010-09-30	Scholaert, Hugh	
	42	20060072451		2006-04-06	Ross, Alan D.	
	43	20070294410		2007-12-20	Pandya et al.	
	44	20070293191		2007-12-20	Mir et al.	
	45	20110145920		2011-06-16	Mahaffey et al.	
	46	20130326356		2013-12-05	Zheng et al.	
	47	20070005795		2007-01-04	Gonzalez, Ruben	
	48	20080282319		2008-11-13	Fontijn et al.	
	49	20080050715		2008-02-28	Golczewski et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	50	20040259534		2004-12-23	Chaudhari et al.	
	51	20090197612		2009-08-06	Kiiskinen, Arto	
	52	20100151866		2010-06-17	Karpov et al.	
	53	20060143066		2006-06-29	Calabria, Hermann	
	54	20040133668		2004-07-08	Nicholas III, Henry T.	
	55	20070073899		2007-03-29	Judge et al.	
	56	20060136882		2006-06-22	Noonan et al.	
	57	20070234402		2007-10-04	Khosravi et al.	
	58	20020154751		2002-10-24	Thompson et al.	
	59	20030084321		2003-05-01	Tarquini et al.	
	60	20070174490		2007-07-26	Choi et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	61	20090048913		2009-02-19	Shenfield et al.	
	62	20090181662		2009-07-16	Fleischman et al.	
	63	20020191573		2002-12-19	Whitehill et al.	
	64	20060098627		2006-05-11	Karaoguz, Jeyhan et al.	
	65	20090070379		2009-03-12	Rappaport, Theodore R.	
	66	20060095517		2006-05-04	O'Connor et al.	
	67	20040260766		2004-12-23	Barros et al.	
	68	20080034063		2008-02-07	Yee, Robert	
	69	20050041617		2005-02-24	Huotari et al.	
	70	20080018494		2008-01-24	Waite et al.	
	71	20060075506		2006-04-06	Sanda et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	72	20030159030		2003-08-21	Evans, Junius A.	
	73	20070257767		2007-11-08	Beeson, Curt	
	74	20060277590		2006-12-07	Limont et al.	
	75	20090036111		2009-02-05	Danford et al.	
	76	20050096024		2005-05-05	Bicker et al.	
	77	20040127208		2004-07-01	Nair et al.	
	78	20030134650		2003-07-17	Sundar et al.	
	79	20060291419		2006-12-28	McConnell et al.	
	80	20060126562		2006-06-15	Liu, Huitao	
	81	20090203352		2009-08-13	Fordon et al.	
	82	20100041365		2010-02-18	Lott et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	83	20140073291		2014-03-13	Hildner et al.	
	84	20080066181		2008-03-13	Haveson et al.	
	85	20080212751		2008-09-04	Chung, Simon	
	86	20070255769		2007-11-01	Agrawal et al.	
	87	20100121744		2010-05-13	Belz et al.	
	88	20080126287		2008-05-29	Cox et al.	
	89	20030028623		2003-02-06	Hennessey et al.	
	90	20070299965		2007-12-27	Nieh et al.	
	91	20070061800		2007-03-15	Cheng et al.	
	92	20060200663		2006-09-07	Thornton, Andrew J.	
	93	20050060525		2005-03-17	Schwartz et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	94	20070297378		2007-12-27	Poyhonen et al.	
	95	20090006229		2009-01-01	Sweeney et al.	
	96	20090217364		2009-08-27	Salmela et al.	
	97	20050108075		2005-05-19	Douglis et al.	
	98	20070255797		2007-11-01	Dunn et al.	
	99	20090042536		2009-02-12	Bernard et al.	
	100	20090307696		2009-12-10	Vals et al.	
	101	20040176104		2004-09-09	Arcens, Suzanne	
	102	20060099970		2006-05-11	Morgan et al.	
	103	20020120370		2002-08-29	Parupudi et al.	
	104	20040243680		2004-12-02	Mayer, Georg	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	105	20080279216		2008-11-13	Sharif-Ahmadi et al.	
	106	20040225561		2004-11-11	Hertzberg et al.	
	107	20090016310		2009-01-15	Rasal, Digambar L.	
	108	20080096559		2008-04-24	Phillips 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	1310401A	CN		2000-02-22	Wang, Di Xing		
	2	1878160A	CN		2006-12-13	Jiang, Yong		
	3	101127988A	CN		2008-02-20	ZTE Corporation		
	4	1503548 A1	EP		2005-02-02	FG Microtec GmbH		
	5	3148713 B2	JP		2001-03-26	ATR Kankyo Tekio Tsushin Kenkyusho		

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	6	2009-218773	JP		2009-09-24	Advanced Telecommunication Research Institute Inte		
	7	2006093961	WO		2006-09-08	Kyocera Wireless Corp.		
	8	2007-318354	JP		2007-12-06	Fujitsu Ten Ltd.		
	9	2007126352	WO		2007-11-08	Telefonaktiebolaget LM Ericsson		
	10	2009-212707	JP		2009-09-17	Fujitsu Ltd.		
	11	2008-301121	JP		2008-12-11	Kyocera Corp.		
	12	101335666A	CN		2008-12-31	Hangzhou H3C Technologies Co., Ltd.		
	13	101080055A	CN		2007-11-28	Tencent Technology (Shenzhen) Co., Ltd.		
	14	2009-232107	JP		2009-10-08	Fujitsu Ltd.		
	15	2009-111919	JP		2009-05-21	Kyocera Communications Systems		
	16	2009008817	WO		2009-01-15	Ericsson		

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	17	2002045315	WO		2002-06-06	Micromuse		
	18	2009091295	WO		2009-07-23	Telefonaktiebolaget LM Ericsson		
	19	2002093877	WO		2002-11-21	Nokia Corp.		
	20	2006004784	WO		2006-01-12	Japan Communications Inc.		
	21	2005339247A	JP		2005-12-08	Secured Communications		
	22	2006155263A	JP		2006-06-15	NEC Corporation		
	23	1345154A	CN		2002-04-17	Datang Microelectronics Tech. Co.		
	24	2006-197137	JP		2006-07-27	NTT Docomo Inc.		
	25	2006-344007	JP		2006-12-21	Hitachi Ltd.		
	26	2005083934	WO		2005-09-09	Research In Motion Limited		

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

NON-PATENT LITERATURE DOCUMENTS Remove

EFS Web 2.1.17

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	Dixon et al., "Triple Play Digital Services: Comcast and Verizon (Digital Phone, Television, and Internet), August 2007	

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

EXAMINER SIGNATURE

Examiner Signature		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	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

CERTIFICATION STATEMENT

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

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

OR

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

See attached certification statement.

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

☒ None

SIGNATURE

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

Signature	/James E. Harris/	Date (YYYY-MM-DD)	2016-07-25
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.

Electronic Acknowledgement Receipt

EFS ID:	26468424
Application Number:	15217538
International Application Number:	
Confirmation Number:	3305
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:	RALEP007C11C3C2C2
Receipt Date:	27-JUL-2016
Filing Date:	
Time Stamp:	12:42:26
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Assignee showing of ownership per 37 CFR 3.73	P007C11C3C2C2_Statement.pdf	117960 7d1f05f40d5f5b7af28d02d653cdf06c9c35279b	no	3

Warnings:

Information:					
2	Transmittal Letter	P007C11C3C2C2_IDSTransLtr.pdf	60565 46218d725c7cf39c7786adfcc8cf35a9c99f2915	no	2
Warnings:					
Information:					
3	Information Disclosure Statement (IDS) Form (SB08)	IDS1.pdf	622629 b32cfbcc51a958ebe32160b6b1e11c9799ce2421	no	36
Warnings:					
Information:					
4	Information Disclosure Statement (IDS) Form (SB08)	IDS2.pdf	621513 1a6706d065fe91ae94588b33f15f6181a5a9e142	no	33
Warnings:					
Information:					
5	Information Disclosure Statement (IDS) Form (SB08)	IDS3.pdf	617644 dbf75e64884eb518562342b86da1a37045e6633d	no	20
Warnings:					
Information:					
6	Information Disclosure Statement (IDS) Form (SB08)	IDS4.pdf	619084 e609afff25e1f7c9fcfe73bf3ff328ea782cf065	no	31
Warnings:					
Information:					
7	Information Disclosure Statement (IDS) Form (SB08)	IDS5.pdf	615847 972bf36ece5b0cb5992db3fd86ff3729ce5fdb8d	no	16
Warnings:					
Information:					
			Total Files Size (in bytes):	3275242	

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

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

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

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

PTO/AIA/96 (08-12)
Approved for use through 01/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act 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: Raleigh

Application No./Patent No.: 15/217,538 Filed/Issue Date: July 22, 2016

Titled: Mobile Device and Method With Secure Network Messaging for Authorized Components

Headwater Partners I LLC, a limited liability company

(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

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

1. ☑ The assignee of the entire right, title, and interest.

2. ☐ An assignee of less than the entire right, title, and interest (check applicable box):

   ☐ The extent (by percentage) of its ownership interest is _____%. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.

   ☐ There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

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

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

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

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

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

A. ☑ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel 039236, Frame 0607, or for which a copy thereof is attached.

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

   1. From: _____ To: _____

      The document was recorded in the United States Patent and Trademark Office at

      Reel _____, Frame _____, or for which a copy thereof is attached.

   2. From: _____ To: _____

      The document was recorded in the United States Patent and Trademark Office at

      Reel _____, Frame _____, or for which a copy thereof is attached.

This collection of information is required 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.

PTO/AIA/96 (08-12)
Approved for use through 01/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

3. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

4. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

5. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

6. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

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

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

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

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

/James E.Harris/	2016-07-25
Signature	Date
James E. Harris	40013
Printed or Typed Name	Title or Registration Number

Privacy Act Statement

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

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

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Raleigh	Examiner:	not yet assigned
Serial No.:	15/217,538	Art Unit:	2447
Filed:	July 22, 2016	Conf. No.:	3305
Title:	Mobile Device and Method With Secure Network Messaging for Authorized Components		

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. 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: July 25, 2016

By: /James E. Harris/

James E. Harris
Reg. No. 40013
Headwater Partners I 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: July 27, 2016 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
15/217,538	07/22/2016	2447	1530	RALEP007C11C3C2C2	14	2

CONFIRMATION NO. 3305

106963
Headwater Partners I LLC
1011 Pruitt Place
Tyler, TX 75703

FILING RECEIPT

OC000000084833741

Date Mailed: 08/05/2016

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

Inventor(s)

Gregory G. Raleigh, Woodside, CA;

Applicant(s)

Headwater Partners I 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 14/979,233 12/22/2015
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: 08/03/2016

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 15/217,538**

Projected Publication Date: 11/10/2016

Non-Publication Request: No

Early Publication Request: No
**** 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.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 15/217,538

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))	14 minus 20 =	*	x 40 =	0.00	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	2 minus 3 =	*	x 210 =	0.00			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			800			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	1530		TOTAL	

APPLICATION AS AMENDED - PART II

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

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

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

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

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/217,538	07/22/2016	Gregory G. Raleigh	RALEP007C11C3C2C2	3305

106963 7590 08/25/2016

Headwater Partners I LLC
1011 Pruitt Place
Tyler, TX 75703

EXAMINER	
RUDY, ANDREW J	

ART UNIT	PAPER NUMBER
3687	

NOTIFICATION DATE	DELIVERY MODE
08/25/2016	ELECTRONIC

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

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

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

patent@headwaterllc.com
krista@jacobseniplaw.com

UNITED STATES PATENT AND TRADEMARK OFFICE

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

Doc Code: TRACK1.GRANT

Decision Granting Request for Prioritized Examination (Track I or After RCE)	Application No.:15/217,538

1. THE REQUEST FILED July 22, 2016 IS **GRANTED.**

The above-identified application has met the requirements for prioritized examination
- A. ☒ for an original nonprovisional application (Track I).
- B. ☐ for an application undergoing continued examination (RCE).

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

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

Telephone inquiries with regard to this decision should be directed to Vanitha Elgart at 571-272-7395.

/Vanitha Elgart/
Vanitha Elgart
[Signature]

Petitions Examiner, Office of Petitions
(Title)

U.S. Patent and Trademark Office
PTO-2298 (Rev. 02-2012)

Office of Petitions: Routing Sheet



Application No. 15/217,538

This application is being forwarded to your office for further processing. A decision has been rendered on a petition filed in this application, as indicated below. For details of this decision, please see the document PET.OP.DEC filed on the same date as this document.

- [X] **GRANTED**
- [ ] **DISMISSED**
- [ ] **DENIED**

Office of Petitions: Decision Count Sheet

Mailing Month

Application No. 15217538

15217538

For US serial numbers: enter number only, no slashes or commas. Ex: 10123456
For PCT: enter "51+single digit of year of filing+last 5 numbers", Ex. for PCT/US05/12345, enter 51512345

Deciding Official: ELGART, VANITHA

Count (1) - Palm Credit 15/217,538

Decision: GRANT

FINANCE WORK NEEDED
☐ Select Check Box for YES

GRANT

Decision Type: 643 - Track One request

643

Notes:

Count (2)

Decision: n/a

FINANCE WORK NEEDED
☐ Select Check Box for YES

Decision Type: NONE

Notes:

Count (3)

Decision: n/a

FINANCE WORK NEEDED
☐ Select Check Box for YES

Decision Type: NONE

Notes:

Initials of Approving Official (if required)

If more than 3 decisions, attach 2nd count sheet & mark this box ☐

Printed on:

Office of Petitions Internal Document - Ver. 5.0

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 09/16/2016

Headwater Partners I LLC
1011 Pruitt Place
Tyler, TX 75703

EXAMINER
RUDY, ANDREW J

ART UNIT	PAPER NUMBER
3687	

DATE MAILED: 09/16/2016

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/217,538	07/22/2016	Gregory G. Raleigh	RALEP007C11C3C2C2	3305

TITLE OF INVENTION: AUTOMATED DEVICE PROVISIONING AND ACTIVATION

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	12/16/2016

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

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

HOW TO REPLY TO THIS NOTICE:

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

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

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

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

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

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

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

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

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

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

106963 7590 09/16/2016
Headwater Partners I 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 facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/217,538	07/22/2016	Gregory G. Raleigh	RALEP007C11C3C2C2	3305

TITLE OF INVENTION: AUTOMATED DEVICE PROVISIONING AND ACTIVATION

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	12/16/2016

EXAMINER	ART UNIT	CLASS-SUBCLASS
RUDY, ANDREW J	3687	455-411000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
- ❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

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

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

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

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

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

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

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

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

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

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/217,538	07/22/2016	Gregory G. Raleigh	RALEP007C11C3C2C2	3305

106963 7590 09/16/2016

Headwater Partners I LLC
1011 Pruitt Place
Tyler, TX 75703

EXAMINER	
RUDY, ANDREW J	
ART UNIT	PAPER NUMBER
3687	

DATE MAILED: 09/16/2016

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

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

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

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

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

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

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

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

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

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

Notice of Allowability	Application No. 15/217,538	Applicant(s) RALEIGH, GREGORY G.	
	Examiner ANDREW JOSEPH RUDY	Art Unit 3687	AIA (First Inventor to File) Status No

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

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

1. ☒ This communication is responsive to *the 23 July 2016 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 *2-15*. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

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

   * Certified copies not received: _____.

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

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

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

Attachment(s)

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

DETAILED ACTION

Notice of Pre-AIA or AIA Status

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

2. Applicant cancelled claim 1 from the July 23, 2016 Amendment.

3. Pertinent references of interest are noted on the attached PTO-892.

4. Applicant's five (5) Information Disclosure Statement's (IDS's) have been reviewed. Note the attached IDS's.

Allowable Subject Matter

5. Claims 2-15 are allowed.

6. The following is an examiner's statement of reasons for allowance: Applicant's April 3, 2015 Amendment regarding claims 2-15 have been reviewed. Claims 2-15 are allowed as the prior art, either alone or in combination, does not disclose Applicant's inventive claim language.

Claims 2-15 have been reviewed in light of Alice Corporation Pty. Ltd. v. CLS Bank International, et al., 573 U. S. ___ (2014) and are not deemed invalidated by such.

Claims 2-15 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.”

7. 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, Fahd A. Obeid can be reached on 571-270-3324. 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. 15/217,538	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-9,298,723 B1	03-2016	Vincent; Pradeep	G06F17/30156	1/1
*	B	US-8,819,253 B2	08-2014	Simeloff; Ezra	G06F21/31	709/229
*	C	US-8,788,661 B2	07-2014	Raleigh; Gregory G.	G06Q50/06	455/406
*	D	US-8,787,249 B2	07-2014	Giaretta; Gerardo	H04L12/14	370/328
*	E	US-8,639,215 B2	01-2014	McGregor; Gregory M.	G06Q20/32	455/406
*	F	US-8,160,056 B2	04-2012	Van der Merwe; Jacobus E.	H04L45/04	370/351
*	G	US-8,140,690 B2	03-2012	Ly; Kand	H04L67/2814	709/226
*	H	US-8,044,792 B2	10-2011	Orr; David	G05B19/0428	340/3.1
*	I	US-8,036,387 B2	10-2011	Kudelski; Henri	H04N7/162	380/278
*	J	US-7,660,419 B1	02-2010	Ho; Jin-Meng	H04L9/0844	380/270
*	K	US-6,601,040 B1	07-2003	Kolls; H. Brock	G07F5/18	705/14.23
*	L	US-6,401,113 B2	06-2002	Lazaridis; Mihal	H04L51/14	340/7.21
*	M	US-5,617,539 A	04-1997	Ludwig; Lester F.	G06Q10/10	348/14.03

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
	15217538	RALEIGH, GREGORY G.
	Examiner	**Art Unit**
	ANDREW J RUDY	3687

CPC						
Symbol					**Type**	**Version**
H04W		4	/	001	F	2013-01-01
H04W		28	/	0215	I	2013-01-01
H04L		47	/	20	I	2013-01-01
H04W		88	/	06	A	2013-01-01
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			

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

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	14	
/ANDREW JOSEPH RUDY/ Primary Examiner.Art Unit 3687	9/12/2016	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	25

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15217538	RALEIGH, GREGORY G.
	Examiner	**Art Unit**
	ANDREW J RUDY	3687

US ORIGINAL CLASSIFICATION		INTERNATIONAL CLASSIFICATION										
CLASS	SUBCLASS	CLAIMED					NON-CLAIMED					
455	411	H	0	4	M	1 / 66 (2006.01.01)						
CROSS REFERENCE(S)												
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)											
370	252											

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	14	
/ANDREW JOSEPH RUDY/ Primary Examiner.Art Unit 3687	9/12/2016	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	25

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15217538	RALEIGH, GREGORY G.
	Examiner	**Art Unit**
	ANDREW J RUDY	3687

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

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

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	14	
/ANDREW JOSEPH RUDY/ Primary Examiner.Art Unit 3687	9/12/2016	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	25

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

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

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

Application Number	15217538
Filing Date	2016-07-22
First Named Inventor	Raleigh
Art Unit	2447
Examiner Name	not yet assigned
Attorney Docket Number	RALEP007C11C3C2C2

U.S.PATENTS Remove

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

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20100030890		2010-02-04	Dutta, Satadip et al.	
	2	20080025230		2008-01-31	Patel, Alpesh et al.	
	3	20040170191		2004-09-02	Guo, Zihua et al.	
	4	20020188732		2002-12-12	Buckman, Charles R. et al.	
	5	20080034419		2008-02-07	Mullick, Amarnath et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	39	20080080457		2008-04-03	Cole, Terry L.	
	40	20090049518		2009-02-19	Roman et al.	
	41	20100248719		2010-09-30	Scholaert, Hugh	
	42	20060072451		2006-04-06	Ross, Alan D.	
	43	20070294410		2007-12-20	Pandya et al.	
	44	20070293191		2007-12-20	Mir et al.	
	45	20110145920		2011-06-16	Mahaffey et al.	
	46	20130326356		2013-12-05	Zheng et al.	
	47	20070005795		2007-01-04	Gonzalez, Ruben	
	48	20080282319		2008-11-13	Fontijn et al.	
	49	20080050715		2008-02-28	Golczewski et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	50	20040259534		2004-12-23	Chaudhari et al.	
	51	20090197612		2009-08-06	Kiiskinen, Arto	
	52	20100151866		2010-06-17	Karpov et al.	
	53	20060143066		2006-06-29	Calabria, Hermann	
	54	20040133668		2004-07-08	Nicholas III, Henry T.	
	55	20070073899		2007-03-29	Judge et al.	
	56	20060136882		2006-06-22	Noonan et al.	
	57	20070234402		2007-10-04	Khosravi et al.	
	58	20020154751		2002-10-24	Thompson et al.	
	59	20030084321		2003-05-01	Tarquini et al.	
	60	20070174490		2007-07-26	Choi et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	61	20090048913		2009-02-19	Shenfield et al.	
	62	20090181662		2009-07-16	Fleischman et al.	
	63	20020191573		2002-12-19	Whitehill et al.	
	64	20060098627		2006-05-11	Karaoguz, Jeyhan et al.	
	65	20090070379		2009-03-12	Rappaport, Theodore R.	
	66	20060095517		2006-05-04	O'Connor et al.	
	67	20040260766		2004-12-23	Barros et al.	
	68	20080034063		2008-02-07	Yee, Robert	
	69	20050041617		2005-02-24	Huotari et al.	
	70	20080018494		2008-01-24	Waite et al.	
	71	20060075506		2006-04-06	Sanda et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	72	20030159030		2003-08-21	Evans, Junius A.	
	73	20070257767		2007-11-08	Beeson, Curt	
	74	20060277590		2006-12-07	Limont et al.	
	75	20090036111		2009-02-05	Danford et al.	
	76	20050096024		2005-05-05	Bicker et al.	
	77	20040127208		2004-07-01	Nair et al.	
	78	20030134650		2003-07-17	Sundar et al.	
	79	20060291419		2006-12-28	McConnell et al.	
	80	20060126562		2006-06-15	Liu, Huitao	
	81	20090203352		2009-08-13	Fordon et al.	
	82	20100041365		2010-02-18	Lott et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	83	20140073291		2014-03-13	Hildner et al.	
	84	20080066181		2008-03-13	Haveson et al.	
	85	20080212751		2008-09-04	Chung, Simon	
	86	20070255769		2007-11-01	Agrawal et al.	
	87	20100121744		2010-05-13	Belz et al.	
	88	20080126287		2008-05-29	Cox et al.	
	89	20030028623		2003-02-06	Hennessey et al.	
	90	20070299965		2007-12-27	Nieh et al.	
	91	20070061800		2007-03-15	Cheng et al.	
	92	20060200663		2006-09-07	Thornton, Andrew J.	
	93	20050060525		2005-03-17	Schwartz et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	94	20070297378		2007-12-27	Poyhonen et al.	
	95	20090006229		2009-01-01	Sweeney et al.	
	96	20090217364		2009-08-27	Salmela et al.	
	97	20050108075		2005-05-19	Douglis et al.	
	98	20070255797		2007-11-01	Dunn et al.	
	99	20090042536		2009-02-12	Bernard et al.	
	100	20090307696		2009-12-10	Vals et al.	
	101	20040176104		2004-09-09	Arcens, Suzanne	
	102	20060099970		2006-05-11	Morgan et al.	
	103	20020120370		2002-08-29	Parupudi et al.	
	104	20040243680		2004-12-02	Mayer, Georg	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	105	20080279216		2008-11-13	Sharif-Ahmadi et al.	
	106	20040225561		2004-11-11	Hertzberg et al.	
	107	20090016310		2009-01-15	Rasal, Digambar L.	
	108	20080096559		2008-04-24	Phillips 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]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	1310401A	CN		2000-02-22	Wang, Di Xing		
	2	1878160A	CN		2006-12-13	Jiang, Yong		
	3	101127988A	CN		2008-02-20	ZTE Corporation		
	4	1503548 A1	EP		2005-02-02	FG Microtec GmbH		
	5	3148713 B2	JP		2001-03-26	ATR Kankyo Tekio Tsushin Kenkyusho		

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	6	2009-218773	JP		2009-09-24	Advanced Telecommunication Research Institute Inte		
	7	2006093961	WO		2006-09-08	Kyocera Wireless Corp.		
	8	2007-318354	JP		2007-12-06	Fujitsu Ten Ltd.		
	9	2007126352	WO		2007-11-08	Telefonaktiebolaget LM Ericsson		
	10	2009-212707	JP		2009-09-17	Fujitsu Ltd.		
	11	2008-301121	JP		2008-12-11	Kyocera Corp.		
	12	101335666A	CN		2008-12-31	Hangzhou H3C Technologies Co., Ltd.		
	13	101080055A	CN		2007-11-28	Tencent Technology (Shenzhen) Co., Ltd.		
	14	2009-232107	JP		2009-10-08	Fujitsu Ltd.		
	15	2009-111919	JP		2009-05-21	Kyocera Communications Systems		
	16	2009008817	WO		2009-01-15	Ericsson		

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	17	2002045315	WO		2002-06-06	Micromuse		
	18	2009091295	WO		2009-07-23	Telefonaktiebolaget LM Ericsson		
	19	2002093877	WO		2002-11-21	Nokia Corp.		
	20	2006004784	WO		2006-01-12	Japan Communications Inc.		
	21	2005339247A	JP		2005-12-08	Secured Communications		
	22	2006155263A	JP		2006-06-15	NEC Corporation		
	23	1345154A	CN		2002-04-17	Datang Microelectronics Tech. Co.		
	24	2006-197137	JP		2006-07-27	NTT Docomo Inc.		
	25	2006-344007	JP		2006-12-21	Hitachi Ltd.		
	26	2005083934	WO		2005-09-09	Research In Motion Limited		

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

NON-PATENT LITERATURE DOCUMENTS [Remove]

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	Dixon et al., "Triple Play Digital Services: Comcast and Verizon (Digital Phone, Television, and Internet), August 2007	

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

EXAMINER SIGNATURE

Examiner Signature	/Andrew Joseph Rudy/	Date Considered	09/12/2016

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

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.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. 3305

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
15/217,538	07/22/2016 RULE	705	3687	RALEP007C11C3C2C2

APPLICANTS
Headwater Partners I LLC, Tyler, TX;

INVENTORS
Gregory G. Raleigh, Woodside, CA;

**** CONTINUING DATA **************************
This application is a CON of 14/979,233 12/22/2015
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 **
08/03/2016

Foreign Priority claimed ☐ Yes ☑ No 35 USC 119(a-d) conditions met ☐ Yes ☑ No Verified and Acknowledged /ANDREW JOSEPH RUDY/ Examiner's Signature	☐ Met after Allowance Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
		CA	106	14	2

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

TITLE
Automated Device Provisioning and Activation

FILING FEE RECEIVED	FEES: Authority has been given in Paper	☐ All Fees
1530	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

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

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

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

Application Number	15217538
Filing Date	2016-07-22
First Named Inventor	Raleigh
Art Unit	2447
Examiner Name	not yet assigned
Attorney Docket Number	RALEP007C11C3C2C2

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5577100		1996-11-19	McGREGOR et al.	
	2	5794142		1998-08-11	VANTTILA et al.	
	3	5892900		1999-04-06	GINTER et al.	
	4	5903845		1999-05-11	BUHRMANN et al.	
	5	5933778		1999-08-03	BUHRMANN et al.	
	6	5940472		1999-08-17	NEWMAN et al.	
	7	6047268		2000-04-04	BARTOLI et al.	
	8	6078953		2000-06-20	VAID et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

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

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

FOREIGN PATENT DOCUMENTS Remove

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

EFS Web 2.1.17

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5
	1	3rd Generation Partnership Project, "Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) Enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) Access," Release 8, Document No. 3GPP TS 23.401, V8.4.0, December 2008	
	2	3rd Generation Partnership Project, "Technical Specification Group Services and System Aspects; Policy and Charging Control Architecture," Release 8, Document No. 3GPP TS 23.203, V8.4.0, December 2008	
	3	ALONISTIOTI et al., "Intelligent Architectures Enabling Flexible Service Provision and Adaptability," 2002	
	4	Amazon Technologies, Inc., "Kindle™ User's Guide," 3rd Edition, Copyright 2004-2009	
	5	CHANDRASEKHAR et al., "Femtocell Networks: A Survey," June 28, 2008	
	6	CHAOUCHI et al., "Policy Based Networking in the Integration Effort of 4G Networks and Services," 2004 IEEE	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

EXAMINER SIGNATURE

Examiner Signature	/Andrew Joseph Rudy/	Date Considered	09/12/2016

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

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

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

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

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

Application Number	15217538
Filing Date	2016-07-22
First Named Inventor	Raleigh
Art Unit	2447
Examiner Name	not yet assigned
Attorney Docket Number	RALEP007C11C3C2C2

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	8447980		2013-05-21	Godfrey, James A. et al.	
	2	8429403		2013-04-23	Moret, Eric et al.	
	3	8411587		2013-04-02	Curtis, William et al.	
	4	8396929		2013-03-12	Helfman, Nadav et al.	
	5	8363658		2013-01-29	Delker, Jason R. et al.	
	6	8265004		2012-09-11	Toutonghi, Michael J.	
	7	8233895		2012-07-31	Tysowski, Piotr Konrad	
	8	7685254		2010-03-23	Pandya, Ashish A.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	240	8634425		2014-01-21	Gorti et al.	
	241	8825109		2014-09-02	Montemurro et al.	
	242	9014973		2015-04-21	Ruckart, John	
	243	8977284		2015-03-10	Reed, Mark J.	
	244	8930238		2015-01-06	Coffman et al.	
	245	8880047		2014-11-04	Konicek et al.	
	246	8739035		2014-05-27	Trethewey, Jim	
	247	8571598		2013-07-16	Valavi, John J.	
	248	8489110		2013-07-16	Frank et al.	
	249	8406736		2013-03-26	Das et al.	
	250	8259692		2012-09-04	Bajko, Gabor	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	251	8233433		2012-07-31	Kalhan, Amit	
	252	8155666		2012-04-10	Alizadeh-Shabdiz, Farshid	
	253	8103285		2012-01-24	Kalhan, Amit	
	254	7936736		2011-05-03	Proctor Jr., James Arthur et al.	
	255	7925778		2011-04-12	Wijnands et al.	
	256	7760137		2010-07-20	Martucci et al.	
	257	7684370		2010-03-23	Kezys, Vytautas Robertas	
	258	7084775		2006-08-01	Smith, Michael R.	
	259	6578076		2003-06-10	Putzolu, David Matthew	
	260	7133695		2006-11-07	Beyda, William J.	
	261	7260382		2007-08-21	Lamb et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	262	7685530		2010-03-23	Sherrard et al.	
	263	7937450		2011-05-03	Janik, Craig M.	
	264	8019846		2011-09-13	Roelens et al.	
	265	8050705		2011-11-01	Sicher et al.	
	266	8086791		2011-12-27	Caulkins, Jason	
	267	7627872		2009-12-01	Hebeler et al.	
	268	8532610		2013-09-10	Manning Cassett et al.	
	269	8831561		2014-09-09	Sutaria et al.	
	270	8010082		2011-08-30	Sutaria et al.	
	271	7271765		2007-09-18	Stilp et al.	
	272	7843843		2010-11-30	Papp III et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	273	8495181		2013-07-23	Venkatraman et al.	
	274	9049010		2015-06-02	Jueneman et al.	
	275	8174378		2012-05-08	Richman et al.	
	276	6757717		2004-06-29	Goldstein, Leonid	
	277	7007295		2006-02-28	Rose et al.	
	278	8208788		2012-06-26	Ando et al.	
	279	8326828		2012-12-04	Zhou et al.	
	280	8761711		2014-06-24	Grignani et al.	
	281	7222190		2007-05-22	Klinker, Eric et al.	
	282	8713535		2014-04-29	Malhotra et al.	
	283	5572528		1996-11-05	Shuen, Pauline	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	284	5754953		1998-05-19	Briancon et al.	
	285	6628934		2003-09-30	Rosenberg et al.	
	286	6662014		2003-12-09	Walsh, Patrick Jay	
	287	6901440		2005-05-31	Bimm et al.	
	288	6970692		2005-11-29	Tysor, Arthur James	
	289	7203752		2007-04-10	Rice et al.	
	290	7224968		2007-05-29	Dobson et al.	
	291	7379731		2008-05-27	Natsuno et al.	
	292	7457870		2008-11-25	Lownsbrough et al.	
	293	7515926		2009-04-07	Bu et al.	
	294	7536695		2009-05-19	Alam et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	295	7586871		2009-09-08	Hamilton et al.	
	296	7752330		2010-07-06	Olsen et al.	
	297	7792257		2010-09-07	Vanier et al.	
	298	7801783		2010-09-21	Kende et al.	
	299	7865187		2011-01-04	Ramer et al.	
	300	7933274		2011-04-26	Verma 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.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	1	1538730A	CN		2004-10-20	Zhongxing Communication Co., Ltd.		
	2	101115248A	CN		2008-01-30	Lenovo Beijing Ltd.		
	3	101341764A	CN		2009-01-07	Telefonaktiebolaget LM Ericsson		
	4	2007068288A1	WO		2007-06-21	Telefonaktiebolaget LM Ericsson		
	5	1802839A	CN		2006-07-12	Motorola Inc.		
	6	2004064306A2	WO		2004-07-29	Motorola Inc.		
	7	101123553A	CN		2007-09-11	SouTheast University		
	8	1937511A	CN		2007-03-28	ZTE		
	9	1999027723 A1	WO		1999-06-03	Telefonaktiebolaget LM Ericsson		
	10	2007133844	WO		2007-11-22	Camiant, Inc.		
	11	101183958A	CN		2008-05-21	Huawei Tech. Co. Ltd.		

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	12	1801829A	CN		2006-07-12	Kunda Computer Technology (Kunshan) Co., Ltd.		
	13	1867024A	CN		2006-11-22	Huawei Technologies Co., Ltd.		
	14	101815275A	CN		2010-08-25	Yang, Liu		
	15	1567818A	CN		2005-01-19	Huawei Tech. Co. Ltd.		
	16	2006012610	WO		2006-02-02	Citrix Systems, Inc.		
	17	1508734A	CN		2004-06-30	Chinese Creative Corp.		

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

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5
	1	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	
	2	"The Construction of Intelligent Residential District in Use of Cable Television Network," Shandong Science, Vol. 13, No. 2, June 2000	
	3	"Communication Concepts for Mobile Agent Systems," by Joachim Baumann et al.; Inst. Of Parallel and Distributed High-Performance Systems, Univ. of Stuttgart, Germany, pp. 123-135, 1997	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	4	"End to End QoS Solution for Real-time Multimedia Application;" Computer Engineering and Applications, 2007, 43 (4): 155-159, by Tan Zu-guo, Wang Wen-juan; Information and Science School, Zhanjian Normal College, Zhan jiang, Guangdong 524048, China	
	5	"ASA/PIX: Allow Split Tunneling for VPN Clients on the ASA Configuration Example," Document ID 70917, January 10, 2008	
	6	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	
	7	Kassar et al., "An overview of vertical handover decision strategies in heterogeneous wireless networks," ScienceDirect, University Pierre & Marie Curie, Paris, France, 6/5/2007	
	8	Schiller et al., "Location-Based Services," The Morgan Kaufmann Series in Data Management Systems, 2004	
	9	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	

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

EXAMINER SIGNATURE

Examiner Signature	/Andrew Joseph Rudy/	Date Considered	09/12/2016

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

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

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

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

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

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

Application Number	15217538
Filing Date	2016-07-22
First Named Inventor	Raleigh
Art Unit	2447
Examiner Name	not yet assigned
Attorney Docket Number	RALEP007C11C3C2C2

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	8005726		2011-08-23	Bao, Yulin	
	2	8050690		2011-11-01	Neeraj, Chawla	
	3	8086398		2011-12-27	Sanchez et al.	
	4	8107953		2012-01-31	Zimmerman et al.	
	5	8112435		2012-02-07	Epstein et al.	
	6	8195661		2012-06-05	Kalavade, Asawaree	
	7	8200163		2012-06-12	Hoffman, George E.	
	8	8200818		2012-06-12	Freund et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	9	8254880		2012-08-28	Aaltonen et al.	
	10	8270955		2012-09-18	Ramer et al.	
	11	8331223		2012-12-11	Hill et al.	
	12	8358975		2013-01-22	Bahl et al.	
	13	8533775		2013-09-10	Alcorn et al.	
	14	8538394		2013-09-17	Zimmerman et al.	
	15	8538458		2013-09-17	Haney, Richard D.	
	16	8565746		2013-10-22	Hoffman, George E.	
	17	8571501		2013-10-29	Miller et al.	
	18	8644702		2014-02-04	Kalajan, Kevin E.	
	19	8713641		2014-04-29	Pagan et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	20	8730842		2014-05-20	Collins et al.	
	21	8732808		2014-05-20	Sewall et al.	
	22	6445777		2002-09-03	Clark, Curtis	
	23	7039027		2006-05-02	Bridgelall, Raj	
	24	7990049		2011-08-02	Shioya, Shunsuke	
	25	8180886		2012-05-15	Overcash et al.	
	26	8339991		2012-12-25	Biswas et al.	
	27	7149521		2006-12-12	Sundar et al.	
	28	7200112		2007-04-03	Sundar et al.	
	29	7395244		2008-07-01	Kingsford, Bryan	
	30	7411930		2008-08-12	Montojo, Juan et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	31	7508799		2009-03-24	Sumner et al.	
	32	7554983		2009-06-30	Muppala, Suresh	
	33	7564799		2009-07-21	Holland et al.	
	34	7849477		2010-12-07	Cristofalo et al.	
	35	7987496		2011-07-26	Bryce et al.	
	36	8503455		2013-08-06	Heikens, Heico	
	37	RE44412		2013-08-06	Naqvi et al.	
	38	5974439		1999-10-26	Bollella, Gregory	
	39	6882718		2005-04-19	Smith, Benjamin V.	
	40	7058022		2006-06-06	Carolan et al.	
	41	7017189		2006-03-21	DeMello et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	42	7266371		2007-09-04	Amin et al.	
	43	8190122		2012-05-29	Alexander et al.	
	44	9002342		2015-04-07	Tenhunen et al.	
	45	8385964		2013-02-26	Haney, Richard D.	
	46	8504032		2013-08-06	Lott et al.	
	47	7366654		2008-04-29	Moore, Robert C.	
	48	7391724		2008-06-24	Alakoski et al.	
	49	7978686		2011-07-12	Goyal et al.	
	50	8644813		2014-02-04	Gailloux et al.	
	51	6393014		2002-05-21	Daly et al.	
	52	6397259		2002-05-28	Lincke et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	53	7047276		2006-05-16	Liu et al.	
	54	7627767		2009-12-01	Sherman et al.	
	55	7849161		2010-12-07	Koch et al.	
	56	7894431		2011-02-22	Goring et al.	
	57	8073427		2011-12-06	Koch et al.	
	58	8522337		2013-08-27	Adusumilli et al.	
	59	8527662		2013-09-03	Biswas et al.	
	60	8572256		2013-10-29	Babbar, Uppinder Singh	
	61	8966018		2015-02-24	Bugwadia et al.	
	62	7162237		2007-01-09	Silver et al.	
	63	7454191		2008-11-18	Dawson et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	64	7817615		2010-10-19	Breau et al.	
	65	7844034		2010-11-30	Oh et al.	
	66	7899039		2011-03-01	Andreasen et al.	
	67	8104080		2012-01-24	Burns et al.	
	68	8150394		2012-04-03	Bianconi et al.	
	69	8667542		2014-03-04	Bertz et al.	
	70	8793304		2014-07-29	Lu et al.	
	71	8948726		2015-02-03	Smith et al.	
	72	7860088		2010-12-28	Lioy, Marcello	
	73	8407763		2013-03-26	Weller et al.	
	74	8131840		2012-03-06	Denker, Richard E.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	75	7676673		2010-03-09	Weller et al.	
	76	7512128		2009-03-31	DiMambro et al.	
	77	7248570		2007-07-24	Bahl et al.	
	78	7024460		2006-04-04	Koopmas et al.	
	79	6748437		2004-06-08	Mankude et al.	
	80	6735206		2004-05-11	Oki et al.	
	81	6058434		2000-05-02	Wilt et al.	
	82	8032168		2011-10-04	Ikaheimo, Jorma	
	83	7966405		2011-06-21	Sundaresan et al.	
	84	7889384		2011-02-15	Armentrout et al.	
	85	6125391		2000-09-26	Meltzer et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	86	6038540		2000-03-14	Krist et al.	
	87	8504687		2013-08-06	Maffione et al.	
	88	7043225		2006-05-09	Patel et al.	
	89	6725256		2004-04-20	Albal et al.	
	90	6751296		2004-06-15	Albal et al.	
	91	6934751		2005-08-23	Jayapalan et al.	
	92	7174156		2007-02-06	Mangal, Manish	
	93	7636626		2009-12-22	Oesterling et al.	
	94	7720206		2010-05-18	Devolites et al.	
	95	8340678		2012-12-25	Pandey, Vinod	
	96	8005913		2011-08-23	Carlander, Carrie	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	97	6792461		2004-09-14	Hericourt, Olivier	
	98	7027055		2006-04-11	Anderson et al	
	99	8160056		2012-04-17	Van der Merwe et al.	
	100	5633868		1997-05-27	Baldwin et al.	
	101	7680086		2010-03-16	Eglin, Matthew George	
	102	7765294		2010-07-27	Edwards et al.	
	103	7843831		2010-11-30	Morrill et al.	
	104	8131858		2012-03-06	Agulnik et al.	
	105	8223655		2012-07-17	Heinz et al.	
	106	8385199		2013-02-26	Coward et al.	
	107	6061571		2000-05-09	Tamura, Hideo	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	108	6157636		2000-12-05	Voit et al.	
	109	7110753		2006-09-19	Campen, Kenneth Brian	
	110	8523547		2013-09-03	Pekrul, Merton W.	
	111	8875042		2014-10-28	Lejeune et al.	
	112	8315198		2012-11-20	Corneille et al.	
	113	9172553		2015-10-27	Dawes et al.	
	114	7770785		2010-08-10	Jha et al.	
	115	7817983		2010-10-19	Cassett et al.	
	116	8600895		2013-12-03	Felsher, David Paul	
	117	6535855		2003-03-18	Cahill et al.	
	118	6654786		2003-11-25	Fox et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	119	7272660		2007-09-18	Powers et al.	
	120	8065365		2011-11-22	Saxena et al.	
	121	8085808		2011-12-27	Brusca et al.	
	122	8325906		2012-12-04	Fullarton et al.	
	123	8448015		2013-05-21	Gerhart, David	
	124	8675852		2014-03-18	Maes, Stephane H.	
	125	8971912		2015-03-03	Chou et al.	
	126	8151205		2012-04-03	Follmann et al.	
	127	7133386		2006-11-07	Holur et al.	
	128	8744339		2014-06-03	Halfmann et al.	
	129	8811338		2014-08-19	Jin et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	130	8908516		2014-12-09	Tzamaloukas et al.	
	131	9030934		2015-05-12	Shah et al.	
	132	7440433		2008-10-21	Rink et al.	
	133	8191106		2012-05-29	Choyi et al.	
	134	6947985		2005-09-20	Hegli et al.	
	135	8195153		2012-06-05	Frencel et al.	
	136	8505073		2013-08-06	Taglienti et al.	
	137	8995952		2015-03-31	Baker et al.	
	138	8538421		2013-09-17	Brisebois et al.	
	139	8503358		2013-08-06	Hanson et al.	
	140	8271025		2012-09-18	Brisebois et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	141	7661124		2010-02-09	Ramanathan et al.	
	142	6141565		2000-10-31	Feurerstein et al.	
	143	6690918		2004-02-10	Evans et al.	
	144	7657920		2010-02-02	Arseneau et al.	
	145	7724716		2010-05-25	Fadell, Anthony M.	
	146	9325737		2016-04-26	Gutowski et al.	
	147	9344557		2016-05-17	Gruchala et al.	
	148	8731519		2014-05-20	Flynn et al.	
	149	8363799		2013-01-29	Gruchala et al.	
	150	6510152		2003-01-21	Gerszberg et al.	
	151	6542500		2003-04-01	Gerszberg et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	152	6546016		2003-04-08	Gerszberg et al.	
	153	6570974		2003-05-27	Gerszberg et al.	
	154	7082422		2006-07-25	Zirngibl et al.	
	155	7369848		2008-05-06	Jiang, Yue Jun	
	156	7577431		2009-08-18	Jiang, Yue Jun	
	157	7664494		2010-02-16	Jiang, Yue Jun	
	158	7873001		2011-01-18	Silver, Andrew	
	159	8219134		2012-07-10	Maharajh et al.	
	160	8291439		2012-10-16	Jethi et al.	
	161	9367680		2016-06-14	Mahaffey 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

EFS Web 2.1.17

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	2688553	CA		2008-12-04	Yoggie Security Systems, Inc.		
	2	1850575	EP		2007-10-31	Research In Motion Limited		

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	Jing et al., "Client-Server Computing in Mobile Environments," GTE Labs. Inc., Purdue University, ACM Computing Surveys, Vol. 31, No. 2, June 1999	
	2	Rivadeneyra et al., "A communication architecture to access data services through GSM," San Sebastian, Spain, 1998	
	3	Loopt User Guide, metroPCS, 7/17/2008	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	4	"Jentro Technologies launches Zenlet platform to accelerate location-based content delivery to mobile devices," The Mobile Internet, Boston, MA, Feb. 2008	
	5	"Ads and movies on the run," the Gold Coast Bulletin, Southport, Qld, Jan. 29, 2008	
	6	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	
	7	Kim, "Free wireless a high-wire act; MetroFi needs to draw enough ads to make service add profits," San Francisco Chronicle, Aug. 21, 2006	
	8	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	
	9	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	
	10	Sabat, "The evolving mobile wireless value chain and market structure," Nov. 2002	
	11	Nuzman et al., "A compund model for TCP connection arrivals for LAN and WAN applications," Oct. 22, 2002	
	12	Kuntze et al., "Trustworthy content push," Fraunhofer-Institute for Secure Information Technology SIT; Germany; WCNC 2007 proceedings, IEEE	
	13	Blackberry Mobile Data System, version 4.1, Technical Overview, 2006	
	14	Client Guide for Symantec Endpoint Protection and Symantec Network Access Control, 2007	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	15	Ehnert, "Small application to monitor IP trafic on a Blackberry - 1.01.03 ", March 27, 2008; http://www.ehnert.net/MiniMoni/	
	16	NetLimiter Lite 4.0.19.0; http://www.heise.de/download/netlimiter-lite-3617703.html from vol. 14/2007	
	17	Muntermann et al., "Potentiale und Sicherheitsanforderungen mobiler Finanzinformationsdienste und deren Systeminfrastrukturen," Chair of Mobile Commerce & Multilateral Security, Goethe Univ. Frankfurt, 2004	
	18	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	
	19	Fujitsu, "Server Push Technology Survey and Bidirectional Communication in HTTP Browser," January 9, 2008 (JP)	
	20	Windows7 Power Management, published April 2009	
	21	Open Mobile Alliance (OMA), Push Architecture, Candidate Version 2.2; Oct. 2, 2007; OMA-AD-Push-V2_2-20071002-C	

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

EXAMINER SIGNATURE

Examiner Signature	/Andrew Joseph Rudy/	Date Considered	09/12/2016

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

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

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

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

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

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

Application Number	15217538
Filing Date	2016-07-22
First Named Inventor	Raleigh
Art Unit	2447
Examiner Name	not yet assigned
Attorney Docket Number	RALEP007C11C3C2C2

U.S.PATENTS Remove

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

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20020022472		2002-02-21	WATLER et al.	
	2	20020120540		2002-08-29	KENDE et al.	
	3	20020131404		2002-09-19	MEHTA et al.	
	4	20020138601		2002-09-26	PIPONIUS et al.	
	5	20020176377		2002-11-28	HAMILTON, Thomas E.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

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

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

FOREIGN PATENT DOCUMENTS Remove

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

EFS Web 2.1.17

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C11C3C2C2

	1							

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

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		

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

EXAMINER SIGNATURE

Examiner Signature	/Andrew Joseph Rudy/	Date Considered	09/12/2016

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

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

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

Search Notes	Application/Control No.	Applicant(s)/Patent under Reexamination	
	15/217,538	RALEIGH, GREGORY G.	
	Examiner	Art Unit	
	ANDREW JOSEPH RUDY	3687	

SEARCHED			
Class	Subclass	Date	Examiner
455	411,414.1, 432.1	9/9/2016	AJR
370	252	9/9/2016	AJR
H04W	12/06	9/9/2016	AJR
H04W	12/12	9/9/2016	AJR
H04L	47/10	9/12/2016	AJR
H04L	43/50	9/12/2016	AJR
709	219,224	9/12/2016	AJR
709	226,229	9/12/2016	AJR

INTERFERENCE SEARCHED			
Class	Subclass	Date	Examiner
455	**411**	**9/12/2016**	**AJR**
370	252	9/12/2016	AJR

SEARCH NOTES (INCLUDING SEARCH STRATEGY)		
	DATE	EXMR
Continuity data reviewed.	9/9/2016	AJR
Inventor name search conducted.	9/9/2016	AJR
Bibliographic data updated.	9/12/2016	AJR

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	15217538
Filing Date	2016-07-22
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP007C11C3C2C2

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	5617539	A	1997-04-01	Ludwig et al.	
	2	6601040	B1	2003-07-29	Kolls, H. Brock	
	3	6636721	B2	2003-10-21	Threadgill et al.	
	4	6959393	B2	2005-10-25	Hollis et al.	
	5	7177919	B1	2007-02-13	Truong et al.	
	6	7369856	B2	2008-05-06	Ovadia, Shlomo	
	7	7428750	B1	2008-09-23	Dunn et al.	
	8	7486658	B2	2009-02-03	Kumar, Rajneesh	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3C2C2

	9	7599714	B2	2009-10-06	Kuzminskiy, Alexandr	
	10	8943551	B2	2015-01-27	Ganapathy et al.	
	11	7610047	B2	2009-10-27	Hicks III et al.	
	12	7643411	B2	2010-01-05	Andreasen et al.	
	13	7719966	B2	2010-05-18	Luft et al.	
	14	7979069	B2	2011-07-12	Hupp et al.	
	15	8132256	B2	2012-03-06	Bari, Farooq	
	16	8145194	B2	2012-03-27	Yoshikawa et al.	
	17	8194581	B1	2012-06-05	Schroeder et al.	
	18	8380247	B2	2013-02-19	Engstrom	
	19	8418168	B2	2013-04-09	Tyhurst et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3C2C2

	20	8494559	B1	2013-07-23	Malmi	
	21	8543814	B2	2013-09-24	Laitinen et al.	
	22	9413546	B2	2016-08-09	Meier et al.	
	23	8719397	B2	2014-05-06	Levi et al.	
	24	8787249	B2	2014-07-22	Giaretta et al.	
	25	8838752	B2	2014-09-16	Lor et al.	
	26	8855620	B2	2014-10-07	Sievers et al.	
	27	8862751	B2	2014-10-14	Faccin 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

EFS Web 2.1.17

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3C2C2

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	15217538
	Filing Date	2016-07-22
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3C2C2

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)	2016-09-23
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	15217538
Filing Date	2016-07-22
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP007C11C3C2C2

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	20070130283	A1	2007-06-07	Klein 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	1545114	EP	A1	2005-06-22	Alcatel		
	2	1887732	EP	A1	2008-02-13	Huawei Technologies Co., Ltd.		
	3	2007065	EP	A1	2008-12-24	Huawei Technologies Co., Ltd.		

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3C2C2

	4	2002067616	WO	A1	2002-08-29	Sonera Oyj			
	5	2003017063	WO	A2	2003-02-27	Apogee Networks			
	6	2003017065	WO	A2	2003-02-27	Apogee Networks			
	7	2007120310	WO		2007-10-25	Qualcomm 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

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	15217538
	Filing Date	2016-07-22
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3C2C2

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)	2016-09-23
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
25 October 2007 (25.10.2007)

PCT

(10) International Publication Number
WO 2007/120310 A2

(51) International Patent Classification: Not classified

(21) International Application Number:
PCT/US2006/061532

(22) International Filing Date:
1 December 2006 (01.12.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/742,155 1 December 2005 (01.12.2005) US
11/394,782 31 March 2006 (31.03.2006) US

(71) Applicant *(for all designated States except US)*: **QUALCOMM Incorporated** [US/US]; 5775 Morehouse Drive, San Diego, California 92121 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **LIOY, Marcello** [CA/US]; 11629 Miro Circle, San Diego, California 92131 (US). **DYCK, Jeffrey** [CA/US]; 4816 Mt. Harris Drive, San Diego, California 92117 (US).

(74) Agents: **WADSWORTH, Philip R.** et al.; 5775 Morehouse Drive, San Diego, California 92121 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

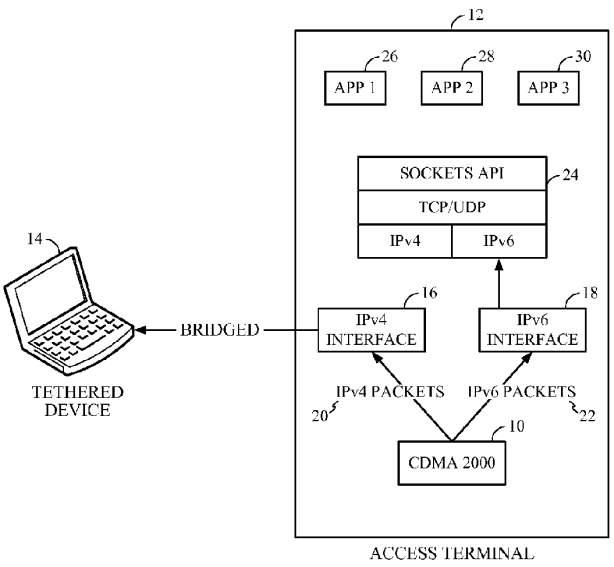
— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

— *without international search report and to be republished upon receipt of that report*

[Continued on next page]

(54) Title: CONCURRENT INTERNET PROTOCOL CONNECTIVITY TO AN ACCESS TERMINAL AND A TETHERED DEVICE



(57) Abstract: Using split interfaces for Internet Protocol version 6 (IPv6) and Internet Protocol version 4 (IPv4), and bridging the IPv4 interface, makes it possible to support a Tethered Device (TD) and an Access Terminal (AT) having concurrent IP connectivity. This configuration enables the support of IP Multimedia Subsystem (IMS) applications in the AT using IPv6 while concurrently supporting general Internet usage on a TD. It is also possible to bridge an IPv6 interface to the TD.

WO 2007/120310 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.

CONCURRENT INTERNET PROTOCOL CONNECTIVITY TO AN ACCESS TERMINAL AND A TETHERED DEVICE

Claim of Priority under 35 U.S.C. §119

[0001] The present Application for Patent claims priority to Provisional Application No. 60/742,155 entitled "Method For Supporting Concurrent IP Connectivity To An Access Terminal And Tethered Device Each Using Different IP Protocols In CDMA 2000 Networks," Filed December 1, 2005, and assigned to the assignee hereof and hereby expressly incorporated by reference herein.

BACKGROUND

Field

[0002] The present disclosed embodiments relates generally to cellular communications, and more specifically to concurrent Internet Protocol (IP) connectivity to an Access Terminal (AT) and a Tethered Device (TD).

Background

[0003] It is desirable to support one Internet Protocol (IP) protocol to an Access Terminal (AT) and another to a Tethered Device (TD). An example of where this is desirable is with the launch of the new IP Multimedia Subsystem (IMS) services, which will provide a rich set of new Multimedia services in the mobile environment. One of these services will the Voice over IP (VoIP), which will replace traditional circuit switched voice, which is how voice services are supported today. In order to support these IMS services, an AT must be continuously connected to the IP Network, which is also known as "always-on." Typically in the case for Code Division Multiple Access (CDMA) 2000 networks this implies that it is not possible to support a TD as the AT is already in a data session.

[0004] There is therefore a need in the art for concurrent IP connectivity to an AT and a TD.

SUMMARY

[0005] Using split interfaces for Internet Protocol version 6 (IPv6) and Internet Protocol version 4 (IPv4), and bridging the IPv4 interface, makes it possible to support a TD and

an AT having concurrent IP connectivity. This configuration enables the support of IMS applications in the AT using IPv6 while concurrently supporting general Internet usage on a TD. It is also possible to bridge the IPv6 interface to the TD.

BRIEF DESCRIPTION OF THE DRAWINGS

[0006] FIG. 1 is an illustration of a concurrently connected Access Terminal and Tethered Device.

DETAILED DESCRIPTION

[0007] The embodiments described herein make it possible to provide service concurrently to the AT and TD. Different IP protocol versions can be used by the AT and TD. In the case of IMS, it is desirable to use IP version 6 (IPv6) for the AT in order to be always on an assigned IP for as long as the AT is powered on. In order to support a wide scale deployment of these services, it would require as many IP addresses as there are ATs. In the case of IPv4 there is a dearth of addresses, so IPv6 is preferred for the AT.

[0008] For most general Internet services, such as web browsing and email, still use IP version 4 (IPv4). Thus for the TD it is desirable to have IPv4 connectivity.

[0009] The embodiments described below with reference to FIG. 1 describe how to provide IPv6 in the AT while concurrently supporting IPv4 to a TD. However, the same technique could be used to provide IPv4 to the AT and IPv6 to the TD.

[0010] IP packets arriving over an air interface 10 and based on an IP version are received by an AT 12 and are either forwarded up an AT stack 24 (for example, IPv6 packets 22) or forwarded to a TD 14 (for example, IPv4 packets 20).

[0011] There are a variety of ways this could be done:

[0012] 1. Examine the incoming packets and apply the forwarding as described in the paragraph above.

[0013] 2. Use the notion of Network Interfaces, which provide an abstraction layer, between the physical layer (in this case the CDMA2000 air interface data protocols, such as Radio Link Protocol (RLP) and Point-to-Point Protocol (PPP)) and the generic IP stack above (commonly referred to as the Transmission Control Protocol/Internet Protocol (TCP/IP) suite). This is described in more detail below.

[0014] The use of the Network Interface can provide a variety of processing options with respect to IP packets passing through them, such as filtering and routing/bridging information.

[0015] It is possible in the interface itself to identify whether or not packets should be forwarded directly to another interface without processing them further. This further processing is typically done at the IP layer, and consists of routing. Routing is the act of examining the IP addresses in the header and determining if the packet is destined for the local host, which is the device doing the routing, or another host. Typically if it is intended for another host, a determination may need to be made over which link to transmit it – if there are multiple links. If the interface is configured to directly forward the packets to another interface (or link), this is referred to as bridging the two interfaces together. This is typically used when it is known that all of the packets arriving in one interface must be transmitted over another interface, regardless of the addressing information they contain. An example of this is a Wireless LAN bridge. Any packets arriving on the Ethernet interface must be forwarded over the WLAN interface without exception.

[0016] In an AT it is desirable to have separate network interfaces for IPv4 and IPv6 as there is much information for each protocol that is independent, but needs to be duplicated, such as the state of the interface (disabled, available, configuring, etc.), IP address(es), and so forth.

[0017] Using the properties of bridging and the separation of the IPv6 and IPv4 interfaces allows an IPv4 interface 16 to be set up in bridging mode such that it forwards all IPv4 packets 20 to the TD, while leaving an IPv6 interface 18 in non-bridged mode, which results in the IPv6 packets 22 being delivered to the IP stack 24, and the payload ultimately being delivered to the IMS application. This allows IPv6 IMS applications 26, 28, and 30 on the AT 12 to work concurrently with generic IPv4 Internet applications on the TD 14.

[0018] Using this split interface/bridging solution, it is also possible to run IPv6 addresses on the TD 14 while supporting IPv4 applications on the AT 12.

[0019] When it becomes desirable to support IPv6 applications on the TD 14 as well, because the IPv6 packets are going to the IP layer 24 they could be routed to the TD as well if they are not destined for the AT 12, but rather for the TD. This would allow

both IPv4 and IPv6 applications on the TD running concurrently with IPv6 applications running on the AT.

WHAT IS CLAIMED IS:

CLAIMS

1. An Access Terminal for having concurrent Internet Protocol Activity with a Tethered Device, the Access Terminal comprising:

an Internet Protocol stack;

a first Internet Protocol version interface adapted in a non-bridged mode for delivering first Internet Protocol version packets to the Internet Protocol stack; and

a second Internet Protocol version interface adapted in a bridged mode for delivering second Internet Protocol version packets to the Tethered Device.

2. The Access Terminal of claim 1 wherein the first Internet Protocol version interface is an Internet Protocol version 6.

3. The Access Terminal of claim 2 wherein the second Internet Protocol version interface is an Internet Protocol version 4.

4. The Access Terminal of claim 1 wherein the first Internet Protocol version interface is an Internet Protocol version 4.

5. The Access Terminal of claim 4 wherein the second Internet Protocol version interface is an Internet Protocol version 6.

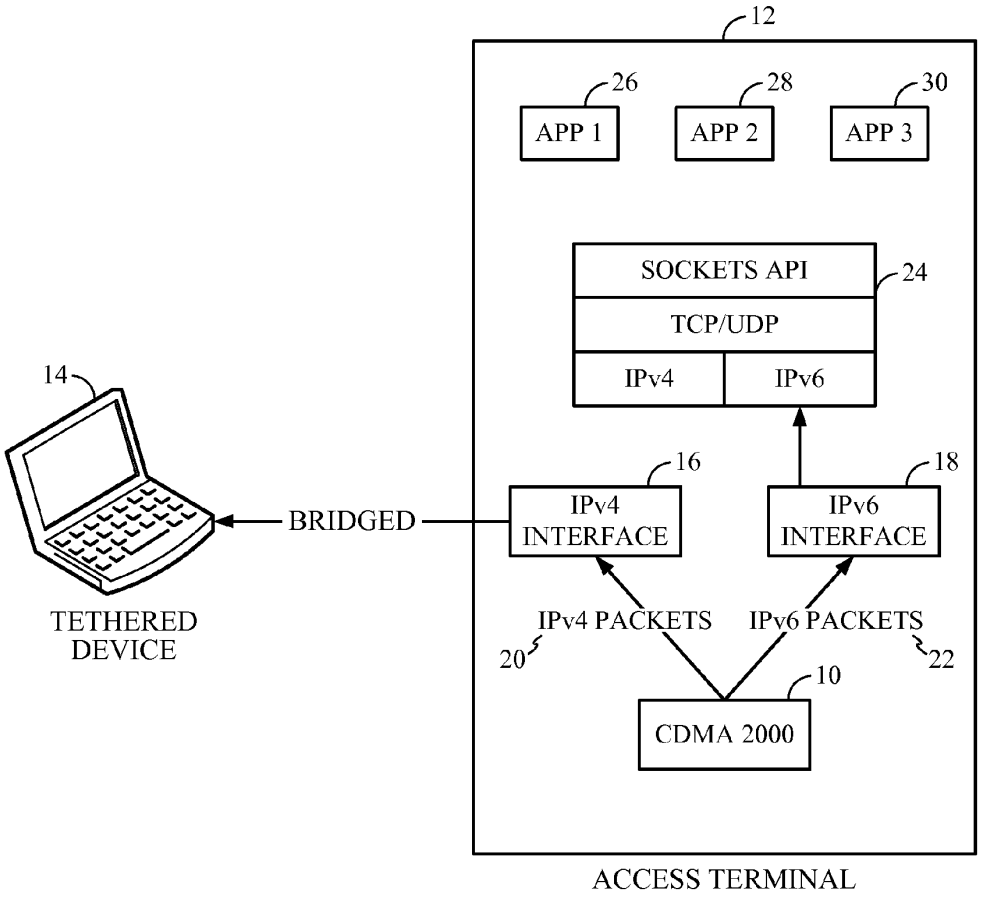

12
26
28
30
APP 1
APP 2
APP 3
SOCKETS API
24
TCP/UDP
IPv4
IPv6
14
16
18
IPv4
INTERFACE
IPv6
INTERFACE
BRIDGED
TETHERED
DEVICE
IPv4 PACKETS
IPv6 PACKETS
20
22
10
CDMA 2000
ACCESS TERMINAL

FIG. 1

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 February 2003 (27.02.2003)

PCT

(10) International Publication Number
WO 03/017063 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number: PCT/US02/26556

(22) International Filing Date: 21 August 2002 (21.08.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/313,968 21 August 2001 (21.08.2001) US

(71) Applicant *(for all designated States except US)*: **APOGEE NETWORKS** [US/US]; 1455 Broad Street, 4th Floor, Bloomfield, NJ 07003 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **LEUNG, Yiu, Kau** [US/US]; 5 Knob Hill Road, Morganville, NJ 07751 (US). **PRICE, John, Davis** [US/US]; 5 Ashland Court, Colts Neck, NJ 07722 (US). **FEINBERG, Brion** [US/US]; 51 Amagansett Drive, Morganville, NJ 07751 (US).

(74) Agents: **DUNNAM, Michael, P.** et al.; Woodcock Washburn LLP, One Liberty Place, 46th Floor, Philadelphia, PA 19103 (US).

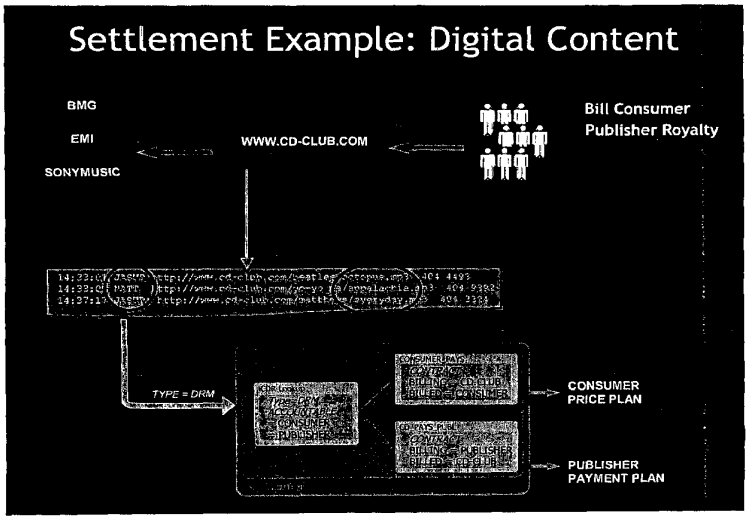
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT,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

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

Published:
— *without international search report and to be republished upon receipt of that report*

[Continued on next page]

(54) Title: SETTLEMENT OF TRANSACTIONS SUBJECT TO MULTIPLE PRICING PLANS____



(57) Abstract: The invention includes a method, system, and computer-readable medium having computer-executable instructions for rating a transaction. The inventive method includes processing a transaction, where the transaction is processed when a service is provided from a service provider to a service consumer, accessing via a computer network multiple pricing plans related to the transaction, and rating the transaction in accordance with the multiple pricing plans. The method further may include receiving output states from at least one pricing plan. The rating may be accomplished within one pricing plan, or within a group of pricing plans.

WO 03/017063 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.

SETTLEMENT OF TRANSACTIONS SUBJECT TO MULTIPLE PRICING PLANS

Cross Reference to Related Applications

This application claims priority under 35 U.S.C. § 119 (e) from provisional application no. 60/313,968 filed August 21, 2001. The provisional application 60/313,968 is incorporated by reference herein, in its entirety, for all purposes.

Technical Field

The invention relates generally to the processing of data, and more particularly to efficiently and generically aggregating data available on a communication network and billing/paying multiple parties for access to the content of the aggregated data.

Background of the Invention

Recently, the collection and processing of data transmitted over communication networks, like the Internet, has moved to the forefront of business objectives. In fact, with the advent of the Internet, new revenue generating business models have been created to account for the consumption of content received from a data network (*i.e.*, content-based billing). For example, content distributors, application service providers (ASPs), Internet service providers (ISPs), and wireless Internet providers have realized new opportunities based on the value of the content that they deliver. As a result of this content-billing initiative, it has become increasingly important to resolve intelligently and flexibly the corresponding transactions according to the business needs of the customer.

Often, even in traditional commerce streams, there are many different participants between the maker and the consumer of the good. Some of these so-called "middlemen" simply may facilitate access to the good, while others may add useful characteristics to the good. This is especially true in a distributed network environment, like the Internet, that impose additional burdens on capturing the

transaction process because of the unlimited number of data sources and the correspondingly unlimited number of data types. As a result, adequately describing the transacting of the goods and services in such an environment, or even across any of the traditional environments requires a technique that is capable of understanding and processing the participants and the various types of data.

To date, resolving the characteristics of a transaction has been accomplished over data-specific environments using certain application-specific (*i.e.*, "non-generic") methods. For example, a typical telephone bill captures the characteristics of a voice-based telecommunications transaction. In particular, the participants may be identified as the party initiating the call (*i.e.*, the "calling party" telephone number), the party receiving the call (*i.e.*, the "called party" telephone number), and one or more parties connecting the communication (*i.e.*, the "local" or "long distance carrier"). This simple example adequately captures all of the necessary aspects of the telephone call to properly account for the transaction by requiring payment from certain parties (*e.g.*, the calling and/or the called party) to certain other parties (*e.g.*, the local and/or long distance carrier). While these "hard-coded" transaction resolution techniques are sufficient to accommodate only specific environments involving well-defined participants, they are correspondingly too rigid to efficiently satisfy the ever-changing face of a communication network like the Internet. Also, these "hard-coded" techniques are too specific to operate across the many and varied transaction environments that exist throughout the business world.

Therefore, there exists a need to provide a flexible technique that can capture and resolve transactions of any type and involving any participants without requiring modification of the technique for each type. Such a technique would serve to accommodate multi-faceted network environments like the Internet, as well as to provide a single solution that would apply to any business environment.

Summary of the Invention

The invention includes a method, system, and computer-readable medium having computer-executable instructions for rating a transaction. The inventive

method includes processing a transaction, where the transaction is processed when a service is provided from a service provider to a service consumer, accessing via a computer network multiple pricing plans related to the transaction, and rating the transaction in accordance with the multiple pricing plans. The method further may include receiving output states from at least one pricing plan. The rating may be accomplished within one pricing plan, or within a group of pricing plans. Also, accessing the multiple pricing plans may be accomplished via interconnected building blocks located within each of the pricing plans. The method also may include a revenue fold that summarizes the output of multiple pricing plans, including child and parent accounts. Selection of the appropriate child accounts may be a function of end dates that are within a parent account's time period. The method further may pool revenue/usage data as a function of billing cycles, and update the pooled revenue/usage data by summing the values of data from selected account plan periods. Values of the pooled revenue/usage data may be obtained via a building block. The inventive method also may determine a commission, wherein the commission is a credit given to an account.

Brief Description of the Drawings

Other features of the invention are further apparent from the following detailed description of the embodiments of the invention taken in conjunction with the accompanying drawings, of which:

Figure 1 is a block diagram of a system for analyzing content transmitted over a communication network, according to the invention;

Figure 2 is a block diagram further describing the components of the system described in Figure 1;

Figures 3A and 3B provide a flow diagram further detailing the operation the system described in Figure 1;

Figure 4 provides a block diagram of the system described in Figure 1, providing greater detail of a configuration and operation of a transaction layer;

Figures 5A and 5B provide a flow diagram of a method for identifying the characteristics of a transaction, according to the invention;

Figure 6 is a block diagram further detailing the operation and configuration of the transaction layer, according to the invention;

Figure 7 is a flow diagram that details the operation and configuration of the transaction layer of transaction layer, according to the invention;

Figure 8 illustrates a sample settlement scenario for settling the fees associated with the download of certain content;

Figure 9 illustrates a general system description of settlement technologies useful in accordance with the invention to accommodate multiple aggregation of usage, multiple ownership of content, and multiple settlement options;

Figure 10 illustrates a settlement example for digital music downloaded by a consumer from an on-line music club that implements a pricing plan to the consumer and a publisher payment plan using the settlement techniques of the invention;

Figure 11 illustrates a transaction pricing usage based settlement model for use in settling low volume, high value transactions;

Figure 12 illustrates a billing cycle pricing, usage based settlement model for use in settling high volume, low value transactions;

Figure 13 illustrates a revenue sharing settlement using folds in accordance with a first embodiment of the invention;

Figure 14 illustrates a revenue sharing settlement using revenue/usage pools in accordance with a second embodiment of the invention;

Figure 15 illustrates a revenue pool contribution example for the embodiment of Figure 14;

Figure 16 illustrates a revenue pool accessor example for the embodiment of Figure 14;

Figure 17 illustrates a revenue sharing settlement using commissions in accordance with a third embodiment of the invention;

Figure 18 provides an example of computing revenue fold;

Figure 19 illustrates how accounts and pools with different billing cycles contribute to and access from pool instances; and

Figure 20 provides an example of how an account with billing period ending will get one commission from account.

Detailed Description of the Invention

System Overview

Figure 1 is a block diagram of a system 100 for analyzing content transmitted over a communication network. Although the following description will be discussed in the context of collecting, processing and billing for data transmitted over the Internet, it should be appreciated that the invention is no so limited. In fact, the invention may be applied to any type of network, including a private local area network, for example. Also, the invention may be used for purposes other than billing for the usage of content. For example, the invention may be used to analyze the type of data transmitted over a particular network, or to determine the routing patterns of data on a network. Furthermore, the invention may be used to facilitate the intelligent collection and aggregation of data relevant to a particular industry. In addition, the invention may be used to track specific Internet protocol (IP) network resources and to detect fraud, for example.

In addition, it should be appreciated that the term "content" may be defined as data that is transmitted over the network. In the context of the Internet, content may include .mp3 files, hypertext markup language (html) pages, videoconferencing data, and streaming audio, for example. The terms "content provider" and "customer" will be used throughout the description as well. Content provider may refer to the primary creator or provider of the content, while customer is the primary recipient of the content. Both the producer and customer may be a human or a computer-based system.

As shown in Figure 1, an instrumentation layer 101 provides raw data to a content collection layer 102. Instrumentation layer 101 may consist of various data sources, for example, network routers. The network routers may provide information

regarding the various types of routed data, including for example, data format, originating Internet protocol (IP) address, and destination IP address. One example of such information is Cisco System's NetFlow™.

Content collection layer 102 collects information about the delivery of the content, as well as the substance of the content itself. Content collection layer 102 also may sort, filter, aggregate, and store the content according to the particular needs of the end user. In effect, content collection layer is responsible for extracting meaningful information about IP traffic, and so it is provided with an understanding of the data sources in instrumentation layer 101. Content collection layer 102 also may transform the data from the plurality of sources in instrumentation layer 101 into standard formats for use in a transaction layer 103.

Content collection layer 102 is in communication with transaction layer 103. Generally, content collection layer 102 reports to transaction layer 103 that a relevant communication event has occurred and should be considered by the remainder of system 100. A communication event may be defined as any transfer of data between systems. Transaction layer 103 captures the predetermined agreements among all of the parties involved in system 100 regarding the value of the transferred content, as well as the value added by each of the individual parties in transferring such content. Therefore, transaction layer 103 is charged with understanding the nature of the parties, as well as the understanding the actions that one or more parties perform and the influence of such action on the respective parties.

Transaction layer 103 is in communication with a settlement layer 104. Settlement layer 104 captures the operations that are necessary to understand the significance of the transaction defined by transaction layer 103. For example, settlement layer 104 may rate a particular transaction by assigning a monetary value to the transaction. Settlement layer 104 also may divide the burdens and benefits of the monetary value among the relevant parties. In this way, settlement layer 104 ensures that certain parties receive a particular portion of the payment made by the other parties. Settlement layer 104 also may be responsible for delivering this burden and benefit information to the appropriate parties with the appropriate identifiers (*e.g.*,

account numbers). As will be explained in more detail below, the present invention is directed to operations of the settlement layer 104.

Figure 2 is a block diagram further describing the components of system 100. As shown in Figure 2, instrumentation layer 101 includes data sources 201-203 that each provide raw data 204-206, respectively, to collection layer 102. As discussed, data sources 201-203 may include various internetworking devices like routers, bridges, and network switches. Data sources 201-203 provide raw data to an input data adapter 207. Accordingly, input data adapter 207 understands the operation of and the data provided by data sources 201-203. Although one input data adapter is shown in Figure 2, it should be appreciated that more than one input data adaptermay be used in system 100. For example, each data source may have a dedicated input data adapter.

Input data adapter 207 understands the incoming data and extracts the data into the appropriate fields. This field-delimited data, called flow objects 208, are sets of attributes. The attributes may be any characteristics that are provided by, or can be derived from, raw data 204-206 provided by data sources 201-203, respectively. For example, flow objects 208 may include a set of attributes describing the source and destination, including source IP address, destination IP address, source interface, and destination interface. Because input data adapter 207 is charged with understanding raw data 204-206 from data sources 201-203, as well as the required flow objects 208 of system 100, it is capable of transforming the raw data to the flow objects, where the flow objects may all be of a standard format.

Input data adapter 207 provides flow objects 208 to a content data language 209. Content data language 209 may transform the attributes in flow objects 208 into other attributes that are desired by a particular customer. For example, content data language 209 may derive a network identifier attribute that is not readily available from a data source, from a source address attribute and a destination address attribute that are provided by flow object 208 attributes from input data adapter 207. This derivation may be based on a customer's desire to determine which network conveyed the transaction between the source and the destination. Therefore, following this

example, content data language 209 will know to extract the source address attribute and the destination address attribute from flow objects 208.

Content data language 209 may perform other functions as well. For example, content data language 209 may perform a generic lookup function 219 that is built into content data language 209. Generally, generic lookup 219 describes a technique for mapping any number of attributes to any number of other derived attributes. For example, generic lookup 219 may be used to map a unique resource locator (URL) attribute to a particular content-type attribute.

Content data language 209 also is in communication with a correlator 211. Generally, correlator 211 connects the many daily network content events from various network devices, like routers for example. Often, the connected data may come from distinctly different data sources at distinctly unrelated times. Correlator 211 allows this data to be intelligently connected to each other, regardless of how different the sources or of how disparate the time received. For example, a Netflow™ enabled router and a Radius™ enabled network access switch may each provide certain data that is relevant to one particular transaction. However, because portions of the data come from different devices, the data may arrive at system 100 at different times, and in different formats. Also, because each provides data that is necessary to complete one transaction, the data from each cannot be considered separately. Correlator 211 allows this data to be intelligently grouped regardless of the format of the data or of the time the data pieces are received.

Furthermore, correlator 209 may rearrange the order of the received flow objects 208 to suit the needs of the remainder of system 100. By performing such correlation without having to first store all of the data on a disk (*e.g.*, a database), significantly faster processing is achieved. Correlator 209 may perform this correlation in real-time, for example.

Although system 100 has been described using content data language 209 and correlator 211, it should be appreciated that flow objects 208 may proceed directly to a filter 212, if no correlation is required and if no attribute derivation is required, for example. Filter 212 analyzes flow objects 208 to ensure that the provided attributes

are desired by system 100. If flow objects 208 are not needed (*i.e.*, a mismatch), filter 212 may prevent flow objects 208 from passing to an aggregator 213. Also, although filter 212 has been shown as a separate device in system 100, it should be appreciated that the functionality of filter 212 may be incorporated into aggregator 213.

Filter 212 passes the matching flow objects to aggregator 213. Aggregator 213 may provide additional filtering and classification of the multitude of daily network content transactions, based on user criteria. Aggregator 213 may perform such filtering and classification in real-time. Aggregator 213 provides the filtered and classified information to an output data adapter 214. Output data adapter 214 may convert the data from aggregator 213 into one or more content detail records for storage in CDR database 215. Therefore, CDR database 215 stores a complete description of a content event.

Transaction layer 103 includes CDR database 215, an ownership resolution component 216, and a transaction resolution component 221. CDR database 215 passes the CDR onto ownership resolution component 216. A proper accounting of a communication event, for any purpose including billing, requires both identifying the participants and defining the relationships among those participants. These tasks are accomplished by ownership resolution component 216 and transaction resolution component 221.

Ownership resolution component 216 serves to define the participants of the communication event. In particular, because raw data 204-206 may not provide sufficient "ownership" data relating to the parties involved in the content transaction, such "ownership" data must be provided by system 100 to properly account for the entire transaction. Ownership resolution component 216 operates to provide such ownership-based data to system 100.

Ownership resolution component 216 is in communication with transaction resolution component 221. Transaction resolution component 221 serves to capture the predetermined relationships and/or agreements among the parties defined by ownership resolution component 216 regarding the value of the transferred content, as well as the value added by each of the individual parties in transferring such content.

Such predetermined relationships may be previously agreed upon by the participants, or may be created and agreed upon with the implementation of system 100. Therefore, transaction component 103 understands the nature of the parties, the actions that one or more parties perform, and the influence of such action on the respective parties.

Transaction component 216 provides the transaction information to a rating component 217. Rating component 217 provides a weight or significance (*e.g.*, a price) to the transaction, so as to provide a tangible value to the transaction. Rating component 217 may make this determination based on various metrics including the type of the content, the quantity of content consumed, the place and time delivered, or the quality of the content, for example. Therefore, rating component 217 allows system 100 to provide some contextual value, indicting the significance or relevance that certain content or information has to the individual customer.

Rating component 217 provides the rated transaction to a presentment component 218. Presentment component 218 may provide the capability for a customer 220 to view their real-time billing information, for example, over the network. Presentment component 218 also may attach relevant identifiers to the bill (*e.g.*, account numbers, etc.).

Figures 3A and 3B provide a flow diagram further detailing the operation 300 of system 100. As shown in Figure 3A, in step 301, raw data 204-206 is received from data sources 201-203. In step 302, input data adapter 207 converts raw data 204-206 to flow objects 208, where flow objects 208 are sets of attributes, determined from raw data 204-206. In step 303, it is determined whether there is a need to derive new attributes from the existing attributes found in flow objects 208. If there is such a need, in step 304, CDL 209 is used to derive new attributes from existing attributes. Also, as discussed above, attributes may be correlated by correlator 211.

In step 305, flow objects 208 are filtered by filter 212. In step 306, the matching flow objects (*i.e.*, those passed by filter 212) are further filtered and classified by aggregator 213. In step 307, output data adapter 214 converts the data aggregated by aggregator 213 to a format compatible with transaction layer 103.

As shown in Figure 3B, in step 308, output adapter 214 may format the aggregated data into one or more content data records for storage in CDR database 215. In step 309, ownership resolution component 216 identifies the parties involved in the transaction. In step 310, transaction resolution component 221 captures the predetermined agreements among the parties, as well as the value added by each of the individual parties. In step 311, the CDR is rated based on predetermined metrics (*e.g.,* time of transmission, quality of content). In step 312, a bill is presented to the customer.

Content Transaction Layer

A transaction, including a business transaction for example, may be any activity between two or more participants that affects certain parties. The affected parties may be considered the participants to the transaction, although parties and participants may be mutually exclusive entities. It should be appreciated that the terms "parties" and "owners" may be used interchangeably throughout. Also, a transaction may include one or more events, where an event may be some action (*e.g.,* the transfer of a service or good) that the participants conduct with each other. Such events may be the exchange of data over a communication network, for example. Also, it should be appreciated that the same event or action may take place in any direction (*e.g.,* from party A to party B or from party B to party A). The "subject" of the action is the party who performs the activity, while the "object" of the action is the party who is affected or influenced in any way by the action.

Transaction layer 103 is responsible for capturing the characteristics of the transaction, including the parties, participants, subject, object, event/action type, direction of the action, for example. The scope of the characteristics captured by transaction layer 103 will vary with the nature of instrumentation layer 101, the capability of content collection layer 102, and the requirements of settlement layer 104. Generally, transaction layer 103 captures the predetermined agreements among all of the parties involved in system 100 regarding the value of the transferred content, as well as the value added by each of the individual parties in transferring such content. Therefore, transaction layer 103 is charged with understanding the nature of

the parties, as well as the understanding the actions that one or more parties perform and the influence of such action on the respective parties.

Transaction layer 103 includes CDR database 215, an ownership resolution component 216, and a transaction resolution component 221. CDR database 215 is a data store that holds each CDR for further processing by ownership resolution component 216 and transaction resolution component 221. In the context of a billable electronic business transaction, a proper accounting of a communication event, for any purpose including billing, requires both identifying the participants and defining the relationships among those participants. As discussed, ownership resolution component 216 serves to define the participants of the communication event, while transaction resolution component 221 serves to capture the predetermined relationships and/or agreements among the parties defined by ownership resolution component 216.

Transaction layer 103 is generic in that it operates without requiring an understanding of instrumentation layer 101 and content collection layer 102. Instead, transaction layer 103 takes the relevant characteristics of the transaction provided by instrumentation layer 101 and content collection layer 102, and selects and generates those characteristics required by settlement layer 104.

Although the operation of transaction layer 103 will be described in the context of an electronic event over a communication network for the purposes of billing for the event, it should be appreciated that the invention is not so limited, but is so described the purpose of clarity. For example, it should be appreciated that the invention may include functions other than billing, including security, network capacity planning, and content monitoring, for example. Also, the generic techniques described may be applied beyond the context of an electronic event over a communication network.

Figure 4 provides a block diagram of system 100 providing greater detail of the configuration and operation of transaction layer 103. As shown in Figure 4, content collection layer 102 provides a usage record 401 to transaction layer 103. A series of fields 403-408 comprise usage record 401. Although fields 403-408 will be

identified by certain labels for the purpose of clarity, it should be appreciated that fields 403-408 may identify any of the many possible characteristics of the transaction.

In the example provided by Figure 4, fields 407 and 408 identify the parties or participants to the transaction. In particular, field 407 identifies "User A" and field 408 identifies "User B." User A may be the subject party and User B may be the object party. For example, in the context of a telecommunication event, User A may be the "calling" party and User B may be the "called" party. Field 405 and field 406 identify a measurable quantity of the event. In particular, following the example of the telecommunications event, field 405 identifies a duration (in minutes) of the event and field 406 identifies the quantity of data exchanged during the event (in megabytes). Field 403 and field 404 may identify a "start time" and an "end time," respectively, of the communication event.

Although fields 403-408 provide just one example, in any case, it should be appreciated that user record 401 will include certain characteristics provided by instrumentation layer 101 and/or derived by content collection layer 102. These characteristics typically are provided to transaction layer 103 because they have some particular significance to identifying the characteristics necessary to allow settlement layer 104 to provide some accounting of the transaction. Therefore, usage record 401 may not necessarily include all of the characteristics provide by instrumentation layer 101 and/or derived by content collection layer 102, because certain characteristics may not relevant to the settlement of the transaction (*e.g.*, network type). Yet, usage record 401 will include those available characteristics that pertain to permitting settlement layer 104 to properly account for the transaction.

Once usage record 401 passes through transaction layer 103, a modified usage record 402 may be provided to settlement layer 104. Modified usage record 402 may be modified by transaction layer 103 to include additional details of the transaction event required by settlement layer 104 and/or required by the customer's system to which the usage record applies (*e.g.*, a usage billing system). As shown for modified usage record 402, an account A field 409 and an account B field 410 may be added to

further identify the transaction. In one example, account A field 409 may include an alphanumeric designator that identifies the account number that has been assigned by the customer's billing system for User A. In the context of the telecommunications system, account A field 409 may hold User A's ten-digit home telephone number, for example.

In any case, the components of transaction layer 103 operate to identify these additional fields, based on the requirements of the customer's system and of settlement layer 104. In particular, ownership resolution component 216 operates to ensure that the necessary participants or parties to the transaction are identified, while transaction resolution component 221 operates to ensure that the relationships among the parties or participants are identified.

Identification of the relevant entities and their relationships may be accomplished using "lookups" in data stores located within ownership resolution component 216 and transaction resolution component 221, for example. For example, a data table may have a "User" data field and an associated "Account" data field. When User A is received by ownership resolution component 216, it will conduct a lookup in the data table and identify Account A as the appropriate account associated with User A. Also, transaction resolution component 221 may have a data table that permits a lookup of the relationship between User A and User B, identified in usage record 401. For example, upon receiving field 407 designating User A and field 408 designating User B, transaction resolution component 221 may conduct a lookup of an algorithm that identifies the appropriate burdens and benefits (*e.g.,* debit and credit of money) assigned to each of the users with respect to each other.

It also should be appreciated that transaction layer 103 may not provide additional characteristics to usage record 401, as described but may select the relevant characteristics (*i.e.,* those characteristics needed by settlement layer 104) from the characteristics made available by instrumentation layer 101 and/or derived by content collection layer 102. In fact, usage record 401 may include all of the necessary characteristics to properly account for the transaction. In this case, ownership resolution component 216 and transaction resolution component 221 select the

relevant characteristics from the available characteristics. As will be explained in more detail below, the information added to the usage record 402 may also constitute pricing plans and the settlement layer may be configured to handle more sophisticated settlement strategies involving multiple parties and multiple pricing plans over a multiplicity of noncontiguous time periods.

Figures 5A and 5B provide a flow diagram of a method 500 for identifying the characteristics of a transaction using system 100. As shown in Figure 5A, in step 501, raw data 204-206 is received into system 100. Raw data 204-206 includes certain characteristics provided by data sources 201-203, respectively, in instrumentation layer 101. In step 502, content collection layer 102 processes (*e.g.*, aggregates, correlates and filters) raw data 204-206. In step 503, content collection layer 102 provides the processed data to CDR database 215 in transaction layer 103. CDR database 215 stores the data for further processing by transaction layer 103.

In step 505, it is determined whether the contents of the data provided to transaction layer 103 already include the needed ownership data. If the data includes the needed ownership data, the relevant data is selected by ownership resolution component 216 and provided to transaction resolution component 221, in step 507. If, on the other hand, the data provided to transaction layer 103 does not already include the needed ownership data, the required data is identified (*e.g.*, using database lookups) by ownership resolution component 216, in step 506. Once ownership resolution component 216 identifies the required ownership data, the relevant data is selected by ownership resolution component 216 and provided to transaction resolution component 221, in step 507.

As shown in Figure 5B, in step 508 it is determined whether the contents of the data provided to transaction layer 103 already include the needed relationship data (*i.e.*, data defining the burdens and benefits encountered by the parties/participants to the transaction). If the data includes the needed relationship data, the relevant data is selected by transaction resolution component 221 and provided to settlement layer 104, in step 510. If, on the other hand, the data provided to transaction layer 103 does not already include the needed relationship data, the required data is identified (*e.g.*,

using database lookups) by transaction resolution component 221, in step 509. Once ownership resolution component 216 identifies the required ownership data, the relevant data is selected by ownership resolution component 216 and provided to transaction resolution component 221, in step 510.

Ownership and Transaction Resolution

Figure 6 is a block diagram further detailing the operation and configuration of transaction layer 103. It should be appreciated that elements described for transaction layer 103 are not exclusive, but provide just one example of a configuration for transaction layer 103. In particular, the functionality of the previously described ownership resolution component 216 and transaction resolution component 221 will be described in greater detail in the various components described with reference to Figure 6. In practice, however, it should be appreciated that transaction layer 103 may comprise of any number of components that ensure that the necessary parties to a transaction are identified generically.

As shown in Figure 6, transaction layer 103 includes a configuration repository 601, a configuration database 610, a configuration manager 603, and a fail over detector 604. In addition, transaction layer 103 includes a transaction layer engine 608 in communication with configuration repository 601, configuration manager 603, and fail over detector 604.

Transaction layer engine 608 includes a rules processor 605, a CDR reader 606, and a transaction writer 607. Transaction layer engine 608 processes raw data 204-206 in usage record 401 and creates a modified usage record 402, based upon the requirements of settlement layer 104. It should be appreciated that there may be more than one transaction layer engine 608 for each transaction layer 103. However, a single transaction layer engine 608 is shown for the purpose of clarity and brevity.

CDR reader 106 understands the nature of the transaction and operates to read a particular usage record 401 stored in CDR database 215. CDR reader 106 then submits usage record 401 to rules processor 605. Rules processor 605 applies rules (*e.g.*, written in XML) to usage record 401 so as to determine ownership and the relationships among the ownership, for each individual usage record 401. Rules

processor 605 may then generate one or more modified usage records 402, based on the application of the rules to usage record 401. Once rules processor 605 generates the modified usage record 402, transaction writer 607 operates to write a transaction (based on the modified usage record 402) to CDR database 215. Modified usage record 402 is then used by settlement layer 104 to further process the transaction (*e.g.*, rate the transactions monetarily).

Fail over detector 604 operates to provide fault tolerance and initiate a fail over engine (not shown) for a failed transaction layer engine, in accordance with one or more mathematical algorithms, the discussion of which is beyond the scope of the invention. Configuration manager 603 provides an external interface to transaction layer 103 using a business editor 609. Business editor 609 may be manipulated by a user or customer using a graphics user interface (GUI). In particular, the GUI of business editor 609 receives commands from a user and translates them into actions to be performed on usage record 401, for example, by rules processor 605. Configuration repository 601 operates to provide an abstraction to configuration database 610. Configuration database 610 may be a relational database or a set of extensible markup language (XML) computer-readable files, for example.

Figure 7 is a flow diagram that details the operation of transaction layer 103, as shown in Figure 6. As discussed, it should be appreciated that multiple transaction engines may be used to implement a process. Where the invention is instituted using computer-readable instruction, transaction layer engine 608 may be implemented as a computer-executable instruction or thread. Therefore, multiple transaction layer engines may be implemented by having multiple computer-readable instructions.

In step 701, transaction layer engine 608 reads usage record 401 using CDR reader 606. In step 702, rules processor 605 applies one or more rules to usage record 401 read by CDR reader 606, so as to determine one or more "accountables." Accountables are labels that are used to facilitate identifying the parties or owners to a transaction. Accountables may be defined and/or modified by an external user (*e.g.*, a customer) using the graphical user interface provided by business editor 609. Also, it should be appreciated that accountables may be defined for a new usage types for

which no rules in rules processor 605 are provided. The identification of accountables is the function of ownership resolution component 216, as described with reference to Figure 4.

In step 703, "contracts" are identified that define the relationships or agreements between one or more accountables. In the context of a billing system, a contract identifies which parties pays (*i.e.,* the billed party) and which party receives payment (*i.e.,* the billing party). A particular contract may be identified and executed when one or more "conditions" are satisfied. The identification of contracts is conducted by transaction resolution component 221, as described with reference to Figures 2 and 4. A condition is an expression of a logical assertion that can be evaluated as true or false. In transaction layer 103, for example, a condition may be true if a certain data element is present and false if the data element is not present. The following is an example of a condition in XML:

```
<condition name="condition1" function="IsPresent" outcome="true"
type="Accountable" id="ColoProvider"/>
```

In step 704, once the contracts are determined, they are executed. In step 705, usage record 401 is changed to modified usage record 402 based upon the execution of the contract and the identification of the accountables. In step 706, modified usage record 402 may be written to a data table using transaction writer 607, so that settlement layer 104 can rate it, in step 707. Therefore, a transaction may be represented as modified usage record 402, where modified usage record may include the elements of usage record 401 in addition to the accountable and contract elements (*e.g.,* fields 409-410 as discussed with reference to Figure 4).

Although the discussion provided an example of a single contract and two accountables for a single usage record, it should be appreciated that many contracts and many accountables (*i.e.,* and therefore many "transactions") may be derived from a single usage record, because there may be multiple transactions implicated from a single usage record 401. For example, usage record 401 may involve three parties

each having a contract with the other respective parties. In this example, therefore, there may be three separate contracts for a single usage record 401, and three individual accountables for each party or owner. Moreover, as will be explained below, the contracts may operate according to pricing plans that vary over time and from party to party.

In addition to requiring a certain accountable, it may be necessary to determine a value of the accountable. For example, transaction layer 103 may determine not only that the "called party" accountable be a part of the transaction, but also that a value for the called party (*e.g.*, "856-555-1212" or "John Doe") be identified. Also, it may be necessary to transform one accountable into another accountable to satisfy the requirement of settlement layer 104. For example, settlement layer 104 may require the called party accountable (either determined by transaction layer 103 or provided in usage record 401) be transformed into a network identifier accountable.

In either case, the value or transformation of accountables or contracts may be determined using certain predetermined functions or "primitives." A primitive defines a transformation or a valuation of an accountable or contract. As discussed, transformations may allow a value of an accountable to be determined using another accountable, for example. Primitives define and direct such transformations. The input to a primitive can be one of fields 403-408 from usage record 401 or a previously determined accountable, for example.

Primitives may be described and distinguished based on their prescribed functionality. For example, one type of primitive may be a database lookup. A database lookup is a primitive that operates to transform one accountable or contract to another accountable or contract. Also, a database lookup primitive may function to assign a value to an accountable or contract, as a result of conducting a lookup of the accountable or contract in a database. It should be appreciated that the database lookup primitive also allows flexibility in that any database that has Java Database Connectivity (JDBC) drivers (*e.g.*, Oracle, Microsoft SQL Server, Sybase, Database 2) can be used to perform complex lookups. In this way, therefore, previous

accountable or contact transformations can be linked to find new accountables or contracts, respectively.

Other types of primitives may include direct value assignment, and a function primitive that looks up data in an external database. Other primitives may include a function primitive that it allows a third party based library (*e.g.,* Java-based) to be used. Another primitive may be a "regular expression" based primitive that allows parsing of complex text-based fields with a full feature (*e.g.,* PERL5 compliant) pattern specification. Common used techniques would include parsing URLs, filenames and paths, calling/called telephone numbers, email address, for example. In addition, a CDR database 215 lookup primitive allows holding on to an ownership entity if no further processing is required. This primitive is used where usage record 401 provides the information needed by settlement layer 104 without any need for more data correlation and/or manipulation by transaction layer 103.

A default primitive may be a hard-coded primitive that is used where the value is known and/or is not dependent on usage record 401. For example, such a primitive may be used where a party is always present in a consumption event, regardless of the other relevant parties. A network address primitive allows determination of a network entity given an arbitrary string. An area code primitive may be used to determine an area code of a telephone number given the complete telephone number. This primitive may be relevant for a Voice-over-IP application. These examples primitives are not exclusive, but are meant to provide a few examples of the manipulation and correlation that may be achieved by the primitives on the accountables and contracts.

The following is an example of an accountable primitive in XML:

```
<accountable>
<name> ColoProvider </name>
<role> ServiceProvider </role>
<usageType> RMONHost </usageType>
<valid from="past" to="present" />
<primitive type="default">
<value> Exodus </value>
</primitive>
</accountable>
```

Each accountable that is involved in a contract will have an assigned "role." It follows, therefore, that an accountable that is not involved in a contract may not need to have an assigned role. The role associates the particular accountable for integration with settlement layer 104.

Similar to the accountable, a contract is implemented using a set of primitives. The following is an example of a contract primitive in XML. In the example, a Web hosting scenario is present where a content provider (*e.g.*, CNN) places content on one or more Web servers and pays a Web Hoster for doing so based on some predefined pricing plan.

In order to define the accountables, certain elements of usage record 401 may be assumed as follows: Web Hit Time, Web Server Name/IP address, Client IP address, bytes, Mime type, and URL. In this example, if a rule in the business world requires the "Content Provider" of the Web Server (*e.g.*, CNN) to pay to the Web Hoster, there are two accountables: Web Hoster and Content Provider. The XML definition of a contract that captures this business rule may be as follows:

```
01  <contract>
02  <name> ContentProvider-Pays-WebHoster </name>
03  <usageType> WebHosting </usageType>
04  <valid from="past" to="present" />
05  <condition function="IsPresent" type="Accountable"
    name="condition1"  id=" ContentProvider " />
06  <condition function="IsPresent" type="Accountable"
    name="condition2" id="WebHoster" />
07  <billedFunction>
08  <status> enabled </status>
09  <primitive type="internal-account-lookup">
10  <database name="GlobalDB"/>
11  <argument order="1" type="Accountable"
    name="ContentProvider"/>
12  </primitive>
13  </billedFunction>
14  <billingFunction>
15  <status> disabled </status>
16  <primitive type="internal-account-lookup">
17  <database name="GlobalDB"/>
```

```
18    <argument order="1" type="Accountable"
name="WebHoster"/>
19    </primitive>
20    </billingFunction>
21    </contract>
```

In this example, a contract has a name defined in line 02 as "ContentProvider-Pays-WebHoster." The contract also defines an element or usage type called "WebHosting" in line 03. The contract also has two sets of conditions in lines 05 and 06, called "IsPresent," which consider whether "ContentProvider" and "WebHoster" elements are present, respectively. Therefore, this particular contract will be selected and executed by transaction layer 103 if these elements are present.

Also, in this contract example, there are two primitives that are specified. There is a first primitive for finding the account number of the billed entity "ContentProvider," which begins on line 07 and ends on line 13, and there is a primitive for determining the account of the billing entity "WebHoster" beginning on line 14 and ending on line 20. Therefore, the example contract contemplates the "who pays to whom" logic, and results in the execution of a contract that creates a modified usage record 402, which captures the transaction. Notably, in lines 09 and 16, both primitives are defined as database lookups.

As noted above, to settle a transaction, the system must determine who should compensate whom and by how much. Many processes contribute to such "settlement." Accordingly, the settlement layer 104 is not necessarily a particular logical component but may be spread throughout the system. In operation, a typical "settlement" might occur as described below with respect to Figure 8.

Figure 8 illustrates a sample content event as received by transaction layer 103 pursuant to the processes described above. In this example, "content.com" is identified as the billed party for a caching service, and IP address "128.33.2.41" is identified as the billed party for consuming content type "audio video interleave" (.avi). This IP address may be mapped to a customer account that may vary over time. The system also may identify the log provider (*e.g.*, web host service) and may identify the content property owner (*e.g.*, "Disney") as the party to receive a royalty,

or some other form of compensation, for the download. This ownership may create rules based on the unique resource locator (URL) substring and other event information. Also, links may be provided from the event to the multiple accounts related to that event. The use of pricing plans and pools, as described below, allow business rules to be captured regarding compensation for events, for example, in ways that greatly increase system flexibility. In this example, a fee may be charged to "content.com," while revenue may be paid back to the log provider.

Settlement of Transactions Subject to Multiple Pricing Plans

In many transactions, the accounts include one or more pricing plans that are customized to particular customers. As shown in Figure 9, the settlement technologies used to settle such transactions may allow for multiple ownership of content, multiple aggregation of usage, and provide a variety of revenue sharing models. Several of such models will be described below including folds with parent account plans, revenue pooling, and commission relationships between plans.

Figure 10 illustrates a settlement example for the case of digital content, such as digital music content downloadable off of the Internet. In this example, an on-line music club (*e.g.,* BMG, EMI, Sony) has a contractual relationship with the consumers as well as the music publishers (*e.g.,* "www.cd-club.com") and, at settlement, allocates payment according to the price plan(s) with the consumer and the payment plan(s) with the publishers. These payment plans recognize that each song may have a different price and that the revenue paid to the publisher, author, etc. may vary over time depending upon the frequency of download, for example. The price to the consumer also may vary with use. Figures 11 and 12 illustrate settlement models that take into account transaction pricing and billing cycle pricing for such usage based settlements. As those skilled in the art will appreciate, the per transaction usage based model may be best utilized for low volume, high value transactions, while the billing cycle pricing usage based model may be better for high volume, low value transactions.

The present invention allows for the networking of a multiplicity of pricing plans during rating process 217 in settlement layer 104. Thus, the system described

below is implemented primarily in ratings 217 described above with respect to Figure 2.

Pricing Plan Overview

In accordance with the invention, pricing plans may be created by interconnecting rating building blocks with customizable properties. Each rating building block may be specialized in one well-defined function that falls roughly into five classes: usage selection and filtering, usage computation, accumulation, rate computation, and bill presentation. By interconnecting these rating building blocks, together with the ability to add new rating building blocks to the system, very flexible and extensible pricing plans can be created. The computation may be desirably constrained within one pricing plan.

A new class of rating building blocks also may be defined to extend the usefulness of pricing plans. This new class of rating building blocks allows a plan to access the states of another pricing plan or a group of pricing plans. These states can be usages and/or charges associated with line items and/or intermediate computations. With this new capability, computation is not constrained within one pricing plan but within a network of pricing plans working together. This new computation offers, but is not limited to, many settlement features.

A revenue fold summarizes revenue, which is the output of a pricing plan, from child accounts and presents the folded revenue to their corresponding parent accounts as input to their pricing plans. This process may start from the lowest level and continue on up to the root level. The value of revenue fold may be available to a parent account in a pricing plan through a building block (*e.g.*, "RevenueToDate"). As illustrated in Figure 13, the revenue fold settlement model of the invention may provide for pricing plans at each level in the hierarchy and allow for the use of resellers.

Revenue/usage pools are similar to global variables except that they include the concept of billing cycles. Different periods of a pool imply different instances and therefore different values. A pool value may be updated during invoice processing by summing the values of invoice line items associated with the pool from appropriate

account plan periods. An account plan period is considered appropriate if the end date is within the period of the particular pool instance. Note that it is possible to have zero or more than one account plan periods from the same account to be included in the same pool instance. The computation of a pool value may not be cumulative between updates. When a pool value needs to be updated, the computation may start over with the previous value of a pool having no consequence. For example, the value of a pool may be accessible from a pricing plan through a building block (*e.g.*, "PoolAccessor") with the pool name as its property. The output of the "PoolAccessor" is the sum of the pool instances having the same pool name and billing period end dates within the start and end dates of the account plan period. As shown in Figure 14, this settlement feature is useful in revenue sharing scenarios where total revenue and resources are pooled together and total revenue is shared among the contributing accounts based on contributed resources. The pools may be hierarchy independent and defined by the pricing plans. A revenue pool contribution example is given in Figure 15, and a revenue pool accessor example is given in Figure 16.

A commission is a credit given to an account. The credit amount is computed based on the revenue, or states of another account. The two accounts involved in the transaction are commission source account and commission destination account. As shown in Figure 17, the commission source account (commission generator plan) generates the commission contribution iCDR using a building block (*e.g.*, "CommissionGenerator") with "AccountNumber" and "CommissionDescription" as its properties. The amount, not necessarily revenue, going into the CommissionGenerator (commission plan) is the commission amount. When used in conjunction with existing rating building blocks, commission features such as the following can be supported: commission going to multiple accounts, commission based on total revenue or a subset of the revenue (*e.g.*, only monthly and usage charges, but not setup charges), commission for the first "n" billing period only (or different rate after first "n" periods), and step rate.

The commission destination account may receive the commission data through a building block (*e.g.*, "CommissionAccumulator"). Additional commission features such as the following can be supported on the destination account: a recurring base commission, promotional commission rate, and step commission rate. The commission settlement model also may be hierarchy independent and permit variable settlement arrangements.

When computation involves a network of pricing plans, the correct output of a particular pricing plan may be dependent on the processing of another pricing plan. The output of the other pricing plan may in turn dependent on yet another pricing plan. A cyclic dependence can even exist. In order to have the correct computation for the network of pricing plans as a whole, the system detects and continues processing until all pricing plans reach their final values. Accordingly, the settlement processing software in accordance with the invention has a built-in mechanism to repeat processing of the pricing plans until their values are final. The algorithm will stop after a configurable loop count to prevent infinite processing in case there is a cyclic dependence.

Billing Cycle Considerations

Because more than one account may be involved in settlement, it is possible that they have different billing periods. The following section details how each settlement feature is processed for the settlement models of the invention when accounts with different billing periods are involved.

Revenue fold summarizes revenue from child accounts and presents the folded revenue to their parent accounts. This process starts from the lowest level and continues up to the root level. In actual settlement processing, revenue fold is a post order traversal of a tree whose nodes are account plan periods, where a post order tree traversal traverses each sub tree of the root in post order followed by the root. The child account plan periods are selected if the end dates are within the parent's account plan period. It is possible to have zero or more than one account plan period from the same account included in one revenue fold. The root account's account plan period is defined by the invoice processing start and end dates.

An iCDR is generated for each revenue fold. The iCDR is rated by the pricing plan for the account plan period receiving the revenue fold. Therefore, pricing plans for non-leaf accounts take revenue fold into consideration. The value of revenue fold is available in a pricing plan through a building block (*e.g.*, "RevenueToDate").

Figure 18 provides an example of computing revenue fold. To compute the revenue fold for account 1001, the revenue from all child accounts of 1001 with account plan period end dates between 3/1 and 4/1 are summed. In this example, the revenue for account 2001 for the billing period 2/7 to 3/7, account 2002 for the billing period 2/15 to 3/15, account 2003 for the billing period 2/22 to 3/22 are summed. Before the summing of the revenue of these accounts can occur, their own revenues are determined. In order to determine the revenue of these child accounts, their child accounts with account plan period end dates between their account plan period start and end dates are selected and summed. The following example shows that to determine the revenue for account 2003 for the billing period 2/22 to 3/22, revenue for account 3001 for the billing period 2/1 to 3/1 and account 3002 for the billing period 2/15 to 3/15 are summed. This process repeats until the leaf level account is reached.

The value of a pool is accessible from a pricing plan through a rating building block (*e.g.*, "PoolAccessor"). The output of "PoolAccessor" is the sum of the pool instances having billing period end dates within the start and end dates of the account plan period. It is possible to have zero or more than one instance selected given a particular account plan period depending on the billing period of the pool and the account. Therefore, given the same plan, "PoolAccessor" output may vary according to the account plan period. This technique ensures that each invoice line item associated with a pool will be included a pool instance and that each pool instance will be accessed once by an account which accesses the pool.

Figure 19 illustrates how accounts and pools with different billing cycles contribute to and access from pool instances. For example, line items associated with pool A for account 1001 with billing period from 4/1 to 6/1 and account 1002 with billing periods from 3/22 to 4/22 and 4/22 to 5/22 will contribute to the pool A's

instance with period from 4/1 to 6/1. The output of the PoolAccessor will be zero for account 2001 during the period 4/1 to 5/1. For billing period from 5/1 to 6/1, account 2001 will get the value of pool A's instance with period from 4/1 to 6/1. Account 2002 with billing period from 4/1 to 6/1 will also get pool A's 4/1 to 6/1 instance. The account plan period from 4/1 to 8/1 for account 2003 will get the sum of the two pool A's instances, 4/1 to 6/1 and 6/1 to 8/1.

During invoice processing, one or more iCDRs will be generated for each commission producing account plan periods. The generated record will have the destination account number, amount, and a timestamp. The timestamp is the end date of the account plan period that generated the record. The record will then be rated by the destination account in the appropriate account plan period.

Figure 20 provides an example of how an account 2001 with billing period ending 6/1 will get one commission from account 1001 for the period 4/1 to 6/1 and two commissions from account 1002 for the periods 3/22 to 4/22 and 4/22 to 5/22.

An invoice output may be dependent on the processing of settlement features. In turn, processing of settlement features may be dependent on correct invoice output. For example, if the pricing plan associated with an invoice accesses one or more pools, revenue/usage pool processing should be completed successfully before a correct invoice can be produced. To process a revenue/usage pool correctly, account plan periods associated with a pool have to produce a correct invoice that in turn may be dependent on revenue fold. There may not be a single, correct pre-defined order of processing for these settlement features. In some cases, the same settlement features may have to be processed more than once (*e.g.*, revenue fold, generate commission and then revenue fold again).

The settlement processing has a built-in mechanism to repeat processing of the settlement features in a fixed sequence until the values are final. To prevent the algorithm from looping forever, there is a configurable maximum loop count. If the result is not final after the maximum loop count, a warning will be given, and the user may remove the circular dependency (if one exists) and/or increases the maximum loop count.

The invention described above is directed to a system and method for handling the networking of pricing plans in the settlement of transactions. The invention often was described in the context of the Internet, but is not so limited to the Internet, regardless of any specific description in the drawing or examples set forth herein. For example, the invention may be applied to wireless networks, as well as non-traditional networks like Voice-over-IP-based networks and/or private networks. It will be understood that the invention is not limited to the use of any of the particular components or devices herein. Indeed, this invention can be used in any application that requires aggregating data. Further, the system disclosed in the invention can be used with the method of the invention or a variety of other applications.

While the invention has been particularly shown and described with reference to the embodiments thereof, it will be understood by those skilled in the art that the invention is not limited to the embodiments specifically disclosed herein. Those skilled in the art will appreciate that various changes and adaptations of the invention may be made in the form and details of these embodiments without departing from the true spirit and scope of the invention as defined by the following claims.

What is claimed is:

1. A method of rating a transaction, comprising:

processing a transaction, wherein the transaction is processed when a service is provided from a service provider to a service consumer;

accessing via a computer network multiple pricing plans related to the transaction; and

rating the transaction in accordance with the multiple pricing plans.

2. The method of claim 1, wherein at least one of the pricing plans includes at least one of the following: revenue folds, revenue/usage pools, and commissions.

3. The method of claim 1, further comprising receiving output states from at least one pricing plan.

4. The method of claim 1, wherein the rating is accomplished within one pricing plan.

5. The method of claim 1, wherein the rating is accomplished within a group of pricing plans.

6. The method of claim 1, wherein the accessing is accomplished via interconnected building blocks located within each of the pricing plans.

7. The method of claim 1, wherein the building blocks perform at least one of the following functions: data usage selection and filtering, data usage computation, data accumulation, rate computation, and presentation of required payment.

8. The method of claim 6, wherein the building blocks have customizable properties.

9. The method of claim 6, wherein the building blocks allow a first pricing plan to access states of another pricing plan.

10. The method of claim 9, wherein the states are usages and charges associated with one or more pricing plans.

11. The method of claim 6, wherein the building blocks allow a first pricing plan to access the states of a group of pricing plans.

12. The method of claim 11, wherein the states are usages and charges associated with one or more pricing plans.

13. The method of claim 1, further comprising a revenue fold, wherein the revenue fold summarizes the output of multiple pricing plans.

14. The method of claim 13, wherein the revenue fold summarizes child accounts and inputs the summary information to pricing plans of corresponding parent accounts.

15. The method of claim 13, wherein the value of the revenue fold is available to the pricing plan via a building block.

16. The method of claim 13, wherein the revenue fold is available to child and parent accounts.

17. The method of claim 13, further comprising selecting child accounts with end dates that are within a parent account's time period.

18. The method of claim 1, further comprising pooling revenue/usage data as a function of billing cycles.

19. The method of claim 18, further comprising updating the pooled revenue/usage data by summing the values of data from selected account plan periods.

20. The method of claim 18, further comprising selecting the account plan period as a function of the end date of the account plan with respect to the pooled revenue/usage data.

21. The method of claim 18, further comprising accessing a value of the pooled revenue/usage data via a building block.

22. The method of claim 1, further comprising determining the value of a pricing plan as a function of another pricing plan.

23. The method of claim 22, further comprising providing a configurable loop count.

24. A computer-readable medium having computer-executable instructions, comprising:

processing a transaction, wherein the transaction is processed when a service is provided from a service provider to a service consumer;

accessing via a computer network multiple pricing plans related to the transaction; and

rating the transaction in accordance with the multiple pricing plans.

25. The computer-readable medium of claim 24, having computer-executable instructions further comprising receiving output states from at least one pricing plan.

26. The computer-readable medium of claim 24, having computer-executable instructions further comprising a revenue fold, wherein the revenue fold summarizes the output of multiple pricing plans.

27. The computer-readable medium of claim 24, having computer-executable instructions further comprising selecting child accounts with end dates that are within a parent account's time period.

28. The computer-readable medium of claim 24, having computer-executable instructions further comprising pooling revenue/usage data as a function of billing cycles.

29. The computer-readable medium of claim 24, having computer-executable instructions further comprising determining a commission, wherein the commission is a credit given to an account.

30. The computer-readable medium of claim 24, having computer-executable instructions further comprising determining the value of a pricing plan as a function of another pricing plan.

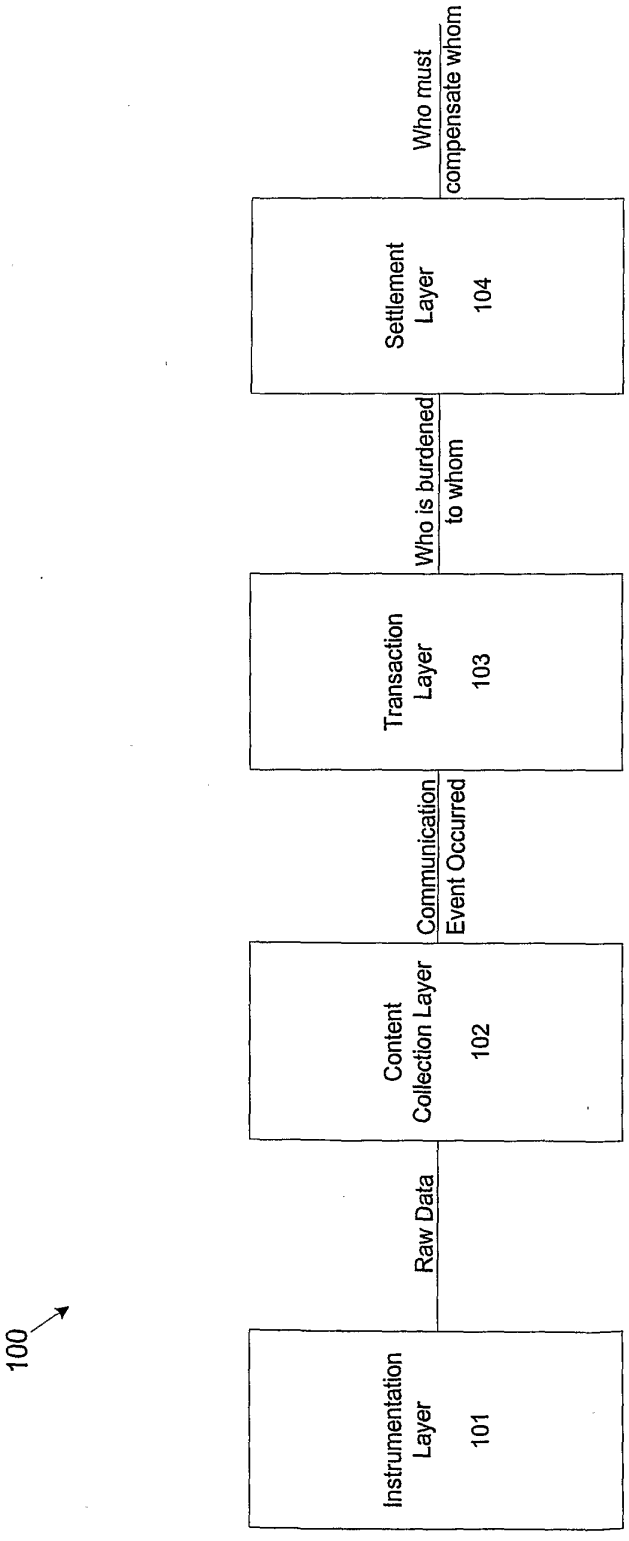

100
Instrumentation Layer 101
Raw Data
Content Collection Layer 102
Communication Event Occurred
Transaction Layer 103
Who is burdened to whom
Settlement Layer 104
Who must compensate whom

Figure 1

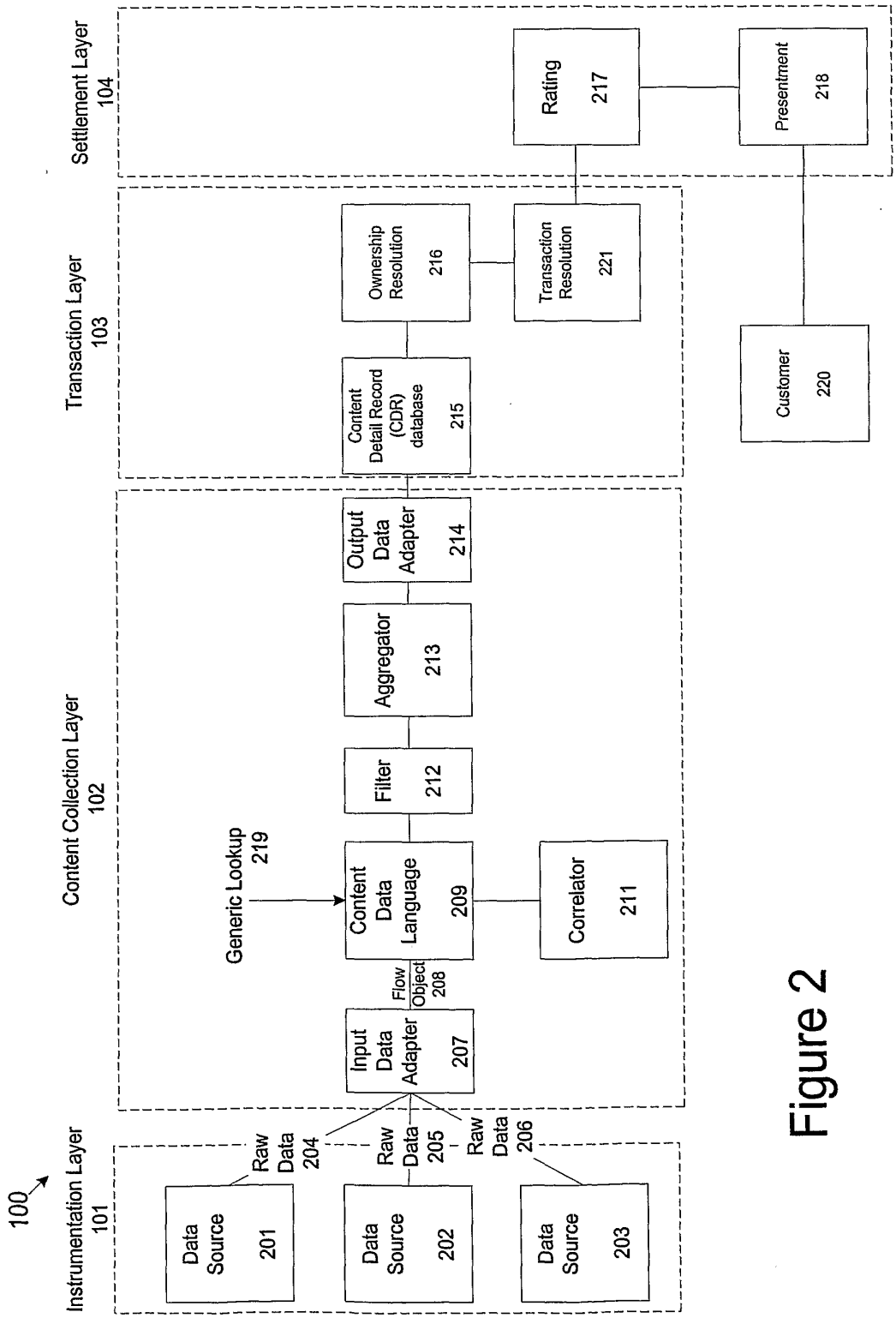

100
Instrumentation Layer
101
Data Source
201
Data Source
202
Data Source
203
Raw Data
204
Raw Data
205
Raw Data
206
Content Collection Layer
102
Input Data Adapter
207
Flow Object
208
Content Data Language
209
Generic Lookup
219
Filter
212
Aggregator
213
Output Data Adapter
214
Correlator
211
Transaction Layer
103
Content Detail Record (CDR) database
215
Ownership Resolution
216
Transaction Resolution
221
Customer
220
Settlement Layer
104
Rating
217
Presentment
218

Figure 2

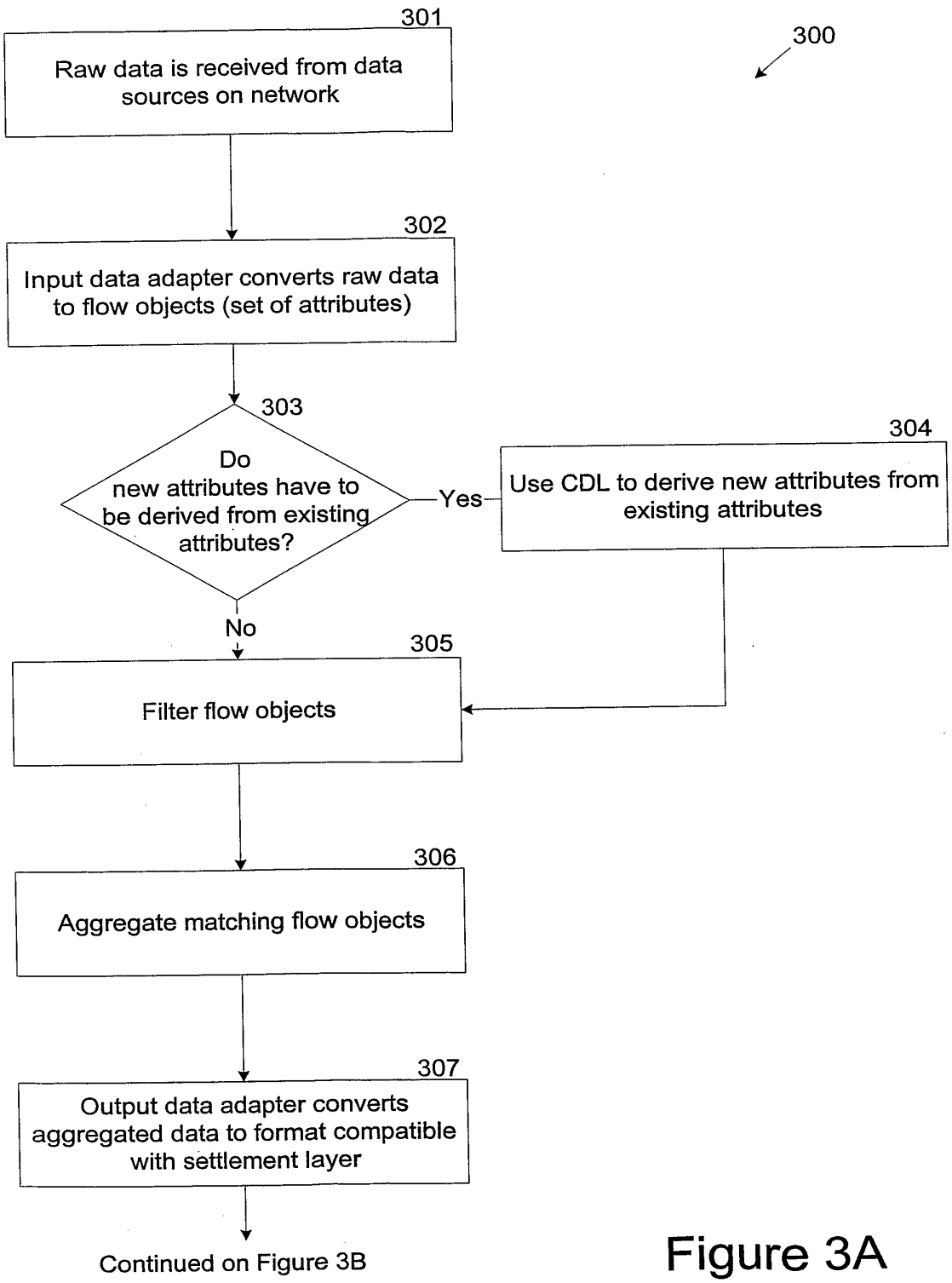

301
Raw data is received from data sources on network
300
302
Input data adapter converts raw data to flow objects (set of attributes)
303
Do new attributes have to be derived from existing attributes?
Yes
304
Use CDL to derive new attributes from existing attributes
No
305
Filter flow objects
306
Aggregate matching flow objects
307
Output data adapter converts aggregated data to format compatible with settlement layer
Continued on Figure 3B

Figure 3A

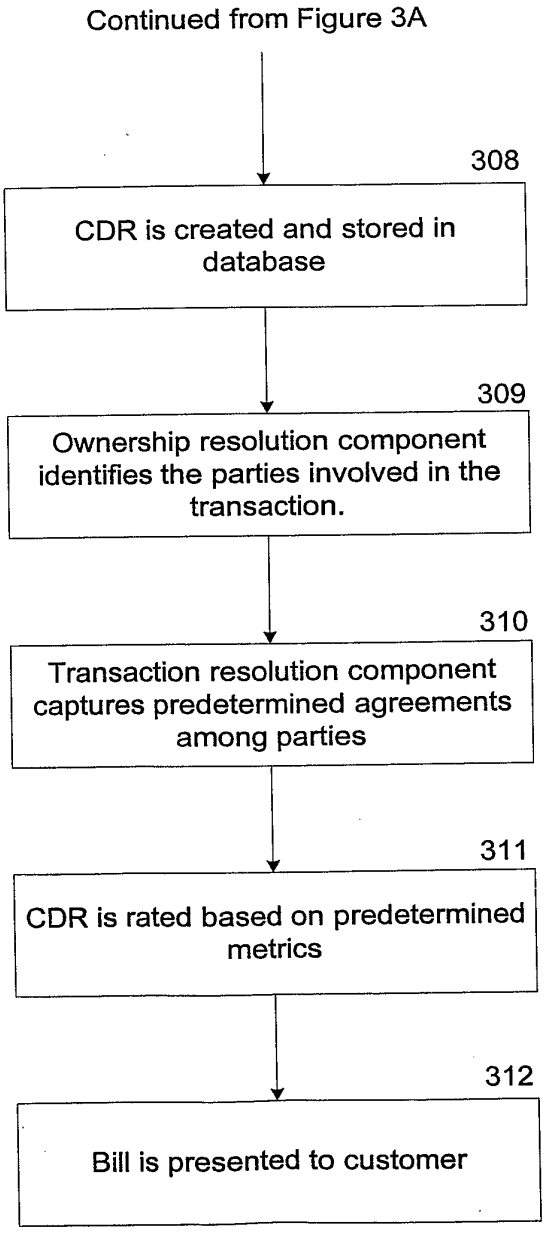

Continued from Figure 3A
308
CDR is created and stored in database
309
Ownership resolution component identifies the parties involved in the transaction.
310
Transaction resolution component captures predetermined agreements among parties
311
CDR is rated based on predetermined metrics
312
Bill is presented to customer

Figure 3B

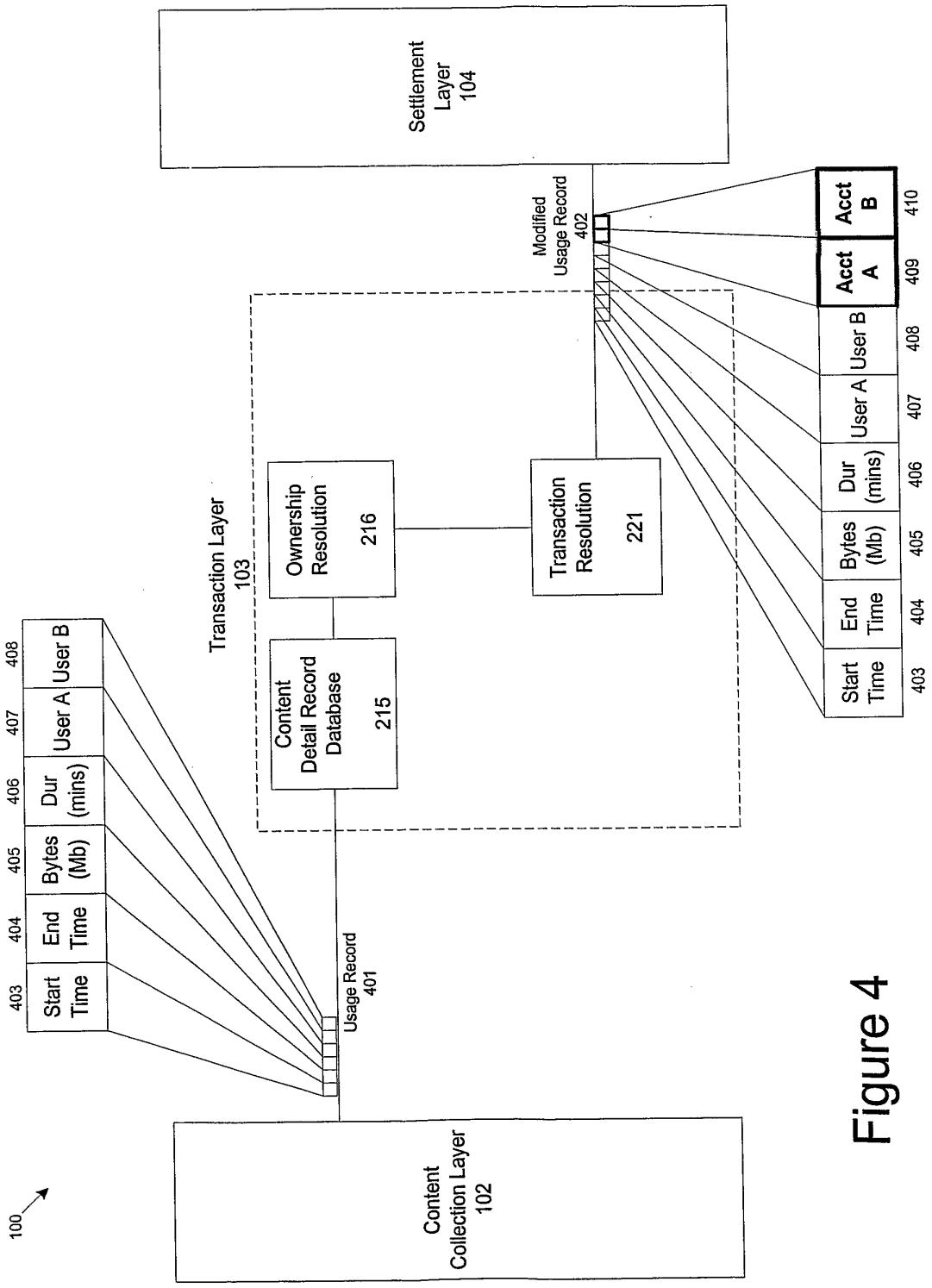

100
Content Collection Layer 102
Usage Record 401
Start Time 403
End Time 404
Bytes (Mb) 405
Dur (mins) 406
User A 407
User B 408
Transaction Layer 103
Content Detail Record Database 215
Ownership Resolution 216
Transaction Resolution 221
Modified Usage Record 402
Settlement Layer 104
Start Time 403
End Time 404
Bytes (Mb) 405
Dur (mins) 406
User A 407
User B 408
Acct A 409
Acct B 410

Figure 4

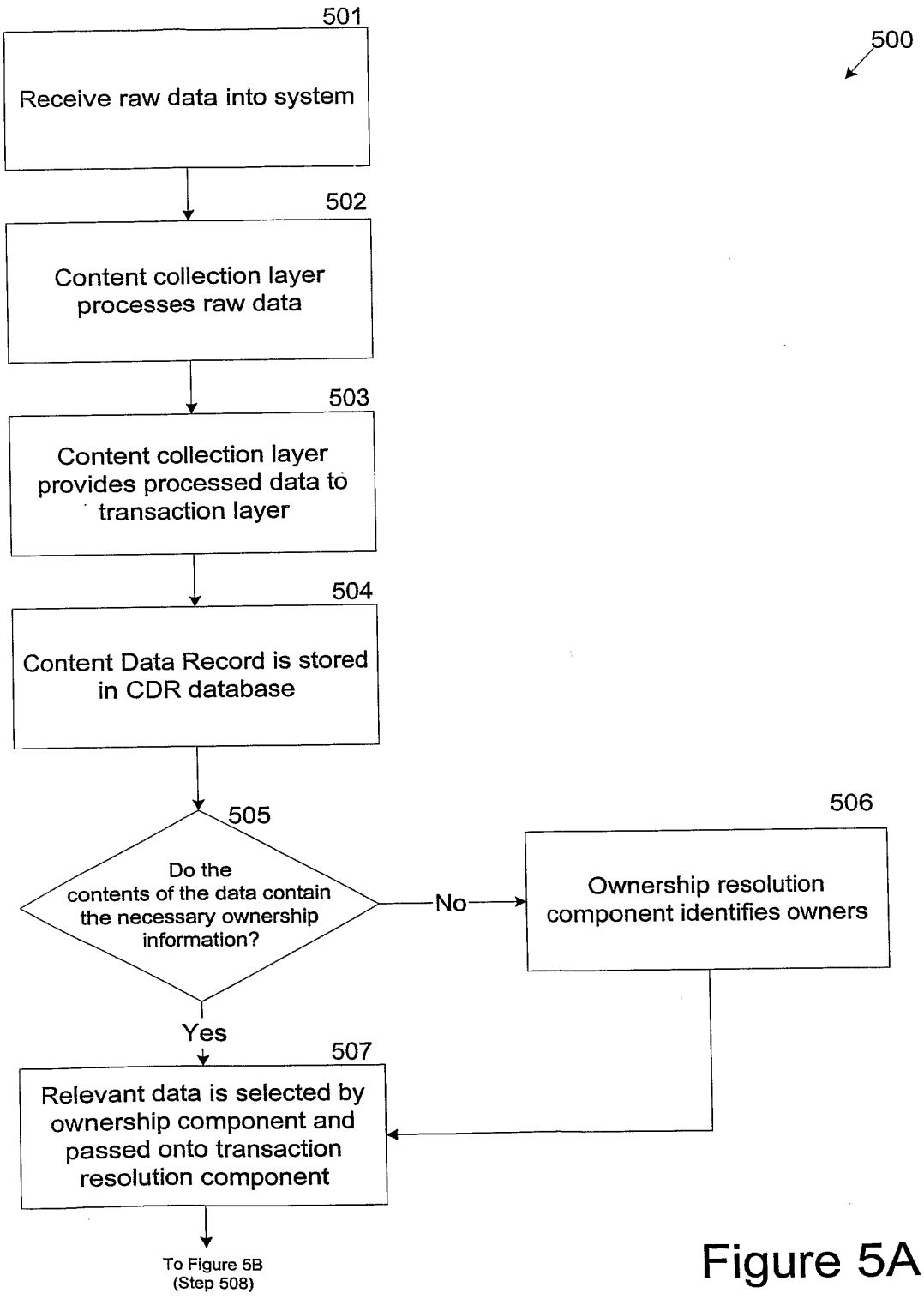

500
501
Receive raw data into system
502
Content collection layer processes raw data
503
Content collection layer provides processed data to transaction layer
504
Content Data Record is stored in CDR database
505
Do the contents of the data contain the necessary ownership information?
No
506
Ownership resolution component identifies owners
Yes
507
Relevant data is selected by ownership component and passed onto transaction resolution component
To Figure 5B (Step 508)

Figure 5A

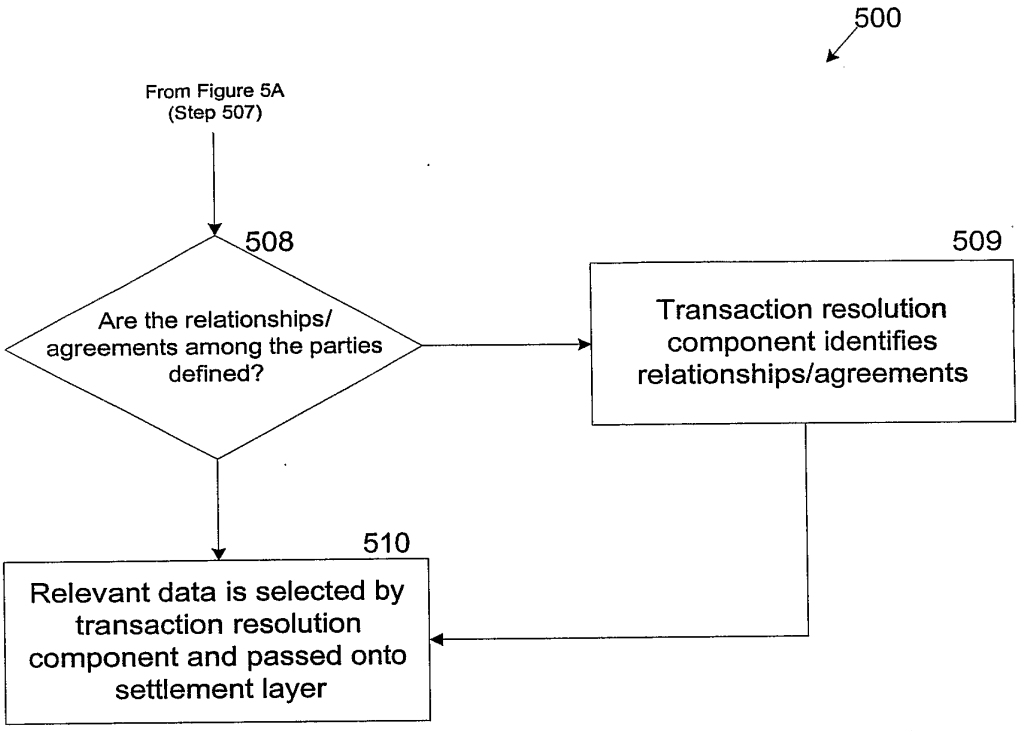

500
From Figure 5A
(Step 507)
508
Are the relationships/ agreements among the parties defined?
509
Transaction resolution component identifies relationships/agreements
510
Relevant data is selected by transaction resolution component and passed onto settlement layer

Figure 5B

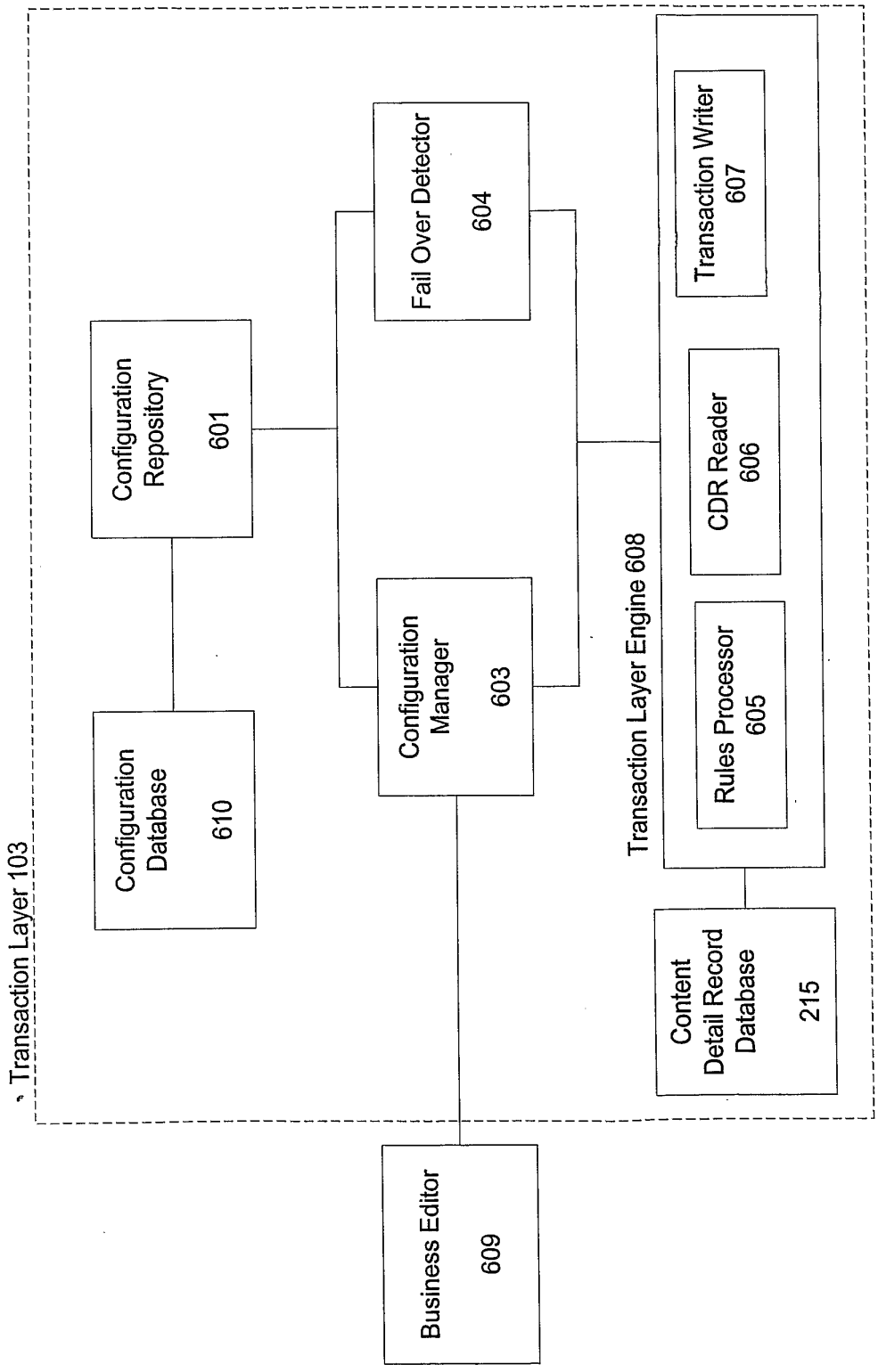

Transaction Layer 103
Configuration Repository 601
Configuration Database 610
Fail Over Detector 604
Configuration Manager 603
Business Editor 609
Transaction Layer Engine 608
Transaction Writer 607
CDR Reader 606
Rules Processor 605
Content Detail Record Database 215

Figure 6

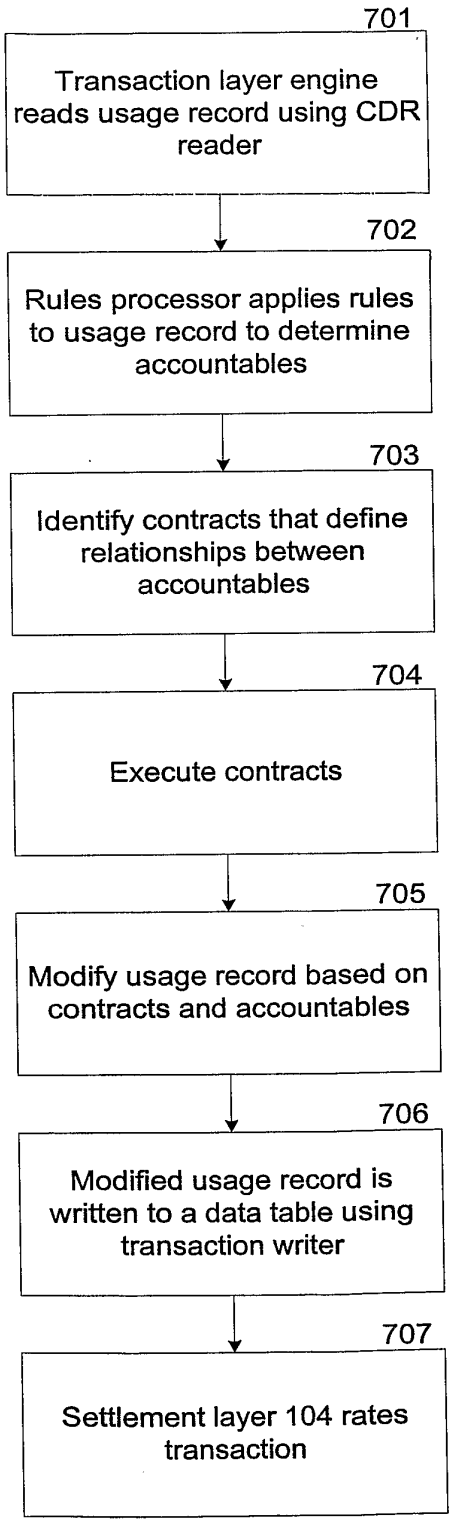

701
Transaction layer engine reads usage record using CDR reader
702
Rules processor applies rules to usage record to determine accountables
703
Identify contracts that define relationships between accountables
704
Execute contracts
705
Modify usage record based on contracts and accountables
706
Modified usage record is written to a data table using transaction writer
707
Settlement layer 104 rates transaction
700

Figure 7

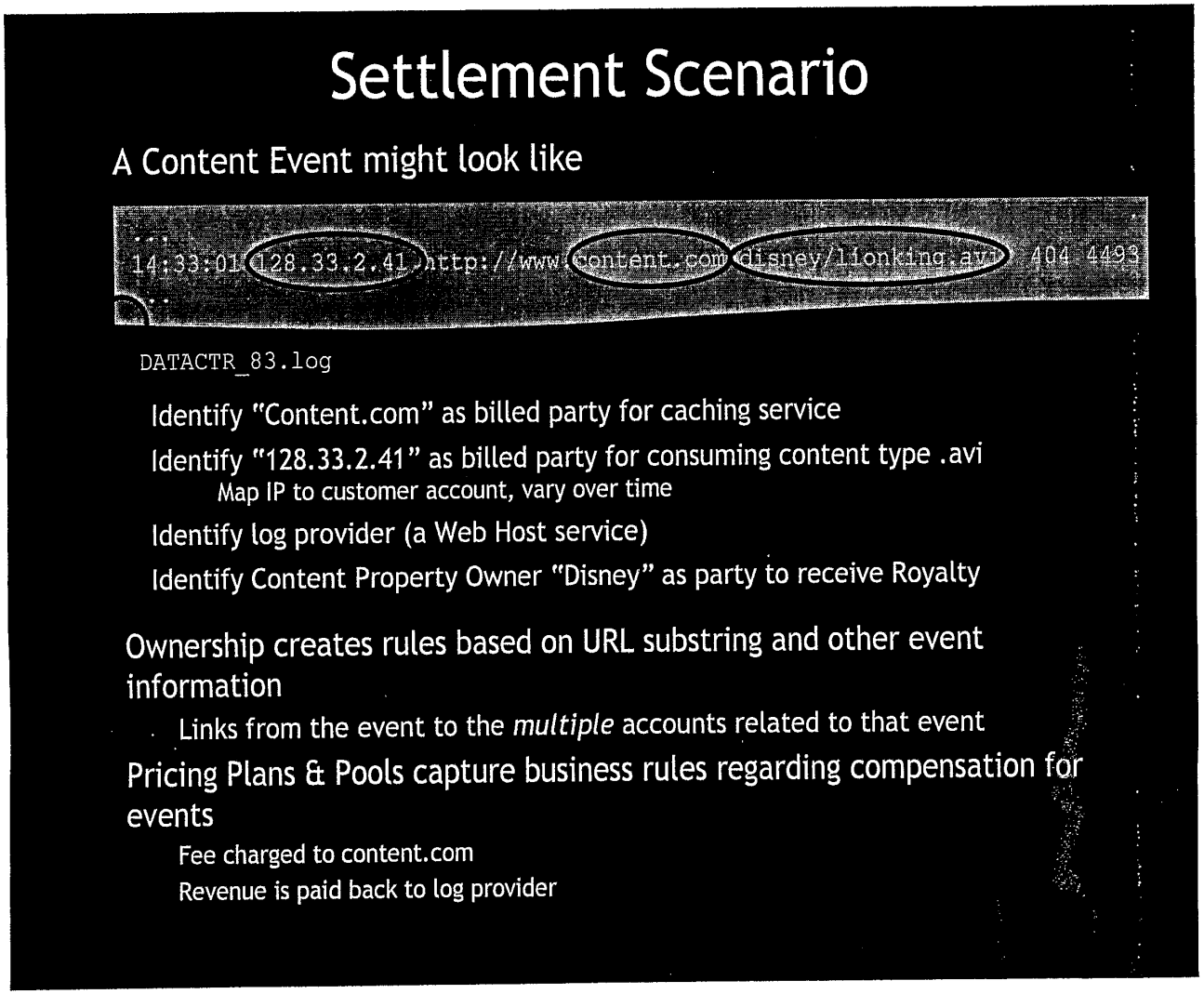

Settlement Scenario
A Content Event might look like
14:33:01 128.33.2.41 http://www.content.com disney/lionking.avi 404 4493
DATACTR_83.log
Identify "Content.com" as billed party for caching service
Identify "128.33.2.41" as billed party for consuming content type .avi
Map IP to customer account, vary over time
Identify log provider (a Web Host service)
Identify Content Property Owner "Disney" as party to receive Royalty
Ownership creates rules based on URL substring and other event information
Links from the event to the multiple accounts related to that event
Pricing Plans & Pools capture business rules regarding compensation for events
Fee charged to content.com
Revenue is paid back to log provider

Figure 8

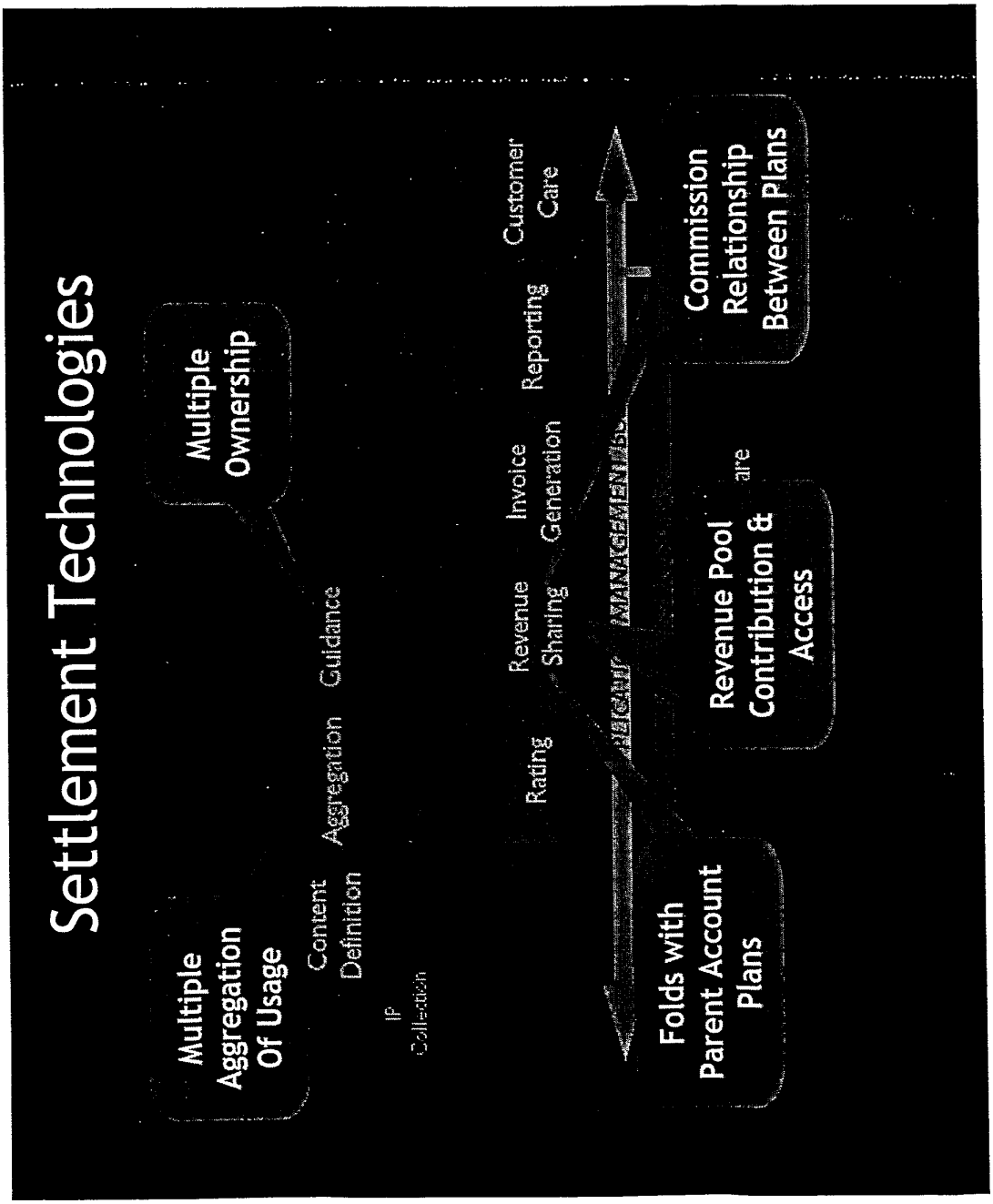

Settlement Technologies
Multiple Aggregation Of Usage
Multiple Ownership
Content Definition
Aggregation
Guidance
IP Collection
Rating
Revenue Sharing
Invoice Generation
Reporting
Customer Care
Folds with Parent Account Plans
Revenue Pool Contribution & Access
Commission Relationship Between Plans

Figure 9

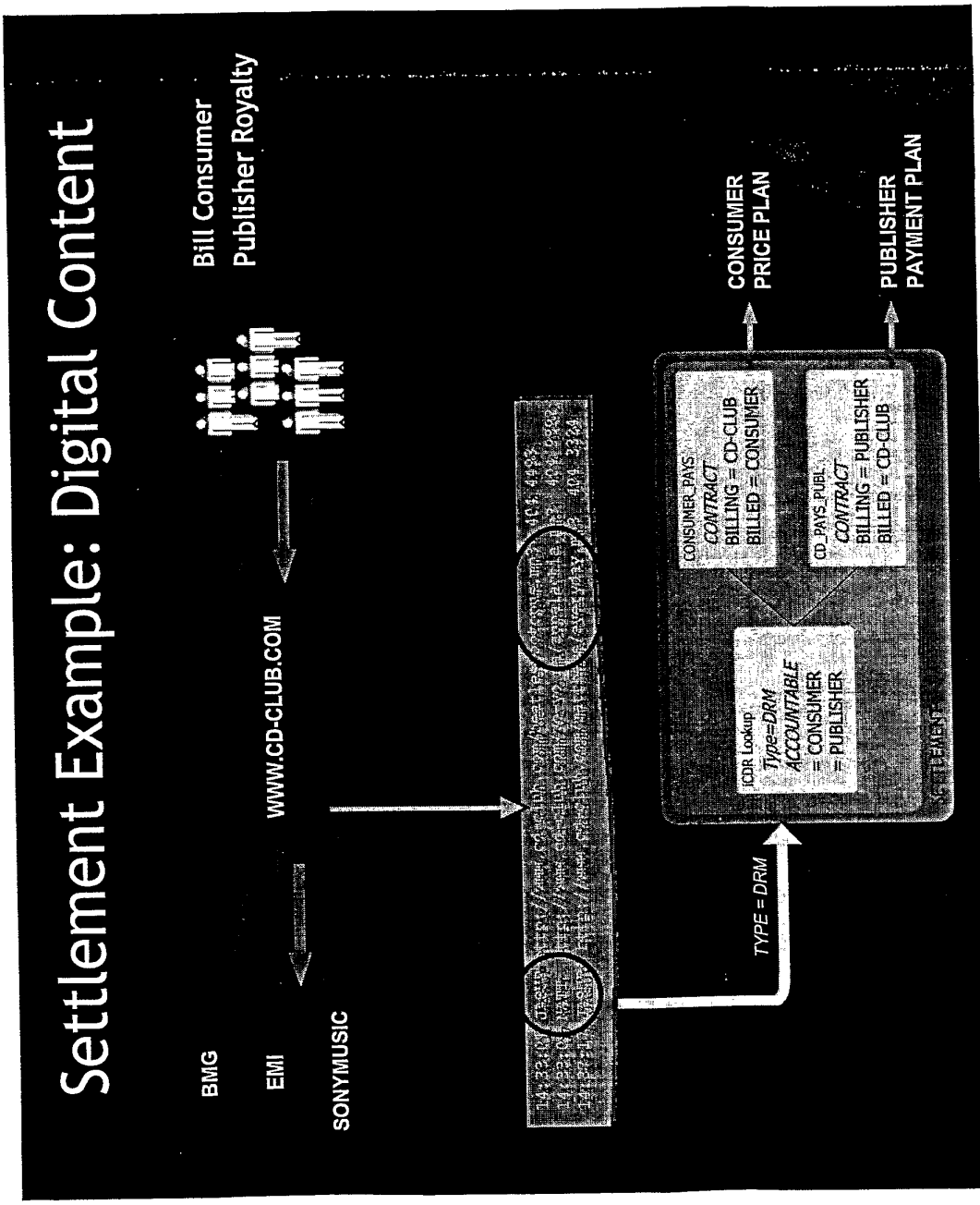

Settlement Example: Digital Content
BMG
EMI
SONYMUSIC
WWW.CD-CLUB.COM
Bill Consumer
Publisher Royalty
CONSUMER
PRICE PLAN
PUBLISHER
PAYMENT PLAN
CONSUMER_PAYS
CONTRACT
BILLING = CD-CLUB
BILLED = CONSUMER
CD_PAYS_PUBL
CONTRACT
BILLING = PUBLISHER
BILLED = CD-CLUB
CDR Lookup
Type=DRM
ACCOUNTABLE
= CONSUMER
= PUBLISHER
TYPE = DRM

Figure 10

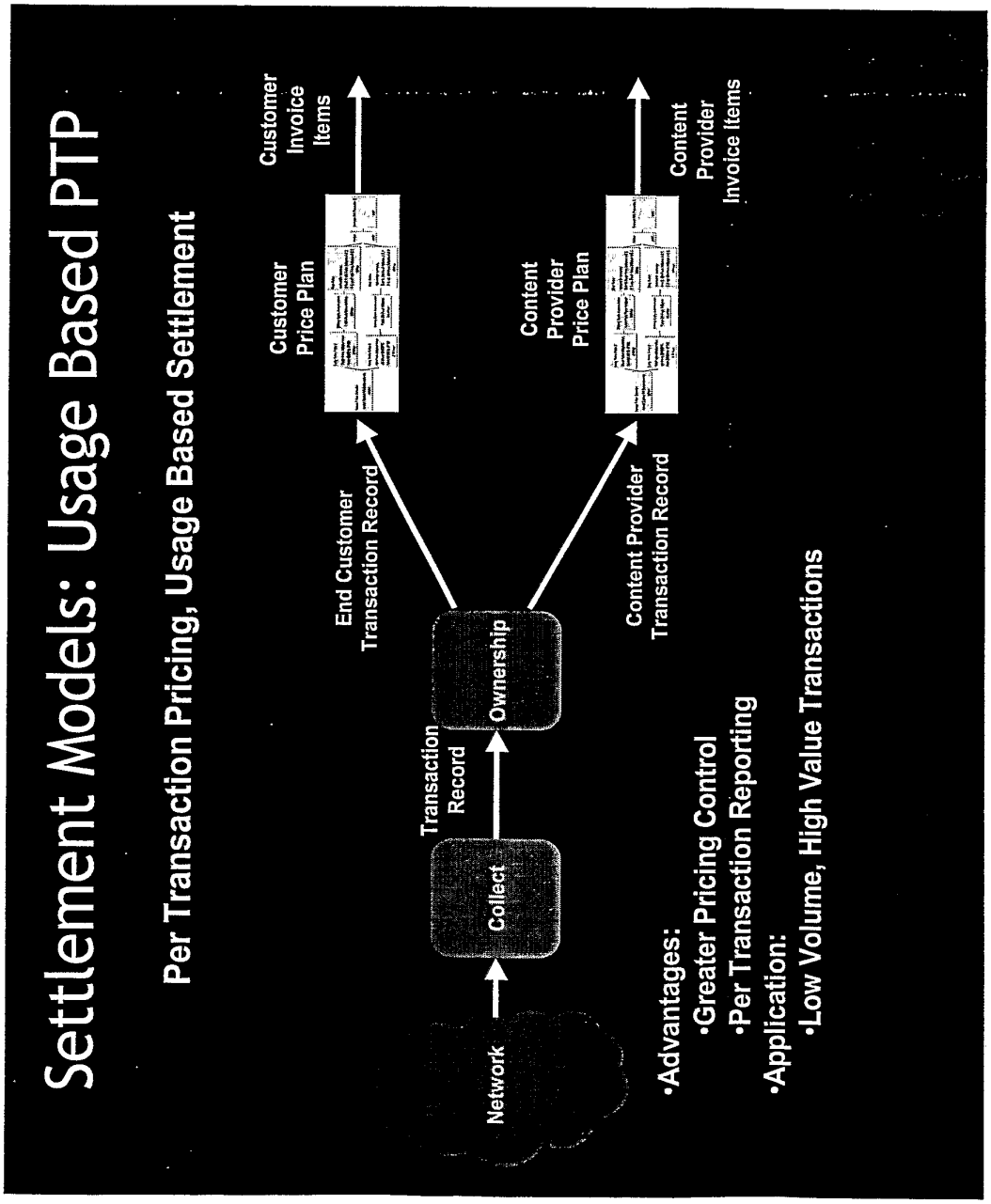

Settlement Models: Usage Based PTP
Per Transaction Pricing, Usage Based Settlement
Customer Invoice Items
Customer Price Plan
Content Provider Price Plan
Content Provider Invoice Items
End Customer Transaction Record
Content Provider Transaction Record
Transaction Record
Ownership
Collect
Network
•Advantages:
•Greater Pricing Control
•Per Transaction Reporting
•Application:
•Low Volume, High Value Transactions

Figure 11

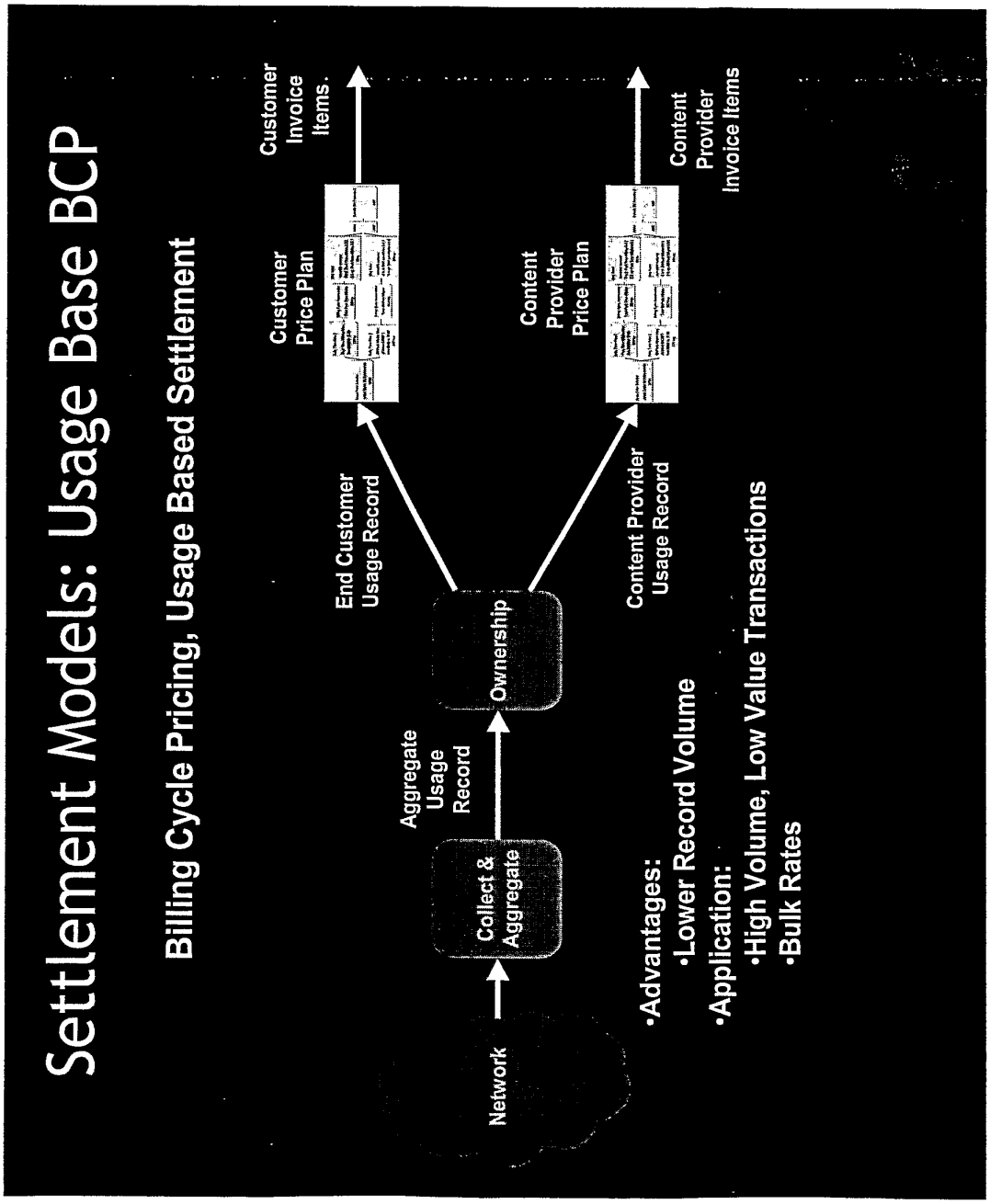

Settlement Models: Usage Base BCP
Billing Cycle Pricing, Usage Based Settlement
Customer Invoice Items.
Customer Price Plan
End Customer Usage Record
Content Provider Price Plan
Content Provider Usage Record
Content Provider Invoice Items
Aggregate Usage Record
Ownership
Collect & Aggregate
Network
•Advantages:
•Lower Record Volume
•Application:
•High Volume, Low Value Transactions
•Bulk Rates

Figure 12

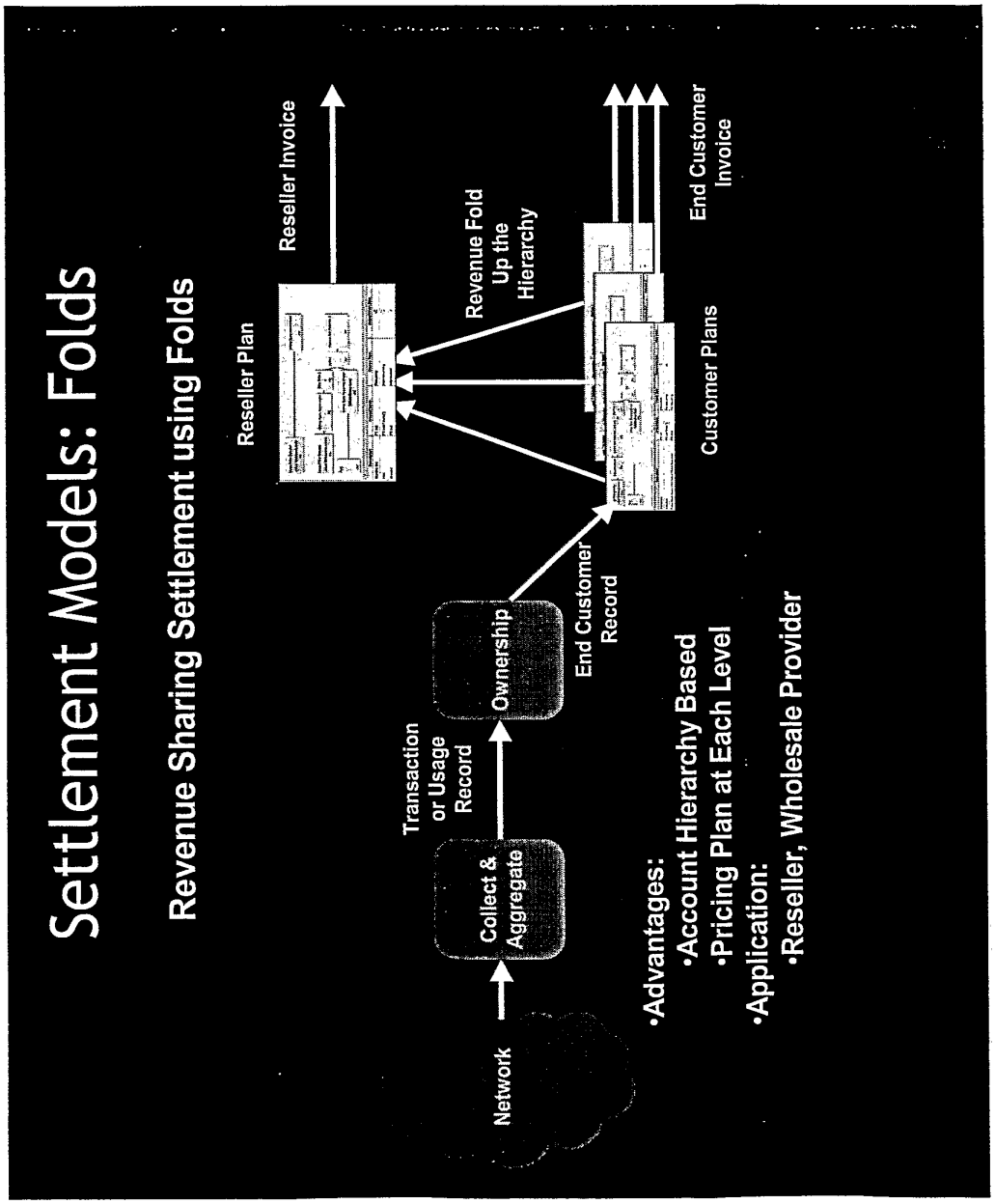

Settlement Models: Folds
Revenue Sharing Settlement using Folds
Reseller Plan
Reseller Invoice
Revenue Fold Up the Hierarchy
End Customer Invoice
Customer Plans
Transaction or Usage Record
Collect & Aggregate
Ownership
End Customer Record
Network
•Advantages:
•Account Hierarchy Based
•Pricing Plan at Each Level
•Application:
•Reseller, Wholesale Provider

Figure 13

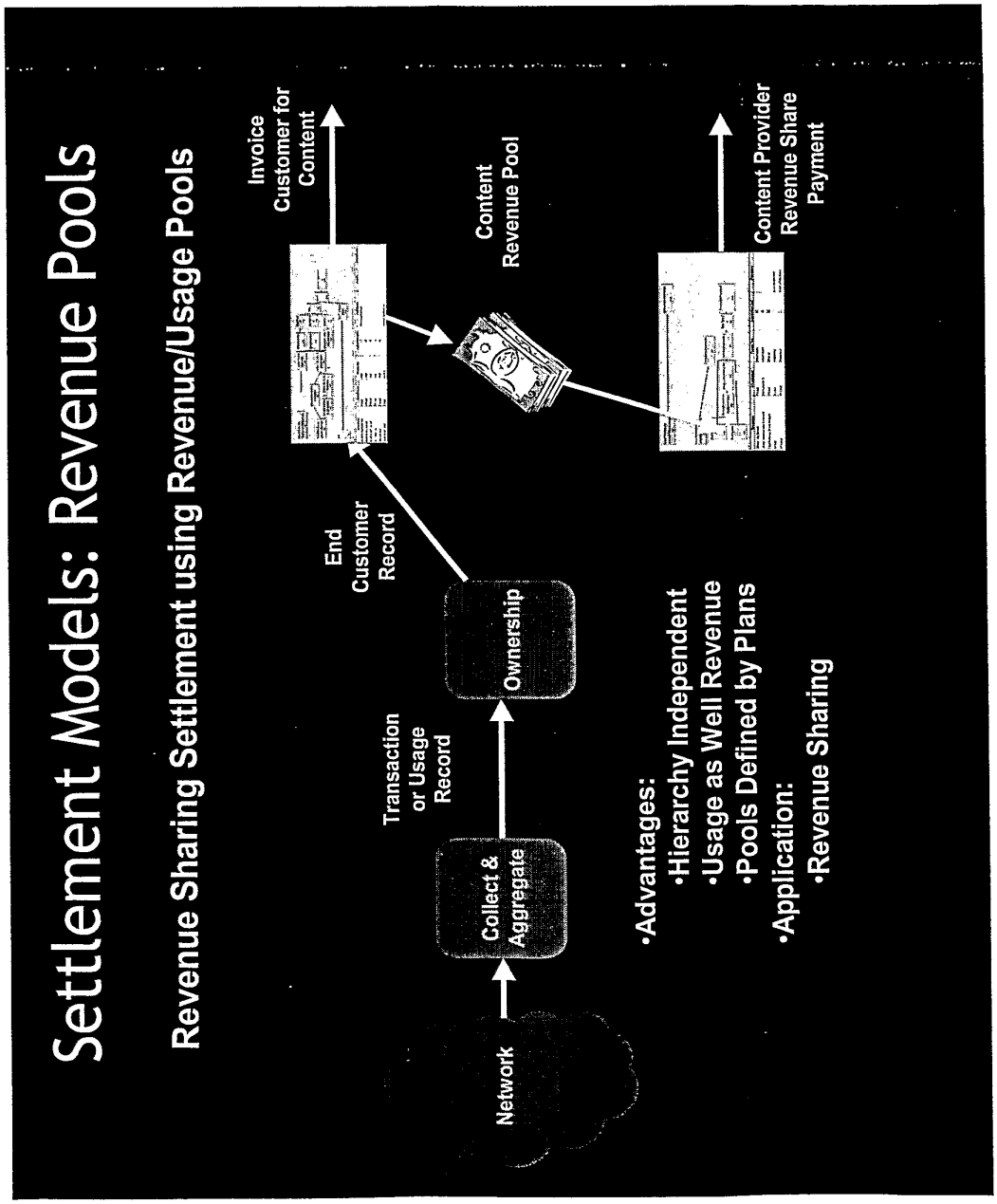

Settlement Models: Revenue Pools
Revenue Sharing Settlement using Revenue/Usage Pools
Network
Collect & Aggregate
Transaction or Usage Record
Ownership
End Customer Record
Invoice Customer for Content
Content Revenue Pool
Content Provider Revenue Share Payment
•Advantages:
•Hierarchy Independent
•Usage as Well Revenue
•Pools Defined by Plans
•Application:
•Revenue Sharing

Figure 14

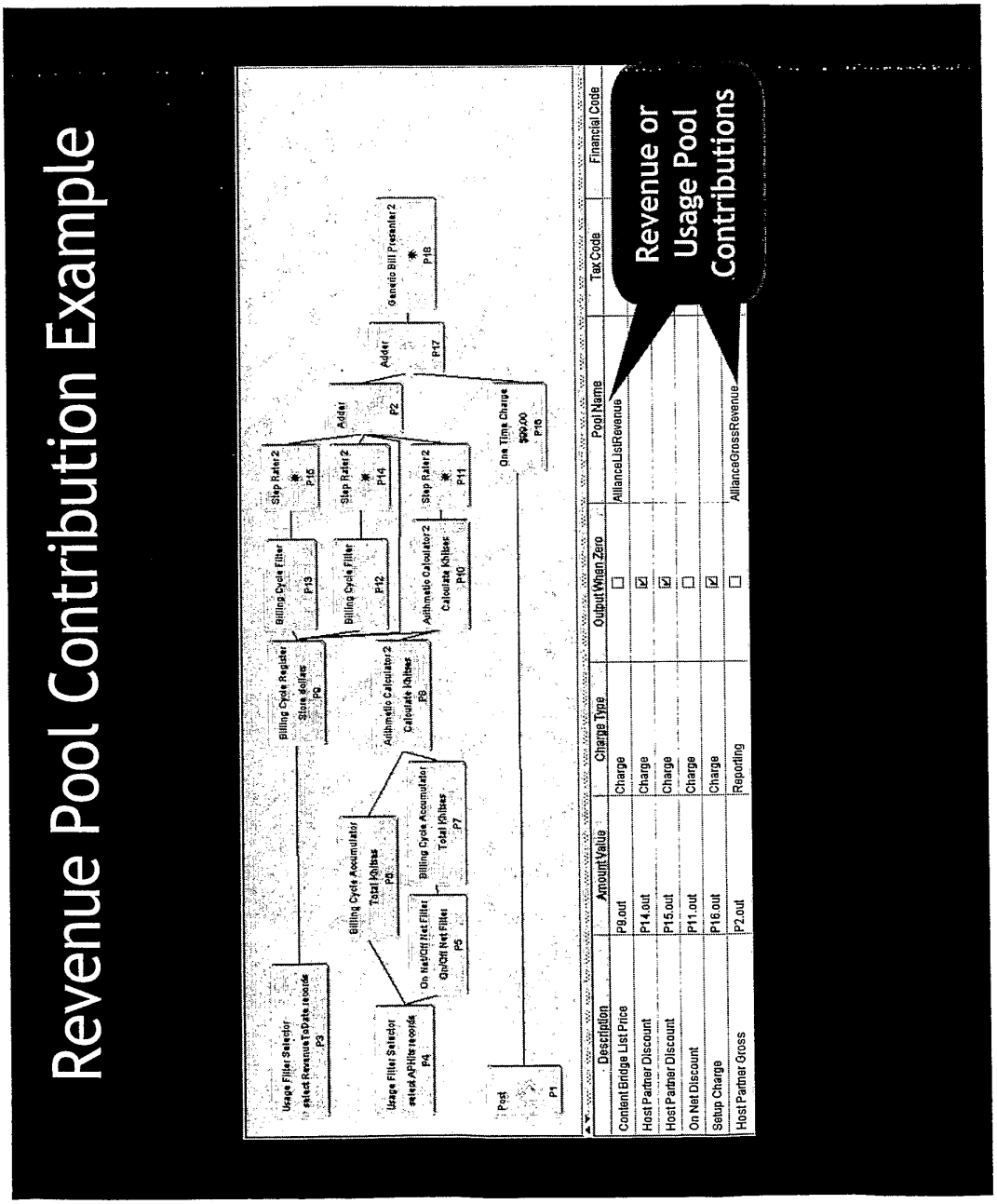

Revenue Pool Contribution Example
Revenue or Usage Pool Contributions
Post
P1
Usage Filter Selector select RevenueToDate records P3
Usage Filter Selector select APIIIs records P4
On Net/Off Net Filter On/Off Net Filter P5
Billing Cycle Accumulator Total KWhrs P6
Billing Cycle Accumulator Total KWhrs P7
Arithmetic Calculator2 Calculate KWhrs P8
Billing Cycle Register Store dollars P9
Arithmetic Calculator2 Calculate KWhrs P10
Step Rater2 P11
Billing Cycle Filter P12
Billing Cycle Filter P13
Step Rater2 P14
Step Rater2 P15
One Time Charge $99.00 P16
Adder P2
Adder P17
Generic Bill Presenter2 P18
Description
Amount Value
Charge Type
Output When Zero
Pool Name
Tax Code
Financial Code
Content Bridge List Price
P8.out
Charge
AllianceListRevenue
Host Partner Discount
P14.out
Charge
Host Partner Discount
P15.out
Charge
On Net Discount
P11.out
Charge
Setup Charge
P16.out
Charge
Host Partner Gross
P2.out
Reporting
AllianceGrossRevenue

Figure 15

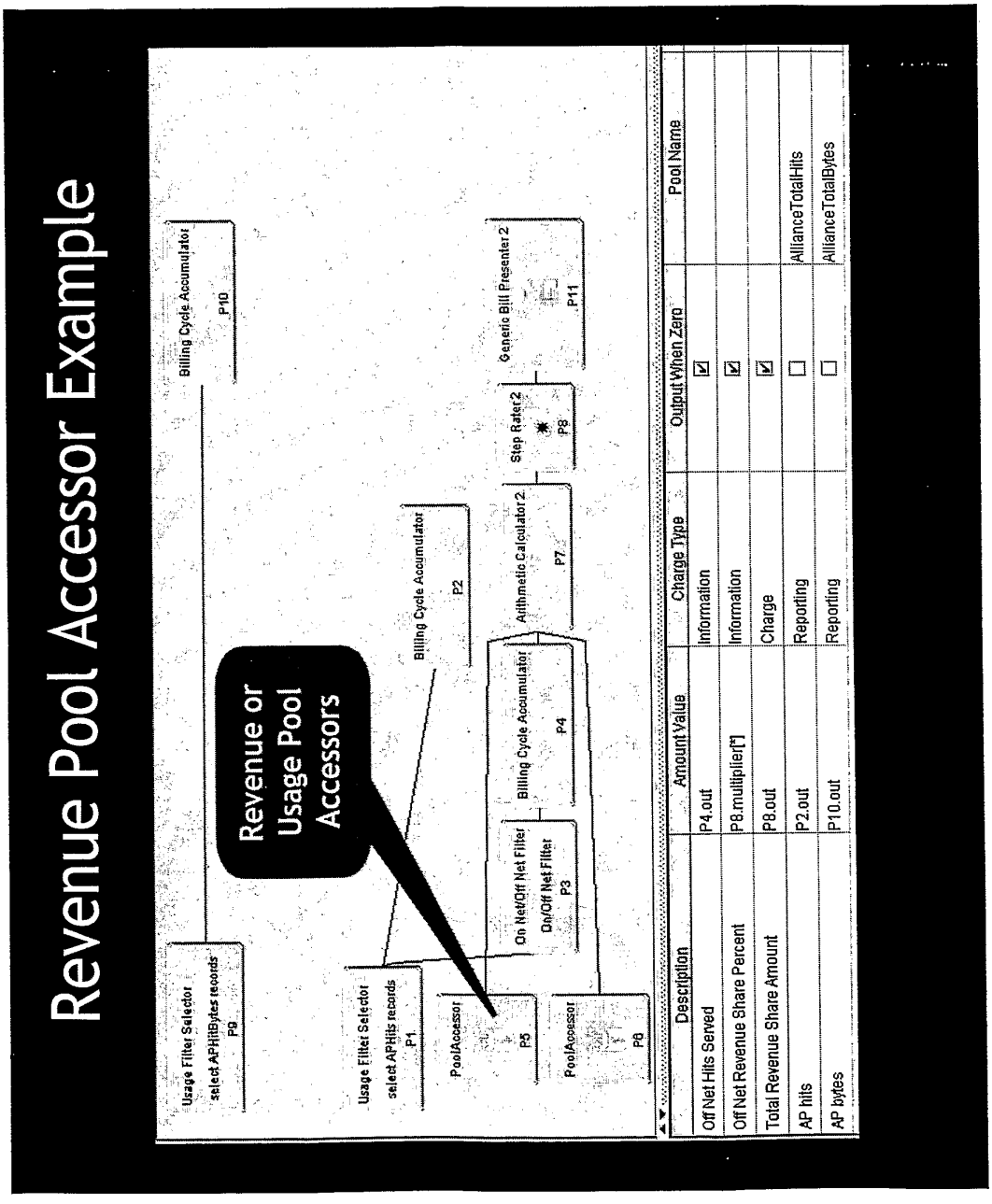

Revenue Pool Accessor Example
Usage Filter Selector
select APHitBytes records
P9
Billing Cycle Accumulator
P10
Revenue or Usage Pool Accessors
Usage Filter Selector
select APHits records
P1
Billing Cycle Accumulator
P2
PoolAccessor
P5
On Net/Off Net Filter
On/Off Net Filter
P3
Billing Cycle Accumulator
P4
Arithmetic Calculator 2
P7
Step Rater2
P8
Generic Bill Presenter 2
P11
PoolAccessor
P6
Description
Amount Value
Charge Type
Output When Zero
Pool Name
Off Net Hits Served
P4.out
Information
Off Net Revenue Share Percent
P8.multiplier[*]
Information
Total Revenue Share Amount
P8.out
Charge
AP hits
P2.out
Reporting
AlianceTotalHits
AP bytes
P10.out
Reporting
AlianceTotalBytes

Figure 16

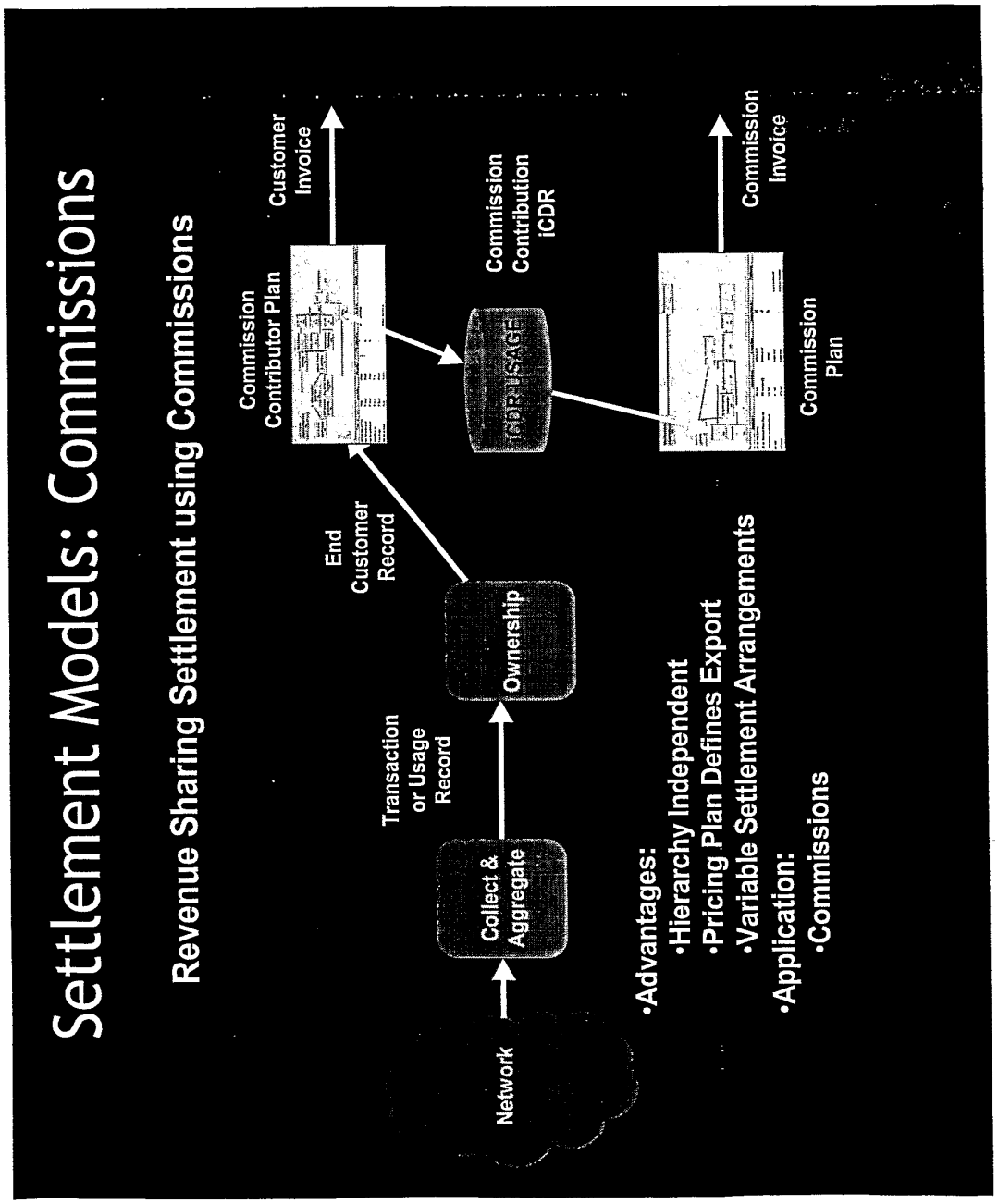

Settlement Models: Commissions
Revenue Sharing Settlement using Commissions
Network
Collect & Aggregate
Transaction or Usage Record
Ownership
End Customer Record
Commission Contributor Plan
Customer Invoice
Commission Contribution iCDR
Commission Plan
Commission Invoice
•Advantages:
•Hierarchy Independent
•Pricing Plan Defines Export
•Variable Settlement Arrangements
•Application:
•Commissions

Figure 17

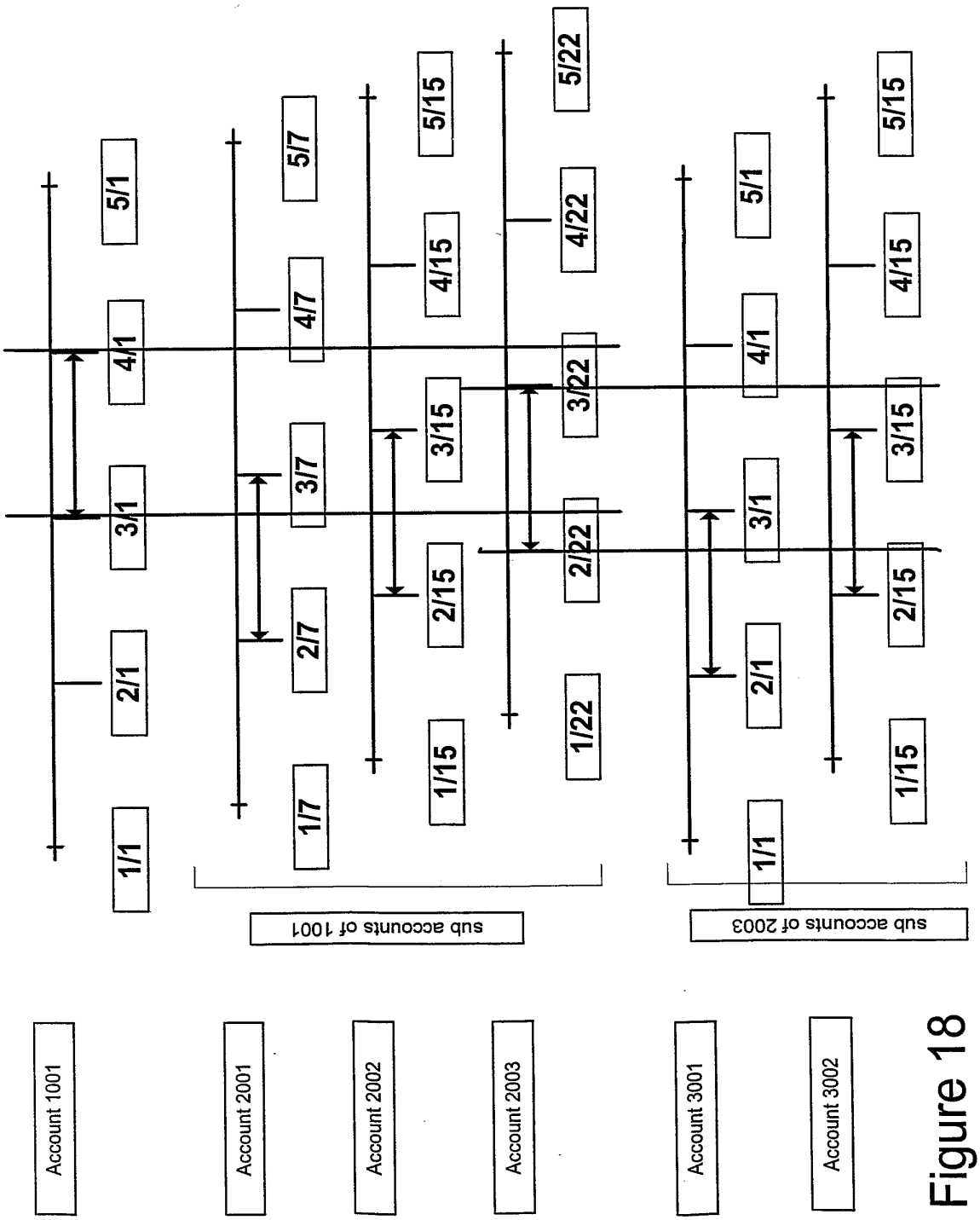

Account 1001
Account 2001
Account 2002
Account 2003
Account 3001
Account 3002
sub accounts of 1001
sub accounts of 2003
1/1
2/1
3/1
4/1
5/1
1/7
2/7
3/7
4/7
5/7
1/15
2/15
3/15
4/15
5/15
1/22
2/22
3/22
4/22
5/22

Figure 18

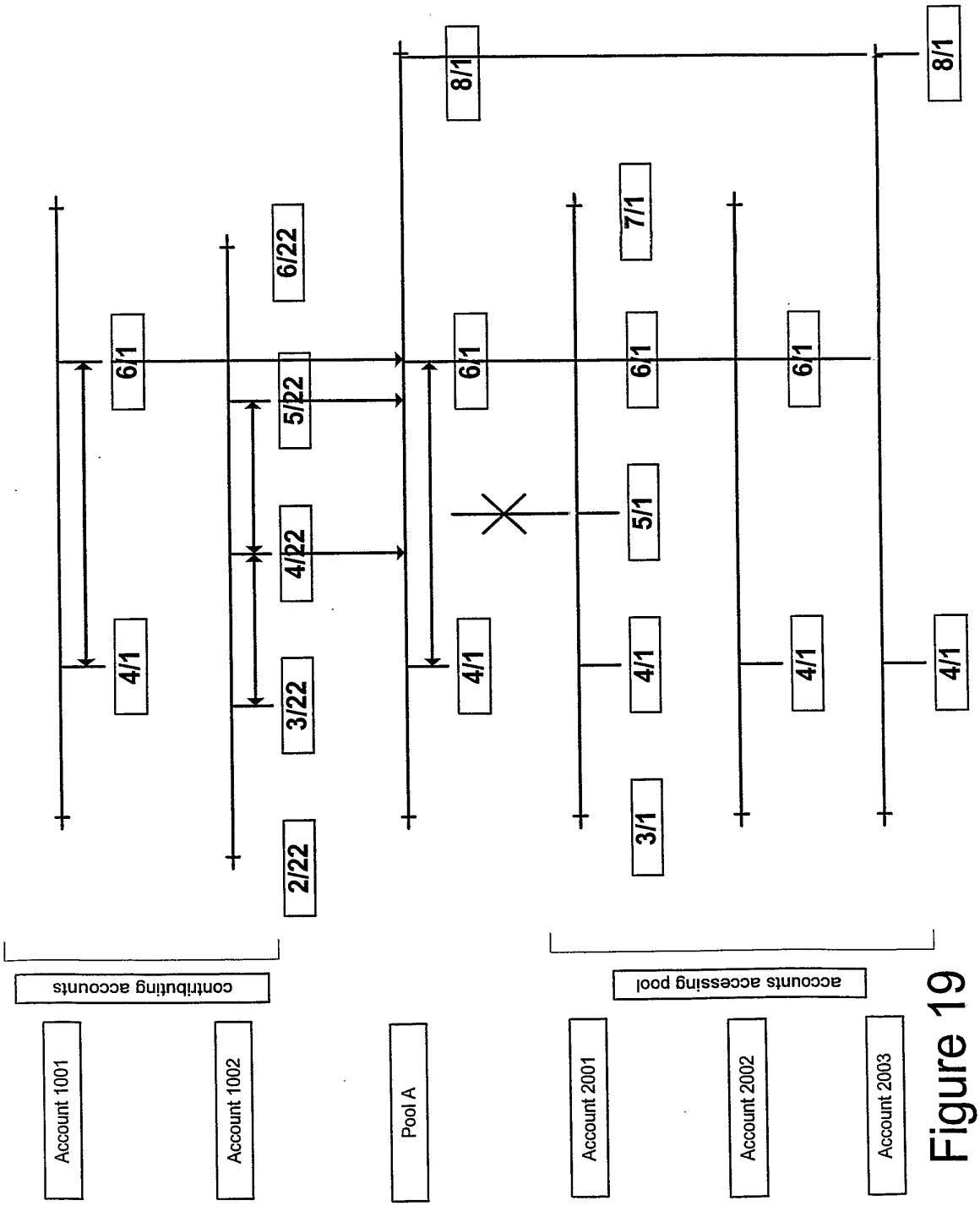

Account 1001
Account 1002
Pool A
Account 2001
Account 2002
Account 2003
contributing accounts
accounts accessing pool
8/1
8/1
6/22
7/1
6/1
6/1
6/1
6/1
5/22
5/1
4/22
4/1
4/1
4/1
4/1
4/1
3/22
3/1
2/22

Figure 19

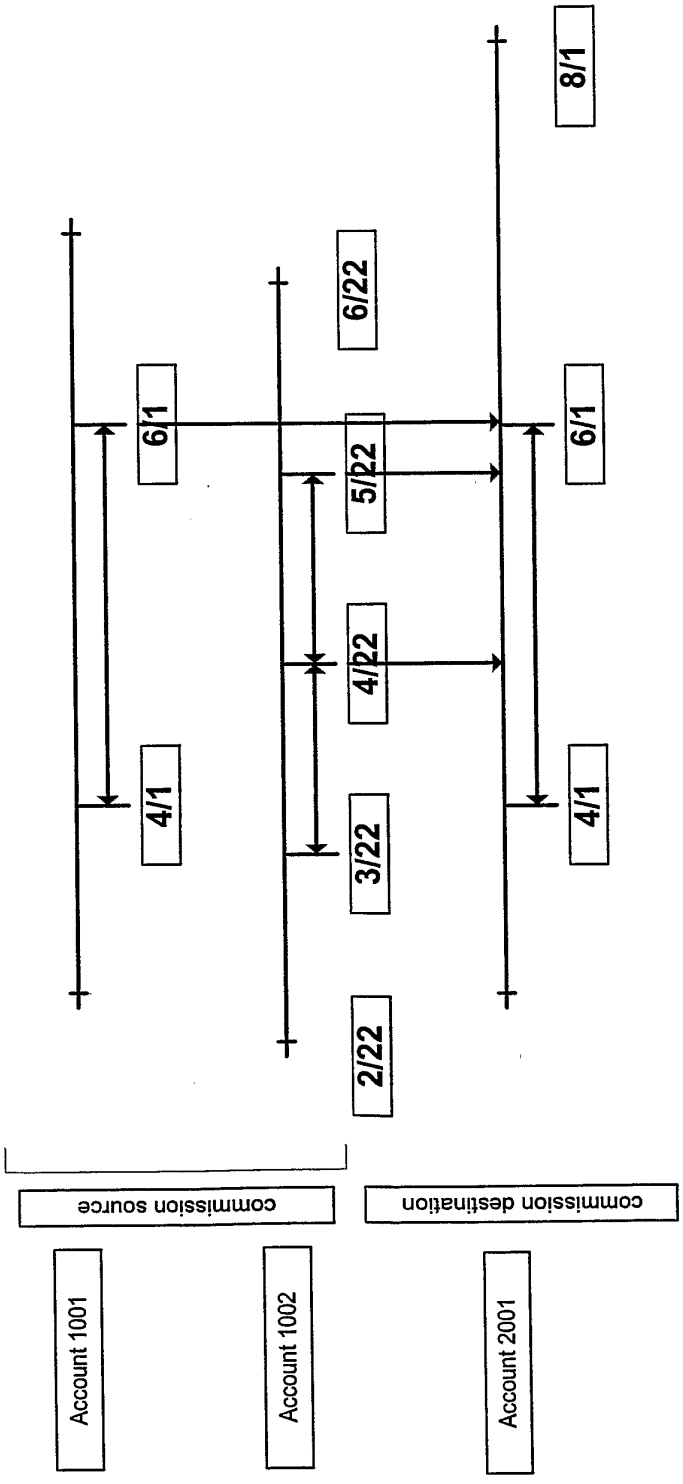

8/1
6/22
6/1
6/1
5/22
4/22
4/1
4/1
3/22
2/22
commission source
commission destination
Account 1001
Account 1002
Account 2001

Figure 20

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 August 2002 (29.08.2002)

PCT

(10) International Publication Number
WO 02/067616 A1

(51) International Patent Classification[7]: H04Q 7/38, H04M 15/00

(21) International Application Number: PCT/FI02/00128

(22) International Filing Date: 15 February 2002 (15.02.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
20010302 16 February 2001 (16.02.2001) FI

(71) Applicant *(for all designated States except US)*: **SONERA OYJ** [FI/FI]; Teollisuuskatu 15, FIN-00510 Helsinki (FI).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **YLI-KORHONEN, Jukka** [FI/FI]; Tarkka-ampujankatu 17 D 56, FIN-90120 Oulu (FI). **JUNTUNEN, Ari** [FI/FI]; Sihtikuja 1 D 51, FIN-90520 Oulu (FI). **KEINÄNEN, Kimmo** [FI/FI]; Talvikkitie 18 A 3, FIN-90580 Oulu (FI).

(74) Agent: **KOLSTER OY AB**; Iso Roobertinkatu 23, P.O.Box 148, FIN-00121 Helsinki (FI).

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

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, 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).

Declarations under Rule 4.17:
— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW, ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, 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)*
— *of inventorship (Rule 4.17(iv)) for US only*

Published:
— *with international search report*

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

(54) Title: SYSTEM, METHOD AND NETWORK NODE FOR PROVIDING SERVICE-SPECIFIC BILLING IN A TELECOMMUNICATIONS SYSTEM

P	ID	N	S1	V	S2	SV	BV
Elvis	PT	price_today	:	number	&	0	500
Elvis	EC	extra_cutback	=	number	&	0	250
Iiris	SP	single_payment	-	number	*	250	250

(57) Abstract: In a multi-provider environment, where a network operator provides bearer services and a service provider provides the actual service, customizing billing for services requires accurate contracts concerning the content and structure of billing data transmitted by the service provider. In order to eliminate this problem, a billing content is determined for a service in such a manner that the content is available to the network operator and it determines parameters (N) provided in service billing data and indicates how to find the parameters from the billing data (ID, S1, S2). For determining billing data, definition rules are defined in advance to indicate at least the type of data that should be specified for each parameter.

WO 02/067616 A1

System, method and network node for providing service-specific billing in a telecommunications system

FIELD OF THE INVENTION

The invention relates to billing for a service transmitted in a telecommunications system, and particularly to providing service-specific billing.

BACKGROUND OF THE INVENTION

Services provided in telecommunications systems are more and more often produced in a multi-provider environment, where a network operator provides bearer services and one or more service providers provide the actual services. A service provider does not maintain a network but purchases the required bearer services from the network operator. Thus, the total price of a service is a combination of the price of the connection and the price of the actual service or content. Even in a multi-provider environment the best way to charge a client is that the network operator attends to authentication and billing of the user of the service according to the user's phone number also on behalf of the service provider. An actual bill is based on billing data transmitted by the service provider in a service response, and collected and processed by a billing data collecting system of the network operator.

A problem with such billing is that the operator and the service provider must have accurate contracts concerning the content and structure of the billing data in order that a service could be billed for in the way the service provider wants. In case of a large number of service providers, the network operator does not necessarily have time or is not able to agree in detail on the contents of the billing data with each service provider, which means that either the introduction of a service into the market will be delayed, or the service provider must arrange billing in some other manner or use an existing billing method, which may not be the best for the service in question.

BRIEF DESCRIPTION OF THE INVENTION

An objective of the invention is to develop a method and equipment implementing the method so as to solve the aforementioned problems. The objective of the invention is achieved by a method, system and network nodes, which are characterized by what is disclosed in the independent claims. The preferred embodiments of the invention are disclosed in the dependent claims.

The invention is based on detecting this problem and on solving it by providing a system of a network operator, preferably a system for process-

ing billing data, with a mechanism for informing the network operator of the form in which the billing data should be disclosed. The mechanism is preferably created by determining rules for defining billing parameters and by determining, by means of these rules, a billing content of a service, which is available to the network operator when forming a call detail record, and by storing the billing content in the system so as to be available to a process producing tickets. A billing content determines the service-specific parameters used in a call detail record, i.e. a ticket, and indicates how to locate the parameters in the billing data. The processing system can constitute a part of the system for collecting billing data.

An advantage of the invention is the ability to transmit and process billing data, which has different contents for different services since the billing parameters can be freely selected. Another advantage of the invention is that no specific service contract is needed between the network operator and the service provider, since the invention enables determining the structure of the billing data in such a manner that the network operator's system identifies the billing parameters and their values. Therefore the operator can provide user authentication and billing services globally to service providers. This even enables billing for free browsing, where a user is able to use all the services and not only the services of the operator or partners thereof.

BRIEF DESCRIPTION OF THE FIGURES

The invention will be described below in more detail by means of the preferred embodiments and with reference to the accompanying drawings, in which

Figure 1 shows a simplified network architecture,

Figure 2 shows an example of determining a billing content according to a first preferred embodiment of the invention,

Figure 3 shows formation of a ticket according to the first preferred embodiment of the invention, and

Figure 4 shows an example of a ticket according to the first preferred embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

The present invention can be applied in connection with any telecommunications system where the data required for billing a subscriber is transmitted together with service data. Such systems include for example third-

generation mobile systems, such as the Universal Mobile Telecommunications System (UMTS), and mobile systems similar to the pan-European GSM (Global System for Mobile Communications), such as the GSM 1800 and the PCS (Personal Communication System), and systems based on the aforementioned systems, such as GSM 2+ systems. GSM 2+ services include the general packet radio service (GPRS) and customized applications for mobile network enhanced logic (CAMEL). The invention can also be applied in fixed systems. The invention will be described below by using as an example the GSM providing a WAP (Wireless Application Protocol) service, without restricting the invention thereto, however. The WAP is a protocol specification that enables apparatuses utilizing wireless data transmission, such as mobile phones, to use Internet services.

Figure 1 shows a simplified network architecture of a first preferred embodiment of the invention, and it illustrates only some elements of a system architecture J. Network nodes shown in Figure 1 are logical units, the implementation of which can differ from that of the figure. It is obvious to a person skilled in the art that the system can also comprise other functions and structures, which do not have to be described in more detail herein. The description of the system is by no means restrictive but only suggestive.

The system shown in Figure 1 consists of a system of a network operator VJ and a system of a service provider PJ. In the example of Figure 1, a mobile station MS user has set up a connection to a server S providing a WAP service via the network operator's network PLMN via a WAP gateway W_GW in a previously known manner. In the first preferred embodiment of the invention, the WAP gateway W_GW picks the billing data from a service response transmitted by the server and stores it in a log file, which is retrieved by a charging gateway CG connected to the network operator's network PLMN and which is processed into call detail records, i.e. tickets. An example of a ticket is shown in Figure 4. The tickets are then transmitted to a billing centre BC, which attends to billing of a user. The picking of billing data refers to picking of data used to form a ticket, such as a part of the service response containing the data required in billing. In a service response, billing data can be located for example in an HTTP (Hyper Text Transport Protocol) header. In another embodiment of the invention, the WAP gateway W_GW does not store the billing-related data that was picked into a log file but transmits the data to the charging gateway CG for example via a real-time interface. The details of

the billing, e.g. how billing data is transmitted, collected and retrieved and where it is stored, are not significant for the invention. For example, arranging billing for the WAP service is described in more detail in Finnish Patent Application 20000589 (Arranging billing in a telecommunications system), which is incorporated herein by reference.

The charging gateway CG comprises an interface I, via which service-specific billing contents LS can be determined in the charging gateway. Examples of such billing contents are shown in Figure 2. The interface I thus provides configuring means for determining the content and structure of the billing data and the ticket and for storing them by means of the definition rules for billing parameters. Billing contents are preferably stored in a memory M of the charging gateway. The network operator has usually determined the definition rules and the service provider determines the actual billing content of the service, i.e. it determines the required parameters and provides parameter specifications. The actual billing content is input/processed into the memory M of the charging gateway via the interface I by the operator or the service provider, depending on their mutual agreement. The interface I can also be arranged to check, in connection with the input or processing of the billing content, that the parameter specifications comply with the definition rules. The definition rules are preferably the same for all the service providers, but the network operator can also customize the rules separately for each service provider. Inputting billing contents does not preferably require a service contract between the service provider and the network operator, but the service provider may be able to input billing contents for example via the Internet after having accepted certain rules and passed a log-in process. The charging gateway CG also comprises processing means, i.e. a process P, which converts the billing data into a ticket by means of the billing content specified for the service. The operation of the process P will be described in more detail in connection with Figure 3.

Depending on the embodiment, the interface I can be located in a different network node than the stored billing contents LS. Neither has to be located in the charging gateway. A network node where the billing contents LS are stored comprises means for receiving requests on billing contents and means for processing and transmitting responses.

In addition to prior art means, a system implementing the functionality of the present invention and the network nodes of the system comprise

means for creating and storing service-specific billing contents. The system and the network nodes can also comprise means for processing a billing content. The means are preferably implemented by using the present network nodes, especially the processors and memory thereof. All the modifications required to implement the invention can be carried out in the form of added or updated software routines, application-specific integrated circuits (ASIC) and/or programmable circuits.

Figure 2 shows a manner according to the first preferred embodiment of the invention of determining service-specific billing contents stored in a database table where each service-specific parameter to be taken into account in billing is provided with required data, i.e. the parameters are determined according to the definition rules. It is assumed in the first preferred embodiment of the invention that a billing ticket consists of standard data and service-specific data. Parameters for the standard data are determined generally in the first preferred embodiment, i.e. they are shared by all services. Such standard data includes for example user identifier, service name, service status data, and time. Standard data or some part of it can be transmitted with service-specific billing data, but for example in case of WAP services they are usually obtained in some other manner. Service-specific data is determined in the billing content of a service. The parameters that should be or may be specified in the billing content naturally depend on the operator, the billing system used by the operator, and the form in which billing data is transmitted. These matters are described in the definition rules. The essential fact in the billing content of an individual service is that it can be connected to a specific service and that at least one billing parameter is determined in such a manner that the billing parameter and the value thereof can be somehow separated from the billing data. However, in the first preferred embodiment of the invention it is not necessary to determine a billing content for all the services if standard data is sufficient to bill for a service.

In the example shown in Figure 2, it is assumed for the sake of clarity that the service name identifies the service sufficiently, i.e. the service cannot be confused with any other service, and different service providers do not have services with similar names. In embodiments where a mere service name does not identify a service sufficiently accurately, a service to be billed for can be identified for example based on the names of both the service provider and the service.

In the first preferred embodiment of the invention, the definition rules do not restrict in any way the ability of service providers to determine the parameters to be taken into account in billing, and the only requirement is that each parameter of a service billing content is provided with not only a name N but also the following data:

- The service P to which the parameter is related. A parameter defined by means of a service can be connected to the service billing content,
- A parameter identifier ID used in billing data to help locate the parameter and the value thereof,
- A separator S1 between an identifier and the value thereof in the billing data,
- Value type V,
- The allowed range of variation of the value indicated by means of the lowest value SV and the highest value GV, and
- A separator S2 between the identifiers.

On the basis of this data, a single ticket may contain 1 to n items of service-specific billing data, which are mutually independent. The billing data can even consist of data not used by the network operator in its own billing. For example based on the specifications shown in Figure 2, a ticket formed of a service called 'Elvis' contains the billing value of two parameters in the service-specific data, and a ticket formed of a service called 'Iiris' contains the billing value of one parameter. The same parameter can also be used in different services and with different ranges of variation. Eliminating parameters from or adding new parameters into a service is easy and simple in the first preferred embodiment of the invention. It is also easy and simple to alter parameter specifications, for example to update the allowed range of variation.

In a preferred embodiment of the invention, the operator can restrict parameter specifications for example by limiting the maximum number of parameters used in one service or by restricting the allowed value types to numbers only. The operator can also determine its own set of billing parameters, which it offers to service providers. The service providers then select from the set of billing parameters the parameters they want to use in billing for each service.

In a preferred embodiment of the invention, parameters and their values to be used in standard data are also specified in the billing content of

each service. In this way standard data can also be configured specifically for each service/service provider.

In another preferred embodiment of the invention, a common billing content is also determined and used for services with no specified billing content of their own. A common billing content can also be determined specifically for each service provider and/or service type. If a service-type-specific billing content is used, the service type is indicated in a service response either directly or indirectly in order that the correct billing content can be selected when forming a ticket. The same applies to service-provider-specific billing contents as well. The service type can be concluded for example based on the service when the system maintains data that links each service to a service type.

In a preferred embodiment of the invention, also a broader description of a parameter, such as the manner of use or the meaning in billing, can be stored in the billing content.

In another preferred embodiment of the invention, several different identifiers with different value ranges can be stored for one parameter in a billing content. In this embodiment, only one such identifier is shown in the billing data.

If the highest allowed value of the identifiers is equal to the lowest allowed value, in a preferred embodiment of the invention the billing data does not have to contain a value for the parameter, but it is possible to use the value determined in the billing content when forming a ticket.

In the other embodiments of the invention, the predetermined definition rules can differ from what is shown in Figure 2. It is sufficient that the definition rules ensure that the parameters in the billing content are known and that they will be found from the billing data.

Figure 3 shows a flowchart of how a ticket (or a part thereof, if one ticket combines the billing data of several service responses) is formed according to the first preferred embodiment of the invention from the billing data in the service response. It is assumed in the example of Figure 3 that the service provider has transmitted billing data or that the billing data field is not empty. An empty billing data field is preferably not processed at all. The example of Figure 3 does not determine at which stage the tickets should be transmitted to the billing centre. In the first preferred embodiment of the invention, service-specific billing data is transmitted in HTTP headers of a service response. Transmitting billing data as a part of an HTTP header has an advantage that

the data is not transmitted from the gateway, such as the WAP gateway, to the subscriber of the service. Furthermore, an HTTP header is an efficient channel of data transmission between a service provider and an operator.

Since it is not significant for the invention how the billing data is found for example from a log file, the starting point of Figure 3 is that in step 301 the processing of billing data is initiated. For example in the first preferred embodiment of the invention, the WAP gateway picks the billing data from the HTTP header of the service response for the WAP service on the basis of a carriage return. An example of billing data will be described below. The payer is identified first in step 302. The payer can be for example the end user or the service provider, such as a service provider providing a commercial WAP/SMS push service. A payer is identified according to the system used. In the present WAP services, a user is identified based on a phone number received during the set-up of the connection. In the future third-generation mobile systems and in general Internet-based services, the end user can be identified for example from the service log-in data transmitted by the service provider. It is also possible to identify both the payer and the user. After the payer has been identified, the service to which the billing data is related is identified in step 303. The service can be identified either directly by means of an identifier indicating the service name in the HTTP header, or by means of an analysis of a URL (Uniform Resource Locator) address. After the service has been identified, the standard data is retrieved from the billing data and stored (or the part of the standard data not received via some other route/earlier) in a ticket in step 304, and the service billing content is retrieved in step 305. The service billing content is retrieved in the first preferred embodiment of the invention by checking the database table shown in Figure 2 and by picking all the parameters with their specifications that relate to the service to be billed for. In step 306, it is checked whether a billing content was obtained. In other words, it is checked whether a billing content has been specified for the service. If a billing content was obtained (i.e. has been specified), the processing of the first parameter is initiated in step 307 and a corresponding identifier is retrieved from the HTTP header in step 308. If such an identifier was found (step 309), the value given for the identifier is retrieved in step 310. It is thereafter checked in step 311 whether the value is allowed, i.e. whether it is within predetermined limits and of a specified type. If the value was allowed, the parameter name and value are stored in the ticket in step 312, and it is checked in step 313 whether the

parameter was the last parameter of the billing content. If the parameter was not the last one, the next parameter is subjected to processing in step 314, whereafter the process proceeds from step 308 by searching the HTTP header for the corresponding identifier.

If the parameter was the last one (step 313), the processing of the billing data is terminated in step 315.

If the parameter value was not allowed (step 311), a failure report is generated to the system in step 316, and the ticket field in question is left empty. After the failure report has been generated, the process proceeds to step 313 to check whether the processed parameter was the last one in the billing content.

If a parameter identifier was not located (step 309), the process proceeds to the last step 313 to check whether the processed parameter was the last parameter in the billing content. In other words, it is assumed in the first preferred embodiment of the invention that this time the service provider did not want to use this parameter for billing. Such a parameter can be for example an additional discount parameter.

If a billing content was not obtained (step 306), it has not been determined for the service, wherefore the processing of the billing data is terminated in step 315.

In a preferred embodiment of the invention, at least some of the parameter specifications of the standard data are contained in the service billing content. In this embodiment, the billing content must be retrieved (step 306) before step 304, i.e. the retrieval and storage of the standard data.

In a preferred embodiment of the invention, all the parameters, including the parameters of the standard data transmitted in the billing data, such as a service identifier, are determined at least specifically for each service provider. In this embodiment, the processing of the billing data is initiated by first identifying the service provider, whereafter the database table is checked in order to retrieve the service-provider-specific parameters, such as a service identifier and possibly at least some of the standard data. After the service has been identified, the parameters specified for the service are retrieved. This provides the billing content, and the parameter values thereof are retrieved in the manner described above.

The steps of Figure 3 are not in an absolute order of time. Some of the aforementioned steps can take place simultaneously or in another order,

such as steps 304 and 305. Some steps can be skipped, or steps not shown in Figure 3 can be implemented between the steps. Some steps can also be replaced with a corresponding step. For example in an embodiment where the log file only comprises notes containing billing data and where a service-type-specific billing content is used for each service, step 306 can be skipped and step 303 can be replaced with a step of identifying the service type.

Figure 4 shows an xml (eXtendable Mark up Language) ticket CDR according to the first preferred embodiment of the invention, where the WAP service 'Elvis' has been subscribed to from mobile phone number 040555555. The billing content of the service has been specified as shown in Figure 2 and the billing data is indicated as follows in the HTTP header of the service response:

X-up-billing-Info:SN=elvis&PT:67&EC=15

In the first preferred embodiment, the ticket comprises standard data 1 and a part 2 that changes according to the service. The service-specific part 2 is determined according to the billing content defined for the service. In the first preferred embodiment of the invention, the standard data 1 includes a calling party identifier 11, billing data 12 in the HTTP header, a service name 13, and a service price class 14, which is used to distribute different services of the same service provider to different price classes. The standard data is followed by the changing part 2 of the ticket, which is not found in tickets related to a service for which a billing content has not been specified. By means of the definitions shown in Figure 2, the process forming a ticket is able to retrieve from the billing data an identifier and a value corresponding to each parameter specified for the service 'Elvis'.

Even though the above description relates to the use of the billing content for altering a ticket, it can also be applied to other functions related to billing, such as selecting what to store in a log file.

It is obvious to a person skilled in the art that as the technology develops, the basic idea of the invention can be implemented in several manners. The embodiments of the invention described above or the individual characteristics thereof can be combined to provide new embodiments. Thus, the invention and the embodiments thereof are not restricted to the above examples, but they may vary within the scope of the claims.

CLAIMS

1. A method of providing service-specific billing in a telecommunications system, where a system of a network operator transmits services of at least one service provider to a subscriber, and forms call detail records to be used in billing and containing at least one billing parameter and the value thereof, **characterized** in that the method comprises at least the following steps of:

determining rules for defining billing parameters,

determining, by means of the definition rules, a billing content for at least one service, the content containing at least one service-specific billing parameter and indicating how the parameter is found from billing data transmitted during the use of the service, and

storing the billing content in the telecommunications system such that it is available to the system of the network operator.

2. A method according to claim 1, **characterized** in that the method also comprises a step of forming, from the billing data, a call detail record, which contains at least a service-specific part comprising service-specific billing parameters and their values defined in the billing content.

3. A method according to claim 1 or 2, **characterized** in that the method also comprises the steps of

determining at least one set of billing parameters, and

selecting the billing parameters to be used in the billing content from the set of billing parameters.

4. A method according to claim 1, 2 or 3, **characterized** by determining a billing content for one service.

5. A method according to claim 1, 2 or 3, **characterized** by determining a billing content for a service type, and indicating the service type in the billing data.

6. A telecommunications system (J) comprising

a system of a service provider (PJ) for transmitting at least one service to a subscriber and for providing billing data related to the service, and

a system of a network operator (VJ) for transmitting the service from the service provider's system to the subscriber of the service, and for providing a call detail record to be used in billing of the subscriber by means of the billing data, and

a memory (M) for storing different specifications,

characterized in that

the system of the network operator (VJ) comprises an interface (I) for storing a billing content (LS) in the memory (M) for the service, the billing content determining at least one service-specific billing parameter of the billing data according to the predetermined definition rules, such that the billing parameter is found from the billing data transmitted during the use of the service.

7. A system according to claim 6, **characterized** in that the system of the network operator (VJ) is arranged to utilize the specifications of the billing content in forming a call detail record from the billing data related to the service.

8. A system according to claim 6, **characterized** in that the system of the network operator (VJ) is arranged to form a call detail record (CDR) for the service from standard data (1) containing the same parameters for all the services, and from service-specific data (2) according to the billing content defined for the service.

9. A system according to claim 6, 7 or 8, **characterized** in that the interface (I) is also arranged to alter the specifications of the billing content.

10. A system according to claim 6, 7, 8 or 9, **characterized** in that the interface (I) is also arranged to check, in connection with said storage, whether the parameter specifications comply with the definition rules.

11. A system according to claim 6, 7, 8, 9 or 10, **characterized** in that the system (J) is based on a GPRS system.

12. A system according to claim 6, 7, 8, 9 or 10, **characterized** in that the system (J) is based on a UMTS.

13. A network node (CG) in a telecommunications system where a system of a network operator transmits services of at least one service provider to a subscriber and provides call detail records used in billing, and where the service provider transmits billing data in connection with a service,

characterized in that

the network node comprises configuring means (I) for specifying parameters contained in the service billing data according to predetermined definition rules, such that the system of the network operator can use the specifications in forming a call detail record related to the service.

14. A network node according to claim 13, **characterized** in

that the configuring means (I) are arranged to alter the parameter specifications.

15. A network node according to claim 13 or 14, **characterized** in that the network node also comprises processing means (P) for forming a call detail record from the billing data related to the service, such that at least a part of the call detail record is formed according to the parameter specifications for the service.

16. A network node (CG) in a telecommunications system, where a system of a network operator transmits services of at least one service provider to a subscriber, and where the service provider transmits billing data in connection with a service, the network node comprising processing means (P) for forming a call detail record from the billing data related to the service,

characterized in that

the processing means (P) are arranged to determine a billing content specified for the service according to predetermined definition rules in the system of the network operator, the billing content containing at least service-specific billing parameters and indicating how the parameters can be found from the billing data, the processing means being also arranged to form a call detail record in such a manner that at least a part of the call detail record complies with the billing content.

17. A network node (CG) according to any one of claims 13 to 16, **characterized** in that the means (I, P) are implemented by software routines.

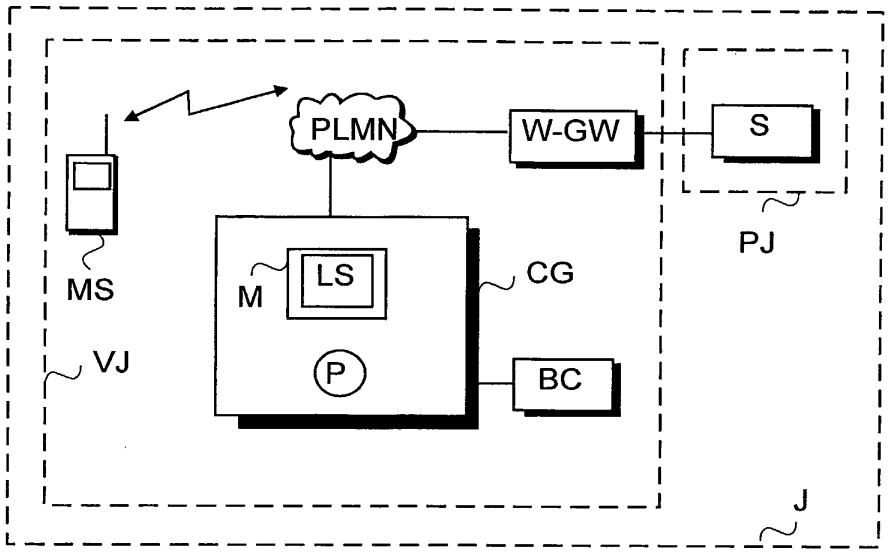


FIG.1

P	ID	N	S1	V	S2	SV	BV
Elvis	PT	price_today	:	number	&	0	500
Elvis	EC	extra_cutback	=	number	&	0	250
Iiris	SP	single_payment	-	number	*	250	250

FIG.2

CDR

<user_msisdn>040555555</user_msisdn>

11 <header>SN=elvis&RC=99&PT:67&EC=15</header>

12 <service_name>ELVIS</service_name>

13 <rate_category>99</rate_category>

1

<psd>
<price_today>67</price_today>
<extra_cutback>15</extra_cutback>
</psd>

2

FIG.4

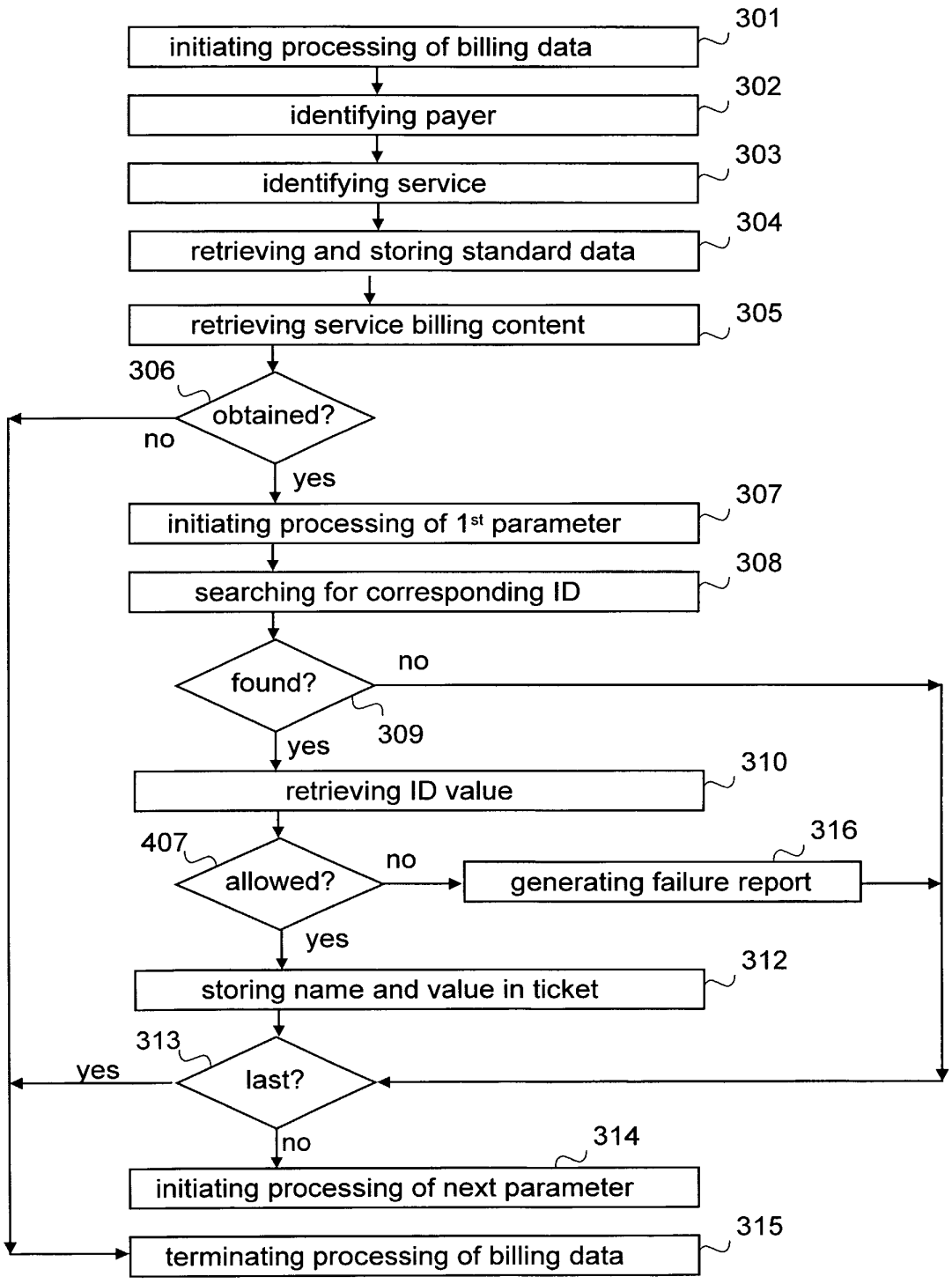

initiating processing of billing data
301
identifying payer
302
identifying service
303
retrieving and storing standard data
304
retrieving service billing content
305
306
obtained?
no
yes
initiating processing of 1st parameter
307
searching for corresponding ID
308
found?
no
309
yes
retrieving ID value
310
407
allowed?
no
316
generating failure report
yes
storing name and value in ticket
312
313
yes
last?
no
314
initiating processing of next parameter
315
terminating processing of billing data

FIG.3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 02/00128

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04Q 7/38, H04M 15/00
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: 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)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5982864 A (JAGADISH ET AL), 9 November 1999 (09.11.99), column 3, line 48 - column 4, line 18, figure 1b, column 7, line 28 - line 32, column 5, line 19 - line 22	1-9,11-17
A	abstract	10
	--	
A	US 6047051 A (GINZBOORG ET AL), 2 April 2000 (02.04.00), abstract	1-17
	--	
P,A	WO 0191003 A2 (ZTANGO, INC), 29 November 2001 (29.11.01), claim 3, abstract	1-17
	--	

[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
23 May 2002	06 -06- 2002
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 Malin Söderman /js Telephone No. +46 8 782 25 00

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

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 02/00128

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,A	WO 0133456 A2 (AP ENGINES, INC), 10 May 2001 (10.05.01), page 2, line 15 - line 21, abstract ---	1-17
A	WO 0065812 A1 (TELIA AB), 2 November 2000 (02.11.00), page 19, line 6 - line 15 --- --------	1-17

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

INTERNATIONAL SEARCH REPORT
Information on patent family members

01/05/02

International application No.
PCT/FI 02/00128

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5982864 A	09/11/99	NONE	
US 6047051 A	02/04/00	AU 730689 B	15/03/01
		AU 4871297 A	03/06/98
		BR 9713014 A	25/01/00
		EP 1012760 A	28/06/00
		FI 964524 A	12/05/98
		NZ 335701 A	27/10/00
		WO 9821676 A	22/05/98
WO 0191003 A2	29/11/01	AU 6333001 A	03/12/01
		US 2002029197 A	07/03/02
WO 0133456 A2	10/05/01	AU 1346901 A	14/05/01
WO 0065812 A1	02/11/00	AU 1191900 A	01/05/00
		EP 1117340 A	25/07/01
		EP 1180297 A	20/02/02
		NO 20015022 A	18/12/01
		SE 9901509 A	28/10/00

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 February 2003 (27.02.2003)

PCT

(10) International Publication Number
WO 03/017065 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number: PCT/US02/26595

(22) International Filing Date: 20 August 2002 (20.08.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/934,123 21 August 2001 (21.08.2001) US

(71) Applicant *(for all designated States except US)*: **APOGEE NETWORKS** [US/US]; 1455 Broad Street, 4th Floor, Bloomfield, NJ 07003 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **DESHMUKH, Abhi** [IN/US]; 253A, Kinderkamack Road, River Edge, NJ 07661 (US). **HERNANDEZ, Milton** [DM/US]; Apt. D, 1 Cononial Court, River Edge, NJ 07661 (US). **GUHA, Jayanta** [—/US]; 860 Main Street, Apt. 5B, Hackensack, NJ 07601 (US).

(74) Agents: **DUNNAM, Michael, P.** et al.; Woodcock Washburn LLP, One Liberty Place, 46th Floor, Philadelphia, PA 19103 (US).

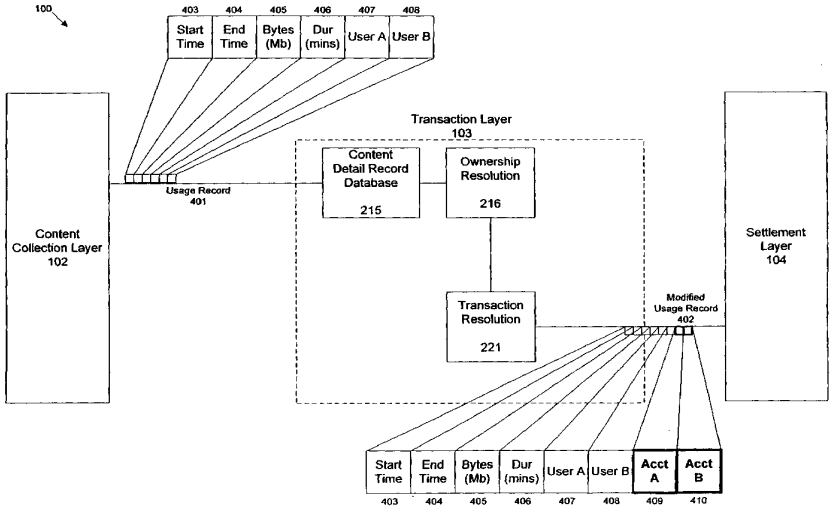
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT,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

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

Published:
— *without international search report and to be republished upon receipt of that report*

[Continued on next page]

(54) Title: CONTENT OWNERSHIP RESOLUTION



(57) Abstract: The invention describes a method, system, and computer-readable medium having computer-executable instructions for determining parties to a transaction. The inventive method includes receiving data related to an event, where the data includes one or more data elements. The inventive method also includes selecting the data elements that identify the parties to the transaction, determining whether additional data elements are required to identify the parties to the transaction, and identifying the additional data elements. The event may be an exchange of data between the parties over a communication network, and the data related to the event may be stored in a usage record. The additional data element may identify an owner or party to the transaction, called an accountable. The party may have direct or indirect association in the transaction and may not be obvious from the record of the transaction itself.

WO 03/017065 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.

CONTENT OWNERSHIP RESOLUTION

Technical Field

The invention relates generally to the processing of data, and more particularly to efficiently and generically aggregating data available on a communication network.

Background of the Invention

Recently, the collection and processing of data transmitted over communication networks, like the Internet, has moved to the forefront of business objectives. In fact, with the advent of the Internet, new revenue generating business models have been created to account for the consumption of content received from a data network (*i.e.*, content-based billing). For example, content distributors, application service providers (ASPs), Internet service providers (ISPs), and wireless Internet providers have realized new opportunities based on the value of the content and services that they deliver. As a result of this content-and-services-billing initiative, it has become increasingly important to resolve intelligently and flexibly the corresponding transactions according to the business needs of the customer.

Often, even in traditional commerce streams, there a many different participants between the maker and the consumer of the goods. Some of these so-called "middlemen" simply may facilitate access to the good, while others may add useful characteristics to the good. This is especially true in a distributed network environment, like the Internet,

that impose additional burdens on capturing the transaction process because of the unlimited number of data sources and the correspondingly unlimited number of data types. As a result, adequately describing the transacting of the goods and services in such an environment, or even across any of the traditional environments requires a technique that is capable of understanding and processing the participants and the various types of data.

To date, resolving the characteristics of a transaction has been accomplished over data-specific environments using certain application-specific (*i.e.*, "non-generic" or custom) methods. For example, a typical telephone bill captures the characteristics of a voice-based telecommunications transaction. In particular, the participants may be identified as the party initiating the call (*i.e.*, the "calling party" telephone number), the party receiving the call (*i.e.*, the "called party" telephone number), and one or more parties connecting the communication (*i.e.*, the "local" or "long distance carrier"). This simple example adequately captures all of the necessary aspects of the telephone call to properly account for the transaction by requiring payment from certain parties (*e.g.*, the calling and/or the called party) to certain other parties (*e.g.*, the local and/or long distance carrier). While these "hard-coded" transaction resolution techniques are sufficient to accommodate only specific environments involving well-defined participants (e.g., the telecommunications network), they are correspondingly too rigid to efficiently satisfy the ever-changing face of a communication network like the Internet. Also, these "hard-

coded" techniques are too specific to operate across the many and varied transaction environments and domains that exist throughout the business world.

Therefore, there exists a need to provide a flexible technique that can capture and resolve transactions of any type in any business domain involving any number and kind of participants without requiring modification of the technique for each type. Such a technique would serve to accommodate multi-faceted networked environments like the Internet, as well as to provide a single solution that would apply to any business environment.

Summary of the Invention

The invention describes a method, system, and computer-readable medium having computer-executable instructions for determining parties to a transaction. The inventive method includes receiving data related to an event, where the data includes one or more data elements. The inventive method also includes selecting the data elements that identify the parties to the transaction, determining whether additional data elements are required to identify all or some of the parties to the transaction, and identifying the additional data elements. The event may be an exchange of data between the parties over a communication network, and the data related to the event may be stored in a usage record. The additional data element may identify an owner or party to the transaction, called an accountable. Determining whether additional elements are required may be a function of the received data, and/or a function of the requirements of a customer

settlement system. The customer settlement system may be a data security system, a network capacity planning system, a content monitoring system, and/or a billing application, for example. The identifying of additional data elements or accountables may be initiated by a building block known as a primitive that includes multiple specific methods, including a database lookup, a direct value assignment, a regular expression parsing or match, a CDR database lookup, hard-coded, network address, area code, substring manipulation or a custom code execution. All or some of the inventive method steps may be conducted on a computer-readable medium using computer-executable instructions.

The inventive system for determining parties to a transaction includes an instrumentation layer, a content collection layer in communication with the instrumentation layer, and a transaction layer in communication with the content collection layer. The instrumentation layer provides raw data, while the content collection layer generically processes the raw data, and the transaction layer identifies one or more parties to the transaction. Also, the content collection layer may provide the raw data to the transaction layer in a usage record, and the transaction layer may modify the usage record as a function of identifying the parties to the transaction. The inventive system may further include a settlement layer in communication with the transaction layer, wherein the settlement layer rates the modified usage record. The transaction layer may include a database for storing the data processed by the content collection layer.

Brief Description of the Drawings

Other features of the invention are further apparent from the following detailed description of the embodiments of the invention taken in conjunction with the accompanying drawings, of which:

Figure 1 is a block diagram of a system for analyzing content transmitted over a communication network, according to the invention;

Figure 2 is a block diagram further describing the components of the system described in Figure 1;

Figures 3A and 3B provide a flow diagram further detailing the operation the system described in Figure 1;

Figure 4 provides a block diagram of the system described in Figure 1, providing greater detail of a configuration and operation of a transaction layer;

Figures 5A and 5B provide a flow diagram of a method for identifying the characteristics of a transaction, according to the invention;

Figure 6 is a block diagram further detailing the operation and configuration of the transaction layer, according to the invention; and

Figure 7 is a flow diagram that details the operation and configuration of the transaction layer of transaction layer, according to the invention.

Detailed Description of the Invention

System Overview

Figure 1 is a block diagram of a system 100 for analyzing content transmitted over a communication network. Although the following description will be discussed in the context of collecting, processing and billing for data transmitted over the Internet, it should be appreciated that the invention is no so limited. In fact, the invention may be applied to any type of network, including a private local area network, for example. Also, the invention may be used for purposes other than billing for the usage of content. For example, the invention may be used to analyze the type of data transmitted over a particular network, or to determine the routing patterns of data on a network. Furthermore, the invention may be used to facilitate the intelligent collection and aggregation of data relevant to a particular industry. In addition, the invention may be used to track specific Internet protocol (IP) network resources and to detect fraud, for example. It should also be appreciated that the invention may contemplate non-network and non-computer related business domains like commodity trading (*e.g.,* grains, crude oil) where multiple parties are involved. Therefore, although the invention is often described in the context of the Internet, it should be appreciated that the invention may equally applied to traditional business environments.

In addition, it should be appreciated that the term "content" may be defined as data that is transmitted over the network. In the context of the Internet, content may include .mp3 files, hypertext markup language (html) pages, videoconferencing data, and streaming audio, for example. The terms "content provider" and "customer" will be used throughout the description as well. Content provider may refer to the primary creator or

provider of the content, while customer is the primary recipient of the content. Both the producer and customer may be a human or a computer-based system.

As shown in Figure 1, an instrumentation layer 101 provides raw data to a content collection layer 102. Instrumentation layer 101 may consist of various data sources, for example, network routers. The network routers may provide information regarding the various types of routed data, including for example, data format, originating Internet protocol (IP) address, and destination IP address. One example of such information is Cisco System's NetFlow™.

Content collection layer 102 collects information about the delivery of the content, as well as the substance of the content itself. Content collection layer 102 also may sort, filter, aggregate, correlate and store the content according to the particular needs of the end user. In effect, content collection layer is responsible for extracting meaningful information about IP traffic, and so it is provided with an understanding of the data sources in instrumentation layer 101. Content collection layer 102 also may transform the data from the plurality of sources in instrumentation layer 101 into standard formats for use in a transaction layer 103.

Content collection layer 102 is in communication with transaction layer 103. Generally, content collection layer 102 reports to transaction layer 103 that a relevant communication event has occurred and should be considered by the remainder of system 100. A communication event may be defined as any transfer of data between systems. Transaction layer 103 captures the predetermined agreements among all of the parties

involved in system 100 regarding the value of the transferred content, as well as the value added by each of the individual parties in transferring such content. Therefore, transaction layer 103 is charged with understanding the nature of the parties, as well as the understanding the actions that one or more parties perform and the influence of such action on the respective parties.

Transaction layer 103 is in communication with a settlement layer 104. Settlement layer 104 captures the operations that are necessary to understand the significance of the transaction defined by transaction layer 103. For example, settlement layer 104 may rate a particular transaction by assigning a monetary value to the transaction. Settlement layer 104 also may divide the burdens and benefits of the monetary value among the relevant parties. In this way, settlement layer 104 ensures that certain parties receive a particular portion of the payment made by the other parties. Settlement layer 104 also may be responsible for delivering this burden and benefit information to the appropriate parties with the appropriate identifiers (*e.g.,* account numbers).

Figure 2 is a block diagram further describing the components of system 100. As shown in Figure 2, instrumentation layer 101 includes data sources 201-203 that each provide raw data 204-206, respectively, to collection layer 102. As discussed, data sources 201-203 may include various internetworking devices like routers, bridges, and network switches. Data sources 201-203 provide raw data to an input data adapter 207. Accordingly, input data adapter 207 understands the operation of and the data provided

by data sources 201-203. Although one input data adapter is shown in Figure 2, it should be appreciated that more than one input data adapter may be used in system 100. For example, each data source may have a dedicated input data adapter.

Input data adapter 207 understands the incoming data and extracts the data into the appropriate fields. This field-delimited data, called flow objects 208, are sets of attributes. The attributes may be any characteristics that are provided by, or can be derived from, raw data 204-206 provided by data sources 201-203, respectively. For example, flow objects 208 may include a set of attributes describing the source and destination, including source IP address, destination IP address, source interface, and destination interface. Because input data adapter 207 is charged with understanding raw data 204-206 from data sources 201-203, as well as the required flow objects 208 of system 100, it is capable of transforming the raw data to the flow objects, where the flow objects may all be of a standard format.

Input data adapter 207 provides flow objects 208 to a content data language 209. Content data language 209 may transform the attributes in flow objects 208 into other attributes that are desired by a particular customer. For example, content data language 209 may derive a network identifier attribute that is not readily available from a data source, from a source address attribute and a destination address attribute that are provided by flow object 208 attributes from input data adapter 207. This derivation may be based on a customer's desire to determine which network conveyed the transaction between the source and the destination. Therefore, following this example, content data

language 209 will know to extract the source address attribute and the destination address attribute from flow objects 208.

Content data language 209 may perform other functions as well. For example, content data language 209 may perform a generic lookup function 219 that is built into content data language 209. Generally, generic lookup 219 describes a technique for mapping any number of attributes to any number of other derived attributes. For example, generic lookup 219 may be used to map a unique resource locator (URL) attribute to a particular content-type attribute.

Content data language 209 also is in communication with a correlator 211. Generally, correlator 211 connects the many daily network content events from various network devices, like routers for example. Often, the connected data may come from distinctly different data sources at distinctly unrelated times. Correlator 211 allows this data to be intelligently connected to each other, regardless of how different the sources or of how disparate the time received. For example, a Netflow™ enabled router and a Radius™ enabled network access switch may each provide certain data that is relevant to one particular transaction. However, because portions of the data come from different devices, the data may arrive at system 100 at different times, and in different formats. Also, because each provides data that is necessary to complete one transaction, the data from each cannot be considered separately. Correlator 211 allows this data to be intelligently grouped regardless of the format of the data or of the time the data pieces are received.

Furthermore, correlator 209 may rearrange the order of the received flow objects 208 to suit the needs of the remainder of system 100. By performing such correlation without having to first store all of the data on a disk (*e.g.*, a database), significantly faster processing is achieved. Correlator 209 may perform this correlation in real-time, for example.

Although system 100 has been described using content data language 209 and correlator 211, it should be appreciated that flow objects 208 may proceed directly to a filter 212, if no correlation is required and if no attribute derivation is required, for example. Filter 212 analyzes flow objects 208 to ensure that the provided attributes are desired by system 100. If flow objects 208 are not needed (*i.e.*, a mismatch), filter 212 may prevent flow objects 208 from passing to an aggregator 213. Also, although filter 212 has been shown as a separate device in system 100, it should be appreciated that the functionality of filter 212 may be incorporated into aggregator 213.

Filter 212 passes the matching flow objects to aggregator 213. Aggregator 213 may provide additional filtering and classification of the multitude of daily network content transactions, based on user criteria. Aggregator 213 may perform such filtering and classification in real-time. Aggregator 213 will be discussed in greater detail with reference to Figures 4-7. Aggregator 213 provides the filtered and classified information to an output data adapter 214. Output data adapter 214 may convert the data from aggregator 213 into one or more content detail records for storage in CDR database 215. Therefore, CDR database 215 stores a complete description of a content event.

Transaction layer 103 includes CDR database 215, an ownership resolution component 216, and a transaction resolution component 221. CDR database 215 passes the CDR onto ownership resolution component 216. A proper accounting of a communication event, for any purpose including billing, requires both identifying the participants and defining the relationships among those participants. These tasks are accomplished by ownership resolution component 216 and transaction resolution component 221.

Ownership resolution component 216 serves to define the direct and indirect participants of the communication event. In particular, because raw data 204-206 may not provide sufficient "ownership" data relating to the parties involved in the content transaction, such "ownership" data must be provided by system 100 to properly account for the entire transaction. Ownership resolution component 216 operates to provide such ownership-based data to system 100.

Ownership resolution component 216 is in communication with transaction resolution component 221. Transaction resolution component 221 serves to capture the predetermined relationships and/or agreements among the parties defined by ownership resolution component 216 regarding the value of the transferred content, as well as the value added by each of the individual parties in transferring such content. Such predetermined relationships may be previously agreed upon by the participants, or may be created and agreed upon with the implementation of system 100. Therefore, transaction component 103 understands the nature of the parties, the actions that one or

more parties perform, and the influence of such action on the respective parties. Ownership resolution component 216 and transaction resolution component 221 will be discussed in greater detail.

Transaction component 216 provides the transaction information to a rating component 217. Rating component 217 provides a weight or significance (*e.g.*, a price) to the transaction, so as to provide a tangible value to the transaction. Rating component 217 may make this determination based on various metrics including the type of the content, the quantity of content consumed, the place and time delivered, or the quality of the content for example. Therefore, rating component 217 allows system 100 to provide some contextual value, indicting the significance or relevance that certain content or information has to the individual customer.

Rating component 217 provides the rated transaction to a presentment component 218. Presentment component 218 may provide the capability for a customer 220 to view their real-time billing information, for example, over the network. Presentment component 218 also may attach relevant identifiers to the bill (*e.g.*, account numbers, etc.).

Figures 3A and 3B provide a flow diagram further detailing the operation 300 of system 100. As shown in Figure 3A, in step 301, raw data 204-206 is received from data sources 201-203. In step 302, input data adapter 207 converts raw data 204-206 to flow objects 208, where flow objects 208 are sets of attributes, determined from raw data 204-206. In step 303, it is determined whether there is a need to derive new attributes from

the existing attributes found in flow objects 208. If there is such a need, in step 304, CDL 209 is used to derive new attributes from existing attributes. Also, as discussed above, attributes may be correlated by correlator 211.

In step 305, flow objects 208 are filtered by filter 212. In step 306, the matching flow objects (*i.e.,* those passed by filter 212) are further filtered and classified by aggregator 213 (as discussed more fully with reference to Figures 4-7). In step 307, output data adapter 214 converts the data aggregated by aggregator 213 to a format compatible with transaction layer 103.

As shown in Figure 3B, in step 308, output adapter 214 may format the aggregated data into one or more content data records for storage in CDR database 215. In step 309, ownership resolution component 216 identifies the parties involved in the transaction. In step 310, transaction resolution component 221 captures the predetermined agreements among the parties, as well as the value added by each of the individual parties. In step 311, the CDR is rated based on predetermined metrics (*e.g.,* time of transmission, quality of content). In step 312, a bill is presented to the customer.

Content Transaction Layer

A transaction, including a business transaction for example, may be any activity between two or more participants that affects certain parties. The affected parties may be considered the participants to the transaction, although parties and participants may be mutually exclusive entities. It should be appreciated that the terms "parties" and "owners" may be used interchangeably throughout. Also, a transaction may include one or more events, where an event may be some action (*e.g.*, the transfer of a service or good) that the participants conduct with each other. Such events may be the exchange of data over a communication network, for example. Also, it should be appreciated that the same event or action may take place in any direction (*e.g.*, from party A to party B or from party B to party A). The "subject" of the action is the party who performs the activity, while the "object" of the action is the party who is affected or influenced in any way by the action.

Transaction layer 103 is responsible for capturing the characteristics of the transaction, including the parties, participants, subject, object, event/action type, direction of the action, for example. The scope of the characteristics captured by transaction layer 103 will vary with the nature of instrumentation layer 101, the capability of content collection layer 102, and the requirements of settlement layer 104. Generally, transaction layer 103 captures the predetermined agreements among all of the parties involved in system 100 regarding the value of the transferred content, as well as the value added by each of the individual parties in transferring such content. Therefore, transaction layer

103 is charged with understanding the nature of the parties, as well as the understanding the actions that one or more parties perform and the influence of such action on the respective parties.

Transaction layer 103 includes CDR database 215, an ownership resolution component 216, and a transaction resolution component 221. CDR database 215 is a data store that holds each CDR for further processing by ownership resolution component 216 and transaction resolution component 221. In the context of a billable electronic business transaction, a proper accounting of a communication event, for any purpose including billing, requires both identifying the participants and defining the relationships among those participants. As discussed, ownership resolution component 216 serves to define the participants of the communication event, while transaction resolution component 221 serves to capture the predetermined relationships and/or agreements among the parties defined by ownership resolution component 216.

Transaction layer 103 is generic in that it operates without requiring an understanding of instrumentation layer 101 and content collection layer 102. Instead, transaction layer 103 takes the relevant characteristics of the transaction provided by instrumentation layer 101 and content collection layer 102, and selects and generates those characteristics required by settlement layer 104.

Although the operation of transaction layer 103 will be described in the context of an electronic event over a communication network for the purposes of billing for the event, it should be appreciated that the invention is not so limited, but is so described the

purpose of clarity. For example, it should be appreciated that the invention may include functions other than billing, including security, network capacity planning, and content monitoring, for example. Also, the generic techniques described may be applied beyond the context of an electronic event over a communication network.

Figure 4 provides a block diagram of system 100 providing greater detail of the configuration and operation of transaction layer 103. As shown in Figure 4, content collection layer 102 provides a usage record 401 to transaction layer 103. A series of fields 403-408 comprise usage record 401. Although fields 403-408 will be identified by certain labels for the purpose of clarity, it should be appreciated that fields 403-408 may identify any of the many possible characteristics of the transaction.

In the example provided by Figure 4, fields 403 and 404 identify the parties or participants to the transaction. In particular, field 403 identifies "User A" and field 404 identifies "User B." User A may be the subject party and User B may be the object party. For example, in the context of a telecommunication event, User A may be the "calling" party and User B may be the "called" party. Field 405 and field 406 identify a measurable quantity of the event. In particular, following the example of the telecommunications event, field 405 identifies a duration (in minutes) of the event and field 406 identifies the quantity of data exchanged during the event (in megabytes). Field 407 and field 408 may identify a "start time" and an "end time," respectively, of the communication event.

Although fields 403-408 provide just one example, in any case, it should be appreciated that user record 401 will include certain characteristics provided by instrumentation layer 101 and/or derived by content collection layer 102. These characteristics typically are provided to transaction layer 103 because they have some particular significance to identifying the characteristics necessary to allow settlement layer 104 to provide some accounting of the transaction. Therefore, usage record 401 may not necessarily include all of the characteristics provide by instrumentation layer 101 and/or derived by content collection layer 102, because certain characteristics may not relevant to the settlement of the transaction (*e.g.*, network type). Yet, usage record 401 will include those available characteristics that pertain to permitting settlement layer 104 to properly account for the transaction.

Once usage record 401 passes through transaction layer 103, a modified usage record 402 may be provided to settlement layer 104. Modified usage record 402 may be modified by transaction layer 103 to include additional details of the transaction event required by settlement layer 104 and/or required by the customer's system to which the usage record applies (*e.g.*, a usage billing system). As shown for modified usage record 402, an account A field 409 and an account B field 410 may be added to further identify the transaction. In one example, account A field 409 may include an alphanumeric designator that identifies the account number that has been assigned by the customer's billing system for User A. In the context of the telecommunications system, account A field 409 may hold User A's ten-digit home telephone number, for example.

In any case, the components of transaction layer 103 operate to identify these additional fields, based on the requirements of the customer's system and of settlement layer 104. In particular, ownership resolution component 216 operates to ensure that the necessary participants or parties to the transaction are identified, while transaction resolution component 221 operates to ensure that the relationships among the parties or participants are identified.

Identification of the relevant entities and their relationships may be accomplished using "lookups" in data stores located within ownership resolution component 216 or user-defined actions specified on external systems and applications and transaction resolution component 221, for example. For example, a data table may have a "User" data field and an associated "Account" data field. When User A is received by ownership resolution component 216, it will conduct a lookup in the data table and identify Account A as the appropriate account associated with User A. Also, transaction resolution component 221 may have a data table that permits a lookup of the relationship between User A and User B, identified in usage record 401. For example, upon receiving field 407 designating User A and field 408 designating User B, transaction resolution component 221 may conduct a lookup of an algorithm that identifies the appropriate burdens and benefits (*e.g.*, debit and credit of money) assigned to each of the users with respect to each other.

It also should be appreciated that transaction layer 103 may not provide additional characteristics to usage record 401, as described but may select the relevant

characteristics (*i.e.*, those characteristics needed by settlement layer 104) from the characteristics made available by instrumentation layer 101 and/or derived by content collection layer 102. In fact, usage record 401 may include all of the necessary characteristics to properly account for the transaction. In this case, ownership resolution component 216 and transaction resolution component 221 select the relevant characteristics from the available characteristics.

Figures 5A and 5B provide a flow diagram of a method 500 for identifying the characteristics of a transaction using system 100. As shown in Figure 5A, in step 501, raw data 204-206 is received into system 100. Raw data 204-206 includes certain characteristics provided by data sources 201-203, respectively, in instrumentation layer 101. In step 502, content collection layer 102 processes (*e.g.*, aggregates, correlates and filters) raw data 204-206. In step 503, content collection layer 102 provides the processed data to CDR database 215 in transaction layer 103. CDR database 215 stores the data for further processing by transaction layer 103.

In step 505, it is determined whether the contents of the data provided to transaction layer 103 already include the needed ownership data. If the data includes the needed ownership data, the relevant data is selected by ownership resolution component 216 and provided to transaction resolution component 221, in step 507. If, on the other hand, the data provided to transaction layer 103 does not already include the needed ownership data, the required data is identified (*e.g.*, using database lookups, accountable primitives) by ownership resolution component 216, in step 506. Once ownership

resolution component 216 identifies the required ownership data, the relevant data is selected by ownership resolution component 216 and provided to transaction resolution component 221, in step 507.

As shown in Figure 5B, in step 508 it is determined whether the contents of the data provided to transaction layer 103 already include the needed relationship data (*i.e.*, data defining the burdens and benefits encountered by the parties/participants to the transaction). If the data includes the needed relationship data, the relevant data is selected by transaction resolution component 221 and provided to settlement layer 104, in step 510. If, on the other hand, the data provided to transaction layer 103 does not already include the needed relationship data, the required data is identified (*e.g.*, using database lookups) by transaction resolution component 221, in step 509. Once ownership resolution component 216 identifies the required ownership data, the relevant data is selected by ownership resolution component 216 and provided to transaction resolution component 221, in step 510.

Ownership and Transaction Resolution

Figure 6 is a block diagram further detailing the operation and configuration of transaction layer 103. It should be appreciated that elements described for transaction layer 103 are not exclusive, but provide just one example of a configuration for transaction layer 103. In particular, the functionality of the previously described ownership resolution component 216 and transaction resolution component 221 will be

descried in greater detail in the various components described with reference to Figure 6. In practice, however, it should be appreciated that transaction layer 103 may comprise of any number of components that ensure that the necessary parties to a transaction are identified generically.

As shown in Figure 6, transaction layer 103 includes a configuration repository 601, a configuration database 610, a configuration manager 603, and a fail over detector 604. In addition, transaction layer 103 includes a transaction layer engine 608 in communication with configuration repository 601, configuration manager 603, and fail over detector 604.

Transaction layer engine 608 includes a rules processor 605, a CDR reader 606, and a transaction writer 607. Transaction layer engine 608 processes raw data 204-206 in usage record 401 and creates a modified usage record 402, based upon the requirements of settlement layer 104. It should be appreciated that there may be more than one transaction layer engine 608 for each transaction layer 103. However, a single transaction layer engine 608 is shown for the purpose of clarity and brevity.

CDR reader 106 understands the nature of the transaction and operates to read a particular usage record 401 stored in CDR database 215. CDR reader 106 then submits usage record 401 to rules processor 605. Rules processor 605 applies rules (*e.g.*, written in XML) to usage record 401 so as to determine ownership and the relationships among the ownership, for each individual usage record 401. Rules processor 605 may then generate one or more modified usage records 402, based on the application of the rules to

usage record 401. Once rules processor 605 generates the modified usage record 402, transaction writer 607 operates to write a transaction (based on the modified usage record 402) to CDR database 215. Modified usage record 402 is then used by settlement layer 104 to further process the transaction (*e.g.*, rate the transactions monetarily).

Fail over detector 604 operates to provide fault tolerance and initiate a fail over engine (not shown) for a failed transaction layer engine, in accordance with one or more mathematical algorithms, the discussion of which is beyond the scope of the invention. Configuration manager 603 provides an external interface to transaction layer 103 using a business editor 609. Business editor 609 may be manipulated by a user or customer using a graphics user interface (GUI). In particular, the GUI of business editor 609 receives commands from a user and translates them into actions to be performed on usage record 401, for example, by rules processor 605. Configuration repository 601 operates to provide an abstraction to configuration database 610. Configuration database 610 may be a relational database or a set of extensible markup language (XML) computer-readable files, for example.

Figure 7 is a flow diagram that details the operation of transaction layer 103, as shown in Figure 6. As discussed, it should be appreciated that multiple transaction engines may be used to implement a process. Where the invention is instituted using computer-readable instruction, transaction layer engine 608 may be implemented as a computer-executable instruction or thread. Therefore, multiple transaction layer engines may be implemented by having multiple computer-readable instructions.

In step 701, transaction layer engine 608 reads usage record 401 using CDR reader 606. In step 702, rules processor 605 applies one or more rules to usage record 401 read by CDR reader 606, so as to determine one or more "accountables." Accountables are labels that are used to facilitate identifying the parties or owners to a transaction. Accountables may be defined and/or modified by an external user (*e.g.*, a customer) using the graphical user interface provided by business editor 609. Also, it should be appreciated that accountables may be defined for a new usage types for which no rules in rules processor 605 are provided. The identification of accountables is the function of ownership resolution component 216, as described with reference to Figure 4.

In step 703, "contracts" are identified that define the relationships or agreements between one or more accountables. In the context of a billing system, a contract identifies which party pays (*i.e.*, the billed party) and which party receives payment (*i.e.*, the billing party). A particular contract may be identified and executed when one based on "conditions" are satisfied, however, such conditions may not be required. The identification of contracts is conducted by transaction resolution component 221, as described with reference to Figures 2 and 4. A condition is an expression of a logical assertion that can be evaluated as true or false. In transaction layer 103, for example, a condition may be true if a certain data element is present and false if the data element is not present. The following is an example of a condition in XML:

<condition name="condition1" function="IsPresent" outcome="true" type="Accountable" id="ColoProvider"/>

In step 704, once the contracts are determined, they are executed. In step 705, usage record 401 is changed to modified usage record 402 based upon the execution of the contract and the identification of the accountables. In step 706, modified usage record 402 may be written to a data table using transaction writer 607, so that settlement layer 104 can rate it, in step 707. Therefore, a transaction may be represented as modified usage record 402, where modified usage record may include the elements of usage record 401 in addition to the accountable and contract elements (*e.g.,* fields 409-410 as discussed with reference to Figure 4).

Although the discussion provided an example of a single contract and two accountables for a single usage record, it should be appreciated that many contracts and many accountables (*i.e.,* and therefore many "transactions") may be derived from a single usage record, because there may be multiple transactions implicated from a single usage record 401. For example, usage record 401 may involve three parties each having a contract with the other respective parties. In this example, therefore, there may be three separate contracts for a single usage record 401, and three individual accountables for each party or owner.

In addition to requiring a certain accountable, it may be necessary to determine a value of the accountable. For example, transaction layer 103 may determine not only that the "called party" accountable be a part of the transaction, but also that a value for the

called party (*e.g.*, "856-555-1212" or "John Doe") be identified. Also, it may be necessary to transform one accountable into another accountable to satisfy the requirement of settlement layer 104. For example, settlement layer 104 may require the called party accountable (either determined by transaction layer 103 or provided in usage record 401) be transformed into a network identifier accountable.

In either case, the value or transformation of accountables or contracts may be determined using certain predetermined functions or "primitives." A primitive allows the user to specify how to find the value of a particular accountable or how to find billing and/or billed account numbers associated with a particular contract. As discussed, transformations may allow a value of an accountable to be determined using another accountable (*i.e.*, called "linked accountables"), for example. Primitives define and direct such transformations. The input to a primitive can be one of fields 403-408 from usage record 401 or a previously determined accountable, for example.

Primitives may be described and distinguished based on their prescribed functionality. For example, one type of primitive may be an external database lookup. A database lookup is a primitive that operates to transform one accountable or contract to another accountable or contract. Also, a database lookup primitive may function to assign a value to an accountable or contract, as a result of conducting a lookup of the accountable or contract in a database. It should be appreciated that the database lookup primitive also allows flexibility in that any database that has Java Database Connectivity (JDBC) drivers (*e.g.*, Oracle, Microsoft SQL Server, Sybase, Database 2) can be used to

perform complex lookups. For native databases that do not have JDBC connectivity, however, it should be appreciated that native methods for native databases may be accommodated through the primitives. In this way, therefore, previous accountable or contact transformations can be linked to find new accountables or contracts, respectively.

Other types of primitives may include direct value assignment, and a function primitive. A function primitive provides flexibility and extensibility by allowing a third party based library (*e.g.*, Java-based or native libraries) to be used. The arguments of a function primitive may be text strings. Also, the arguments of a function primitive may be expressed in terms of fields in CDR database 215 (*i.e.*, string-based fields in usage record 401), and other previously determined accountables. Therefore, function primitives permit the integration of proprietary and domain-specific algorithms to be implemented to perform ownership related processing.

Another primitive may be a "regular expression" based primitive that allows parsing of complex text-based fields with a full feature (*e.g.*, PERL5 compliant) pattern specification. Common used techniques would include parsing URLs, filenames and paths, calling/called telephone numbers, email address, for example. In addition, a CDR database 215 lookup primitive allows holding on to an ownership entity if no further processing is required. This primitive is used where usage record 401 provides the information needed by settlement layer 104 without any need for more data correlation and/or manipulation by transaction layer 103.

A default primitive may be a hard-coded primitive that is used where the value is known and/or is not dependent on usage record 401. For example, such a primitive may be used where a party is always present in a consumption event, regardless of the other relevant parties. A network address primitive allows determination of a network entity given an arbitrary string. An area code primitive may be used to determine an area code of a telephone number given the complete telephone number. This primitive may be relevant for a Voice-over-IP application. These examples primitives are not exclusive, but are meant to provide a few examples of the manipulation and correlation that may be achieved by the primitives on the accountables and contracts.

The following is an example of an accountable primitive in XML:

```
<accountable>
<name> ColoProvider </name>
<role> ServiceProvider </role>
<usageType> RMONHost </usageType>
<valid from="past" to="present" />
<primitive type="default">
<value> Exodus </value>
</primitive>
</accountable>
```

Each accountable that is involved in a contract will have an assigned "role." It follows, therefore, that an accountable that is not involved in a contract may not need to have an assigned role. The role associates the particular accountable for integration with settlement layer 104. This means that the concept of a role is used for the TL/AMI integration.

Similar to the accountable, a contract is implemented using a set of primitives. The following is an example of a contract primitive in XML, and is provided to further describe the invention. In the example, a Web hosting scenario is present where a content provider (*e.g.,* CNN) places content on one or more Web servers and pays a Web Hoster for doing so based on some predefined pricing plan.

In order to define the accountables, certain elements of usage record 401 may be assumed as follows: Web Hit Time, Web Server Name/IP address, Client IP address, bytes, Mime type, and URL. In this example, if a rule in the business world requires the "Content Provider" of the Web Server (*e.g.,* CNN) to pay to the Web Hoster, there are two accountables: Web Hoster and Content Provider. The XML definition of a contract that captures this business rule may be as follows:

```
01  <contract>
02  <name> ContentProvider-Pays-WebHoster </name>
03  <usageType> WebHosting </usageType>
04  <valid from="past" to="present" />
05  <condition function="IsPresent" type="Accountable"
    name="condition1"  id=" ContentProvider " />
06  <condition function="IsPresent" type="Accountable"
    name="condition2" id="WebHoster" />

07  <billedFunction>
08  <status> enabled </status>
09  <primitive type="internal-account-lookup">
10  <database name="GlobalDB"/>
11  <argument order="1" type="Accountable"
    name="ContentProvider"/>
12  </primitive>
13  </billedFunction>
```

```
14    <billingFunction>
15    <status> disabled </status>
16    <primitive type="internal-account-lookup">
17    <database name="GlobalDB"/>
18    <argument order="1" type="Accountable" name="WebHoster"/>
19    </primitive>
20    </billingFunction>
21    </contract>
```

In this example, a contract has a name defined in line 02 as "ContentProvider-Pays-WebHoster." The contract also defines an element or usage type called "WebHosting" in line 03. The contract also has two sets of conditions in lines 05 and 06, called "IsPresent," which consider whether "ContentProvider" and "WebHoster" elements are present, respectively. Therefore, this particular contract will be selected and executed by transaction layer 103 if these elements are present.

Also, in this contract example, there are two primitives that are specified. There is a first primitive for finding the account number of the billed entity "ContentProvider," which begins on line 07 and ends on line 13, and there is a primitive for determining the account of the billing entity "WebHoster" beginning on line 14 and ending on line 20. Therefore, the example contract contemplates the "who pays to whom" logic, and results in the execution of a contract that creates a modified usage record 402, which captures the transaction. Notably, in lines 09 and 16, both primitives are defined as database lookups.

The invention is directed to a system and method for of determining of direct and/or indirect parties involved in a transaction. The invention often was described in the context of the Internet, but is not so limited to the Internet, regardless of any specific description in the drawing or examples set forth herein. For example, the invention may be applied to wireless networks, as well as non-traditional networks like Voice-over-IP-based networks, private networks, and/or non-technology related business environments, like commodity trading for example. It will be understood that the invention is not limited to the use of any of the particular components or devices herein. Indeed, this invention can be used in any application that requires the determining of direct or indirect parties involved in a transaction. Further, the system disclosed in the invention can be used with the method of the invention or a variety of other applications.

While the invention has been particularly shown and described with reference to the embodiments thereof, it will be understood by those skilled in the art that the invention is not limited to the embodiments specifically disclosed herein. Those skilled in the art will appreciate that various changes and adaptations of the invention may be made in the form and details of these embodiments without departing from the true spirit and scope of the invention as defined by the following claims.

What is Claimed is:

1. A method of determining parties to a transaction, comprising:

receiving data related to an event, wherein said data comprises one or more data elements;

selecting said data elements that identify the parties to the transaction;

determining whether additional data elements are required to identify the parties to the transaction; and

identifying the additional data elements.

2. The method of claim 1, wherein said event is an exchange of data between the parties over a communication network.

3. The method of claim 1, wherein said data related to said event is stored in a usage record.

4. The method of claim 1, wherein the parties include at least one of the following: a subject party and an object party.

5. The method of claim 1, wherein said determining is a function of the received data.

6. The method of claim 1, wherein said determining is a function of the requirements of a customer settlement system.

7. The method of claim 6, wherein said customer settlement system includes at least one of the following: a data security system, a network capacity planning system, and a content monitoring system.

8. The method of claim 1, wherein said data element is an accountable.

9. The method of claim 1, wherein said identifying of additional data elements is initiated by a primitive.

10. The method of claim 9, wherein said primitive includes at least one of the following: a database lookup, direct value assignment, regular expression, CDR database lookup, hard-coded, network address, substring manipulation, area code, and a user-specified action.

11. A system for determining parties to a transaction, comprising:

an instrumentation layer, wherein the instrumentation layer provides raw data;

a content collection layer in communication with the instrumentation layer, wherein the content collection layer generically processes the raw data; and

a transaction layer in communication with the content collection layer, wherein the transaction layer identifies one or more parties to the transaction.

12. The system of claim 11, wherein said content collection layer provides said raw data to said transaction layer in a usage record.

13. The system of claim 12, wherein said transaction layer modifies said usage record as a function of identifying the parties to the transaction.

14. The system of claim 11, further comprising a settlement layer in communication with said transaction layer, wherein the settlement layer rates the modified usage record.

15. The system of claim 12, wherein said transaction layer comprises a data base for storing said data processed by said content collection layer.

16. A computer-readable medium having computer-executable instructions for:

receiving data related to an event, wherein said data comprises one or more data elements;

selecting said data elements that identify the parties to the transaction;

determining whether additional data elements are required to identify the parties to the transaction; and

identifying the additional data elements.

17. The computer-readable medium of claim 16, wherein said computer-executable instructions are extensible.

18. The computer-readable medium of claim 16, wherein said event is an exchange of data between the parties over a communication network.

19. The computer-readable medium of claim 16, wherein said data related to said event is stored in a usage record.

20. The computer-readable medium of claim 16, wherein the parties include at least one of the following: a subject party and an object party.

21. The computer-readable medium of claim 16, wherein said determining is a function of the received data.

22. The computer-readable medium of claim 16, wherein said determining is a function of the requirements of a customer settlement system.

23. The computer-readable medium of claim 22, wherein said customer settlement system includes at least one of the following: a data security system, a network capacity planning system, and a content monitoring system.

24. The computer-readable medium of claim 16, wherein said data element is an accountable.

25. The computer-readable medium of claim 16, wherein said identifying of additional data elements is initiated by a primitive.

26. The computer-readable medium of claim 25, wherein said primitive includes at least one of the following: a database lookup, direct value assignment, regular expression, CDR database lookup, hard-coded, network address, substring manipulation, area code, and user-specified action.

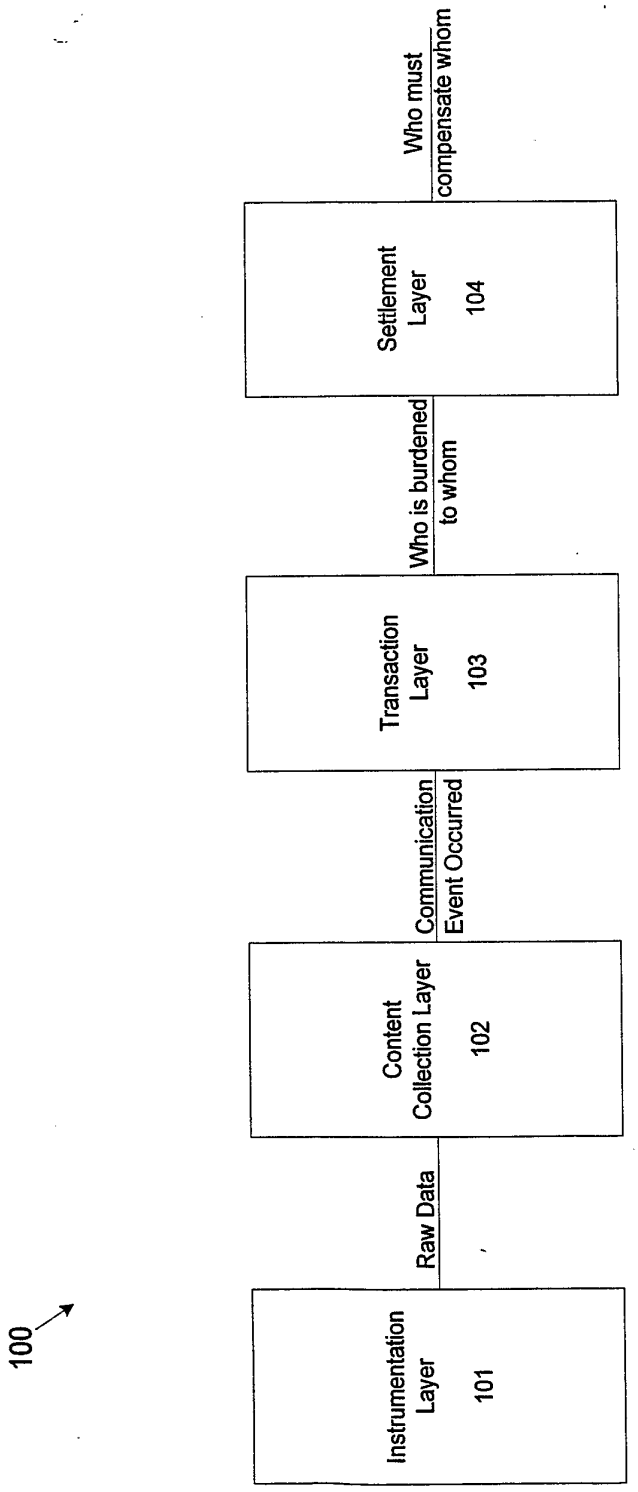

100
Instrumentation Layer 101
Raw Data
Content Collection Layer 102
Communication Event Occurred
Transaction Layer 103
Who is burdened to whom
Settlement Layer 104
Who must compensate whom

Figure 1

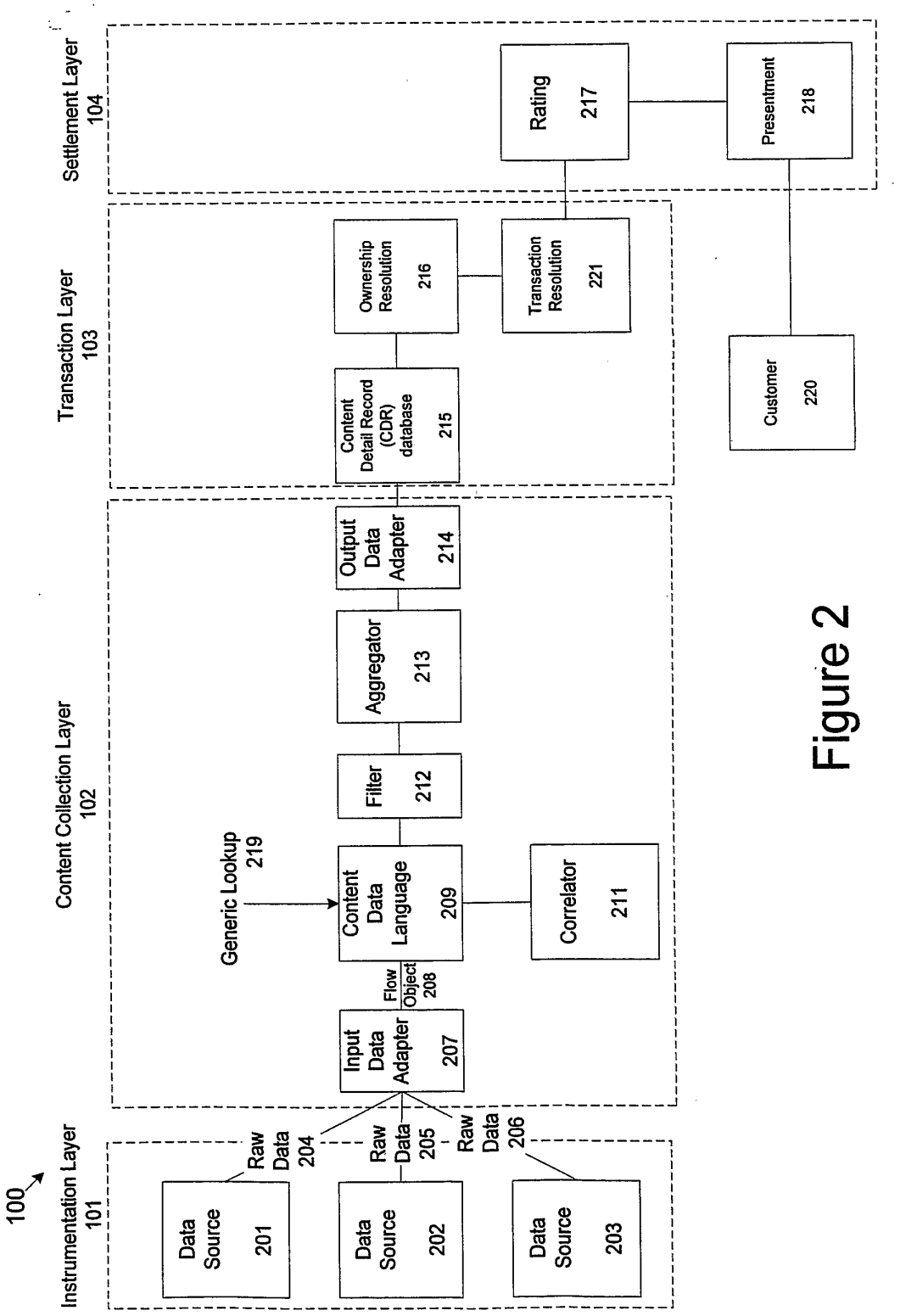

100
Instrumentation Layer 101
Data Source 201
Data Source 202
Data Source 203
Raw Data 204
Raw Data 205
Raw Data 206
Content Collection Layer 102
Input Data Adapter 207
Flow Object 208
Content Data Language 209
Generic Lookup 219
Filter 212
Aggregator 213
Output Data Adapter 214
Correlator 211
Transaction Layer 103
Content Detail Record (CDR) database 215
Ownership Resolution 216
Transaction Resolution 221
Settlement Layer 104
Rating 217
Presentment 218
Customer 220

Figure 2

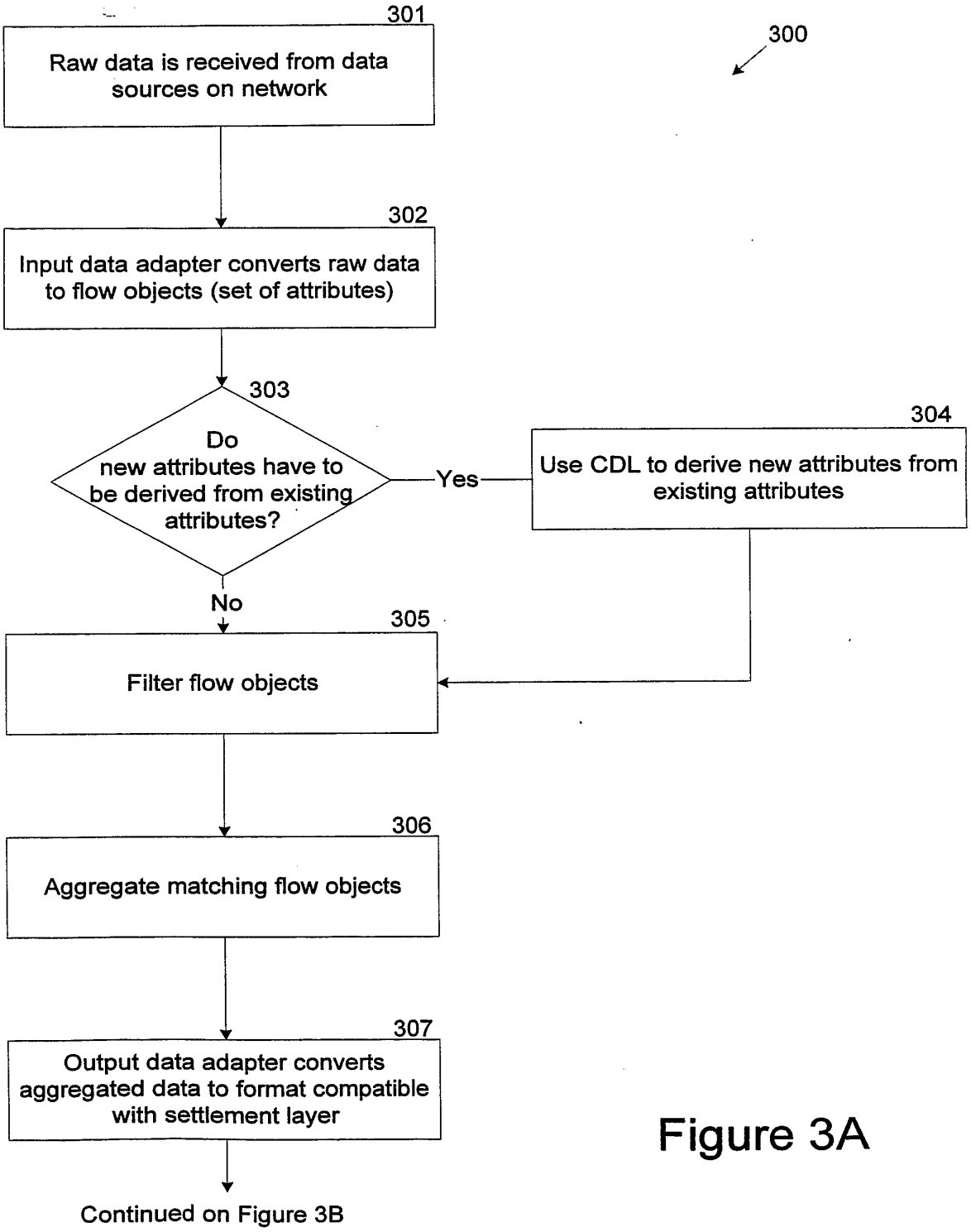

300
301
Raw data is received from data sources on network
302
Input data adapter converts raw data to flow objects (set of attributes)
303
Do new attributes have to be derived from existing attributes?
Yes
304
Use CDL to derive new attributes from existing attributes
No
305
Filter flow objects
306
Aggregate matching flow objects
307
Output data adapter converts aggregated data to format compatible with settlement layer
Continued on Figure 3B

Figure 3A

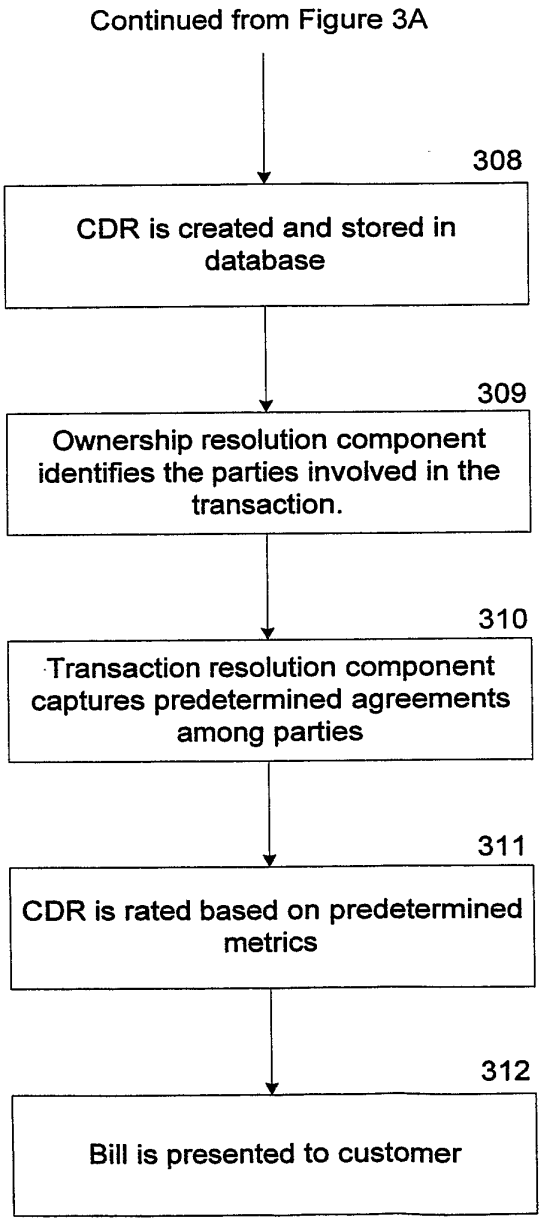

Continued from Figure 3A
308
CDR is created and stored in database
309
Ownership resolution component identifies the parties involved in the transaction.
310
Transaction resolution component captures predetermined agreements among parties
311
CDR is rated based on predetermined metrics
312
Bill is presented to customer

Figure 3B

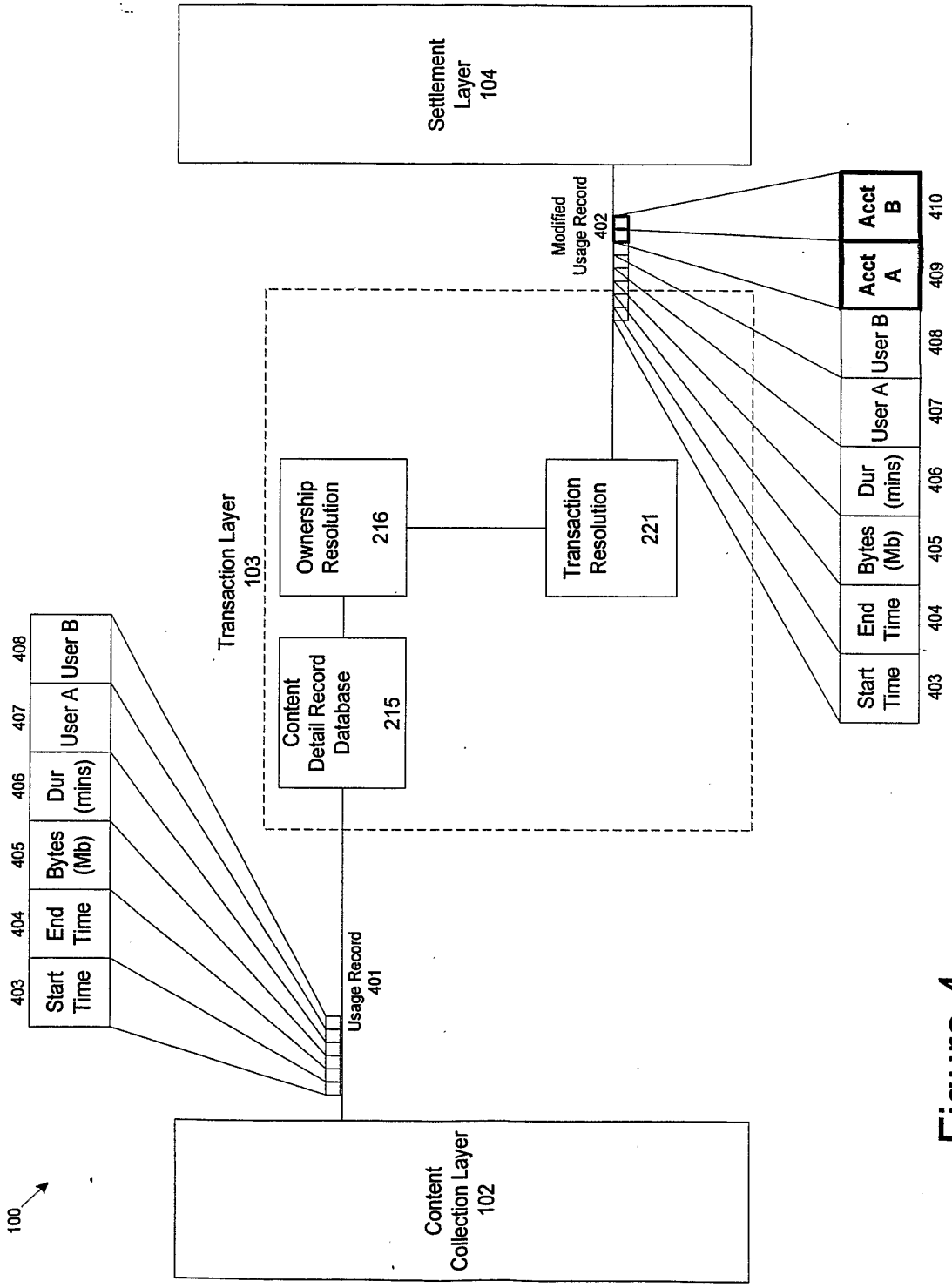

100
Content Collection Layer 102
Settlement Layer 104
Transaction Layer 103
Content Detail Record Database 215
Ownership Resolution 216
Transaction Resolution 221
Usage Record 401
Modified Usage Record 402
403 Start Time
404 End Time
405 Bytes (Mb)
406 Dur (mins)
407 User A
408 User B
409 Acct A
410 Acct B

Figure 4

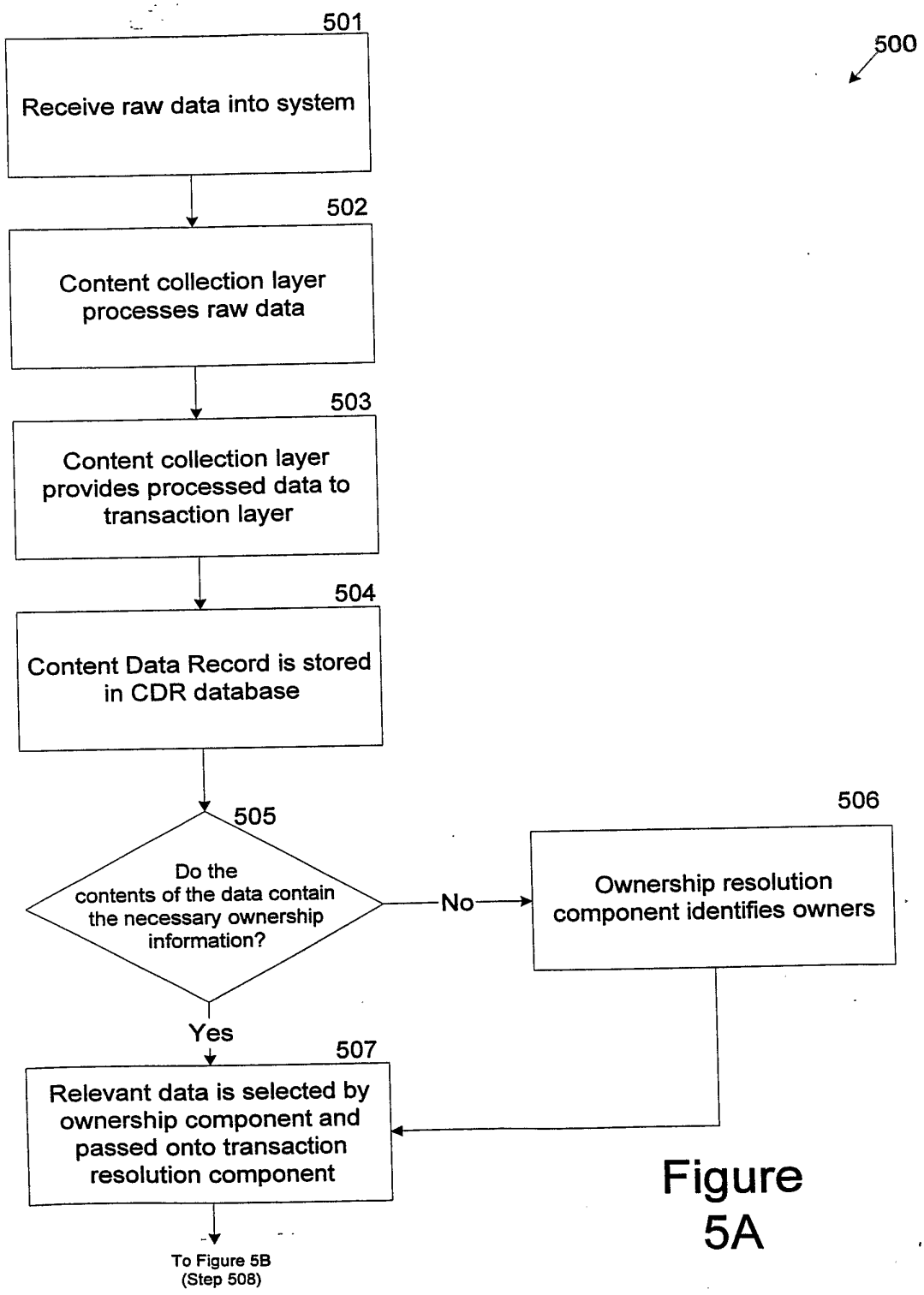

500
501
Receive raw data into system
502
Content collection layer processes raw data
503
Content collection layer provides processed data to transaction layer
504
Content Data Record is stored in CDR database
505
Do the contents of the data contain the necessary ownership information?
No
506
Ownership resolution component identifies owners
Yes
507
Relevant data is selected by ownership component and passed onto transaction resolution component
To Figure 5B (Step 508)

Figure 5A

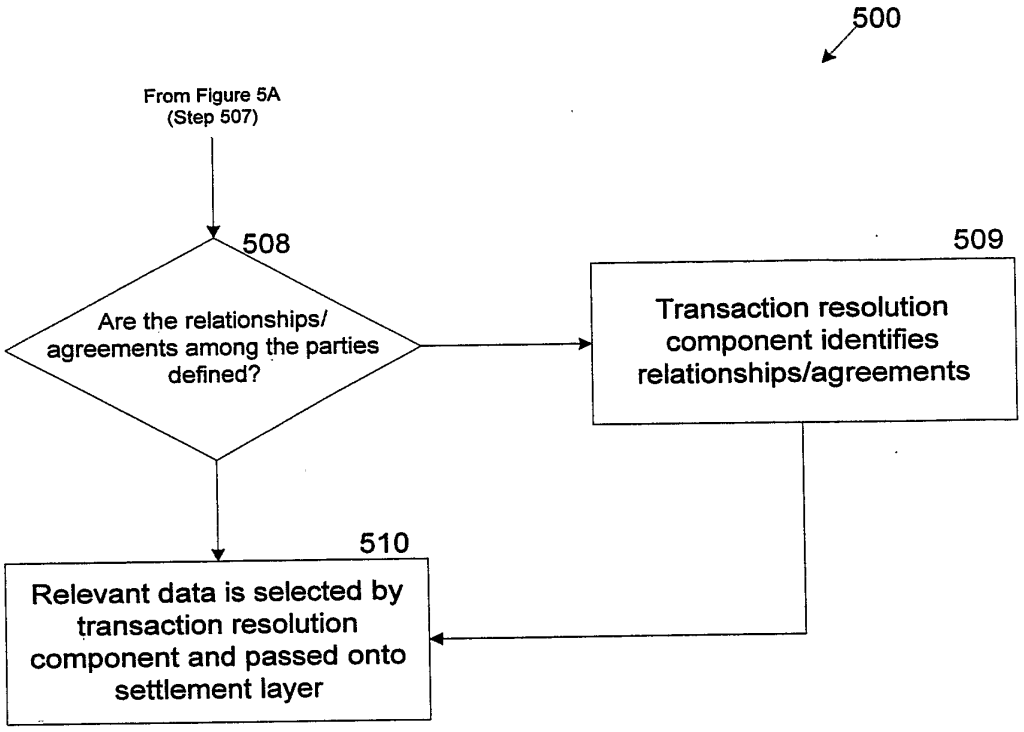

500
From Figure 5A
(Step 507)
508
Are the relationships/ agreements among the parties defined?
509
Transaction resolution component identifies relationships/agreements
510
Relevant data is selected by transaction resolution component and passed onto settlement layer

Figure 5B

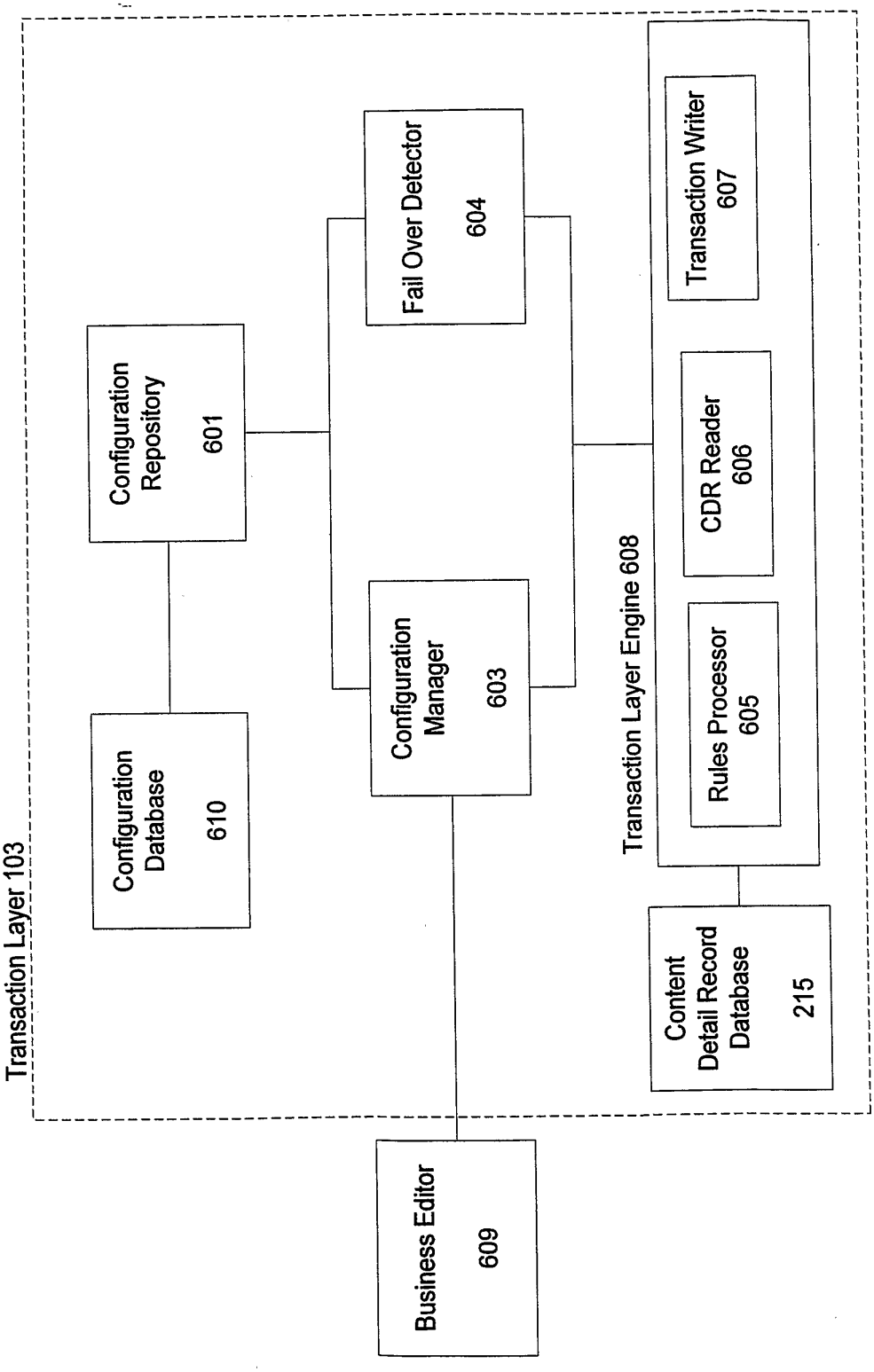

Transaction Layer 103
Configuration Repository 601
Configuration Database 610
Fail Over Detector 604
Configuration Manager 603
Business Editor 609
Transaction Layer Engine 608
Transaction Writer 607
CDR Reader 606
Rules Processor 605
Content Detail Record Database 215

Figure 6

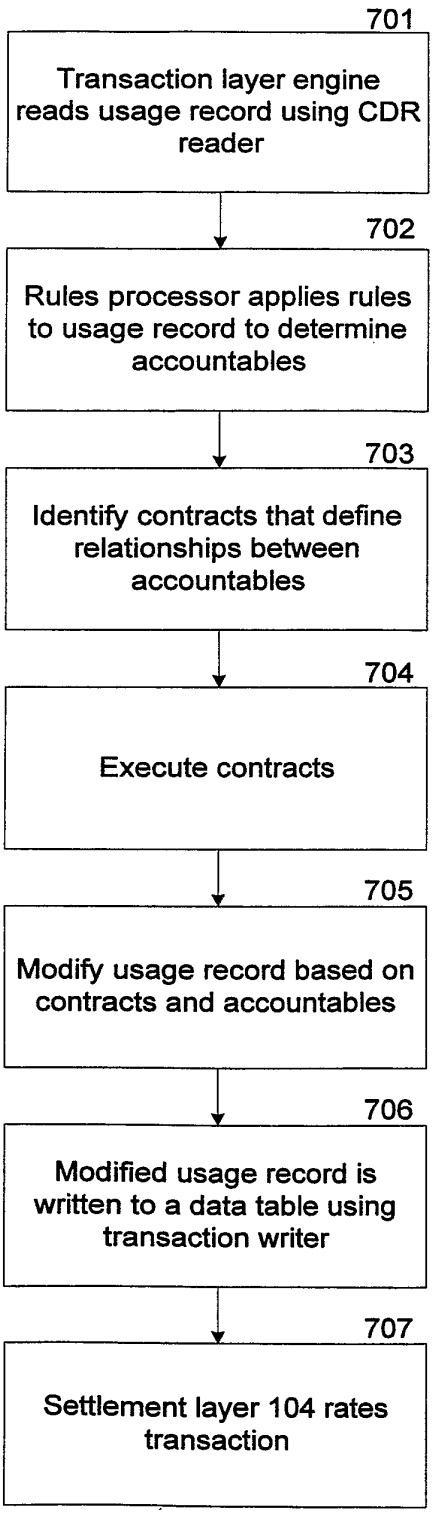

701
Transaction layer engine reads usage record using CDR reader
702
Rules processor applies rules to usage record to determine accountables
703
Identify contracts that define relationships between accountables
704
Execute contracts
705
Modify usage record based on contracts and accountables
706
Modified usage record is written to a data table using transaction writer
707
Settlement layer 104 rates transaction
700

Figure 7

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

(11) EP 1 545 114 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
22.06.2005 Bulletin 2005/25

(51) Int Cl.[7]: **H04M 15/00**, H04Q 3/00

(21) Application number: **04027514.1**

(22) Date of filing: **19.11.2004**

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

(30) Priority: **19.12.2003 CN 200310122726**

(71) Applicant: **ALCATEL**
75008 Paris (FR)

(72) Inventors:
- **ShuGuang, Jin,**
  CTO, Alcatel Shanghai Bell Co. Ltd.
  201206 Shanghai (CN)
- **Yan, Chen, CTO, Alcatel Shanghai Bell Co. Ltd.**
  201206 Shanghai (CN)
- **Peiliang, Xu, CTO, Alcatel Shanghai Bell Co. Ltd.**
  201206 Shanghai (CN)

(74) Representative:
Dreiss, Fuhlendorf, Steimle & Becker
Patentanwälte
Postfach 10 37 62
70032 Stuttgart (DE)

(54) A method and apparatus for division of revenue of communication among different proprietors

(57) A method and apparatus for division of revenue of communication among different proprietors is provided in this invention, where the division of revenue among the different proprietors is performed by a gateway office, wherein the gateway office will set a source parameter and a destination parameter respectively from the source and the destination when a call goes through the gateway office; Judge the two parameters to get a revenue zone index; Judge the value of the revenue zone index, and modulate the revenue zone index to get a revenue class index; The gateway office generates contents related to the revenue class index; A central memory receives all these contents, adds an increment of each counter of the revenue class memory related to the revenue class index to a corresponding counter and carries out multiple safety mechanisms; Output the information in the revenue class memory to a storage medium for storing, then output it to a billing center for revenue sorting. The billing mode present in this invention is based on group pairs, so it is more adaptive for the gateway office to divide revenue.

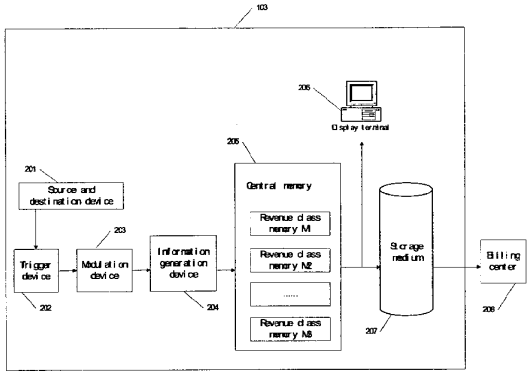


Fig. 2

Printed by Jouve, 75001 PARIS (FR)

EP 1 545 114 A1

Description

TECHNICAL FIELD

[0001] The present invention relates to a method and apparatus for division of revenue of telecommunication among different proprietors.

RELATED ART

[0002] As to the relay jumping table billing, in the SPC exchange, it takes relay groups (income and outgoing) as revenue billing units, and accumulates all metering impulses of the relay group as the billing content. Although this technology is simple, it is not able to provide enough flexibility in resource sorting and billing content selecting.

[0003] As to the detail billing, in the SPC exchange, it generates a detail record for each call. All these records (telephone billing list) will be sent out from the SPC exchange after a specific period. A specific sorting department sorts all received telephone billing list, which will be treated as the billing content after sorting and summation. It can satisfy all kinds of user's customized demands, but there is a large number of temporary data transferring between the SPC exchange and the sorting department, and the investments on the equipments will be expanded greatly in order to satisfy demands.

SUMMARY OF THE INVENTION

[0004] In order to solve said problems of existing technology, this invention provides all kinds of methods for the division of revenue at the SPC exchange level of the gateway office, to satisfy various potential billing demands among the proprietors. Moreover, it is needless for proprietors to add investments immediately to meet with the additional demands for detail billing because of this demand.

[0005] The present invention provides a method for division of revenue of communication among different proprietors, wherein the division of revenue among the different proprietors is performed by a gateway office, the method comprising that:

a) When a call goes through the gateway office, the gateway office gets a source of a calling user and a destination of a called user respectively from different proprietors, and extracts a source parameter and a destination parameter from the source and the destination;

b) The gateway office judges values of the source parameter and the destination parameter as said in step a), and if there is one of values of the parameters corresponding to a parameter value for stopping a function on the division of revenue, the division of revenue function is stopped, otherwise, a corresponding revenue zone index is obtained according to said source parameter and destination parameter and step c) is executed;

c) The gateway office judges a value of the revenue zone index as said in step b), if it corresponds to the parameter value for stopping the division of revenue function, the revenue division function is stopped, otherwise, said revenue area index is modulated according to said call, a corresponding revenue class index R_j, j=1, 2...n is obtained, and step d) is executed;

d) The gateway office generates contents related to the revenue class index R_j as said in step c), and sends the contents to a central memory of the gateway office after said calling is finished;

e) The central memory of the gateway office receives the contents related to said revenue class index R_j as said in step d), and based on these contents, adds an increment of each counter in revenue class memory M_j (j=1,2... n) related to the revenue class index R_j to the corresponding counter and performs multiple safety mechanisms;

f) The central memory sends information in the revenue class memory M_j obtained in step e) to a storage medium. The storage medium stores the information with a predefined formatted scheme and sends the information to a billing center for sorting the revenue

wherein in said step c), said revenue zone index is modulated by a modulation parameter or several modulation parameters, and the obtained revenue class index varies with different modulation parameters which include type of call, bear capacity, high level carrying(HLC), analog or ISDN user.

wherein in said step d), said contents related to the revenue class index R_j as said in step c) include static and dynamic information on the call as said in step a);

[0006] In said step e), the revenue class memory M_j (j=1, 2...n) is set according to user's needs during initialization in the gateway office;

[0007] In said step f), the central memory sends the information in the revenue class memory M_j as said in step e) to a display terminal.

wherein in said step e), the multiple safety mechanisms include:

[0008] The central memory introducing a windowing mechanism during a receiving procedure;

[0009] The accumulation of each counter having a hot backup;

[0010] Each counter backups its information to a pair of hard disks with specific intervals.

wherein in said step f), the predefined formatted scheme is either a general scheme or a scheme customized according to user's needs.

[0011] The present invention provides an apparatus for division of revenue of communication among different proprietors, wherein the division of revenue among the different proprietors is performed by a gateway office, the apparatus comprising a source and destination device located in the gateway office, and further a trigger device, a modulation device, an information generation device□a central memory and a storage medium which are all located in the gateway office, wherein:

[0012] When a call goes through the gateway office, the source and destination device located in the gateway office respectively extracts a source parameter and a destination parameter according to a source of calling user and a destination of called user;

[0013] The trigger device judges values of the source parameter and the destination parameter, and if there is one of the values of the parameters corresponding to a parameter value for stopping a function on the division of revenue , the revenue division is stopped, otherwise, a corresponding revenue zone index is obtained according to said source parameter and destination parameter, and then judges a value of said revenue zone index, if it corresponds to the parameter value for stopping the revenue division function, t the revenue division function is stopped, otherwise, said revenue zone index is sent to the modulation device;

[0014] The modulation device, according to said call, modulates said revenue area index from the trigger device, and obtains the corresponding revenue class index R_j, j=1, 2...n;

[0015] The information generation device, according to said revenue class index R_j, j=1, 2...n, generates contents related to said revenue class index R_j, and sends them to the central memory after said call is finished;

[0016] The central memory receives the contents related to said revenue class index R_j, and based on these contents, adds an increment of each counter in revenue class memory M_j (j=1,2...n) related to the revenue class index R_j to the corresponding counter, and performs multiple safety mechanisms, and then sends information in said revenue class memory M_j to the storage medium;

[0017] The storage medium stores the information in said revenue class memory M_j with a predefined formatted scheme and sends the information to a billing center for sorting the revenue.

wherein said revenue zone index is modulated in the modulation device by a modulation parameter or several modulation parameters, and the obtained revenue class index varies with different modulation parameters which include type of call, bear capacity, high level carrying(HLC), analog or ISDN user.

[0018] Wherein said contents related to the revenue class index R_j include static and dynamic information on the said call;

[0019] Said revenue class memory M_j (j=1, 2...n) is set according to user's needs during initialization in the gateway office;

[0020] Said apparatus also includes a display terminal, which is used to display the information in said revenue class memory M_j.

wherein said multiple safety mechanisms include:

[0021] The central memory introducing a windowing mechanism during a receiving procedure;

[0022] The accumulation of each counter having a hot backup;

[0023] Each counter backups its information to a pair of hard disks with specific intervals.

wherein the predefined formatted scheme is either a general scheme or a customized scheme according to user's needs.

[0024] The division of revenue of this invention is a kind of billing method based on group pairs, making it more adaptive for gateway offices to divide revenue. Moreover, the division of revenue method present in this invention is not only based on relays, but it can also be realized by other billing units, comparing to the present technology whose billing unit is simply based on relays. The revenue class in this invention is abstract, and can be a mixture of several different entity types. Besides, the present invention also adopts a new normalized input and output format for the division of revenue.

DESCRIPTION OF THE DRAWINGS

[0025]

Fig .1 is a flowchart illustrating different proprietors realizing division of revenue by the gateway office in accordance with a preferred embodiment of the invention;

Fig .2 is a map of the gateway office realizing division of revenue in accordance with a preferred embodiment of the invention;

Fig .3 is a flowchart illustrating the safety mechanisms of the central memory in accordance with a preferred embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

[0026] This invention will be further explained with reference to the drawings and an embodiment.

[0027] This invention provides a method and a apparatus for division of revenue of communication among different proprietors, wherein the division of revenue among the different proprietors is performed by a gateway office.

[0028] Here, the gateway office is an interface exchanging office carrying out transmission of telephone services among different proprietors. For instance, a user of the Shanghai Mobile makes a call to another fixed phone user of the Shanghai Telecom, which will reach the fixed phone user via a gateway office between the two companies. Since the Shanghai Telecom proprietor has supplied its resource, it will count this kind of resource at the gateway office, and then come to a settlement with the Shanghai Mobile for the revenue. Therefore, the main function of the gateway office is to separately count resources occupied and divide revenue among different proprietors. At the same time, it also provides other gateway services such as the call identification authority and black/white list. The Division of Revenue (DOR) is used to count communication resource among different proprietors.

[0029] As shown in Fig.1, the user 101 is a user of the proprietor A 102 and the user 105 is a user of the proprietor B 104. When a call from the calling user 101 to the called user 104 go in and out from the gateway office 103, the gateway office 103 will get a source from the proprietor A, such as Beijing, and get a destination from the proprietor B, such as Shanghai.

[0030] Fig.2 is a map of the gateway office implementing division of revenue in accordance with an embodiment of the invention, including a source and destination device 201, a billing center 208, which are existing technology, and a trigger device 202, a modulation device 203, an information generation device 204, a central memory 205, a display terminal 206 and a storage medium 207, which are added in this invention. As shown in Fig.2, the source and destination device 201 of the gateway office 103 gets a source parameter and a destination parameter respectively from the source and the destination, which is a numeric value (0-255). For example, if the source is Beijing, the value of the source parameter is "1", and if the destination is Shanghai, the value of the destination parameter is "2".

[0031] At this time the route is already elected to pass, namely when the called user starts ringing, the trigger device 202 of the gateway office 103 judges the value of source and destination parameters. If there is a parameter's value corresponding to the value for stopping the division of revenue function, for example, in this embodiment, if there is a parameter whose value is 0, the division of revenue function is stopped. Those users who do not need this function shield it to consume the least resources. Otherwise, the trigger device 202 obtains a revenue zone parameter according to the source parameter and the destination parameter, as show in table 1.

Source \ Destination	Beijing	Shanghai	...	...
Beijing	X1 (north china revenue zone index(1))	X2 (north china-east china revenue zone index (2))	...	...
Shanghai	X3 (east china - north china revenue index (3))	X4 (east - china revenue zone index (4))	...	...
...	...	...	...	...
...	...	...	...	Xn

Table.1

[0032] x_1, x_2, x_3, x_4 ... x_n in the table 1 are revenue zone indices. In this embodiment, the source is Beijing (1) and the destination is Shanghai (2). The trigger device 202 judges the source parameter value and the destination parameter value, if neither of them is zero, the corresponding revenue zone index x_2 is obtained, namely North China - East China revenue zone index, whose revenue zone index value is "2". As shown in table 1, in this invention, the revenue zone indices with different values can simply correspond to the different revenue class indices, which means obtaining many different revenue class indices. In existing technology, if the source and the destination are respectively output relay group and input relay group, it realizes the relay jump table function, and the largest number of the relay group soft table is 10 or 14. In this invention, we can dynamically assign many revenue class indices to one input relay group + several destinations, or to one output relay group + several sources, which actually means a relay group can have the nearly infinite number of the soft tables. This already breaks through the number limitation of the relay group soft table,

which is 10 or 14 in the existing technology, therefore, this invention actually functions better than the current relay jump table technology.

[0033] The trigger device 202 judges the revenue zone index value, if the value is 0, the function of division of revenue is stopped. This is helpful to users' flexible choice, and save system resource to the greatest extent. Otherwise, the modulation device 203 will modulate the revenue zone index. For instance, in this embodiment, the value of the revenue zone index x_2 is "2", not "0", so x_2 is modulated. Refer to table 2 for detailed modulation process.

[0034] As shown in table 2, for instance, proprietors are interested in the voice service of this call, namely require to count and charge the voice service, then said revenue zone index is modulated with one of the modulation parameters and the corresponding revenue class index R_j, j=1, 2...n is obtained. In this embodiment, the revenue zone index x_2 is modulated with the type of call (voice) modulation parameter and the corresponding revenue class index R1 is obtained, which corresponds to the voice service of the DDD call, namely the DDD call list. Furthermore, if there are other calls corresponding to the ISDN call, the revenue zone index x_2 will be modulated with the type of call (voice) modulation parameter, and the corresponding revenue class index R2 will be obtained, which means R2 corresponds to the voice service of the ISDN, namely the ISDN call list.

Revenue zone index	Type of call	Revenue class index	Billing list
X2 (north china- east china revenue zone index(2))	Type of call (voice)	R1 (east china - north china revenue class index (1)) (DDD call)	DDD billing list
		R2 (east china - north china revenue class index (2)) (ISDN call)	ISDN billing list
		R3 (east china - north china revenue class index (3)) (IN call)	IN billing list
		...	...

		R4 (east china - north china revenue class index (n)) (other types of call)	Other types of billing lists

Table.2

[0035] This invention provides an extremely flexible modulation method, wherein said modulating characteristics in this invention means modulating said revenue zone index using one or several modulation parameters, and the different corresponding revenue class indices by different combinations of these modulation parameters are obtained. The purpose of the modulation is to further conclude and arrange all revenue by different modulation parameters, and make revenue sortable according to the proprietor's demand, namely to perform revenue class indexing. At the end, various billing data will be obtained through different revenue class indices. The modulation parameters can be type of call (voice), bear capacity, high level carrying(HLC), analog or ISDN user and so on.

[0036] Said modulation in this invention is carried out during the calling process. In the existing technology, the relationship between each revenue zone index and revenue class index is usually one-to-one correspondence, which could satisfy the demand of most users. In this case, the modulation step can be ignored.

[0037] After the called user 105 gives reply, and before the call is released, the information generation device 204 of the gateway office 103 generates contents related to said revenue class index, such as R1, which include static and dynamic information on the call. The static information contains the modulating characteristics as shown in table 2, the calling number, the called number, the route and so on, the dynamic information contains the call holding time, the answering time and so on. These static information and dynamic information related to the call will be sent to the central memory 205 of the gateway office 103 after the call is finished.

[0038] After the call is released, namely the call is finished, the central memory 205 of the gateway office 103 receives these contents related to said revenue class index R_j, and based on these contents, adds the increment values of every counter of the revenue class memory M_j (j=1, 2...n), which is related to said revenue class index R_j, to the corresponding counter. For example, in this call there are several counters in the revenue class memory M1 corresponding to the revenue class index R1 of the central memory 205, such as a total-number-of-calls counter□total-length-of-calls counter, etc, which respectively accumulate the total number of calls and the total length of calls, based on this call. This revenue class memory M_j (j=1, 2...n) is set according to users' needs during the gateway office initializing procedure.

[0039] Because of the importance of the resource, multiple safety mechanisms are performed in the present invention, which including: The central memory 205 introduces a windowing mechanism during the receiving procedure. The accumulation of each counter has a hot backup, as shown in Fig.3, the central memory 205 is comprised of primary central storage region 301, hot backup central storage region 302, primary hard disk 305 and standby hard disk 307, the primary central storage region 301 and the hot backup central storage region 302 stores at the same time, as arrow 303 shows, one-region working task can be performed under certain circumstances. However, synchronous working starts as soon as the two-region working task takes over.Each counter backups its information to a pair of hard disks with specific intervals, namely to the primary hard disk 305 and the standby hard disk 306, the backuping task is executed by the primary central storage region 301, as arrow 304 shows. Since these safety mechanisms are existing technology, just a simply introduction is provided.

[0040] The central memory 205 sends the information of said revenue class memory M_j to the storage medium 207, which stores the information with reference to a predefined formatted scheme and sends the information to the billing center 208 for revenue sorting the same way as other bill documents. The central memory 205 also can send the information of said revenue class memory M_j to the display terminal 206. For example, display contents of each counter of the revenue class memory M_j through display terminal 206, then the network resource occupation situation of each

proprietor can be observed directly and instantly, which realizes flexible online operation. The revenue sorting here means arranging the billing data (such as the detailed billing phone list, the double counting jump table file, all said revenue class indices) generated in the gateway office in a document, sending the entire document to the billing center 208, where the document will be operated according to the predefined procedure and reorganized into a list of each revenue class and the corresponding total number of calls, total length of calls.

[0041] The predefined format can be a general style, as shown in table 3, the first part is a file header, such as information indicating the revenue dividing category, information on the file generation time, information labeling the local gateway office, etc. The following is a revenue class index sequence, the last part is a file trailer, such as an end-of-file indicator; The format can also be a customized style according to the user's need, as shown in table 4, the first part is a file header, such as information indicating the revenue dividing category, information on the file generation time, information labeling the local gateway office, etc, the following is a each revenue class index arranged in an order of the relay group and the bear type, the last part is a file trailer, such as an end-of-file indicator.

Table.3

<table>
<tr><td colspan="2">File header (such as: such as information indicating the revenue dividing category, information on the file generation time, information labeling the local gateway office, etc)</td></tr>
<tr><td rowspan="4">Arranging each revenue class index in order</td><td>Revenue class index sequence number 1</td></tr>
<tr><td>Total number of calls</td></tr>
<tr><td>Total length of calls</td></tr>
<tr><td>Total number of pulses</td></tr>
<tr><td>...</td><td>...</td></tr>
<tr><td colspan="2">File trailer (such as end-of-file indicator)</td></tr>
</table>

Table.4

<table>
<tr><td colspan="2">File header (such as: such as information indicating the revenue dividing category, information on the file generation time, information labeling the local gateway office, etc)</td></tr>
<tr><td rowspan="4">Arranging each revenue class index in an order of the relay group and the bear type</td><td>Revenue class index sequence number (1, 2, 3)</td></tr>
<tr><td>Corresponding relay group name</td></tr>
<tr><td>Corresponding bear type</td></tr>
<tr><td>Total number of calls</td></tr>
<tr><td rowspan="2"></td><td>Total length of calls</td></tr>
<tr><td>Total number of pulses</td></tr>
<tr><td>...</td><td>...</td></tr>
<tr><td colspan="2">File trailer (such as end-of-file indicator)</td></tr>
</table>

[0042] Therefore, the output format adopted in this invention greatly meets the users' demand, and makes it very convenient for the users to introduce this new function. Moreover, the output format can be customized to meet the needs of various high-end users. The output format provides more options, such as bureau name, file generation time, relay group name and other specific information, making it more supportive to on-line transmission.

[0043] More detailed steps corresponding to the embodiment of this invention are as follows:

a) When a call goes through the gateway office, the gateway office gets a source of a calling user and a destination of a called user respectively from different proprietors, and extracts a source parameter and a destination parameter from the source and the destination;

b) The gateway office judges values of the source parameter and the destination parameter as said in step a), and if there is one of values of the parameters corresponding to a parameter value for stopping a function on the division of revenue, the division of revenue function is stopped, otherwise, a corresponding revenue zone index is obtained according to said source parameter and destination parameter and step c) is executed;

c) The gateway office judges a value of the revenue zone index as said in step b), if it corresponds to the parameter value for stopping the division of revenue function, the revenue division function is stopped, otherwise, said revenue

area index is modulated according to said call, a corresponding revenue class index R_j, j=1, 2...n is obtained, and step d) is executed;

d) The gateway office generates contents related to the revenue class index R_j as said in step c), and sends the contents to a central memory of the gateway office after said calling is finished;

e) The central memory of the gateway office receives the contents related to said revenue class index R_j as said in step d), and based on these contents, adds an increment of each counter in revenue class memory M_j (j=1,2...n) related to the revenue class index R_j to the corresponding counter and performs multiple safety mechanisms;

f) The central memory sends information in the revenue class memory M_j obtained in step e) to a storage medium. The storage medium stores the information with a predefined formatted scheme and sends the information to a billing center for sorting the revenue

[0044] As to a medium-sized gateway office (10 hours when busy, 100CAPS bill list), the data volume ratio of detail billing in existing technology to the division of revenue in the present invention is over 100:1.

[0045] The present invention also greatly reduces the massive dump of the exchanger, the mass data processing of the sorting center and the mass data storage and transmission, saving various resources.

[0046] The division of revenue of this invention is a kind of billing method based on group pairs, making it more adaptive for gateway offices to divide telecommunication revenue. Moreover, the division of revenue method present in this invention is not only based on relays, but it can also be realized by other billing units, comparing to the exiting technology whose billing unit is simply based on relays.

[0047] It should be understood that the said embodiment has been presented by way of example only, and not limitation. Thus, all modifications that fall within the scope of this invention are intended to be included therein.

Claims

1. A method for division of revenue of communication among different proprietors, wherein the division of revenue among the different proprietors is performed by a gateway office, the method comprising that:

   a) When a call goes through the gateway office, the gateway office gets a source of a calling user and a destination of a called user respectively from different proprietors, and extracts a source parameter and a destination parameter from the source and the destination;

   b) The gateway office judges values of the source parameter and the destination parameter as said in step a), and if there is one of values of the parameters corresponding to a parameter value for stopping a function on the division of revenue, the division of revenue function is stopped, otherwise, a corresponding revenue zone index is obtained according to said source parameter and destination parameter and step c) is executed;

   c) The gateway office judges a value of the revenue zone index as said in step b), if it corresponds to the parameter value for stopping the division of revenue function, the revenue division function is stopped, otherwise, said revenue area index is modulated according to said call, a corresponding revenue class index R_j, j=1, 2...n is obtained, and step d) is executed;

   d) The gateway office generates contents related to the revenue class index R_j as said in step c), and sends the contents to a central memory of the gateway office after said calling is finished;

   e) The central memory of the gateway office receives the contents related to said revenue class index R_j as said in step d), and based on these contents, adds an increment of each counter in revenue class memory M_j (j=1,2...n) related to the revenue class index R_j to the corresponding counter and performs multiple safety mechanisms;

   f) The central memory sends information in the revenue class memory M_j obtained in step e) to a storage medium. The storage medium stores the information with a predefined formatted scheme and sends the information to a billing center for sorting the revenue.

2. The method according to claim 1, wherein in said step c), said revenue zone index is modulated by a modulation parameter or several modulation parameters, and the obtained revenue class index varies with different modulation parameters which include type of call, bear capacity, high level carrying(HLC), analog or ISDN user.

3. The method according to claim 1, wherein in said step d), said contents related to the revenue class index R_j as said in step c) include static and dynamic information on the call as said in step a);

   In said step e), the revenue class memory M_j (j=1, 2...n) is set according to user's needs during initialization in the gateway office;

   In said step f), the central memory sends the information in the revenue class memory M_j as said in step e)

to a display terminal.

4. The method according to claim 1, wherein in said step e) the multiple safety mechanisms include:

The central memory introducing a windowing mechanism during a receiving procedure;
The accumulation of each counter having a hot backup;
Each counter backups its information to a pair of hard disks with specific intervals.

5. The method according to claim 1, wherein in said step f), the predefined formatted scheme is either a general scheme or a scheme customized according to user's needs.

6. An apparatus for division of revenue of communication among different proprietors, wherein the division of revenue among the different proprietors is performed by a gateway office, the apparatus comprising a source and destination device located in the gateway office, and further a trigger device, a modulation device, an information generation device, a central memory and a storage medium which are all located in the gateway office, wherein:

When a call goes through the gateway office, the source and destination device located in the gateway office respectively extracts a source parameter and a destination parameter according to a source of calling user and a destination of called user;
The trigger device judges values of the source parameter and the destination parameter, and if there is one of the values of the parameters corresponding to a parameter value for stopping a function on the division of revenue ,the revenue division is stopped, otherwise, a corresponding revenue zone index is obtained according to said source parameter and destination parameter, and then judges a value of said revenue zone index, if it corresponds to the parameter value for stopping the revenue division function, the revenue division function is stopped, otherwise, said revenue zone index is sent to the modulation device;
The modulation device, according to said call, modulates said revenue area index from the trigger device, and obtains the corresponding revenue class index R_j, j=1, 2...n;
The information generation device, according to said revenue class index R_j, j=1, 2...n, generates contents related to said revenue class index R_j, and sends them to the central memory after said call is finished;
The central memory receives the contents related to said revenue class index R_j, and based on these contents, adds an increment of each counter in revenue class memory M_j (j=1,2...n) related to the revenue class index R_j to the corresponding counter, and performs multiple safety mechanisms, and then sends information in said revenue class memory M_j to the storage medium;
The storage medium stores the information in said revenue class memory M_j with a predefined formatted scheme and sends the information to a billing center for sorting the revenue.

7. The apparatus according to claim 6, wherein said revenue zone index is modulated in the modulation device by a modulation parameter or several modulation parameters, and the obtained revenue class index varies with different modulation parameters which include type of call, bear capacity, high level carrying(HLC), analog or ISDN user.

8. The apparatus according to claim 6, wherein:

Said contents related to the revenue class index R_j include static and dynamic information on the said call;
Said revenue class memory M_j (j=1, 2...n) is set according to user's needs during initialization in the gateway office;
Said apparatus also includes a display terminal, which is used to display the information in said revenue class memory M_j.

9. The apparatus according to claim 6, wherein said multiple safety mechanisms include:

The central memory introducing a windowing mechanism during a receiving procedure;
The accumulation of each counter having a hot backup;
Each counter backups its information to a pair of hard disks with specific intervals.

10. The apparatus according to claim 6, wherein the predefined formatted scheme is either a general scheme or a customized scheme according to user's needs.

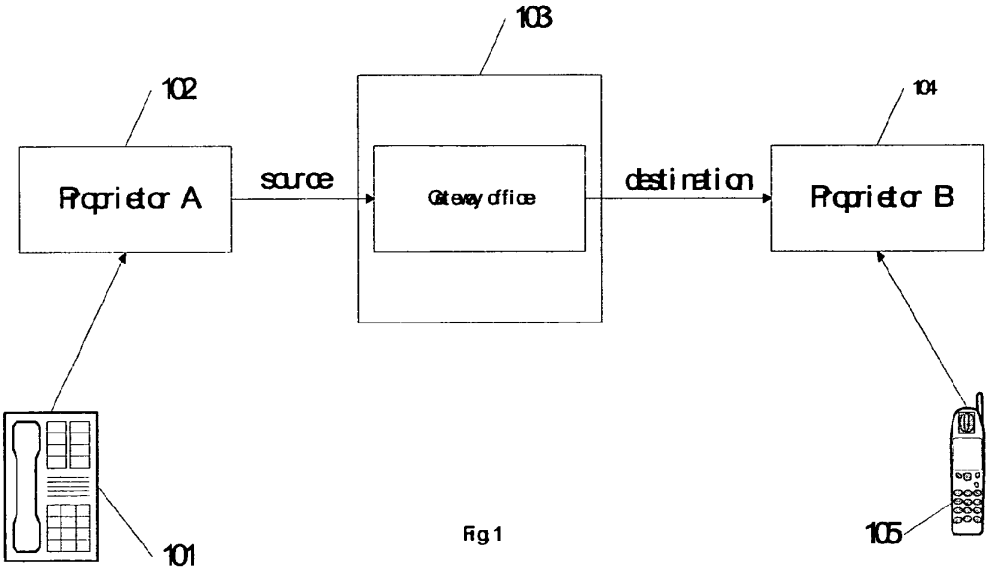

103
102
104
Proprietor A
source
Gateway office
destination
Proprietor B
101
105

Fig 1

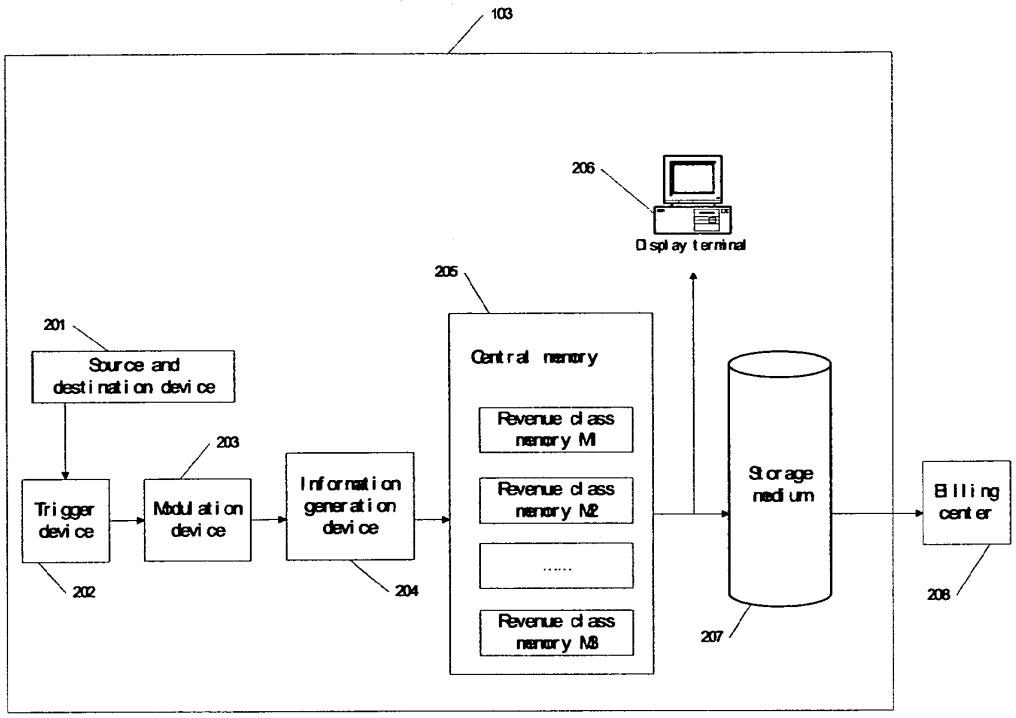

103
206
Display terminal
205
201
Source and destination device
Central memory
Revenue class memory M1
203
Trigger device
Modulation device
Information generation device
Revenue class memory M2
.....
Revenue class memory M3
Storage medium
Billing center
202
204
207
208

Fig. 2

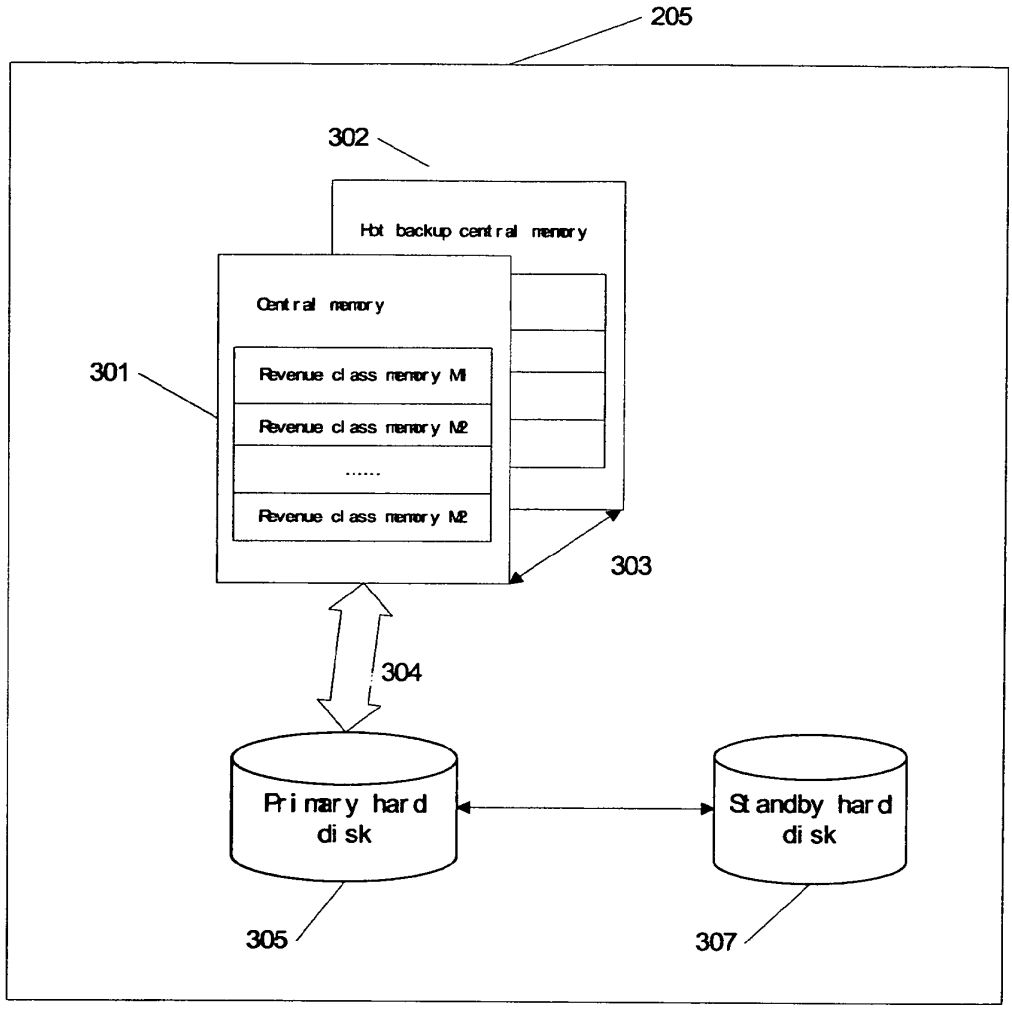

205
302
Hot backup central memory
Central memory
301
Revenue class memory M1
Revenue class memory M2
.....
Revenue class memory M2
303
304
Primary hard disk
Standby hard disk
305
307

Fig. 3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 04 02 7514

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)
A	US 5 768 353 A (BROWNE ET AL) 16 June 1998 (1998-06-16) * column 1, line 33 - column 3, line 26 * * column 5, line 25 - column 7, line 39 * * column 10, line 22 - column 15, line 58 * * claims 1-17 *	1-10	H04M15/00 H04Q3/00
P,A	US 2004/033797 A1 (RAIVISTO TOMMI ET AL) 19 February 2004 (2004-02-19) * claims 1-20 * * figures 1,2 *	1-10	
A	EP 0 483 091 A (ERICSSON - GE MOBILE COMMUNICATIONS HOLDING INC; ERICSSON INC) 29 April 1992 (1992-04-29) * column 2, line 30 - line 47 * * claims 1-3 *	1-10	
A	WO 03/049351 A (CIBERNET, INC) 12 June 2003 (2003-06-12) * page 10, line 3 - page 11, line 29 * * page 12, line 21 - page 13, line 13 * * page 14, line 29 - page 16, line 28 * * page 18, line 1 - page 23, line 16 * * page 41, line 15 - page 44, line 7 * * figures 1-4,9 *	1-10	TECHNICAL FIELDS SEARCHED (Int.Cl.7) H04M H04Q
P,A	US 2004/210522 A1 (BISSANTZ ANNETTE S ET AL) 21 October 2004 (2004-10-21) * paragraph [0027] - paragraph [0029] *	1-10	
A	US 6 134 307 A (BROUCKMAN ET AL) 17 October 2000 (2000-10-17) * column 4, line 13 - column 5, line 17 *	1-10	

-/--

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	19 April 2005	Patlaka, E.

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 04 02 7514

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)
A	EP 0 569 175 A (AMERICAN TELEPHONE AND TELEGRAPH COMPANY; AT&T CORP) 10 November 1993 (1993-11-10) * column 6, line 24 - column 7, line 19 * * figure 5 * * claims 1-3 *	1-10	
A	US 5 910 979 A (GOEL ET AL) 8 June 1999 (1999-06-08) * claims 1-3 *	1-10	
			TECHNICAL FIELDS SEARCHED (Int.Cl.7)

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	19 April 2005	Patlaka, E.

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)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 04 02 7514

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.

19-04-2005

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5768353 A	16-06-1998	AU 697367 B2	01-10-1998
		AU 6383094 A	24-10-1994
		AU 697499 B2	08-10-1998
		AU 6383194 A	24-10-1994
		CA 2159000 A1	13-10-1994
		CA 2159002 A1	13-10-1994
		CN 1122639 A ,C	15-05-1996
		CN 1122640 A ,C	15-05-1996
		DE 69404452 D1	28-08-1997
		DE 69404452 T2	15-01-1998
		DE 69433814 D1	01-07-2004
		DK 692172 T3	02-03-1998
		EP 0692172 A1	17-01-1996
		EP 0692173 A1	17-01-1996
		ES 2107200 T3	16-11-1997
		FI 954627 A	09-11-1995
		FI 954628 A	10-11-1995
		WO 9423529 A1	13-10-1994
		WO 9423530 A1	13-10-1994
		HK 1001747 A1	03-07-1998
		HK 1014410 A1	11-03-2005
		JP 8508619 T	10-09-1996
		JP 8508620 T	10-09-1996
		JP 2002199130 A	12-07-2002
		NO 953898 A	29-11-1995
		NO 953899 A	29-11-1995
		NZ 263224 A	26-07-1996
		NZ 263225 A	26-01-1998
		SG 48839 A1	18-05-1998
		SG 50490 A1	20-07-1998
		US 5802142 A	01-09-1998
		US RE37856 E1	24-09-2002
		US RE37857 E1	24-09-2002
US 2004033797 A1	19-02-2004	AU 2003255864 A1	25-02-2004
		WO 2004015971 A1	19-02-2004
EP 0483091 A	29-04-1992	CA 2098191 A1	02-05-1993
		US 5063591 A	05-11-1991
		CN 1061692 A ,C	03-06-1992
		CN 1108851 A ,C	20-09-1995
		EP 0483091 A2	29-04-1992
		NZ 240072 A	25-02-1994
		WO 9309639 A1	13-05-1993
		DE 69127161 D1	11-09-1997
		DE 69127161 T2	18-12-1997

EPO FORM P0459

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

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 04 02 7514

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.

19-04-2005

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0483091 A		ES 2107448 T3	01-12-1997
		HK 1001948 A1	17-07-1998
WO 03049351 A	12-06-2003	US 2003120594 A1	26-06-2003
		AU 2002365834 A1	17-06-2003
		WO 03049351 A2	12-06-2003
US 2004210522 A1	21-10-2004	NONE	
US 6134307 A	17-10-2000	NONE	
EP 0569175 A	10-11-1993	US 5333184 A	26-07-1994
		CA 2092590 A1	07-11-1993
		DE 69332461 D1	12-12-2002
		DE 69332461 T2	28-08-2003
		EP 0569175 A2	10-11-1993
		ES 2184736 T3	16-04-2003
		JP 2795596 B2	10-09-1998
		JP 6037936 A	10-02-1994
US 5910979 A	08-06-1999	NONE	

EPO FORM P0459

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

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

(11) EP 1 887 732 A1

(12) EUROPEAN PATENT APPLICATION

published in accordance with Art. 153(4) EPC

(43) Date of publication:
13.02.2008 Bulletin 2008/07

(21) Application number: **06742044.8**

(22) Date of filing: **30.05.2006**

(51) Int Cl.:
H04L 12/14 *(2006.01)*

(86) International application number:
PCT/CN2006/001156

(87) International publication number:
WO 2006/128371 (07.12.2006 Gazette 2006/49)

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

(30) Priority: **30.05.2005 CN 200510073415**

(71) Applicant: **Huawei Technologies Co., Ltd.**
Longgang District
Shenzhen
Guangdong 518129 (CN)

(72) Inventor: **ZHAO, Hang,**
Huawei Administration Building
Shenzhen Guangdong 518129 (CN)

(74) Representative: **Pfenning, Meinig & Partner GbR**
Patent- und Rechtsanwälte
Theresienhöhe 13
80339 München (DE)

(54) A METHOD AND SYSTEM FOR CONTENT CHARGING

(57) A method for content charging includes: the portal server transmits the service activation request to the policy server based on the request for user using the service; the policy server determines the service policy corresponding to the service request after responding to the service activation request and distributes the service policy activation message to the content control gateway; the content control gateway performs the service policy and reports the user service usage message to the policy server; the policy server performs the charging according to the user service usage message. The solution provided by the present invention can realize the exact and low-cost charging for the content service and meet the requirement of QoS dynamic adjustment of the content service.

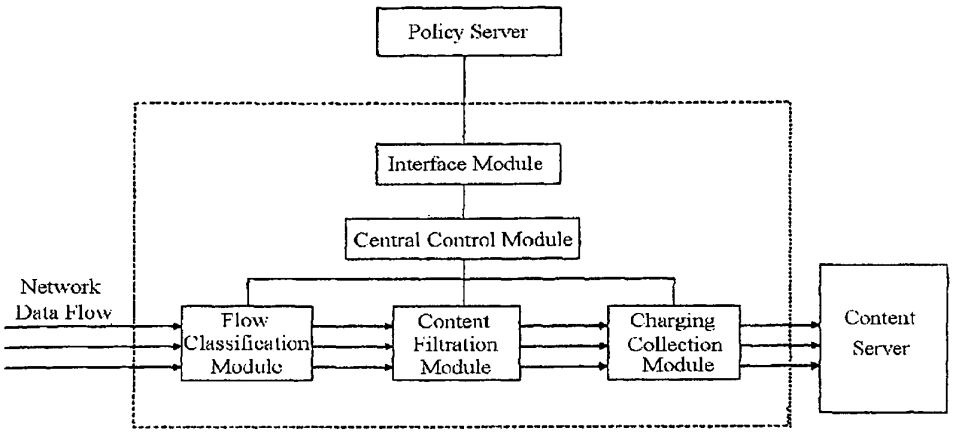


Fig.3

EP 1 887 732 A1

Printed by Jouve, 75001 PARIS (FR)

Description

Field of the Invention

[0001] The present invention relates to the technical field of network communications, in particular, to a method and a system for content charging.

Background of the Invention

[0002] With the rapid development of the Internet, content services become more and more abundant. Correspondingly, Internet Content Providers (ICPs) for getting profit by providing contents come on the scene. By cooperating with the ICP, service providers may increase the income of the access service by expanding the scale of network userson one hand, and earn the profit sharing of content income of the ICP on the other hand. At the same time, the ICP may obtain a low-cost channel for selling its content service rapidly.

[0003] The content platform of the service provider is developed on such background. The general mode of the content platform is as follows: The service provider provides a technical platform, and the ICP issues its content service via this platform. The service provider performs advertising, authentication, charging for the use of the content service via the platform. The user uses the content service provided by each ICP via the platform. The content platform records various fees caused by the user, and all of the fees will be recorded on a content account provided to the user by the service provider. With this content platform, the user does not need to settle accounts with each ICP; instead, the user only needs to settle accounts with the service provider.

[0004] The existing content charging solution for this content platform is usually implemented as follows:

[0005] A user connects to the network, logs in a portal website Portal Server, and connects to a Content Server of an ICP via a content channel. If the user is interested in a content provided by the ICP, then he/she clicks the button "OK", and the ICP Content Server will send an authentication request to the content platform of the service provider. If the authentication is passed, the right to use the content is assigned to the user and a charging start message is sent to the content platform.

[0006] To ensure the accuracy of the charging, the Content Server of the ICP sends an intermediate charging message to the content platform at a certain time interval during the usage of the content. When the user logs out the Content Server, the Content Server of the ICP sends a charging completion message to the content platform.

[0007] The content platform processes the charging message in real time, and performs rating and accounting on the content consumption of the user according to the information in the charging message such as service number, time length traffic flow, etc., together with the charging policy of the service.

[0008] In the prior art, strict requirements are laid on the interconnection technology between the content platform and the ICP. The ICP has to carry out customized development according to the content platform authentication and charging interface provided by the service provider, and joint debugging and testing should be performed after the development. Services may only be formally issued after the testing is passed. Thus, the cost is very high.

[0009] Some small-scale ICPs are weak in technical strength and they are not able to carry out customized development according to the charging interface. Some other ICPs purchase their service contents, such as multiplayer-fighting games, from other software company, so they have no source code for interface development, and are not able to implement content charging for such services.

[0010] Quality of Service (QoS) is required for some content services. For example, Video On Demand (VOD) service requires a broad bandwidth. However, in the mode aforementioned, the bandwidth may not be dynamically adjusted according to the service, and it is disadvantageous for operation and management.

[0011] In the actual operation of the ICP, it is difficult for the service provider to control the correctness of the service number, traffic flow and time length in the charging message, thus accurate charging may not be performed.

Summary of the Invention

[0012] The present invention provides a method and a system for implementing content charging at low cost, so that the service charging may be more accurate and reasonable, and the bandwidth may be adjusted dynamically according to the service.

[0013] The present invention provides a method for content charging, including:

[0014] sending, by a Portal Server, a service activation request to a Policy Server, based on a service request from a user;

[0015] responding to the service activation request, determining a service policy corresponding to the service request, and delivering a service policy activation message to a content control gateway, by the Policy Server;

[0016] executing the service policy and reporting user service consumption information to the Policy Server by the content control gateway; and permitting the user to use the service, and charging according to the user service consumption information reported by the content control gateway, by the Policy Server.

[0017] The method further includes:

[0018] sending, by the Portal Server, a service deactivation request to the Policy Server, when a request for stopping the service from the user is received; and

[0019] responding to the service deactivation request, delivering a service policy cancellation message, performing rating and accounting according to the consump-

tion information, by the Policy Server.

[0020] The content control gateway reports the user service consumption information to the Policy Server periodically during the service;

[0021] The Policy Server performs rating according to the user service consumption information, and settles accounts on the service consumption of the user according to each rating information after the user stops using the service.

[0022] After responding to the service activation request, the Policy Server queries a preset correlation table between the service and the service policy according to the service activation request, determines the service policy corresponding to the service, and extracts the parameters needed for executing the service policy, then fills the parameters in the service policy activation message and delivers the service policy activation message to the content control gateway.

[0023] Wherein, the service policy message includes the information of the source IP address, destination IP address, destination port, destination service resource and traffic flow information of the network packet.

[0024] The content control gateway grants the right to the source IP address of the user network packet to access the destination IP address, destination port and destination service resource, and controls the network flow according to the traffic flow information in the policy message.

[0025] The content control gateway distinguishes between the content data flows according to the Content Server or the service port of the content, controls the content data flow and collects the consumption information.

[0026] In another aspect of the invention, there is provided a system for content charging, which includes a Portal Server and a Content Server, wherein

[0027] the system further includes a Policy Server and a content control gateway, the Policy Server is connected with the Portal Server and the content control gateway and is adapted to deliver a service policy activation message and a service policy cancellation message, perform rating and charging according to user service consumption information reported by the content control gateway;

[0028] the content control gateway is connected with the Content Server and is adapted to control access to the Content Server of the user according to the access right, count the service consumption information and report the user service consumption information to the Policy Server for charging.

[0029] The Policy Server includes a central control module, a charging engine module, a portal interface module and a device interface module.

[0030] The central control module is connected with the charging engine module, portal interface module and device interface module, and is adapted to respond to a service activation request sent by the portal interface module, convert the service activation request into a service policy message corresponding to the service, deliver a service policy activation message via the device interface module, receive user service consumption information reported by the device interface module, and invoke the charging engine module for rating.

[0031] The portal interface module is adapted to receive a service request from the user, send a service activation request or a service deactivation request to the central control module, and return the execution result of the service request.

[0032] The device interface module is adapted to forward the policy information delivered by the central control module, and report policy execution information and service consumption information to the central control module.

[0033] The charging engine module is adapted to receive an invoking instruction from the central control module and perform rating and charging according to the user service consumption information.

[0034] The content control gateway includes a central control module, a flow classification module, a content filtration module, a charging collection module and an interface module.

[0035] The central control module is adapted to receive a policy sent by the Policy Server, and interact with the flow classification module, content filtration module and charging collection module for interpreting and executing the policy.

[0036] The flow classification module is adapted to check, classify, control a source IP address, a destination IP address and destination port information of a network packet on the IP layer, and permit a network flow that conforms to the policy to pass.

[0037] The content filtration module is adapted to check, classify, control resources to be accessed by the network packet on the application layer, and permit the network flow that conforms to the policy to pass.

[0038] The charging collection module is adapted to collect the time length and the traffic flow information of the network flow, and report the original charging data to the central control module.

[0039] The interface module is adapted to provide an interface between the central control module and the Policy Server.

[0040] In still another aspect of the invention, there is provided a Policy Server for implementing content charging, which includes a central control module, a charging engine module, a portal interface module and a device interface module.

[0041] The central control module is connected with the charging engine module, portal interface module and device interface module, and is adapted to receive a service activation request sent by the portal interface module, convert the service activation request into a service policy message corresponding to the service, deliver the service policy activation message via the device interface, receive user service consumption information reported by the device interface module, and invoke the charging engine module for rating.

[0042] The portal interface module is adapted to receive a service request from the user, send a service activation request or a service deactivation request to the central control module, and return the execution result of the service request.

[0043] The device interface module is adapted to forward the policy information delivered by the central control module, and report policy execution information and service consumption information to the central control module.

[0044] The charging engine module is adapted to receive an invoking instruction from the central control module and perform rating and charging according to the user service consumption information.

[0045] The server further includes a database interface and a memory database, Through the database interface, an external database and the memory database may be accessed. The memory database is adapted to store policy data, charging data, configuration data and user session data, and receive an instruction from the central control module for updating the data.

[0046] The invention further provides a content control gateway for implementing the charging method according to claim 1, which includes a central control module, a flow classification module, a content filtration module, a charging collection module and an interface module.

[0047] The central control module is adapted to receive a policy sent by the Policy Server, and interact with the flow classification module, content filtration module and charging collection module for interpreting and executing the policy.

[0048] The flow classification module is adapted to check, classify and control a source IP address, a destination IP address and destination port information of a network packet on the IP layer, and only permit a network flow that conforms to the policy to pass.

[0049] The content filtration module is adapted to check, classify and control resources to be accessed by the network packet on the application layer, and only permit the network flow that conforms to the policy to pass.

[0050] The charging collection module is adapted to collect the time length and the traffic flow information of the network flow, and report the original charging data to the central control module.

[0051] The interface module is adapted to provide an interface between the central control module and the Policy Server.

[0052] In summary, in the method and system for content charging according to the embodiments of the invention, by determining the service policy corresponding to the service information and executing the service policy, the user is controlled to use the service, the content data flows are distinguished according to the Content Server or the service port of the content, and the content data flow is controlled and the consumption information is collected. So that charging may be performed according to the user service consumption information reported. As a result, the interconnection difficulty and interconnection cost between the ICP Content Server and the content platform of the service provider may be lowered greatly, and a non-coding interconnection operation solution may be provided. Thus, the service provider may rapidly dispose a content service, the ICP may be effectively prevented from falsifying data, and accurate charging data may be provided. At the same time, the corresponding network QoS may be ensured according to the requirements of a certain content service, thus an overall QoS may be provided, and the market competitive power may be improved.

Brief Description of the Drawings

[0053] Figure 1 is a schematic diagram showing an exemplary system structure according to an embodiment of the invention;

[0054] Figure 2 is a schematic diagram showing the structure of the Policy Server according to an embodiment of the invention;

[0055] Figure 3 is a schematic diagram showing the structure of the content control gateway according to an embodiment of the invention; and

[0056] Figure 4 is a flow chart of the method according to an embodiment of the invention.

Detailed Description of the Embodiments

[0057] To make the principle, characteristics and advantages of the invention clearer, the invention will now be described in detail hereinafter in conjunction with the embodiments and the drawings of the invention.

[0058] As shown in Figure 1, the system for content charging according to an embodiment of the invention includes a Portal Server, a Policy Server, a Content Control Gateway (CCG) and a Content Server. Wherein, the Policy Server is connected with the Portal Server and the content control gateway, for delivering or canceling a service policy message, and performing rating and charging according to the service usage information reported by the CCG, such as traffic flow and time length. The CCG is connected with the Content Server, for controlling the access to the Content Server of the user, counting the service consumption information, and periodically reporting the related data to the Policy Server for charging. The Portal Server provides a portal for user access, and provides the user with functions such as login, service channel, service selection, self-help service. The Content Server is a server through which the ICP provides contents. There may be a plurality of Content Servers connected with a CCG, and various contents may also be issued on a Content Server. The servers on which the contents exist may be different, and the service ports of the contents, i.e. Transmission Control Protocol/User Data Protocol (TCP/UDP) ports may be different. The CCG distinguishes between the content data flows according to the server on which the contents exist or the service port of the content, and controls the content

data flows and collects data respectively for executing the policy.

[0059] The service policy message may be regarded as an indication message for the service data flow rules, which comprises parameters such as the source IP address, destination IP address, destination port, service resource information and traffic flow information of a network packet. For example, when a Content Server provides a game service, if a user wants to access the game server, the content of the corresponding service policy message may include the following information: the source IP address (which may be the IP address of the user), the IP address of the game server, the port of the game server (which may refer to the TCP/UDP port), the upstream bandwidth, the downstream bandwidth, the Universal Resource Locator (URL), etc. Thus, if the Policy Server delivers the policy and notifies the CCG, the CCG grants the user the right to access the game server after applying the policy. If the Policy Server instructs the CCG to remove the policy, the current user will lose the right to access the game server.

[0060] If the user wants to access a streaming server, the content of the corresponding service policy message may include the following information: the source IP address, the IP address of the streaming server, the port of the streaming server, the upstream bandwidth, the downstream bandwidth and the URL. The Policy Server delivers a policy and notifies the CCG, and the CCG grants the user the right to access the streaming server after applying the policy and reserves a designated bandwidth for the video/audio stream. If the Policy Server instructs the CCG to remove the policy, then the current user will lose the right to access the streaming server.

[0061] Similarly, if the user wants to access a download server, the content of the corresponding service policy message may include the following information: the source IP address, the IP address of the download server, the port of the download server, the upstream bandwidth, the downstream bandwidth, and the path of the download file. The Policy Server delivers a policy and notifies the CCG, and the CCG grants the user the right to access the download server after applying the policy and reserves a designated download bandwidth. If the Policy Server instructs the CCG to delete the policy, then the current user will lose the right to access the download server.

[0062] Each service and its corresponding service policy are stored in the form of a correlation table between the service and the service policy.

[0063] The internal structure of the Policy Server is as shown in Figure 2, which may include a central control module, a charging engine, a portal interface module, a device interface module, a database interface module and a local memory database (Built-in-Memory).

[0064] The central control module is the core module of the Policy Server, and is mainly responsible for scheduling and controlling other modules in the system. The central control module receives a service activation request sent from the portal interface module, converts it into a service policy message corresponding to the service, and sends the service policy message to the CCG via the device interface. If the policy is executed successfully, the CCG will periodically report the user service consumption information (mainly including time length and traffic flow information), and the central control module invokes the charging engine module for performing rating after receiving the original charging information from the device interface module.

[0065] The portal interface is responsible for interconnecting with the Portal Server, sending the service activation request or the service deactivation request to the central control module, and returning the service request execution result to the Portal Server.

[0066] The device interface module is responsible for interconnecting with the CCG, forwarding the policy information delivered by the central control module to the CCG, and reporting the policy execution information and service usage information to the central control module.

[0067] The charging engine is the charging component of the Policy Server. The central control module invokes the charging engine for performing rating and accounting according to the user service consumption record.

[0068] The database interface enables other subsystems to access the database and the memory database.

[0069] The memory database is an optional component, which may be regarded as a buffer for the external database. The memory database is mainly adapted to store policy data, charging data, configuration data and user session data. By using the memory database, the performance of the system may be improved greatly. The central control module periodically sends an instruction to the memory database for reading the policy data, charging data, configuration data from the external database and refreshing the local memory data.

[0070] The CCG is adapted to control the access to the Content Server of the user, count the service consumption information, and periodically report related data to the Policy Server for performing charging. As shown in Figure 3, the internal structure of the CCG includes a central control module, a flow classification module, a content filtration module, a charging collection module and an interface module.

[0071] The central control module is responsible for receiving the policy sent from the Policy Server and interpreting and executing the policy. During the execution of the policy, the central control module needs to interact with and control the flow classification module, the content filtration module and the charging collection module.

[0072] The flow classification module checks, classifies and controls the information such as the source IP, the destination IP, the destination port of the network packet, on the IP layer. The network flow that conforms to the policy may pass.

[0073] The content filtration module checks, classifies and controls the resources to be accessed by the network packet, such as the URL address applied by the HTTP,

the file path applied by the FTP (File Transfer Protocol) and the RTICP (Real-Time Streaming Protocol) path applied by the stream media, on the application layer. The network flow that conforms to the policy may pass.

[0074] The charging collection module collects the time length and the traffic flow information of the network flow, and reports the original charging data to the central control module. The central control module reports the original charging data to the Policy Server.

[0075] In the method according to an embodiment of the invention, Portal Server receives a service request from a user, and sends a service activation request to Policy Server. The Policy Server determines the corresponding service policy message according to the service after receiving the service activation request, and delivers the service policy message to CCG. The CCG executes the policy message, permits the user to use the service, and periodically reports the user service consumption information to the Policy Server. The Policy Server performs rating and charging according to the consumption information.

[0076] Specifically, as shown in Figure 4, the method includes following steps.

[0077] (1) A user sends a login request to the Portal Server, and the Portal Server authenticates the identity of the user.

[0078] (2) If the authentication is passed, the Portal Server receives the service selection data input by the user.

[0079] (3) The Portal Server sends a service activation request, which carries information such as the user IP, destination IP, service resources, to the Policy Server.

[0080] (4) The Policy Server determines the corresponding service policy message according to the service after receiving the service activation request, and delivers the service policy message to the CCG. Each service and its corresponding service policy are stored in the form of a correlation table between the service and the service policy. This table may be stored on the Policy Server or on a third party device. The Policy Server determines the policy corresponding to the service by querying the correlation table according to the activation request, extracts the parameters needed by the policy according to the activation request and the service policy, fills the parameters in the policy message and delivers the policy message. For example, for a game service, the content of the corresponding service policy message may include the following information: the source IP address (which may be the IP address of the user), the IP address of the game server, the port of the game server (which may refer to the TCP/UDP port), the upstream bandwidth, the downstream bandwidth and the URL.

[0081] (5) The CCG receives the service policy message, executes the service policy according to the instruction of the message, releases the access right from the user IP (which may be a source IP) to the destination IP, destination port or destination URL, and controls the network flow according to the bandwidth parameters in the policy. The CCG sends the policy execution result to the Policy Server after executing the policy.

[0082] (6) The Policy server informs the Portal Server of the service activation result.

[0083] (7) The Portal Server displays the service activation result to the user.

[0084] (8) If the service is activated, the user starts an application client end and performs content consumption, after knowing from the Portal Server that the service is available.

[0085] (9) The CCG periodically reports the service consumption information to the Policy Server during the content service used by the user.

[0086] (10) The Policy Server processes the service consumption information reported by the CCG in real time, and performs rating for the user content consumption.

[0087] (11) The Portal Server receives a request for stopping the service from the user when the user wants to logout the Content Server.

[0088] (12) The Portal Server sends a service deactivation request to the Policy Server.

[0089] (13) The Policy Server delivers a policy cancellation request to the CCG.

[0090] (14) The CCG cancels the policy and returns the policy cancellation result to the Policy server.

[0091] (15) The Policy server informs the Portal Server of the service cancellation result.

[0092] (16) The Portal Server displays the service cancellation result to the user.

[0093] (17) The CCG reports the last service consumption information of the user to the Policy Server.

[0094] (18) The Policy Server processes the service consumption information, performs rating, and settles accounts on the current content consumption according to each rating information.

[0095] In another embodiment of the invention, the content control gateway does not need to periodically report the user service consumption information to the Policy Server. Instead, the content control gateway reports the total service consumption information of the user to the Policy Server at a time after receiving the policy cancellation request delivered by the Policy Server. The Policy Server performs rating and accounting according to the consumption information.

[0096] The invention provides a novel content charging solution, by means of which the interconnection difficulty and the interconnection cost between the ICP Content Server and the content platform of the service provider may be lowered greatly, and the ICP may be effectively prevented from falsifying data, and accurate charging data may be provided. In the meanwhile, the corresponding network QoS may be ensured according to the requirements of a certain content service.

Claims

1. A method for content charging, comprising:

   sending, by a Portal Server, a service activation request to a Policy Server based on a service request from a user;
   responding to the service activation request, determining a service policy corresponding to the service request, and delivering a service policy activation message to a content control gateway, by the Policy Server;
   executing the service policy and reporting user service consumption information to the Policy Server by the content control gateway; and
   permitting the user to use the service, and charging according to the user service consumption information reported by the content control gateway, by the Policy Server.

2. The method according to claim 1, wherein the method further comprises:

   sending, by the Portal Server, a service deactivation request to the Policy Server, when a request for stopping the service from the user is received; and
   responding to the service deactivation request, delivering a service policy cancellation message, performing rating and accounting according to the consumption information, by the Policy Server.

3. The method according to claim 1 or 2, wherein the method further comprises:

   reporting, by the content control gateway, the user service consumption information to the Policy Server periodically during the use of the service;
   rating according to the user service consumption information, and accounting on the service consumption of the user according to each rating information after the user stops using the service, by the Policy Server.

4. The method according to claim 1, wherein the method further comprises:

   after responding to the service activation request, querying a preset correlation table between the service and the service policy according to the service activation request, determining the service policy corresponding to the service, extracting the parameters needed for executing the service policy, filling the parameters in the service policy activation message and delivering the service policy activation message to the content control gateway by the Policy Server.

5. The method according to claim 1, 2 or 4, wherein: the service policy activation message comprises the information of the source IP address, destination IP address, destination port, destination service resource and traffic flow information of the network packet.

6. The method according to claim 5, wherein the method further comprises:

   granting the source IP address of the user network packet a right to access the destination IP address, destination port and destination service resource, and controlling the network flow according to the traffic flow information in the service policy message, by the content control gateway.

7. The method according to claim 1, wherein the method further comprises:

   obtaining the content data flows according to the Content Server or the service port of the content, controlling the content data flow and collecting the consumption information, by the content control gateway.

8. A system for content charging, comprising a Portal Server and a Content Server, wherein the system further comprises a Policy Server and a content control gateway, the Policy Server is connected with the Portal Server and the content control gateway and is adapted to deliver a service policy activation message and a service policy cancellation message, perform rating and charging according to user service consumption information reported by the content control gateway;
   the content control gateway is connected with the Content Server and is adapted to control access to the Content Server of the user according to the access right, count the service consumption information and report the user service consumption information to the Policy Server for charging.

9. The system according to claim 8, wherein the Policy Server comprises a central control module, a charging engine module, a portal interface module and a device interface module, wherein:

   the central control module is connected with the charging engine module, portal interface module and device interface module, and is adapted to respond to a service activation request sent by the portal interface module, convert the service activation request into a service policy message corresponding to the service, deliver a

service policy activation message via the device interface module, receive user service consumption information reported by the device interface module, and invoke the charging engine module for rating;
the portal interface module is adapted to receive a service request from the user, send a service activation request or a service deactivation request to the central control module, and return the execution result of the service request;
the device interface module is adapted to forward the policy information delivered by the central control module, and report policy execution information and service consumption information to the central control module;
the charging engine module is adapted to receive an invoking instruction from the central control module and perform rating and charging according to the user service consumption information.

10. The system according to claim 8, wherein the content control gateway comprises a central control module, a flow classification module, a content filtration module, a charging collection module and an interface module, wherein:

the central control module is adapted to receive a policy sent by the Policy Server, and interact with the flow classification module, content filtration module and charging collection module for interpreting and executing the policy;
the flow classification module is adapted to check, classify, control a source IP address, a destination IP address and destination port information of a network packet on the IP layer, and permit a network flow that conforms to the policy to pass;
the content filtration module is adapted to check, classify, control resources to be accessed by the network packet on the application layer, and permit the network flow that conforms to the policy to pass;
the charging collection module is adapted to collect the time length and the traffic flow information of the network flow, and report the original charging data to the central control module;
the interface module is adapted to provide an interface between the central control module and the Policy Server.

11. A Policy Server, for realizing the charging method according to claim 1, wherein the Policy Server comprises a central control module, a charging engine module, a portal interface module and a device interface module, wherein:

the central control module is connected with the charging engine module, portal interface module and device interface module, and is adapted to receive a service activation request sent by the portal interface module, convert the service activation request into a service policy message corresponding to the service, deliver the service policy activation message via the device interface, receive user service consumption information reported by the device interface module, and invoke the charging engine module for rating;
the portal interface module is adapted to receive a service request from the user, send a service activation request or a service deactivation request to the central control module, and return the execution result of the service request;
the device interface module is adapted to forward the policy information delivered by the central control module, and report policy execution information and service consumption information to the central control module;
the charging engine module is adapted to receive an invoking instruction from the central control module and perform rating and charging according to the user service consumption information.

12. The server according to claim 11, wherein the server further comprises a database interface and a memory database, through the database interface, an external database and the memory database is accessed; the memory database is adapted to store policy data, charging data, configuration data and user session data, and receive an instruction from the central control module for updating the data.

13. A content control gateway, for implementing the charging method according to claim 1, comprising a central control module, a flow classification module, a content filtration module, a charging collection module and an interface module, wherein:

the central control module is adapted to receive a policy sent by the Policy Server, and interact with the flow classification module, content filtration module and charging collection module for interpreting and executing the policy;
the flow classification module is adapted to check, classify and control a source IP address, a destination IP address and destination port information of a network packet on the IP layer, and only permit a network flow that conforms to the policy to pass;
the content filtration module is adapted to check, classify and control resources to be accessed by the network packet on the application layer, and only permit the network flow that conforms to the policy to pass;

the charging collection module is adapted to collect the time length and the traffic flow information of the network flow, and report the original charging data to the central control module;
the interface module is adapted to provide an interface between the central control module and the Policy Server.

EX1002 - Page 838

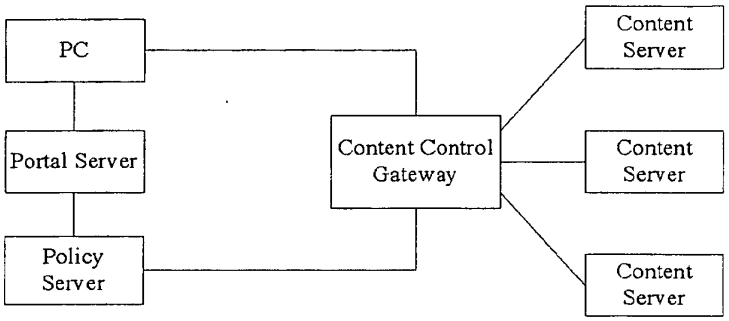

PC
Portal Server
Policy Server
Content Control Gateway
Content Server
Content Server
Content Server

Fig.1

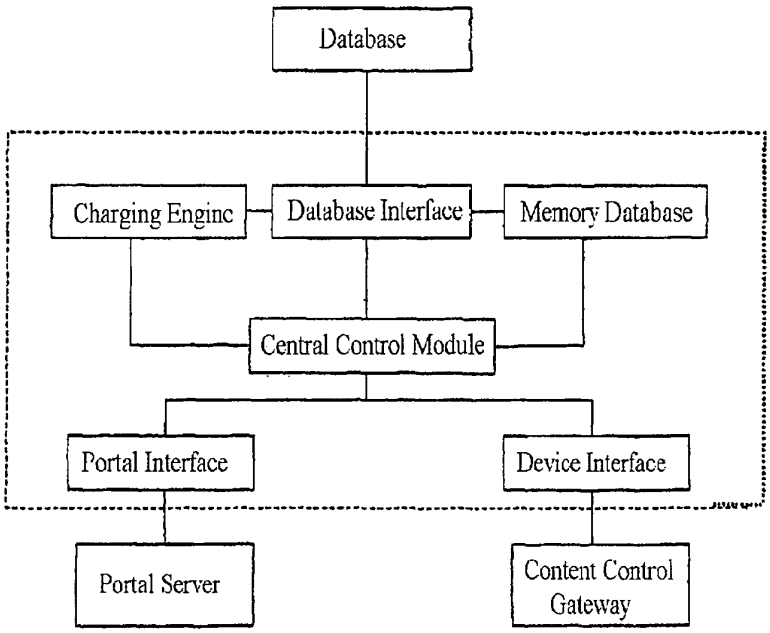

Database
Charging Engine
Database Interface
Memory Database
Central Control Module
Portal Interface
Device Interface
Portal Server
Content Control Gateway

Fig.2

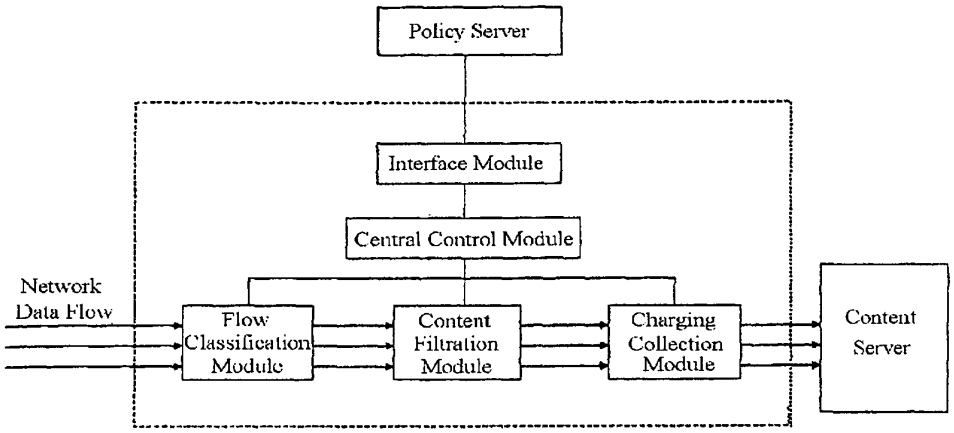

Policy Server
Interface Module
Central Control Module
Network Data Flow
Flow Classification Module
Content Filtration Module
Charging Collection Module
Content Server

Fig.3

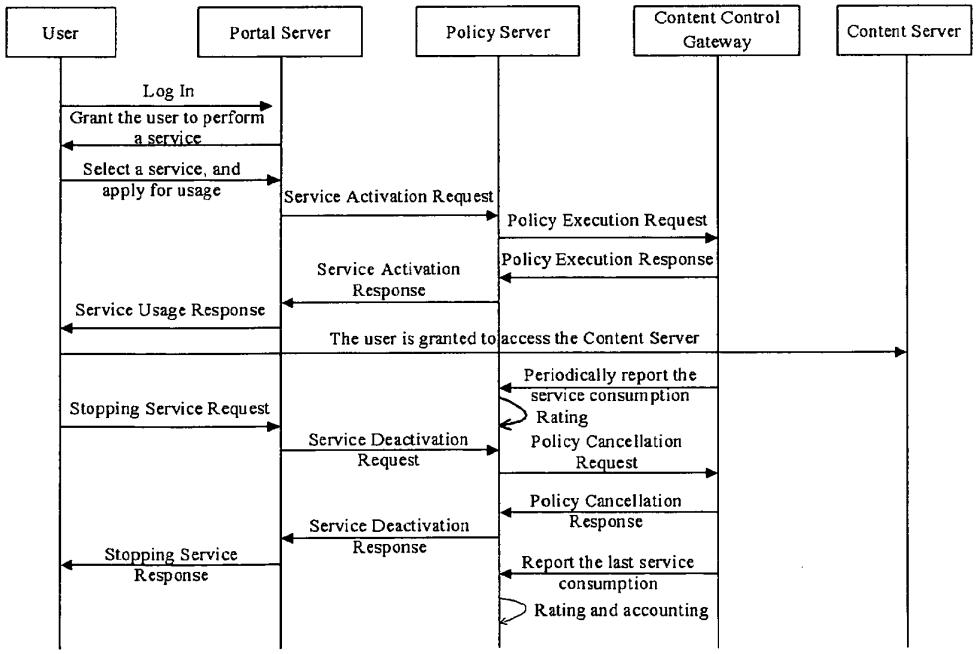

User
Portal Server
Policy Server
Content Control Gateway
Content Server
Log In
Grant the user to perform a service
Select a service, and apply for usage
Service Activation Request
Policy Execution Request
Policy Execution Response
Service Activation Response
Service Usage Response
The user is granted to access the Content Server
Periodically report the service consumption
Rating
Stopping Service Request
Service Deactivation Request
Policy Cancellation Request
Policy Cancellation Response
Service Deactivation Response
Stopping Service Response
Report the last service consumption
Rating and accounting

Fig.4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2006/001156

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/14 (2006.01) i

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)

H04L (2006.01), G07F (2006.01)

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)

CNPAT, CNKI, WPI, EPODOC, PAJ: bill+, charg+, account, content, policy, strategy, request, gateway, server

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO, A1, 0159990 (FUTURE TECH INC) 16.AUG. 2001 (16.08.2001), the whole document.	1-13
A	EP, A1, 1400934 (OPENWAVE SYSTEMS INC) 24.MAR. 2004 (24.03.2004), the whole document.	1-13
A	CN, A, 1556634 (ZHONGXING COMMUNICATION CO LTD SHENZHEN) 22.DEC. 2004 (22.12.2004), the whole document.	1-13

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
29. AUG. 2006 (29. 08. 2006)	21 · SEP 2006 (21 · 09 · 2006)
Name and mailing address of the ISA/CN The State Intellectual Property Office, the P.R.China 6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China 100088 Facsimile No. 86-10-62019451	Authorized officer WANG,Hongli Telephone No. (86-10) 62084525

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2006/001156

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
WO0159990A1	16.08.2001	JP2003523031T	29.07.2003
		KR2000024368 A	06.05.2000
		AU200136124 A	20.08.2001
		KR331219 B	06.04.2002
		US2003023550 A1	30.01.2003
		CN1397125 A	12.02.2003
EP1400934A1	24.03.2004	NONE	
CN1556634A	22.12.2004	NONE	

Form PCT/ISA /210 (patent family annex) (April 2005)

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

(11) EP 2 007 065 A1

(12) EUROPEAN PATENT APPLICATION

published in accordance with Art. 153(4) EPC

(43) Date of publication:
24.12.2008 Bulletin 2008/52

(21) Application number: **07720622.5**

(22) Date of filing: **30.03.2007**

(51) Int Cl.:
H04L 12/14 *(2006.01)*

(86) International application number:
PCT/CN2007/001048

(87) International publication number:
WO 2007/112685 (11.10.2007 Gazette 2007/41)

(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

(30) Priority: **31.03.2006 CN 200610067080**

(71) Applicant: **Huawei Technologies Co., Ltd.**
Longgang District, Shenzhen
Guangdong 518129 (CN)

(72) Inventors:
- **WU, Yajuan**
  Shenzhen Guangdong 518129 (CN)
- **LUO, Long**
  Shenzhen Guangdong 518129 (CN)

(74) Representative: **Haley, Stephen**
Gill Jennings & Every LLP
Broadgate House
7 Eldon Street
London EC2M 7LH (GB)

(54) CHARGING ASSOCIATING METHOD, SYSTEM, CHARGING CENTER, AND DEVICE FOR APPLICATION SERVICE

(57) A method for charging correlation for an application or service is provided. The method may include: receiving a service identifier assigned for an application or service; and correlating Charging Data Records CDRs generated for the application or service based on the service identifier. A system for charging correlation, a billing center and an apparatus for charging correlation are also provided. These method and apparatus may provide a simple charging correlation process for an application or service.

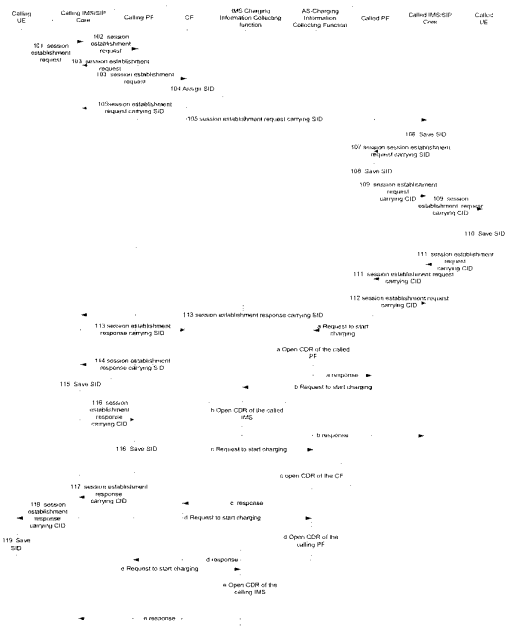


Fig. 1

EP 2 007 065 A1

Printed by Jouve, 75001 PARIS (FR)

Description

Field of the Invention

[0001] The present invention relates to applications and services, and particularly, to a method and system for charging correlation of applications and services, a billing center and an apparatus for generating charging data record.

Background of the Invention

[0002] At present, communication systems have provided applications and services for individual user and/or group users, and communication media employed in these applications and services may include text, audio, video, and varieties combinations of multimedia. A general application or service is mainly oriented to individuals, and there usually is only one or two User Equipments (UEs) communicating with an Application Server or with each other. However, in an application or service in which group users take part, users of one or more groups usually communicate with other users at the same time. In other words, this kind of communication is not a two-party communication including one calling user and one called user, but a communication including a plurality of calling users and a plurality of called users. Such an application or service in which group users take part is also called a multi-party service.

[0003] In a session-based service, a Charging Identifier (CID) is allocated each time when an Application Server (AS) establishes a session with a UE, and all CIDs allocated are saved in the AS and a service bearer network. A billing center retrieves Charging Data Records (CDRs) corresponding to the CIDs from the service bearer network and the AS via a charging function collecting entity, and combines CDRs that correspond to the same CID in order to perform a charging. For applications and services employing an IP Multi-media Subsystem (IMS) as a service bearer network, the CIDs allocated are also called IMS Charging Identifiers (ICIDs). However, the applicant finds out that the CID-based charging method described above has some disadvantages in practical applications and services.

[0004] For example, in a service communication, when a UE establishes a session with an AS for a first time, the UE is given a CID. For some reasons, the UE may exit the service communication temporarily before the service communication is end. Later, the UE re-enters the service communication. In such a case the UE is given a new CID for a session established after re-entering the service communication. From a perspective of a user using the UE, the two sessions, established for the first entering and established for the re-entering, respectively, are two related sessions, and need to be combined for a charging. However, from a perspective of the billing center, the two sessions correspond to different CIDs, thus the two sessions are considered as unrelated sessions. If the two sessions need to be correlated, the billing center needs to analyze CDRs of the two sessions and perform complicated calculation based on user information recorded in the CDRs, yet it is still difficult to guarantee an accurate correlation of the two sessions. Such problem becomes more apparent in multi-party services.

[0005] In a multi-party service, UEs used by users of various parties of this service access a center control server via respective access servers. The center control server provides centralized session handling, which includes session signaling controls, media transmission authorization to communication parties, media data duplication and distribution, etc. One multi-party service has one center control server and at least one access server. The center control server performs controlling function (CF) and the access server performs participating function (PF). Logically, a CF corresponds to a multi-party service. In a multi-party service, the CF establishes one session for each UE, and the sessions of each UE correspond to a PF. Therefore, the center control server is looked as a CF while the access server is looked as at least one PF corresponding to at least one UE connected to the access server.

[0006] Therefore, multi-party services have a common feature that, a multi-party service has at least one session and each session corresponds to a UE of one user and corresponds to its CID. Due to such feature of multi-party services, the billing center needs to correlate a great number of CIDs when performing charging, which leads to poor charging accuracy and difficult implementation. Moreover, for a multi-party service, there is also a need to charge a user by correlating a plurality of sessions of the user in one multi-party service. However, according to the charging technique in the prior art, the billing center needs to generate CDRs based on ICIDs first and make further calculations based on group information in the CDRs, which is still complicated and tends to be inaccurate.

[0007] As discussed above, CID-based charging method in the prior art cannot correlate different sessions of a user in one service communication, but only can correlate actions of the user in one session. Such charging method may easily result in a repeated charging for one action and may omit an action which needs to be charged, thereby threatening security and reliability of charging operations and reducing user satisfaction.

[0008] Furthermore, as new demands emerge, it is becoming more and more difficult to use a single AS to handle a plurality of applications or services. In order to provide more flexible and richer services, operators or service providers are developing multi-services which includes a plurality of sub-services. For a perspective of a multi-service, the above application or service provided by the AS can be called single-service. In a multi-service, each sub-service has a sub-service server e.g. an AS, and an entire multi-service also has a service control function adapted to perform a centralized control of all the sub-service servers. For example, the service control

function controls initiation procedures of the respective sub-services and controls assignment of session identifiers of the respective sub-services, etc. A current typical multi-service has a structure that one of the sub-services is considered as the primary service, and all other sub-services of the multi-service are considered as supplementary services. The sub-service server serves the primary service can be called a primary service server and the sub-service servers serve the supplementary services can be called supplementary service servers. The implementation of the supplementary services depends on the implementation of the primary service in certain degree and provides supplementary functions for the implementation of the primary service. For example, a Presence Server may be configured in a PoC service network and be used to display group status to users during a PoC service session. For another example, a Location Service Server (LCS Server) may also be used in a PoC service network to provide location information of participating users.

[0009] As the development of multi-services, operators or service providers may develop correlating charging policies for multi-services. However, as discussed above, the conventional charging method is based on CIDs corresponding to separate sessions. Therefore the billing center needs to correlate CDRs of a plurality of services in a multi-service charging to perform a charging. Because a CID corresponds to only one session of a sub-service of a user, the billing center needs to analyze each CDR and performs comprehensive calculation by using complicated processes, thereby resulting in low charging accuracy and low feasibility.

[0010] Therefore, the conventional CID-based charging method is only applicable to correlate a plurality of actions of a user in one session, but is not applicable to correlate a plurality of sessions of a user in a single-service and says nothing of correlating a plurality of sessions of a user in a plurality of sub-services of a multi-service.

Summary of the Invention

[0011] Embodiments of a method and a system for charging correlation, a billing center and an apparatus for generating charging data record for implementing a charging correlation for an application or service are provided, which enables a charging correlation process to be easily performed and to greatly improve charging accuracy.

[0012] A method for charging correlation for an application or service may include:

assigning a service identifier by a service control function to an application or service;
sending the service identifier to a charging system; and
correlating, by the charging system, at least one Charging Data Record CDR generated for the application or service based on the service identifier.

[0013] A system for charging correlation for an application or service may include:

a service control function, adapted to assign a service identifier for an application or service; and
a charging system, adapted to correlate Data Records CDRs generated for the application or service based on the service identifier.

[0014] A billing center may include:

a first module, adapted to receive a service identifier assigned to an application or service and CDRs generated for the application or service; and
a second module, adapted to correlate the CDRs based on the service identifier from the first module.

[0015] An apparatus for generating charging data record may include:

a first module, adapted to receive a service identifier assigned to an application or service; and
a second module, adapted to generate Charging Data Records CDRs carrying the service identifier from the first module for the application or service.

[0016] The method for charging correlation, the system for charging correlation, the billing center and the apparatus for generating charging data record for implementing a charging correlation for an application or service provided in accordance with embodiments of the present invention are able to correlate a plurality of CDRs generated during an application or service, thereby implementing a correlated charging of a plurality of users participating in the application or service in a simple way. A plurality of CDRs generated for one user in the application or service may be correlated and the user can be accurately charged. Furthermore, correlated charging for multi-services can also be implemented. The technical solution provided in embodiments of the present invention is easy to be implemented and does not need to make many modifications to the existing networks, and therefore is highly feasible.

Brief description of the drawings

[0017]

Figure 1 is a flowchart of a charging correlation process in a session establishment in accordance with an embodiment of the present invention.
Figure 2 is a flowchart of a charging correlation process in a session establishment in accordance with an embodiment of the present invention.
Figure 3 is a flowchart of a charging correlation process in a session modification in accordance with an embodiment of the present invention.
Figure 4 is a flowchart of a charging correlation proc-

ess when a new user is added in accordance with an embodiment of the present invention.

Figure 5 is a flowchart of a charging correlation process of an on-demand session in accordance with an embodiment of the present invention.

Figure 6 is a flowchart of a charging correlation process of a pre-established session in accordance with an embodiment of the present invention.

Figure 7 is a flowchart of a charging correlation process when a user who established an on-demand session re-enters the session in accordance with an embodiment of the present invention.

Figure 8 is a flowchart of a charging correlation process when a user who established a pre-established session re-enters the session in accordance with an embodiment of the present invention.

Figure 9 is a flowchart of a charging correlation process for a multi-service in accordance with an embodiment of the present invention.

Figure 10 is a flowchart of a charging correlation process for a multi-service in accordance with an embodiment of the present invention.

Figure 11 is a structure diagram of a system for implementing a charging correlation of an application or service in accordance with an embodiment of the present invention.

Detailed Description of the Embodiments

[0018] This invention will hereinafter be described in detail with reference to accompanying drawings and embodiments.

[0019] A charging method for an application or service according to an embodiment of the present invention may include: assigning a service identifier to an application or service session, sending the service identifier to a charging system, and correlating, by the charging system, the CDRs generated in this service based on the service identifier. The charging method is described in detail in the following embodiments.

[0020] The charging system may include a charging information collecting function used to receive CDRs from ASs and bearer control layer entities, a charging gateway, and a billing center used to correlate the CDRs and perform other operations for charging. The charging information collecting function functions as an interface of the charging system, receives CDRs from network nodes e.g., ASs or bearer control layer entities connected to the charging information collecting function, and sends the CDRs to the billing center via the charging gateway. ASs and the bearer control layer entities have respective charging information collecting functions. A charging information collecting function corresponding to ASs is usually called an AS-charging information collecting function and a charging information collecting function corresponding to bearer control layer entities is usually called a bearer control layer-charging information collecting function. For bearer control layer in an IMS network, the bearer control layer-charging information collecting function is also called an IMS charging information collecting function. Embodiments of the present invention mainly concerns about transmission of service identifiers among ASs, bearer control layer entities and charging information collecting functions, therefore the figures and illustrations of the embodiments of the present invention omit the processes that the charging information collecting functions send CDRs and service identifiers to the billing center. In the figures and illustrations of the embodiments of the present invention, the AS-charging information collecting function entities and IMS charging information collecting function entities are referred to as AS-charging information collecting functions and IMS charging information collecting functions.

[0021] A first charging correlation scheme given in an embodiment of the present invention implements charging with a plurality of CDRs generated for one user in a single-service. In this embodiment, a service control function, e.g. an AS of a single-service session, assigns a uniform service identifier for the single-service, generates CDRs of participating users and sends the service identifier and the CDRs to a charging system. The charging system correlates the CDRs of a user in this single-service session.

[0022] In practical applications, a user may establish one or a plurality of sessions in one service and a CDR corresponds to one session of the user. Different ways may be adapted to correlate CDRs based on the service identifier. The CDRs to be correlated may be CDRs corresponding to a plurality of sessions established for one user in one service, or may be CDRs corresponding to a plurality of sessions established for a part of users or all users in one service. The specific way of correlating CDRs is chosen in accordance with an applied correlation policy and will not be described further herein.

[0023] The AS sends the service identifier and the CDRs to a charging information collecting function of a charging system. The charging information collecting function sends the CDRs collected and the service identifier to a billing center which performs charging correlation operations. When this charging correlation scheme is applied to application service layer, the charging information collecting function includes an AS-charging information collecting function corresponding to the service control function entity. The charging correlation scheme may also be applied to bearer control layer, and in such a case the charging information collecting function includes a bearer control layer-charging information collecting function corresponding to a bearer control layer entity that the service control function entity corresponds to, wherein the bearer control layer entity that the service control function corresponds to is used to bear the service control function. At this time, the bearer control layer entity corresponding to the service control function records the service identifier and generates CDRs for the current application or service, and sends the service identifier and the CDRs to the bearer control layer-charging infor-

mation collecting function of the bearer control layer entity. The AS-charging information collecting function and the bearer control layer-charging information collecting function respectively send the CDRs and service identifiers to the billing center. The billing center correlates the CDRs received from the AS-charging information collecting function and correlates the CDRs received from the bearer control layer-charging information collecting function, respectively. Or the billing center may correlates the CDRs received from the AS-charging information collecting function with the CDRs received from the bearer control layer-charging information collecting function. This charging correlation scheme in an embodiment of the present invention may be applied to both the application service layer and the bearer control layer in the embodiments shown in Figures 1 to 8. When the charging correlation scheme is applied only to the application service layer, the charging correlation process involves UE, AS, AS-charging information collecting function and billing center, without involving the bearer control layer entity and the bearer control layer-charging information collecting function. The charging correlation process in which the charging correlation scheme is applied only to the application service layer will not be described in detail herein, yet such process is still covered by the protection scope of the present invention.

[0024] The embodiments of the present invention are mainly oriented to session-based applications or services such as multi-party services. In conventional session-based services, session IDs (SIDs) corresponding to different service sessions are already employed. The existing SIDs may be used as service identifiers to correlate a plurality of CDRs. Also new identifiers may be defined as the service identifiers. Usually information exchanged among entities on the application service layer is sent via corresponding bearer control layer entities. For example, servers that perform PF of the multi-party service, a server performing CF, and UEs are used to exchange information via corresponding bearer control layer entities such as an IMS/SIP Core network (IMS/SIP Core). At the same time, network functions in the IMS/SIP Core may also generate CDRs for the current application or service in order to implement a charging process on the bearer control layer. In such process the AS of each application or service corresponds to a bearer control layer entity that is adapted to bear the AS.

[0025] At present, the mainstream multi-party services include Push-to-Talk over Cellular network (PoC) service, Conference service, etc. In a PoC service session, a server performing CF is a PoC server that performs CF, also called Controlling PoC Server; and the server performing PF is the PoC server that performs PF, also called Participating PoC Server. In a Conference service session, the server that performs CF is the Conference server that performs CF, also called a Controlling Conference Server; and the server performing PF is the Conference server that performs PF, also called a Participating Conference Server. The server performing PF and the server performing CF are logical functions of multi-party service servers, and the server performing PF and the server performing CF may be physically located in different ASs or in one AS. The server performing CF is referred to as the CF and the server performing PF is referred to as PF herein for the sake of simplicity. The embodiments of the present invention are described in detail herein taken a SIP based multi-party service as an example.

[0026] Figure 1 shows a flowchart of a charging correlation process in a session establishment in accordance with an embodiment of the present invention. The entities involved in this embodiment include a calling UE and a calling PF of the calling UE, a calling IMS/SIP Core corresponding to the calling PF and the calling UE, a CF of a present multi-party service, a called UE and a called PF of the called UE, a called IMS/SIP Core corresponding to the called PF and the called UE. The entities involved in this embodiment also include an AS-charging information collecting function corresponding to the calling PF, CF, and the called PF, and an IMS charging information collecting function corresponding to the calling IMS/SIP Core and the called IMS/SIP Core. The calling UE, the calling PF and the CF correspond to a same bearer control layer entity i.e., the calling IMS/SIP Core, the called UE and the called PF correspond to a same bearer control layer entity i.e., the called IMS/SIP Core. The service control function of the current application or service performs CF of the multi-party service.

[0027] When the calling/called PF and CF are provided by servers in a network of one service provider, the calling/called PF and the CF may correspond to a same AS-charging information collecting function. In this embodiment, suppose that the calling/called PF and the CF correspond to a same AS-charging information collecting function. However, when the calling/called PF and the CF are provided by servers in different networks of different service providers, the calling/called PF and the CF may correspond to different AS-charging information collecting functions respectively, and accordingly, the calling/called PF and the CF send service identifiers and the CDRs to different AS-charging information collecting functions respectively. Similarly, when IMS/SIP Cores of the calling UE and the called UE are provided in a same network of a same operator, the calling/called IMS/SIP Cores may correspond to one IMS charging information collecting function. When the IMS/SIP Cores of the calling UE and the called UE are in different networks provided by different operators, the calling/called IMS/SIP Cores may correspond to different IMS charging information collecting functions and send service identifiers and the CDRs to different IMS charging information collecting functions respectively. In this embodiment, suppose that the calling/called IMS/SIP Cores correspond to one IMS charging information collecting function.

[0028] As shown in Figure 1, the process includes as follows.

[0029] 101-102: The calling UE sends a session es-

tablishment request to the calling PF via a corresponding calling IMS/SIP Core. The session establishment request may be carried in an SIP INVITE message in this embodiment; however, the present invention is not limited to this.

[0030] The application service layer entities such as the UE, PF, CF, etc., and the corresponding bearer control layer entities such as the IMS/SIP Core, etc., may be in a same network or in different networks. The present invention is not limited to this.

[0031] 103: The calling PF sends the session establishment request to the CF via the calling IMS/SIP Core.

[0032] 104: The CF assigns a service identifier (SID) for the current multi-party service session and the followings shall be performed once for each of the called UEs.

[0033] 105: The CF sends the session establishment request to the called IMS/SIP Core corresponding to the called PF via the calling IMS/SIP Core of the CF. The session establishment request carries the SID assigned in 104.

[0034] 106-107: The called IMS/SIP Core saves the received SID and sends the session establishment request carrying the SID to the called PF.

[0035] 108-109: The called PF saves the received SID and sends the session establishment request carrying the SID to the called UE via the called IMS/SIP Core.

[0036] 110-111: The called UE saves the received SID and returns a session establishment response carrying the SID to the called PF via the called IMS/SIP Core. The session establishment response is carried in an SIP 2000K message in this embodiment, however, the present invention does not limit to this.

[0037] 112-113: The called PF sends the session establishment response carrying the SID to the CF via the called IMS/SIP Core and the calling IMS/SIP Core.

[0038] 114: The CF returns the session establishment response carrying the SID to the calling IMS/SIP Core.

[0039] 115-116: The calling IMS/SIP Core saves the received SID and returns the session establishment response carrying the SID to the calling PF, the calling PF also saves the received SID.

[0040] 117-119: The calling PF returns the session establishment response carrying the SID to the calling UE via the calling IMS/SIP Core, and the calling UE saves the received SID. By now, a session establishment process is completed.

[0041] In this embodiment, after receiving the SID, the service layer entities and bearer control layer entities related to the charging correlation process may insert the SID into or with the CDRs generated for the current application or service and send the CDRs to the corresponding charging information collecting functions. Specifically, the application service layer entities and bearer control layer entities generate CDRs after receiving a session establishment response indicating a successful session set-up or after sending the session establishment request, and the SID is included in the CDRs and the CDRs are sent to the charging information collecting functions. This embodiment describes a process in which the session is successfully established; hence it is supposed that the session establishment response always indicates a successful session set-up. In Figure 1, the application service layer entities related to the charging correlation process include a calling PF, a called PF and a CF; the bearer control layer entities related to the charging correlation process include a calling IMS/SIP Core and a called IMS/SIP Core. The procedure of sending the SID and the CDRs by the application service layer entities and bearer control layer entities related to the charging correlation process includes the followings.

[0042] The called PF may perform step ***a*** after sending the session establishment request in 109 or after receiving the session establishment response in 111. Step ***a*** is independent of other following steps and this embodiment of the present invention does not limit the sequence order of performing ***a*** and the steps following 111. Step ***a*** may include followings. The called PF requests the AS-charging information collecting function to start charging and sends the CDR of the called UE carrying the SID to the AS-charging information collecting function. The AS-charging information collecting function opens the CDR and starts to record actions performed by the called UE with the called PF during a current multi-party service.

[0043] The called IMS/SIP Core may save the SID when sending the session establishment request or when sending session establishment response that carries the SID. The called IMS/SIP Core may further perform step ***b*** after receiving the session establishment response in 112. Step ***b*** is independent of other following steps and this embodiment of the present invention does not limit the sequence order of performing step ***b*** and the steps following 112. Step ***b*** may include followings. The called IMS/SIP Core requests the IMS charging information collecting function to start charging, and sends the CDR of the called UE carrying the SID to the IMS charging information collecting function. The IMS charging information collecting function opens the CDR and starts to record actions performed by the called UE with the called IMS/SIP Core during the current multi-party service.

[0044] The CF may perform step c after receiving the session establishment response in 113. Step c is independent of other following steps and this embodiment of the present invention does not limit the sequence order of performing step ***c*** and the steps following 113. Step c may include followings. The CF requests the AS-charging information collecting function to start charging and sends CDRs of the calling and called UEs carrying the SID to the AS-charging information collecting function. The AS-charging information collecting function opens the CDRs and starts to record actions performed by the calling and called UE with the CF during the current multi-party service.

[0045] The calling PF may perform step ***d*** after receiving the session establishment response in 116. Step ***d*** is independent of other following steps and this embodiment of the present invention does not limit the sequence

order of performing step ***d*** and the steps following 116. Step ***d*** may include followings. The calling PF requests the AS-charging information collecting function to start charging and sends the CDR of the calling UE carrying the SID to the AS-charging information collecting function. The AS-charging information collecting function opens the CDR and starts to record actions performed by the calling UE with the calling PF during the current multi-party service.

[0046] The calling IMS/SIP Core may save the SID after sending the session establishment response that carries the SID. The calling IMS/SIP Core may further perform step ***e*** after receiving the session establishment response in 117. Step ***e*** is independent of other following steps and this embodiment of the present invention does not limit the sequence order of performing step ***e*** and the steps following 117. Step ***e*** may include followings. The calling IMS/SIP Core requests the IMS charging information collecting function to start charging and sends the CDR of the calling UE that carries the SID to the IMS charging information collecting function. the IMS charging information collecting function opens the CDR and starts to record actions performed by the calling UE with the calling IMS/SIP Core during the current multi-party service.

[0047] When the calling UE and the called UE establish a session and start a multi-party service communication, the AS-charging information collecting function or the IMS charging information collecting function starts to record the actions of the calling and called UEs that are performed on the entities during the multi-party service in real-time.

[0048] In the embodiment shown in Figure 1, the calling and the called PFs send the received SID to the calling and the called UEs, respectively. As such, when it needs to modify the session, or to add a new user into a session, or to make a user re-enter into a session, or to make a user exit the session, it is possible for the UEs to send the SID to a server performing PF or a server performing CF, in order to generate partial CDRs corresponding to the SID, or to generate a new CDR corresponding to the SID, or to update the CDR corresponding to the SID, or to close the CDR corresponding to the SID, respectively. However, sending the SID to the calling and the called UEs is not essential. Only when the above factors are taking into consideration, it is necessary to send the SID to the calling and the called UEs. In Figure 1, the calling and called UEs do not negotiate media parameters before establishing a session i.e., the calling and the called UEs establish an on-demand session. When the calling and called UEs negotiate media parameters before establishing a session i.e., the calling and the called UEs establish a pre-established session, the charging correlation process will be different from the process shown in Figure 1, as shown in Figure 2.

[0049] Figure 2 shows a flowchart of a charging correlation process in a session establishment in accordance with an embodiment of the present invention. In this embodiment, media parameters have been negotiated between the calling UEs and the calling PF that servers the calling UEs before establishing a session, and media parameters have been negotiated also between the called UEs and the called PF that servers the called UEs. The entities involved in the process are the same as the entities in Figure 1. A brief description of the pre-established session is given as follows. Before establishing a session, the UE negotiates session parameters with the server performing PF for the UE. The UE initiates a session establishment process by a session modify request such as a parameter message (REFER message). Therefore in the session establishment process, session parameters negotiation may be omitted and the UE does not need to upload session parameters. The UE just needs to indicate the server performing PF which service is to be joined by the UE. As such, SIP signaling that is exchanged with the UE has fewer bits, and air interface resources may be saved. The server performing PF then initiates a normal session establishment process with the server performing CF according to the indication from the UE, and informs the UE of a successful set-up by sending a media data control protocol message to the UE after the session between the PF and the CF is established. The media data control protocol may be the Talk Burst Control Protocol (TBCP) or the Media Burst Control Protocol (MBCP).

[0050] Figure 2 mainly includes followings.

[0051] 201-202: The calling UE sends a session modify request to the calling PF via the calling IMS/SIP Core corresponding to the calling UE. The calling PF returns a session modify response to the calling UE. The session modify request may be carried in an SIP parameter message (SIP REFER message) and the session modify response may be carried in an SIP accepted message (SIP ACCEPTED message), however, the present invention is not limited to this.

[0052] 203: The calling PF sends a session establishment request to the CF via the calling IMS/SIP Core corresponding to the calling PF.

[0053] 204: The CF assigns a service identifier SID for a current multi-party service and the followings is performed once for each of the called UEs.

[0054] 205: The CF sends the session establishment request to the called IMS/SIP Core via the calling IMS/SIP Core. The session establishment request carries the SID assigned in 204.

[0055] 206-207: The called IMS/SIP Core saves the received SID and sends the session establishment request that carries the SID to the called PF.

[0056] 208-210: The called PF saves the received SID and returns a session establishment response carrying the SID to the CF via the called IMS/SIP Core and the calling IMS/SIP Core.

[0057] While returning the session establishment response to the CF, the called PF also performs 210'. 210' may include followings. The called PF sends to the called IMS/SIP Core a media data control protocol message

carrying the SID, such as a TBCP Connect message used to notify the called UE to join the current service. The called UE saves the SID and returns an acknowledgment e.g. a TBCP Talk Burst Acknowledge message to the called PF via the called IMS/SIP Core. The called PF sends a confirmation e.g. a TBCP Talk Burst Confirm message to the called UE and then media data streams may be transmitted to the called UE.

[0058] In this embodiment, suppose that the called UE has negotiated parameters with the called PF and an auto-answer mode Has been set. That is, the called PF may send the media data control protocol message to the called UE, and return a session establishment response to the CF, without requesting the called UE in advance. The media data control protocol message, such as a TBCP Connect message or a Talk Burst Confirm message that is sent to the called UE, carries the SID. In another example, the called UE may also be configured to a manual response mode. That is, the called PF first sends a session establishment request e.g. an INVITE message to the called UE and then sends the media data control protocol message to the called UE. The called PF sends a session establishment response to the CF after the called user agrees to join the current service. In such a case, the media data control protocol message such as a TBCP Connect message or Talk Burst Confirm message, or the session establishment request such as an INVITE message that is sent to the called UE, may carry the SID.

[0059] 211-214: The CF returns a session establishment response carrying the SID to the calling IMS/SIP Core. The calling IMS/SIP Core saves the received SID and returns a session establishment response carrying the SID to the calling PF. The calling PF also saves the received SID.

[0060] 215-217: The calling PF sends a media data control protocol message, such as a TBCP Connect message, to the calling UE via the calling IMS/SIP Core to inform the calling UE that it is ready for a service session setup. The calling UE returns an acknowledgment, such as a TBCP Talk Burst Acknowledge message, to the calling PF via the calling IMS/SIP Core. The calling PF sends a confirmation such as a TBCP Talk Burst Confirm message to the called UE and is ready to receive media data streams from the calling UE. After that, the calling PF sends a session setup notification such as a NOTIFY message carrying the SID to the calling UE via the calling IMS/SIP Core. The calling UE saves the received SID and a whole session establishment process is completed.

[0061] In this process, the calling PF sends the SID to the calling UE by carrying the SID in a session setup notification or in a media data control protocol message such as a TBCP Connect message or a Talk Burst Confirm message.

[0062] The procedure of sending the SID and the CDRs received from the application service layer entities and bearer control layer entities that are related to the charging correlation process may include the followings.

[0063] The called IMS/SIP Core may save the SID after sending the session establishment request that carries the SID, the media data control protocol message that carries the SID, or the session establishment response that carries the SID. The called IMS/SIP Core may perform Step ***a*** after receiving the session establishment response, e.g., the response to the session establishment request or the response to the media data control protocol message, from the called UE. Step ***a*** is independent of other following steps and this embodiment of the present invention does not limit the sequence order of performing step ***a*** and other steps. Step ***a*** may include followings. The called IMS/SIP Core requests the IMS charging information collecting function to start charging, and sends the CDR of the called UE to the IMS charging information collecting function, wherein the CDR of the called UE carries the SID. The IMS charging information collecting function opens the CDR and starts to record actions performed by the called UE with the called IMS/SIP Core during the current multi-party service.

[0064] The called PF may perform step ***b*** after sending the session establishment request or media data control protocol message to the called UE, or after receiving the session establishment response e.g., a response to the session establishment request or a response to the media data control protocol message from the called UE. Step ***b*** is independent of other following steps and this embodiment of the present invention does not limit the sequence order of performing step ***b*** and other steps. Step ***b*** may include followings. The called PF requests the AS-charging information collecting function to start charging and sends the CDR of the called UE that carries the SID to the AS-charging information collecting function. The AS-charging information collecting function opens the CDR and starts to record actions performed by the called UE with the called PF during the current multi-party service.

[0065] The CF may perform step c after receiving the session establishment response in 210. Step c is independent of other following steps and this embodiment of the present invention does not limit the sequence order of performing step c and the steps following 210. Step c may include followings. The CF requests the AS-charging information collecting function to start charging and sends CDRs of the calling and called UEs that carry the SID to the AS-charging information collecting function. The AS-charging information collecting function opens the CDRs and starts to record actions performed by the calling and called UE with the CF during the current multi-party service.

[0066] The calling PF may perform step ***d*** after receiving the session establishment response in 213. Step ***d*** is independent of other following steps and this embodiment of the present invention does not limit the sequence order of performing step ***d*** and the steps following 213. Step ***d*** may include followings. The calling PF requests the AS-charging information collecting function to start

charging and sends the CDR of the calling UE that carries the SID to the AS-charging information collecting function. The AS-charging information collecting function opens the CDR and starts to record actions performed by the calling UE with the calling PF during the current multi-party service.

[0067] The calling IMS/SIP Core may save the SID after sending the session establishment response carrying the SID. The calling IMS/SIP Core may further perform step e after receiving the session establishment response in 211. Step e is independent of other following steps and this embodiment of the present invention does not limit the sequence order of performing step e and the steps following 211. Step e may include followings. The calling IMS/SIP Core requests the IMS charging information collecting function to start charging and sends the CDR of the calling UE that carries the SID to the IMS charging information collecting function. the IMS charging information collecting function opens the CDR and starts to record actions performed by the calling UE with the calling IMS/SIP Core during the current multi-party service.

[0068] During a multi-party service, a UE may modify the session, for example, the UE may modify the session media parameters, which may result that the AS-charging information collecting function or IMS charging information collecting function may generate a partial CDR. The partial CDR and original CDRs belong to the same multi-party service and need to be correlated in the charging correlation process. Therefore, in a session modification process, the UE needs to send the SID saved during the session establishment process to entities such as the server performing PF and the server performing CF which are related to the charging correlation process, so that the entities can generate partial CDRs corresponding to the SID. In this way the partial CDR may be correlated with other CDRs generated for the multi-party service.

[0069] Figure 3 shows a flowchart of a charging correlation process in a session modification process in accordance with an embodiment of the present invention. The entities involved in this embodiment may include: a calling UE and a calling PF of the calling UE, a calling IMS/SIP Core corresponding to the calling PF and the calling UE, a CF of a current multi-party service, a called UE and a called PF of the called UE, and a called IMS/SIP Core corresponding to the called PF and the called UE. This embodiment also involves: a AS-charging information collecting function corresponding to the calling PF, the called PF and the CF, and an IMS charging information collecting function corresponding to the calling IMS/SIP Core and the called IMS/SIP Core. Figure 3 includes the following processes.

[0070] 301: The calling UE sends a session modify request that carries the SID to the calling PF via the calling IMS/SIP Core. The session modify request is carried in an SIP UPDATE message or in an SIP Re-INVITE message in this embodiment, however, the present invention is not limited to this.

[0071] 302: The calling PF sends the session modify request that carries the SID to the calling IMS/SIP Core.

[0072] 303: The calling IMS/SIP Core sends the session modify request that carries the SID to the CF, and the followings is performed once for each of the called UEs.

[0073] 304-305: The CF sends the session modify request that carries the SID to the called IMS/SIP Core via the calling IMS/SIP Core.

[0074] 306: The called IMS/SIP Core sends the session modify request that carries the SID to the called PF.

[0075] 307-308: The called PF sends the session modify request that carries the SID to the called UE via the called IMS/SIP Core.

[0076] 309-310: The called UE returns a session modify response that carries the SID to the called PF via the called IMS/SIP Core. The session modify response may be carried in an SIP 2000K message in this embodiment, however, the present invention is not limited to this.

[0077] 311-313: The called PF sends the session modify response that carries the SID to the CF via the called IMS/SIP Core and the calling IMS/SIP Core.

[0078] 314-315: The CF returns the session modify response that carries the SID to the calling IMS/SIP Core, the calling IMS/SIP Core returns the session modify response that carries the SID to the calling PF.

[0079] 316-317: The calling PF returns the session modify response that carries the SID to the calling UE via the calling IMS/SIP Core and the session modify process is completed.

[0080] In the above process, the procedure of sending the SID and the CDRs by the application service layer entities and bearer control layer entities that are related to the charging correlation process includes the followings.

[0081] The called PF may perform step ***a*** after sending the session modify request to the called UE or after receiving the session modify response from the called UE. Step ***a*** is independent from steps following 307 and the present invention does not limit the sequence order of performing step ***a*** and the steps following 307. Step ***a*** may include followings. The called PF requests the AS-charging information collecting function to start an intermediate charging and sends a partial CDR of the called UE, that is generated by the called PF and carries the SID, to the AS-charging information collecting function. The AS-charging information collecting function updates CDR of the called PF, saves the partial CDR, and starts to record actions that may affect an accounting and are performed by the called UE on the called PF after the session is modified in the current multi-party service.

[0082] The called IMS/SIP Core may save the SID after sending the session modify request or the session modify request response carrying the SID. The called IMS/SIP Core may further perform step ***b*** after receiving the session modify response from the called UE. Step ***b*** is independent from steps following 309 and the present inven-

tion does not limit the sequence order of performing step ***b*** and the steps following 309. Step ***b*** may include followings. The called IMS/SIP Core requests the IMS charging information collecting function to start an intermediate charging and sends a partial CDR of the called UE, that is generated by the called IMS/SIP Core and carries the SID, to the IMS charging information collecting function. The IMS charging information collecting function updates CDR of the called IMS/SIP Core, saves the partial CDR and starts to record actions that may affect an accounting and are performed by the called UE on the called IMS/SIP Core after the session is modified in the current multi-party service.

[0083] The CF may perform step c after receiving the session modify response in 313. Step c is independent from steps following 313 and the present invention does not limit the sequence order of performing step ***c*** and the steps following 313. Step ***c*** may include followings. The CF requests the AS-charging information collecting function to start an intermediate charging and sends the partial CDRs of the calling UEs and the called UEs, that is generated by the CF and carries the SID, to the AS-charging information collecting function. The AS-charging information collecting function updates CDR of the CF, saves the partial CDRs of the calling and the called UEs and starts to record actions that may affect an accounting and are performed by the calling and called UE on the CF after the session is modified in the current multi-party service.

[0084] The calling PF may perform step ***d*** after receiving the session modify response in 315. Step ***d*** is independent from steps following 315 and the present invention does not limit the sequence order of performing step ***d*** and the steps following 315. Step ***d*** may include followings. The calling PF requests the AS-charging information collecting function to start an intermediate charging and sends the partial CDR of the calling UE, which is generated by the calling PF and carries the SID, to the AS-charging information collecting function. The AS-charging information collecting function updates CDR of the calling PF, saves the partial CDR of the calling UE and starts to record actions that may affect an accounting and are performed by the calling UE on the calling PF after the session is modified in the current multi-party service.

[0085] The calling IMS/SIP Core may save the SID while sending the session modify response carrying the SID. The calling IMS/SIP Core may further perform step ***e*** after receiving the session modify response in 314. Step e is independent from steps following 314 and the present invention does not limit the sequence order of performing step e and the steps following 314. Step e may include followings, the calling IMS/SIP Core requests the IMS charging information collecting function to start an intermediate charging and sends the partial CDR of the calling user, which is generated by the calling IMS/SIP Core and carries the SID, to the IMS charging information collecting function. The IMS charging information collecting function updates CDR of the calling IMS/SIP Core, saves the partial CDR of the calling user and starts to record actions that may affect an accounting and are performed by the calling UE on the calling IMS/SIP Core after the session is modified in the current multi-party service.

[0086] In the embodiments shown in Figures 1 to 3, the calling PF, the CF and the called PF are separated entities. In practical applications, any one or any combination of the calling PF, the CF and the called PF may be provided by one entity, in which case the basic processes are the same as the embodiments shown in Figures 1 to 3, and will not be described in detail herein but are still covered by the protection scope of the present invention.

[0087] In Figures 1 and 2, the calling PF and the CF correspond to a same IMS/SIP Core and the called PF corresponds to another IMS/SIP Core. In practical applications, the calling PF, the CF and the called PF may correspond to different IMS/SIP Cores. When the calling UE and a called UE are in one network provided by an operator, the calling PF and the called PF of the called UE may correspond to the same IMS/SIP Core. When the calling UE and a called UE are in different networks provided by different operators, the calling PF and the called PF correspond to different IMS/SIP Cores. When the calling PF and the CF are in one network provided by the same operator, the calling PF and the CF correspond to the same IMS/SIP Core. When the called PF and the CF are in different networks provided by different operators, the called PF and the CF correspond to different IMS/SIP Cores. However, no matter the calling PF, the CF and the called PF correspond to the same IMS/SIP Core or to different IMS/SIP Cores, the processes in embodiments of the present invention are essentially the same. In one word, the application service layer entities such as the calling PF, the CF and the called PF send/receive session establishment/modify requests or session establishment/modify responses via corresponding IMS/SIP Cores, and the detailed processes thereof will not be described herein, but are still covered by the protection scope of the present invention.

[0088] During an existing multi-party service, when adding a new user, the control function entity (e.g., the CF) of the multi-party service generates a new CDR for a session of the new user. A service identifier will be adapted to correlate the CDRs of the new user when adding the new user.

[0089] Figure 4 shows a flowchart of a charging correlation process when adding a new user to an existing multi-party service in accordance with an embodiment of the present invention. A process of adding a new user includes: requesting by a UE to add another user (a third party user) into a current multi-party service. The third party user is shown as an added UE in Figure 4. The entities involved in this embodiment include: a UE and a PF of the UE, an IMS/SIP Core corresponding to the UE, an added UE, a CF of the current multi-party service, an

AS-charging information collecting function and an IMS charging information collecting function. In this embodiment, suppose that the UE and the new user added to the current service (the added UE) are served by the same PF, and the UE, the added UE, the PF and the CF correspond to the same IMS/SIP Core.

[0090] As shown in Figure 4, the process includes followings.

[0091] 401-402: The UE sends an adding request that carries an SID to the PF via the IMS/SIP Core. The adding request may be carried in an SIP REFER message in this embodiment, however, the present invention is not limited to this.

[0092] 403-404: The PF sends the adding request that carries the SID to the CF via the IMS/SIP Core.

[0093] 405-406: The CF sends the adding request that carries the SID to the PF of the added UE via the IMS/SIP Core, and the PF sends the adding request that carries the SID to the added UE. The added UE returns an adding response that carries the SID to the PF via the IMS/SIP Core after receiving the adding request. The PF returns the adding response that carries the SID to the CF via the IMS/SIP Core. As such, the new UE is added to the current service.

[0094] The adding request may be carried in an SIP INVITE message and the adding response may be carried in an SIP 2000K message, however, the present invention is not limited to this.

[0095] 407: The CF returns the adding response that carries the SID to the PF of the UE via the IMS/SIP Core. The PF informs the UE that the new user has been added to the current service by returning the adding response that carries the SID to the UE via the IMS/SIP Core. The adding response may be carried in an SIP ACCEPTED message in this embodiment; however, the present invention is not limited to this.

[0096] In Figure 4, the application service layer entities related to the charging correlation process include the PF and the CF. The CF may perform step ***a*** after receiving the adding response in 406. Step ***a*** is independent of other following steps and the present invention does not limit the sequence order of performing step ***a*** and the follow-up steps. The PF may perform step ***b*** after receiving the adding response in 406 and step ***b*** is independent of other following steps and the present invention does not limit the sequence order of performing step ***b*** and the follow-up steps.

[0097] Step ***a*** may include followings. The CF requests the AS-charging information collecting function to start charging and sends the CDR of the new user (the added UE) that is generated by the CF and carries the SID to the AS-charging information collecting function. The AS-charging information collecting function opens the CDR of the new user from the CF and starts to record actions performed by the new user on the CF during the current multi-party service.

[0098] Step ***b*** may include followings. The PF requests the AS-charging information collecting function to start charging and sends the CDR of the new user that is generated by the PF and carries the SID to the AS-charging information collecting function. The AS-charging information collecting function opens the CDR of the new user from the PF and starts to record actions performed by the new user on the PF during the current multi-party service.

[0099] The bearer control layer entity related to the charging correlation process in Figure 4 is the IMS/SIP Core. The IMS/SIP Core may perform step c after receiving the adding response in 406, and step c is independent of other following steps and the present invention does not limit the sequence order of performing step c and the follow-up steps. Step ***c*** may include followings. The IMS/SIP Core requests the IMS charging information collecting function to start charging and sends the CDR of the new user that is generated by the IMS/SIP Core and carries the SID to the IMS charging information collecting function. The IMS charging information collecting function opens the CDR of the new user from the IMS/SIP Core and starts to record actions performed by the new user on the IMS/SIP Core during the current multi-party service.

[0100] In embodiments shown in Figures 3 and 4, the UE may establish an on-demand session or have a pre-established session, the processes in Figures 3 and 4 may be applied to both cases.

[0101] If a UE exits a session, the AS-charging information collecting function and the IMS charging information collecting function need to close the CDRs of the multi-party service of the UE. In such a case, the SID of the current multi-party service needs to be sent to the AS-charging information collecting function and the IMS charging information collecting function so that the CDRs corresponding to the same SID among all CDRs of the UE may be closed based on the same SID.

[0102] Figure 5 shows a flowchart of a charging correlation process when a UE that has established a pre-established session exits a session in accordance with an embodiment of the present invention. The entities involved in this embodiment include: a UE and a PF of the UE, an IMS/SIP Core corresponding to the UE, a CF of a current multi-party service, an AS-charging information collecting function and an IMS charging information collecting function. In this embodiment, the UE, the PF and the CF correspond to the same IMS/SIP Core.

[0103] As shown in Figure 5, the process includes followings.

[0104] 501-502: The UE sends a release session request that carries an SID to the PF via the IMS/SIP Core. The release session request is carried in an SIP BYE message in this embodiment, however, the present invention is not limited to this.

[0105] 503: The PF sends the release session request that carries the SID to the CF via the IMS/SIP Core.

[0106] 504: The CF returns a release session response that carries the SID to the PF via the IMS/SIP Core. The release session response may be carried in

an SIP 200OK message in this embodiment, however, the present invention is not limited to this.

[0107] 505-506: The PF sends the release session response that carries the SID to the UE via the IMS/SIP Core.

[0108] In Figure 5, the application service layer entities related to the charging correlation process include the PF and the CF. The CF may perform step ***a*** after receiving the release session response in 503. Step ***a*** is independent of following steps and the present invention does not limit the sequence order of performing step ***a*** and the steps following 503. The PF may perform step ***b*** after receiving the release session response in 504 and step ***b*** is independent of following steps and the present invention does not limit the sequence order of performing step ***b*** and the steps following 504.

[0109] Step ***a*** may include followings. The CF requests the AS-charging information collecting function to stop charging and sends the SID to the AS-charging information collecting function. The AS-charging information collecting function closes CDR of the UE from the CF and stops recording charging data of the UE.

[0110] Step ***b*** may include followings. The PF requests the AS-charging information collecting function to stop charging and sends the SID to the AS-charging information collecting function. The AS-charging information collecting function closes CDR of the UE from the PF and stops recording the charging data of the UE.

[0111] The bearer control layer entity related to the charging correlation process in Figure 5 is the IMS/SIP Core. The IMS/SIP Core may perform step ***c*** after receiving the release session response in 505, and step ***c*** is independent of following steps and the present invention does not limit the sequence order of performing step c and the steps following 505.

[0112] Step ***c*** may include followings. The IMS/SIP Core requests the IMS charging information collecting function to stop charging and sends the SID to the IMS charging information collecting function. The IMS charging information collecting function closes CDR of the UE from the PF.

[0113] The release session process shown in Figure 5 is suitable to be used for a user who establishes an on-demand session. For a user who establishes a pre-established session, a different release session process shall be used. Figure 6 shows a flowchart of a charging correlation process for a user who establishes a pre-established session in accordance with an embodiment of the present invention. The entities involved in this embodiment include: a UE and a PF of the UE, an IMS/SIP Core corresponding to the UE, a CF of a current multi-party service, an AS-charging information collecting function and an IMS charging information collecting function. In this embodiment, the UE, the PF and the CF correspond to the same IMS/SIP Core.

[0114] A whole session establishment process for a user who establishes a pre-established session includes two parts: firstly, the UE and the PF negotiate session parameters before establishing a session; then, the PF establishes a session with the CF for the UE when the UE is ready for establishing the session. Therefore this kind of session establishment process shall be ended in two steps: firstly, the session that is pre-established between the UE and the PF is modified; then, the session between the PF and the CF is released. As shown in Figure 6, the process includes followings.

[0115] 601-602: The UE sends a session modify and release request that carries an SID to the PF via the IMS/SIP Core in order to release the session. The session modify and release request may be carried in an SIP REFER BYE message in this embodiment, however, the present invention is not limited to this.

[0116] 603: The PF returns a session modify response to the UE via the IMS/SIP Core. The session modify response may be carried in an SIP ACCEPTED message in this embodiment, however, the present invention is not limited to this.

[0117] 604: The PF sends a release session request carrying the SID to the CF via the IMS/SIP Core. The release session request may be carried in a BYE message, however, the present invention is not limited to this.

[0118] 605: The CF returns a release session response to the PF via the IMS/SIP Core. The release session response may be carried in an SIP 2000K message in this embodiment, however, the present invention is not limited to this.

[0119] 606-607: The PF sends a release session notification to the UE via the IMS/SIP Core to notify the UE of a successful release of the session between the UE and the CF. The UE returns a release session response to the PF. The release session response may be carried in a NOTIFY message, and the release session response may be carried in an OK message, however, the present invention is not limited to this.

[0120] In Figure 6, the application service layer entities related to the charging correlation process include the PF and the CF. The CF may perform step ***a*** after receiving the release session request in 604 and after successful releasing the session. Step ***a*** is independent of following steps and the present invention does not limit the sequence order of performing step ***a*** and the steps following 604. The PF may perform step ***a*** after receiving the release session response in 607.

[0121] Step ***a*** may include followings. The CF requests the AS-charging information collecting function to stop charging and sends the SID to the AS-charging information collecting function. The AS-charging information collecting function closes CDR of the UE from the CF and stops recording the charging data of the UE.

[0122] Step ***b*** may include followings. The PF requests the AS-charging information collecting function to stop charging and sends the SID to the AS-charging information collecting function. The AS-charging information collecting function closes CDR of the UE from the PF and stops recording the charging data of the UE.

[0123] The bearer control layer entity related to the

charging correlation process in Figure 6 is the IMS/SIP Core. The IMS/SIP Core may perform step ***c*** after receiving the release session response in 605, and step ***c*** is independent of following steps and the present invention does not limit the sequence order of performing step c and the steps following 605.

[0124] Step ***c*** may include followings. The IMS/SIP Core requests the IMS charging information collecting function to stop charging and sends the SID to the IMS charging information collecting function. The IMS charging information collecting function closes CDR of the UE from the PF.

[0125] Besides the situations described above, new CDRs may be generated by the entities related to the charging correlation process in two other situation. The charging correlation processes in accordance with the embodiments of the present invention are suitable in such two situations. In the first situation, a user who establishes an on-demand session exits a current multi-party service session temporarily while the current multi-party service proceeds, then the user re-enters the multi-party service. In the other of the two situations, a user who establishes a pre-established session exits a current multi-party service session temporarily while the current multi-party service proceeds, then the user re-enters the multi-party service. The charging correlation processes in the two situations are described with reference to Figures 7 and 8.

[0126] Figure 7 shows a flowchart of a charging correlation process in a case that a user who establishes an on-demand session re-enters a session after the user exits the session in accordance with an embodiment of the present invention. The entities involved in this embodiment include: a UE and a PF of the UE, an IMS/SIP Core corresponding to the UE, a CF of a current multi-party service, an AS-charging information collecting function and an IMS charging information collecting function. In this embodiment, the UE, the PF and the CF correspond to a same IMS/SIP Core. As shown in Figure 7, the process includes followings.

[0127] 701-702: The UE sends a session joining request carrying an SID to the PF via the IMS/SIP Core. The session joining request may be carried in an SIP REFER message or an SIP INVITE message in this embodiment, however, the present invention is not limited to this.

[0128] 703: The PF sends the session joining request carrying the SID to the CF via the IMS/SIP Core.

[0129] 704: The CF returns a session joining response carrying the SID to the PF via the IMS/SIP Core. The session joining response may be carried in an SIP 2000K message or an SIP ACCEPTED message in this embodiment, however, the present invention is not limited to this.

[0130] 705-706: The PF sends the session joining response carrying the SID to the UE via the IMS/SIP Core.

[0131] In Figure 7, the application service layer entities related to the charging correlation process include the PF and the CF. The CF may perform step ***a*** after receiving the session joining response in 703. Step ***a*** is independent of following steps and the present invention does not limit the sequence order of performing step ***a*** and the steps following 703. The PF may perform step ***b*** after receiving the session joining response in 704 and step ***b*** is independent of following steps and the present invention does not limit the sequence order of performing step ***b*** and the steps following 704.

[0132] Step ***a*** may include followings, the CF requests the AS-charging information collecting function to start charging and sends the CDR of the user who requests to re-enter the session (the UE), which is generated by the CF and carries the SID, to the AS-charging information collecting function. The AS-charging information collecting function opens the CDR of the UE received from the CF and starts to record actions that affect an accounting and are performed by the UE on the CF during the current multi-party service. It need to be noted that when the user re-enters the session, the opened CDR of the UE is a new CDR instead of the CDR of the UE generated before the UE dropped out of the session. However, the two CDRs have the same SID and can be correlated based on the SID.

[0133] Step ***b*** may include followings. The PF requests the AS-charging information collecting function to start charging and sends the CDR of the UE, which is generated by the PF and carries the SID, to the AS-charging information collecting function. The AS-charging information collecting function opens the CDR of the UE received from the PF and starts to record actions that affect the accounting and are performed by the UE on the PF during the current multi-party service.

[0134] The bearer control layer entity related to the charging correlation process in Figure 7 is the IMS/SIP Core. The IMS/SIP Core may perform step c after receiving the session joining response in 705, and step c is independent of following steps and the present invention does not limit the sequence order of performing step ***c*** and the steps following 705.

[0135] Step ***c*** may include followings. The IMS/SIP Core requests the IMS charging information collecting function to start charging and sends the CDR of the UE, which is generated by the IMS/SIP Core and carries the SID, to the IMS charging information collecting function. The IMS charging information collecting function opens the CDR of the UE from the IMS/SIP Core and starts to record actions that affect the accounting and are performed by the UE on the IMS/SIP Core during the current multi-party service.

[0136] Figure 8 shows a flowchart of a charging correlation process in a case where a user who establishes a pre-established session re-enters a session after the user exits the session in accordance with an embodiment of the present invention. The entities involved in this embodiment include: a UE and a PF of the UE, an IMS/SIP Core corresponding to the UE, a CF of the current multi-party service, an AS-charging information collecting function and an IMS charging information collecting func-

tion. In this embodiment, the UE, the PF and the CF correspond to the same IMS/SIP Core. As shown in Figure 8, the process includes followings.

[0137] 801-802: The UE and the PF negotiate session parameters before establishing a session. Then the UE sends a session modify request carrying an SID to the PF via the IMS/SIP Core. The session modify request may be carried in an SIP REFER message in this embodiment, however, the present invention is not limited to this.

[0138] 803: The PF returns a session modify response carrying the SID to the UE via the IMS/SIP Core. The session modify response may be carried in an SIP ACCEPTED message in this embodiment. However, the present invention is not limited to this.

[0139] 804: The PF sends a session joining request carrying the SID to the CF via the IMS/SIP Core to establish a session between the UE and the CF. The session joining request may be carried in an SIP INVITE message. However, the present invention is not limited to this.

[0140] 805-806: The CF returns a session joining response carrying the SID to the PF via the IMS/SIP Core. The session joining response may be carried in an SIP 200OK or an OK message. However, the present invention is not limited to this.

[0141] 807-809: The PF sends to the UE a session joining notification (e.g., a NOTIFY message) carrying a result of the session setup via the IMS/SIP Core. The UE returns a session joining response (e.g., an OK response) to the PF via the IMS/SIP Core. As such, the session re-entering process is completed.

[0142] In Figure 8, the service layer entities related to the charging correlation process include the PF and the CF. The CF may perform step ***a*** after receiving the session joining request in 804 and after successful adding the UE into the session. Step ***a*** is independent of other following steps and the present invention does not limit the sequence order of performing step ***a*** and the steps following 804. The PF may perform step b after receiving the session joining response in 809 and similarly, the bearer control layer entity related to the charging correlation process, i.e., the IMS/SIP Core, may perform step c after receiving the response in 809.

[0143] Step ***a*** may include followings, the CF requests the AS-charging information collecting function to start charging and sends the CDR of the user (the UE) who requests to re-enter the session, which is generated by the CF and carries the SID, to the AS-charging information collecting function. The AS-charging information collecting function opens the CDR of the UE from the CF and starts to record actions that affect an accounting and are performed by the UE on the CF during the current multi-party service. It need to be noted that when the user re-enters the session, the opened CDR of the UE is a new CDR instead of the CDR of the UE that is generated before the UE dropped out of the session. However, the two CDRs have the same SID and can be correlated based on the SID.

[0144] Step ***b*** may include followings. The PF requests the AS-charging information collecting function to start charging and sends the CDR of the UE, which is generated by the PF and carries the SID, to the AS-charging information collecting function. The AS-charging information collecting function opens the CDR of the UE received from the PF and starts to record actions that affect the accounting and are performed by the UE on the PF during the current multi-party service.

[0145] The bearer control layer entity related to the charging correlation process in Figure 8 is the IMS/SIP Core. The IMS/SIP Core may perform step c after receiving the session joining response in 805, and step c is independent of following steps and the present invention does not limit the sequence order of performing step c and the steps following 805.

[0146] Step c may include followings. The IMS/SIP Core requests the IMS charging information collecting function to start charging and sends the CDR of the UE, which is generated by the IMS/SIP Core and carries the SID, to the IMS charging information collecting function. The IMS charging information collecting function opens the CDR of the UE from the IMS/SIP Core and starts to record actions that affect the accounting and are performed by the UE on the IMS/SIP Core during the current multi-party service.

[0147] In embodiments shown in Figures 4 to 8, the PF and the CF are performed by two separated entities. In practical applications, the PF and the CF may be performed by one entity. In such a case, the essential processes of the embodiments in which the PF and the CF are performed by one entity are similar to the processes shown in Figures 4 to 8 and will not be described in detail herein, but are still covered by the protection scope of the invention.

[0148] Moreover, the PF and the CF correspond to the same bearer control layer entity e.g., the IMS/SIP Core in Figures 4 to 8. In practical applications, the PF and the CF may correspond to different bearer control layer entities. When the PF and the CF are in the same network of an operator, the PF and the CF correspond to the same IMS/SIP Core. When the PF and the CF are in different networks of different operators, the PF and the CF correspond to different IMS/SIP Cores. No matter the PF and the CF correspond to the same IMS/SIP Core or to different IMS/SIP Cores, the method in accordance with embodiments of the present invention is applicable. No matter the PF and the CF correspond to the same bearer control layer entity or to different bearer control layer entities, the method in accordance with embodiments of the present invention is applicable. In one word, the application service layer entities such as the PF and the CF send/receive messages comprising session modify requests/responses, session joining requests/responses, release session requests/responses, session modify requests/responses and session modify and release requests via corresponding IMS/SIP Cores. Detailed proc-

esses will not be described herein, but are still covered by the protection scope of the present invention.

[0149] In the flowcharts of the above embodiments, the responses returned by the called UE to the CF carry the SID. However, since the CF has learnt the SID of the current service, the responses from the called UE to the CF may not carry the SID.

[0150] In the above embodiments, the SID is sent to the AS-charging information collecting function and IMS charging information collecting function, thus the application service layer of the AS and the bearer control layer of the IMS can perform a function in accordance with the charging correlation scheme provided by embodiments of the present invention. In practical applications, it may be unnecessary for the application service layer or the bearer control layer to implement the charging correlation process, and in such a case the SID and CRDs needs not to be sent to the AS-charging information collecting function or the IMS charging information collecting function.

[0151] The embodiments of the present invention adopt SIDs as service identifiers, and a description of the SID used in a PoC service is given herein. In a PoC service, SID is assigned by a service control function to a calling/called PoC client. The SID is used to identify a PoC group session in an SIP communication, but is not used in charging data generation processes. A PoC Session Identity (PoC SID) is constructed in a format of a SIP Uniform Resource Identifier (URI) and is sent during a PoC session establishment process to a PoC client in a Contact header field and/or a TBCP CONNECT message. The PoC SID may be assigned and available for a long period, or be assigned temporarily. A long term PoC SID is adapted to a pre-arranged PoC group session. A temporary PoC SID is assigned by a server performing CF in the network to a PoC client when the PoC client establishes a PoC session for a PoC service for a first time, and is remained valid as long as the PoC service is in progress. When the PoC client establishes a session for another PoC service, the new PoC service is assigned a different PoC SID. However, if the PoC client exits a session of a PoC service temporarily and re-enters the same PoC service later, the PoC SID to used in the session will remain the same. It can be seen that the PoC SID may be used to identify a PoC service, therefore the PoC SID can also be used to charge correlation information of the service. Such PoC SID cannot be modified easily in transmission and the PoC client cannot modify the PoC SID after receiving the PoC SID, hence it is safe and reliable to use the PoC SID in a charging correlation process.

[0152] Embodiments of the present invention also propose a second charging correlation scheme to implement a charging correlation for a plurality of CDRs generated for one user in a multi-service that comprises a plurality of sub-services. The charging correlation scheme provides two ways to implement this charging correlation.

[0153] According to a first method, a service control function assigns a multi-service identifier for a current multi-service and assigns a sub-service identifier to each of the sub-services included in the current multi-service. The multi-service identifier and the sub-service identifiers are sent to a charging system. The charging system correlates CDRs of a sub-service based on the sub-service identifier of the sub-service, and correlates CDRs of the plurality of sub-services based on the multi-service identifier.

[0154] According to a second method, a service control function just assigns a multi-service identifier for a current multi-service. The multi-service identifier is sent to a charging system which correlates the CDRs of a plurality of sub-services of the current multi-service based on the multi-service identifier.

[0155] In a multi-service, a user may establish one or a plurality of sessions in each of the sub-services and a CDR is generated for each of the sessions of the user. Different methods may be used to correlate the CDRs based on the multi-service identifier. The CDRs to be correlated based on the multi-service identifier may be: CDRs corresponding to a plurality of sub-services (or a plurality of sessions of a plurality of sub-services) establish for one user in the current multi-service, or CDRs corresponding to a plurality of sub-services (or a plurality of sessions of a plurality of sub-services) established for a part of users or all users in the current multi-service. The method of correlating CDRs may be chosen based on special correlation policy applied. The contents and forms of correlation policies are not the technical problem to be solved by the present invention and will not be described further herein.

[0156] In a multi-service, a sub-service corresponds to a sub-service server. A service control function controls the sub-service servers to initiate, modify and terminate sub-services in order to initiate, modify and terminate the multi-service. According to the first method described above, for a sub-service, after the service control function assigns the multi-service identifier and the sub-service identifiers corresponding to the sub-services, the service control function sends the multi-service identifier and a sub-service identifier corresponding to a sub-service to a sub-service server corresponding to the sub-service. The sub-service server generates CDRs for the sub-service and sends the CDRs, the received multi-service identifier and the sub-service identifier to an AS-charging information collecting function of the sub-service server. The AS-charging information collecting function sends the received multi-service identifier, the sub-service identifier and the CDRs to a billing center. The billing center correlates the CDRs generated by one sub-service server based on the sub-service identifier, and further correlates CDRs generated by the sub-service servers based on the multi-service identifier. According to the second method described above, after assigning the multi-service identifier, the service control function sends the multi-service identifier to each sub-service server corresponding to each sub-service. A sub-service

server generates CDRs for each corresponding sub-service and sends the received multi-service identifier and the CDRs generated to the AS-charging information collecting function of the sub-service server. The AS-charging information collecting function sends the received multi-service identifier and the CDRs to the billing center. The billing center correlates the CDRs from different sub-service servers based on the multi-service identifier.

[0157] When the charging correlation scheme is applied to the application service layer, the charging information collecting function includes the AS-charging information collecting functions corresponding to the sub-service servers. The scheme can further be applied to the bearer control layer, and in such a case the charging information collecting function includes bearer control layer-charging information collecting functions of the bearer control layer entities corresponding to the sub-service servers. The bearer control layer entities corresponding to the sub-service servers are used to implement the service control functions. The bearer control layer entities corresponding to the sub-service servers are further used to record the multi-service identifier or a combination of the multi-service identifier and a sub-service identifier, and generate CDRs for corresponding sub-services. The bearer control layer entities send the multi-service identifier or the combination of the multi-service identifier and a sub-service identifier, and the CDRs to the bearer control layer-charging information collecting function of the bearer control layer entities. The AS-charging information collecting function and the bearer control layer-charging information collecting function send the received CDRs, and the multi-service identifier or the combination of the multi-service identifier and a sub-service identifier to the billing center. In Figures 9 and 10, the application service layer is taken as an example. When the present invention is applied only to the bearer control layer, charging correlation process involves UEs, service control functions, bearer control layer entities corresponding to sub-service servers, bearer control layer-charging information collecting functions and a billing center, without involving sub-service servers and AS-charging information collecting functions. Embodiments that the bearer control layer is employed are not described in detailed herein, but are still covered by the protection scope of the present invention. When the multi-service identifier or the combination of the multi-service identifier and the sub-service identifier is sent to an AS-charging information collecting function or to bearer control layer-charging information collecting function, the multi-service identifier or the combination of the multi-service identifier and the sub-service identifiers may be carried in CDRs.

[0158] Moreover, a multi-service usually includes a primary service and one or more supplementary services. That is, a multi-service includes a sub-service as the primary service and at least one sub-service as the supplementary service. The sub-service server and sub-service identifier corresponding to the primary service are called primary server and primary service identifier respectively, and the sub-service server and sub-service identifier corresponding to a supplementary service are called supplementary server and supplementary service identifier respectively. The service control function may be performed by a separated entity or be performed by the primary server. The multi-service identifier assigned to the multi-service may be identical with or different from the sub-service identifiers. When the multi-service includes a primary service and at least one supplementary service, the multi-service identifier may be identical with the primary service identifier.

[0159] The embodiments of the present invention are mainly applied to session-based applications or services such as multi-party services, the session IDs (SIDs) corresponding to different service sessions are already applied to conventional session-based services. The existing SIDs may be used as service identifiers to correlate a plurality of CDRs. Also new identifiers may be defined as the service identifiers. Usually information exchanged among entities on the application service layer is sent via corresponding bearer control layer entities. For example, servers performing PF of the multi-party service, the server performing CF, and the UEs may exchange information via corresponding bearer control layer entities such as an IMS/SIP Core network (IMS/SIP Core). At the same time, the network functions in the IMS/SIP Core may also generate CDRs for the current application or service in order to implement the charging correlation process on the bearer control layer. Each sub-service server of a sub-service corresponds to a bearer control layer entity, and the bearer control layer entity is adapted to bear the sub-service server.

[0160] At present, mainstream multi-services include: combinations of a plurality of multi-party services, a combination of a multi-party service and a Location Service or a combination of a multi-party service and a Presence Service. The second charging correlation scheme of the present invention is described hereinafter with reference to a multi-service comprising two multi-party services, e.g. a PoC service and a Conference service. A server performing CF and a server performing PF in the multi-party service are used to provide the services, yet the second charging correlation scheme focuses on the charging correlation of the sub-services, not internal flows of the sub-services. Therefore, for the sake of simplicity, the service processes between the server performing CF and the server performing PF in the multi-party service are omitted, and the server performing CF and the server performing PF are considered as sub-service servers of the multi-party service. A sub-service server corresponding to the PoC service is called a PoC server, and a sub-service server corresponding to the Conference service is called a Conference server. In embodiments of the present invention, the service control function is implemented by a PoC server.

[0161] Figure 9 shows a flowchart of a charging cor-

relation process for a multi-service in accordance with an embodiment of the present invention. In this embodiment, the service control function assigns a multi-service identifier. In this embodiment, the SID adapted to an individual PoC service in a conventional PoC service is used as the multi-service identifier. The entities involved in the embodiment include: PoC Client 1, PoC Client 2, a PoC server, a Conference server and a charging information collecting function. In this embodiment, PoC Client 1 initiates a multi-service and adds PoC Client 2 into the multi-service. As shown in Figure 9, the process includes followings.

[0162] 901: PoC Client 1 sends a session establishment request to the PoC server to initiate a PoC service. The session establishment request carries information of PoC Client 2, and is used to instruct to establish a multi-service comprising a Conference service and to add PoC Client 2 into the multi-service. The PoC server implements PoC service logic. A service control function in the PoC server assigns a multi-service identifier to the current multi-service. The multi-service identifier is the SID assigned to the PoC service. The session establishment request may be carried in an SIP INVITE message. However, the present invention is not limited to this.

[0163] 902: The service control function in the PoC server sends the session establishment request (e.g., an INVITE message) carrying the SID to the Conference server to initiate a Conference service. The Conference server returns a session establishment response (e.g., a 200OK message). The session establishment request carries the information of PoC Client 2 to indicate that PoC Client 2 need to be added into the Conference service.

[0164] After 902, both the PoC service and the Conference service are originated and the PoC server and the Conference server will perform steps ***b*** and ***a*** respectively to generate CDRs of the PoC service and CDRs of the Conference service on the AS-charging information collecting function.

[0165] Step ***a*** may include the followings. The Conference server generates CDRs for the present Conference service, requests the AS-charging information collecting function to start charging, and sends to the AS-charging information collecting function the CDRs that are generated by the Conference server and carries the SID. The AS-charging information collecting function opens the CDR received from the Conference server, starts to record actions which affect the accountings and, are performed on the Conference server by users of the Conference service, and returns a response to the Conference server.

[0166] Step ***b*** may include the followings. The PoC server generates a CDR for the current PoC service, requests the AS-charging information collecting function to start charging, and sends to the AS-charging information collecting function the CDR that is generated by the PoC server and carries the SID. The AS-charging information collecting function opens the CDR received from the PoC server, starts to record actions which affect the accountings and are performed on the PoC server by users of the PoC service, and returns a response to the PoC server.

[0167] 903: The PoC server sends a session joining request carrying the SID to PoC Client 2 in order to add PoC Client 2 into the current PoC service session. PoC Client 2 returns a session joining response to the PoC server in order to indicate that PoC Client 2 has successfully joined the current PoC service session.

[0168] After the PoC server has successfully added PoC Client 2 into the current PoC service, the information of PoC Client 2 needs to be recorded in the CDRs of the current PoC service session on the AS-charging information collecting function, therefore step c needs to be performed. Step c may include the followings. The PoC server requests the AS-charging information collecting function to update the charging, and sends the CDR carrying the SID of PoC Client 2 to the AS-charging information collecting function. The AS-charging information collecting function updates the CDR of PoC Client 2 that carries the SID and is received from the PoC server, records the information of PoC Client 2 in the CDR, starts to record actions that affect the accounting and are performed by PoC Client 2 on the PoC server during the current multi-service, and returns a response to the PoC server.

[0169] 904: The PoC server sends an acknowledgement (ACK) to the Conference server after PoC Client 2 has successfully joined the current PoC service session, in order to indicate that it is ready for the Conference server to add PoC Client 2 into the service session. The Conference server performs operations similar to the operations in 903 to add PoC Client 2 into the current Conference service session.

[0170] The information of PoC Client 2 needs to be recorded in the CDRs of the current Conference service session on the AS-charging information collecting function, therefore step ***d*** needs to be performed. Step ***d*** may include the followings. The Conference server requests the AS-charging information collecting function to update the charging, sends the CDRs that carries the SID of PoC Client 2 to the AS-charging information collecting function. The AS-charging information collecting function updates the CDRs of PoC Client 2 that carries the SID and is received from the Conference server, records the information of PoC Client 2 in the CDRs, starts to record actions that are performed by PoC Client 2 on the Conference server and affect the accounting during the current multi-service, and returns a response to the Conference server.

[0171] 905-906: The PoC server sends a session joining request (e.g., an INVITE message) carrying the SID to the Conference server, and the Conference server returns a session joining response (e.g., a 200OK message). The session joining request carries information of PoC Client 1 to indicate that PoC Client 1 need to be added into the Conference service. At the same time, the

PoC server adds PoC Client 1 into the current PoC service session and returns a session joining response (e.g., a 2000K message) to PoC Client 1.

[0172] After the PoC server has successfully added PoC Client 1 into the current PoC service session, the information of PoC Client 1 needs to be recorded in the CDRs of the current PoC service session on the AS-charging information collecting function, therefore step e needs to be performed. Step e may include the followings. The PoC server requests the AS-charging information collecting function to update the charging, and sends the CDRs carrying the SID of PoC Client 1 to the AS-charging information collecting function. The AS-charging information collecting function updates the CDRs of PoC Client 1 that carries the SID and is received from the PoC server, records the information of PoC Client 1 in the CDR, starts to record actions that are performed by PoC Client 1 on the PoC server and affect the accounting during the current multi-service, and returns a response to the PoC server.

[0173] 907: The PoC server sends an acknowledgement (ACK) to the Conference server after PoC Client 1 has successfully joined the current PoC service session, in order to indicate that it is ready for the Conference server to add PoC Client 1 into the service session. The Conference server performs operations similar to the operations in 903 to add PoC Client 1 into the current Conference service session.

[0174] The information of PoC Client 1 needs to be recorded in the CDRs of the current Conference service session on the AS-charging information collecting function, therefore step ***f*** needs to be performed. Step ***f*** may include the followings. The Conference server requests the AS-charging information collecting function to update the charging, and sends the CDRs carrying the SID of PoC Client I to the AS-charging information collecting function. The AS-charging information collecting function updates the CDRs of PoC Client 1 that carries the SID and is received from the Conference server, records the information of PoC Client 1 in the CDR, starts to record actions that are performed by PoC Client 1 on the Conference server and affect the accounting during the current multi-service, and returns a response to the Conference server.

[0175] After the processes described above, the CDRs of the sub-services, which are saved in the AS-charging information collecting function, carry the multi-service identifier, therefore, the CDRs of the sub-services can be correlated based on the multi-service identifier.

[0176] Figure 10 shows a flowchart of a charging correlation process for a multi-service in accordance with an embodiment of the present invention. In this embodiment, the service control function assigns a multi-service identifier for the multi-service and assigns a sub-service identifier to each sub-service. In this embodiment, the sub-service identifier of the PoC service adopts the SID assigned for an individual PoC service in the conventional PoC service, called SID1. The sub-service identifier of the Conference service adopts the SID assigned for an individual Conference service in the conventional Conference service, called SID2. The entities involved in this embodiment include: PoC Client 1, PoC Client 2, a PoC server, a Conference server and a charging information collecting function. In this embodiment, PoC Client 1 initiates a multi-service and adds PoC Client 2 into the multi-service. As shown in Figure 10, the process includes followings.

[0177] 1001: PoC Client 1 sends a session establishment request to the PoC server to initiate a PoC service. The session establishment request carries information of PoC Client 2 and is used to instruct to establish a multi-service comprising a Conference service and to add PoC Client 2 into the multi-service. The PoC server implements PoC service logic. A service control function in the PoC server assigns a multi-service identifier for the current multi-service, assigns one or more sub-service identifiers to the PoC service and assigns one or more sub-service identifiers to the Conference service.

[0178] The sub-service identifier of the PoC service adopts the SID assigned to the PoC service, called SID1; the sub-service identifier of the Conference service adopts the SID assigned to the Conference service, called SID2; and the multi-service identifier adopts the SID assigned to the multi-service, called SID0. The session establishment request may be carried in an SIP INVITE message in this embodiment. However, the present invention is not limited to this.

[0179] 1002: The service control function in the PoC server sends the session establishment request (e.g., an INVITE message) carrying the SID0 and SID2 to the Conference server to initiate a Conference service. The Conference server returns a session establishment response (e.g., a 2000K message). The session establishment request carries information of PoC Client 2 to indicate that PoC Client 2 need to be added into the Conference service.

[0180] After 1002, both the PoC service and the Conference service are originated, and the PoC server and the Conference server will perform steps ***b*** and ***a*** respectively to generate CDRs of the PoC service session and CDRs of the Conference service session on the AS-charging information collecting function.

[0181] Step ***a*** may include the followings. The Conference server generates CDRs for the current Conference service, requests the AS-charging information collecting function to start charging, and sends to the AS-charging information collecting function the CDRs that is generated by the Conference server and carries the SID0 and SID2. The AS-charging information collecting function opens the CDRs received from the Conference server, starts to record actions of the Conference service which are performed on the Conference server by users and affect the accounting, and returns a response from the AS-charging information collecting function to the Conference server.

[0182] Step ***b*** may include the followings. The PoC

server generates CDRs for the current PoC service, requests the AS-charging information collecting function to start charging, and sends to the AS-charging information collecting function the CDRs that is generated by the PoC server and carries the SID0 and SID1. The AS-charging information collecting function opens the CDRs from the PoC server, starts to record actions of the PoC service which are performed on the PoC server by users and affect the accounting, and returns a response to the PoC server.

[0183] 1003: The PoC server sends a session joining request carrying the SID0 and SID1 to PoC Client 2 in order to add PoC Client 2 into the current PoC service session. PoC Client 2 returns a session joining response to the PoC server in order to indicate that PoC Client 2 has successfully joined the current PoC service session.

[0184] After the PoC server has successfully added PoC Client 2 into the current PoC service, the information of PoC Client 2 needs to be recorded in the CDRs of the current PoC service session on the AS-charging information collecting function, therefore step ***c*** needs to be performed. Step ***c*** may include the followings. The PoC server requests the AS-charging information collecting function to update the charging, and sends the CDRs carrying the SID0 and SID1 of PoC Client 2 to the AS-charging information collecting function. The AS-charging information collecting function updates the CDRs of PoC Client 2 that carry the SID0 and SID1 and are received from the PoC server, records the information of PoC Client 2 in the CDRs, starts to record actions that are performed by PoC Client 2 on the PoC server and affect the accounting during the current multi-service, and returns a response to the PoC server.

[0185] 1004: The PoC server sends an acknowledgement (ACK) to the Conference server after PoC Client 2 has successfully joined the current PoC service session, in order to indicate that it is ready for the Conference server to add PoC Client 2 into the service session. The Conference server performs operations similar to the operations in 1003 in order to add PoC Client 2 into the current Conference service.

[0186] The information of PoC Client 2 needs to be recorded in the CDRs of the current Conference service on the AS-charging information collecting function, therefore step ***d*** needs to be performed. Step ***d*** may include the followings. The Conference server requests the AS-charging information collecting function to update the charging, and sends to the AS-charging information collecting function the CDRs carrying the SID0 and SID2 of PoC Client 2. The AS-charging information collecting function updates the CDRs of PoC Client 2 that carry the SID0 and SID2 are received from the Conference server, records the information of PoC Client 2 in the CDRs, starts to record actions that are performed by PoC Client 2 on the Conference server and affect the accounting during the current multi-service, and returns a response to the Conference server.

[0187] 1005-1006: The PoC server sends a session joining request (e.g., an INVITE message) carrying the SID0 and SID2 to the Conference server, and the Conference server returns a session joining response (e.g., a 2000K message). The session joining request carries information of PoC Client 1 to indicate that PoC Client 1 can be added into the Conference service session. At the same time, the PoC server adds PoC Client 1 into the current PoC service session and returns a session joining response (e.g., a 2000K message) to PoC Client 1.

[0188] After the PoC server has successfully added PoC Client 1 into the current PoC service session, the information of PoC Client 1 needs to be recorded in the CDRs of the current PoC service on the AS-charging information collecting function, therefore step ***e*** needs to be performed. Step e may include the followings. The PoC server requests the AS-charging information collecting function to update the charging, and sends to the AS-charging information collecting function the CDRs carrying the SID0 and SID1 of PoC Client 1. The AS-charging information collecting function updates the CDRs of PoC Client 1 that carry the SID0 and SID1 are received from the PoC server, records the information of PoC Client 1 in the CDRs, starts to record actions that are performed by PoC Client 1 on the PoC server and affect the accounting during the current multi-service, and returns a response to the PoC server.

[0189] 1007: The PoC server sends an acknowledgement (ACK) to the Conference server after PoC Client 1 has successfully joined the current PoC service session, in order to indicate that it is ready for the Conference server to add PoC Client 1 into the service session. The Conference server performs operations similar to the operations in 1003 to add PoC Client 1 into the current Conference service session.

[0190] The information of PoC Client 1 needs to be recorded in the CDRs of the current Conference service on the AS-charging information collecting function, therefore step ***f*** needs to be performed. Step ***f*** may include the followings. The Conference server requests the AS-charging information collecting function to update the charging, and sends to the AS-charging information collecting function the CDRs carrying the SID0 and SID2 of PoC Client 1. The AS-charging information collecting function updates the CDRs of PoC Client 1 that carry the SID0 and SID2 are received from the Conference server, records the information of PoC Client 1 in the CDRs, starts to record actions that are performed by PoC Client 1 on the Conference server and affect the accounting during the current multi-service, and returns a response to the Conference server.

[0191] After the processes described above, CDRs of the sub-services in the AS-charging information collecting function have the multi-service identifier and the sub-service identifiers corresponding to the sub-services. Therefore the CDRs of a sub-service may be correlated based on the sub-service identifier of the sub-service, and the CDRs of different sub-services, which have al-

ready been correlated based on the sub-service identifiers, are then correlated based on the multi-service identifier.

[0192] Figures 9 and 10 illustrate the second charging correlation scheme of the present invention which is applied to the application service layer. When the charging correlation scheme is applied to the bearer control layer, the entities involved include: a bearer control layer entity corresponding to the sub-service servers, a bearer control layer-charging information collecting function, and UEs. The bearer control layer entities corresponding to the sub-service servers may record the multi-service identifier and/or sub-service identifiers when the multi-service identifier and/or sub-service identifiers are received by the sub-service servers, generate CDRs, and send the received multi-service identifier and/or sub-service identifiers and the CDRs to the corresponding bearer control layer-charging information collecting functions. The processes in which the charging correlation scheme is applied to the bearer control layer is similar to that in Figures 9 and 10 and will not be described in detail herein, but is covered by the protection scope of the present invention.

[0193] Moreover, the charging correlation process may be variable based on different multi-services to be charged for, yet the charging correlation process will always be in accordance with the two methods of implementing the second charging correlation scheme provided in the above embodiments of the present invention. Since different multi-services may include various sub-services, the charging flow may vary in different ways. For example, the service control function may send the multi-service identifier and the sub-service identifiers to the primary server and the supplementary servers in different ways: 1) the service control function may send a primary service identifier when initiating a primary service session, or when setting up the primary service session, or when setting up all supplementary service sessions, or when setting up the current multi-service session; 2) the service control function may send the multi-service identifier when initiating the primary service session, or when setting up the primary service session, or when setting up all supplementary service sessions, or when setting up the current multi-service session; 3) the service control function may send a supplementary service identifier when initiating corresponding supplementary service session, or when setting up corresponding supplementary service session, or when setting up the current multi-service session; 4) the service control function may send the multi-service identifier when initiating each of the supplementary service sessions, or when setting up each of the supplementary service sessions, or when setting up the current multi-service session. Various charging correlation processes for various multi-services will not be listed herein. However, any charging correlation process for multi-service that is in accordance with the principles of the current invention falls in the scope of the present invention.

[0194] In embodiments of the present invention, a sub-service included in a multi-service can be any application or service. A multi-service may include sub-services such as PoC service, Conference service, Location service, Presence service and any combination of the above applications and services.

[0195] A system for charging correlation for an application or service is further proposed. Figure 11 is a structure diagram of a system for implementing a charging correlation of an application or service in accordance with an embodiment of the present invention. In an embodiment of the present invention, the system includes a service identifier generating unit, a CDR generating unit and a CDR correlating unit.

[0196] The service identifier generating unit is adapted to assign a service identifier to a current application or service and send the service identifier to the CDR generating unit. The CDR generating unit is adapted to receive the service identifier from the service identifier generating unit, generate a plurality of CDRs for the current application or service and send the received service identifier and the CDRs generated to the CDR correlating unit. The CDR correlating unit is adapted to receive the CDRs and the service identifier from the CDR generating unit and correlate the CDRs of the current application or service based on the service identifier.

[0197] The service identifier generating unit may be a separated entity or be integrated into the service control function of the application or service. When the system is applied to a single-service, the service control function is an AS of the current application or service, e.g., a server performing CF for a multi-party service such as PoC service and Conference service. When the system is applied to a multi-service, the service control function is a service control function of the current multi-service. The service control function may be integrated into an AS of a sub-service (i.e., a sub-service server) of the multi-service or be integrated into a server performing CF for the multi-party service such as the PoC service and the Conference service. The CDR correlating unit may also be a separated entity or be integrated into a charging system.

[0198] Moreover, the CDR generating unit may further add the received service identifier into the CDRs generated so that the CDRs and the service identifier may be sent.

[0199] In the system provided by embodiments of the present invention, the units may function according to the processes described in the preceding embodiments, and detailed functions of the units are not described anymore.

[0200] A system for charging correlation is also proposed by embodiments of the present invention. The system for charging correlation includes a service control function entity and a charging system. The service control function entity is adapted to assign a service identifier to a current application or service and the charging system is adapted to correlate at least one set of CDRs generated for the application or service based on the service iden-

tifier that is assigned by the service control function entity. The charging system may further include a charging information collecting function entity and a billing center. The charging information collecting function entity is adapted to receive the service identifier from the service control function entity and collect at least one set of CDRs, and the billing center is adapted to correlate at least one set of CDRs based on the service identifier.

[0201] The service control function entity may be an AS adapted to generate at least one set of CDRs for the application or service. The system may further include a bearer control layer entity adapted to record the service identifier assigned by the service control function entity, and generate at least one set of CDRs. In such a case the charging information collecting function entity further includes an AS-charging information collecting function entity and a bearer control layer-charging information collecting function entity. The AS-charging information collecting function is adapted to receive the service identifier from the service control function entity (i.e., the AS) and the at least one set of CDRs generated by the service control function entity, and the bearer control layer-charging information collecting function entity is adapted to receive the service identifier from a bearer control entity and the at least one set of CDRs generated by the bearer control layer entity. Therefore the billing center can correlate the at least one set of CDRs received from the bearer control layer-charging information collecting function entity based on the service identifier, or correlate the at least one set of CDRs received from the AS-charging information collecting function entity based on the service identifier, or correlate the at least one set of CDRs from the bearer control layer-charging information collecting function entity and the at least one set of CDRs from the AS-charging information collecting function entity based on the service identifier.

[0202] When the application or service is a multi-party service, the service control function entity is a server performing CF. At least one server performing PF may further be included. The bearer control layer entity may include a bearer control layer entity corresponding to the server performing CF, and at least one bearer control layer entity corresponding to the server performing PF. The bearer control layer entity corresponding to the server performing CF is adapted to bear the server performing CF, and a bearer control layer entity corresponding to a server performing PF is adapted to bear the server performing PF. The AS-charging information collecting function entity may further include an AS-charging information collecting function entity of the server performing CF and at least one AS-charging information collecting function entity of the server performing PF. The bearer control layer-charging information collecting function entity may further include a bearing control layer charging information collecting function entity of the bearer control layer entity corresponding to the server performing CF, and at least one bearer control layer-charging information collecting function entity of a bearer control layer entity corresponding to a server performing PF.

[0203] When the application or service is a multi-service comprising a plurality of sub-services, the system may further include sub-service servers of a plurality of sub-services. The bearer control layer entity may further include at least one bearer control layer entity corresponding to a plurality of sub-service servers. The bearer control layer entity corresponding to the sub-service servers is adapted to bear the sub-service servers. The AS-charging information collecting function entity may further include AS-charging information collecting function entities of sub-service servers, and the bearer control layer-charging information collecting function entity may further include bearer control layer-charging information collecting function entities of bearer control layer entities of sub-service servers.

[0204] The functions of the components of the system in various cases have been given in the preceding description and will not be explained further herein, but are still covered by the protection scope of the present invention.

[0205] A billing center is also proposed in embodiments of the present invention. The billing center may include a first module adapted to receive a service identifier of the current application or service, and receive at least one set of CDRs generated for the application or service, and a second module adapted to correlate at least one set of CDRs based on the service identifier received by the first module and generate a bill. The CDRs received by the first module may be CDRs generated by an AS and CDRs generated by a bearer control layer entity. The second module may correlate the CDRs generated by the AS based on the service identifier, or correlate the CDRs generated by the bearer control layer entity based on the service identifier, or correlate the CDRs generated by the AS and the CDRs generated by the bearer control layer entity together based on the service identifier.

[0206] An apparatus for generating charging data record is also proposed in embodiments of the present invention. The an apparatus for generating charging data record may include a first module and a second module. The first module is adapted to receive a service identifier assigned to the current application or service, and the second module is adapted to generate for the application or service at least one set of CDRs carrying the service identifier that is received by the first module and adapted to export the at least one set of CDRs. The an apparatus for generating charging data record may be an AS or a bearer control layer entity in embodiments of the present invention.

[0207] In one word, in embodiments of the present invention, a plurality of CDRs generated for a user in a service session may be correlated for charging, and the CDRs of a plurality of sub-services in a multi-service of the user can also be correlated for charging. Furthermore, the embodiments of the present invention is easy to implement and can improve accuracy of correlated

charging. Therefore the methods and apparatus proposed in the embodiments of the present invention are beneficial in supplementing and improving the conventional application or service charging correlation process (especially the charging correlation process of a multi-party service).

[0208] The previous description of the disclosed embodiments is provided to enable those skilled in the art to make or use the present invention. Various modifications to these embodiments will be readily apparent to those skilled in the art and generic principles defined herein may be applied to other embodiments without departing from the scope of the invention. Thus, the present invention is not intended to be limited to the embodiments shown herein but is to be accorded the widest scope consistent with the principles and novel features disclosed herein.

Claims

1. A method for charging correlation for an application or service, comprising:

   assigning a service identifier by a service control function to an application or service;
   sending the service identifier to a charging system; and
   correlating, by the charging system, at least one Charging Data Record CDR generated for the application or service based on the service identifier.

2. The method according to Claim 1, wherein the charging system comprises a charging information collecting function entity and a billing center; and the method further comprises:

   sending the service identifier to the billing center via the charging information collecting function entity; and
   correlating, by the billing center, the at least one CDR generated by the service control function entity based on the service identifier.

3. The method according to Claim 2, wherein the application or service is a single-service, the service control function entity comprises an Application Server AS and the charging information collecting function entity comprises an AS charging information collecting function entity corresponding to the AS; and the method further comprises:

   assigning a service identifier by the AS to the single-service;
   sending the service identifier to the billing center via the AS charging information collecting function entity; and
   correlating, by the billing center, the at least one CDR generated by the AS based on the service identifier.

4. The method according to Claim 3, wherein the charging information collecting function entity further comprises: a bearer control layer charging information collecting function entity corresponding to a bearer control layer entity that corresponds to the AS, and the method further comprises:

   assigning the service identifier by the AS to the single-service;
   sending the service identifier to the billing center via the AS charging information collecting function entity;
   recording the service identifier by the bearer control layer entity that corresponds to the AS;
   sending the service identifier to the billing center via the bearer control layer charging information collecting function entity; and
   correlating, by the billing center, the at least one CDR generated by the AS based on the service identifier and correlating the at least one CDR generated by the bearer control layer entity based on the service identifier; or correlating the at least one CDR generated by the AS together with the at least one CDR generated by the bearer control layer entity based on the service identifier.

5. The method according to Claim 4, wherein the application or service is a multi-party service, the AS further comprises a server performing Control Function CF and at least one server performing Participating Function PF, and the service control function entity is the server performing CF; the AS charging information collecting function entity further comprises: at least one AS charging information collecting function entity covered by the server performing CF and at least one AS charging information collecting function entity covered by at least one server performing PF; the bearer control layer charging information collecting function entity further comprises at least one bearer control layer charging information collecting function entity covering the bearer control layer entities corresponding to the server performing CF and at least one server performing PF respectively, the bearer control layer entity corresponding to the server performing CF is used for bearing the server performing CF and the bearer control layer entity corresponding to a server performing PF is used for bearing the server performing PF;
   the server performing CF assigns the service identifier to the multi-party service and sends the service identifier to the at least one server performing PF, the server performing CF and the at least one server performing PF send the service identifier to the billing

EX1002 - Page 864

center respectively via the AS charging information collecting function entity which corresponds to the server performing CF and the AS charging information collecting function entity which corresponds to the server performing PF;
the bearer control layer entities corresponding respectively to the server performing CF and the at least one server performing the PF record the service identifier, and send the server identifier to the billing center via the at least one bearer control layer charging information collecting function entity;
correlating, by the billing center, the CDRs generated by the server performing CF and generated by the at least server performing PF based on the service identifier, and correlating the CDRs generated by the bear control layer entities; or, correlating, by the billing center, the CDRs generated by the bear control layer entities, the CDRs generated by the server performing CF and generated by the at least server performing PF based on the service identifier.

6. The method according to any one of Claims 1 to 5, wherein sending the service identifier to the charging system comprises:

sending the at least CDR that carries the service identifier to the charging system.

7. The method according to any one of Claims 1 to 5, wherein in the application or service, one user is established at least one session, and one CDR corresponds to one session of one user; and
the at least CDR correlated for the application or service based on the service identifier comprises: CDRs corresponding to a plurality of sessions of one user in the application or service, or CDRs corresponding to a plurality of sessions of a part of or all users in the application or service.

8. The method according to Claim 2, wherein the application or service is a multi-service comprising a plurality of sub-services; the charging information collecting function entity comprises: at least one AS charging information collecting function entity which respectively corresponds to multiple sub-service server providing multiple sub-services; the service identifier assigned by the service control function entity for the application or service comprises: multi-service identifier of the multi-service and multiple sub-service identifiers of the multiple sub-services;
respectively receiving, by the multiple sub-service servers, the multi-service identifier and the respective sub-service identifier from the service control function entity, and sending the multi-service identifier and the respective sub-service identifier to the billing center via respective AS charging information collecting function entity; and
correlating, the billing center, the CDRs each sub-service server using the respective sub-service identifier, and correlating, the CDRs generated by all sub-service servers using the multi-service identifier.

9. The method according to Claim 8, wherein the charging information collecting function entity comprises: multiple bear control layer charging information collecting function entities of bear control layer entities that respectively correspond to the multiple sub-service servers; and the bear control layer entities that respectively correspond to the multiple sub-service servers are adapted to respectively bear the bear control layers;
recording, by the bear control layer entities that respectively correspond to the multiple sub-service servers, the corresponding sub-service identifier and the multi-service identifier, and sending the corresponding sub-service identifier and the multi-service identifier to the billing center via respective bear control layer charging information collecting function entities;
correlating, by the billing center, the CDRs generated by each bear control layer entity based on the corresponding sub-service identifier, and correlating CDRs generated by all the bear control layer entities based on the multi-service identifier.

10. The method according to Claim 8 or 9, wherein sending the multi-service identifier and the sub-service identifier comprises:

sending the CDRs that carry the multi-service identifier and the sub-service identifier.

11. The method according to Claim 8 or 9, wherein the multi-service identifier is identical to one of the sub-service identifiers, or is not identical to any one of the sub-service identifiers.

12. The method according to Claim 2, wherein the application or service is a multi-service comprising a plurality of sub-services; the service identifier assigned by the service control function entity for the application or service comprises: multi-service identifier of the multi-service; the charging information collecting function comprises: at least one AS charging information collecting function entity that respectively correspond to the multiple sub-service servers;
receiving, by the multiple sub-service servers, the multi-service identifier from the service charging information collecting function entity, and respectively sending the multi-service identifier to the billing center via respective AS charging information collecting function entity; correlating, by the billing center, the CDRs generated by the multiple sub-service servers based on the multi-service identifier.

13. The method according to Claim 12, wherein the

charging information collecting function entity comprises: multiple bear control layer charging information collecting function entities of bear control layer entities that respectively correspond to the multiple sub-service servers; and the bear control layer entities that respectively correspond to the multiple sub-service servers are adapted to respectively bear the bear control layers;
the method further comprises:

recording, by the bear control layer entities that respectively correspond to the multiple sub-service servers, the multi-service identifier, and sending the multi-service identifier to the billing center via respective bear control layer charging information collecting function entities; correlating, by the billing center, the CDRs generated by the bear control layer entities based on the the multi-service identifier.

14. The method according to Claim 12 or 13, wherein sending the multi-service identifier comprises: sending the CDRs that carry the multi-service identifier.

15. A system for charging correlation for an application or service, comprising:

a service control function, adapted to assign a service identifier for an application or service; and
a charging system, adapted to correlate at least one Charging Data Records CDR generated for the application or service based on the service identifier.

16. The system according to Claim 15, wherein the charging system comprises:

a charging information collecting function entity, adapted to receive the service identifier assigned by the service control function entity and collect the at least one CDR; and
a billing center, adapted to correlate the at least one CDR based on the service identifier received from the charging information collecting function entity.

17. The system according to Claim 16, wherein the service control function comprises an Application Server AS adapted to generate at least one CDR for the application or service; and the system further comprises a bearer control layer entity, adapted to record the service identifier and generate at least one CDR for the application or service.
wherein the charging information collecting function entity comprises:

an AS-charging information collecting function entity, adapted to receive the service identifier and the at least one CDR from the service control function entity;
a bearer control layer-charging information collecting function entity, adapted to receive the service identifier and the at least one CDR from the bearer control layer entity;

wherein
the billing center is further adapted to correlate the at least one CDR from the bearer control layer-charging information collecting function entity based on the service identifier, and correlate the at least one CDR from the AS-charging information collecting function entity based on the service identifier respectively, or adapted to correlate the at least one CDR from the bearer control layer-charging information collecting function entity with the at least one CDR from the AS-charging information collecting function entity based on the service identifier.

18. The system according to Claim 17, wherein the application or service is a multi-party service and the service control function entity is a server performing Controlling Function CF,
the system further comprises at least one server performing Participating Function PF,
wherein the bearer control layer entity comprises a bearer control layer entity corresponding to the server performing CF and at least one bearer control layer entity corresponding to the at least one server performing PF; the bearer control layer entity corresponding to the server performing CF is adapted to bear the server performing CF and the bearer control layer entity corresponding to the server performing PF is adapted to bear the server performing PF;
the AS-charging information collecting function entity comprises an AS-charging information collecting function entity corresponding to the server performing CF and at least one AS-charging information collecting function corresponding to the at least one server performing PF;
the bearer control layer-charging information collecting function comprises a bearer control layer-charging information collecting function entity of the bearer control layer entity corresponding to the server performing CF and at least a bearer control layer-charging information collecting function of the bearer control layer entity corresponding to the at least one server performing PF;
the server performing CF is adapted to assign the service identifier, send the service identifier to the at least one server performing PF, generate at least one set of CDR and send the service identifier and the CDRs to the AS-charging information collecting function entity of the server performing CF;
each server performing PF is adapted to record the service identifier, generate at least one set of CDR

EX1002 - Page 866

and send the at least one set of CDR and the service identifier to the AS-charging information collecting function entity of the server performing PF;
the bearer control layer entity corresponding to the server performing CF is adapted to record the service identifier, generate the CDRs and send the CDRs and the service identifier to the bearer control layer-charging information collecting function entity of the bearer control layer entity;
each bearer control layer entity corresponding to a server performing PF is adapted to record the service identifier, generate the CDRs and send the CDRs and the service identifier to the bearer control layer-charging information collecting function entity of the bearer control layer entity;
the AS-charging information collecting function entity is adapted to send the service identifier and the CDRs to the billing center; and
the bearer control layer-charging information collecting function entity is adapted to send the service identifier and the CDRs to the billing center.

19. The system according to Claim 17, wherein the application or service is a multi-service comprising a plurality of sub-services, and
the system further comprises a plurality of sub-service servers providing the plurality of sub-services respectively; wherein
the bearer control layer entity comprises at least one bearer control layer entity corresponding to the sub-service servers and is adapted to bear the sub-service servers;
the AS-charging information collecting function entity comprises AS-charging information collecting function entities of respective sub-service servers;
the bearer control layer-charging information collecting function entity comprises bearer control layer-charging information collecting function entities of the bearer control layer entities corresponding to respective sub-service servers;
the service control function entity is further adapted to assign sub-service identifiers for the sub-services and send the service identifier and the sub-service identifiers to the sub-service servers;
each sub-service server is adapted to record the service identifier and the sub-service identifiers from the service control function entity, generate at least one set of CDRs for the sub-service provided by the sub-service server and send the service identifier, the sub-service identifier and the at least one set of CDRs to the AS-charging information collecting function entity of the sub-service server;
the bearer control layer entity corresponding to the sub-service server is adapted to record the service identifier and the sub-service identifier from the sub-service server, generate at least one set of CDRs for the sub-service provided by the sub-service server and send the service identifier, the sub-service identifier and the at least one set of CDRs to the bearer control layer-charging information collecting function entity of the bearer control layer entity;
the AS-charging information collecting function entity is adapted to send the service identifier, sub-service identifiers and the CDRs to the billing center;
the bearer control layer-charging information collecting function entity is adapted to send the service identifier, sub-service identifiers and the CDRs to the billing center; and
the billing center is further adapted to correlate CDRs of each sub-service according to the sub-service identifier corresponding to the sub-service, and correlate CDRs of the plurality of sub-services according to the service identifier.

20. The system according to Claim 17, wherein the application or service is a multi-service comprising a plurality of sub-services, and
the system further comprises a plurality of sub-service servers providing the sub-services; wherein
the bearer control layer entity comprises at least one bearer control layer entity corresponding to the sub-service servers and is adapted to bear the sub-service servers;
the AS-charging information collecting function entity comprises AS-charging information collecting function entities corresponding to the sub-service servers; the bearer control layer-charging information collecting function entity comprises bearer control layer-charging information collecting function entities corresponding to the bearer control layer entities corresponding to the sub-service servers;
the service control function entity is adapted to send the service identifier to the sub-service servers;
the sub-service server is adapted to record the service identifier from the service control function entity, generate at least one set of CDRs for the sub-service provided by the sub-service server and send the at least one set of CDRs and the service identifier to the AS-charging information collecting function entity of the sub-service server;
the bearer control layer entity corresponding to a sub-service server is adapted to record the service identifier from the sub-service server, generate at least one set of CDRs for the sub-service provided by the sub-service server and send the service identifier and the at least one set of CDRs to the bearer control layer-charging information collecting function entity of the bearer control layer entity;
an AS-charging information collecting function entity is adapted to send the service identifier and the CDRs to the billing center;
a bearer control layer-charging information collecting function entity is adapted to send the service identifier and the CDRs to the billing center; and
the billing center is adapted to correlate the CDRs of the sub-services based on the service identifier.

21. A billing center, comprising:

a first module, adapted to receive a service identifier assigned for an application or service and Charging Data Records CDRs generated for the application or service; and
a second module, adapted to correlate the CDRs based on the service identifier from the first module.

22. The billing center according to Claim 21, wherein the CDRs received by the first module comprise CDRs generated by an Application Server AS and CDRs generated by a bearer control layer entity; and
the second module is adapted to correlate the CDRs generated by the AS based on the service identifier and correlate the CDRs generated by the bearer control layer entity based on the service identifier respectively, or adapted to correlate the CDRs generated by the AS and the CDRs generated by the bearer control layer entity based on the service identifier.

23. The billing center according to any of Claim 21 or 22, wherein the application or service comprises at least one session and each set of the CDRs identified by ICID corresponds to one session; and
the second module is adapted to correlate a plurality of CDRs corresponding to a plurality of sessions of one user in the application or service based on the service identifier, or adapted to correlate a plurality of CDRs corresponding to a plurality of sessions of a part of or all users in the application or service based on the service identifier.

24. A apparatus for generating a charging data record, comprising:

a first module, adapted to receive a service identifier assigned for an application or service; and
a second module, adapted to generate Charging Data Records, CDRs, carrying the service identifier from the first module for the application or service.

25. The apparatus according to Claim 24, wherein the apparatus is an AS or a bearer control layer entity.

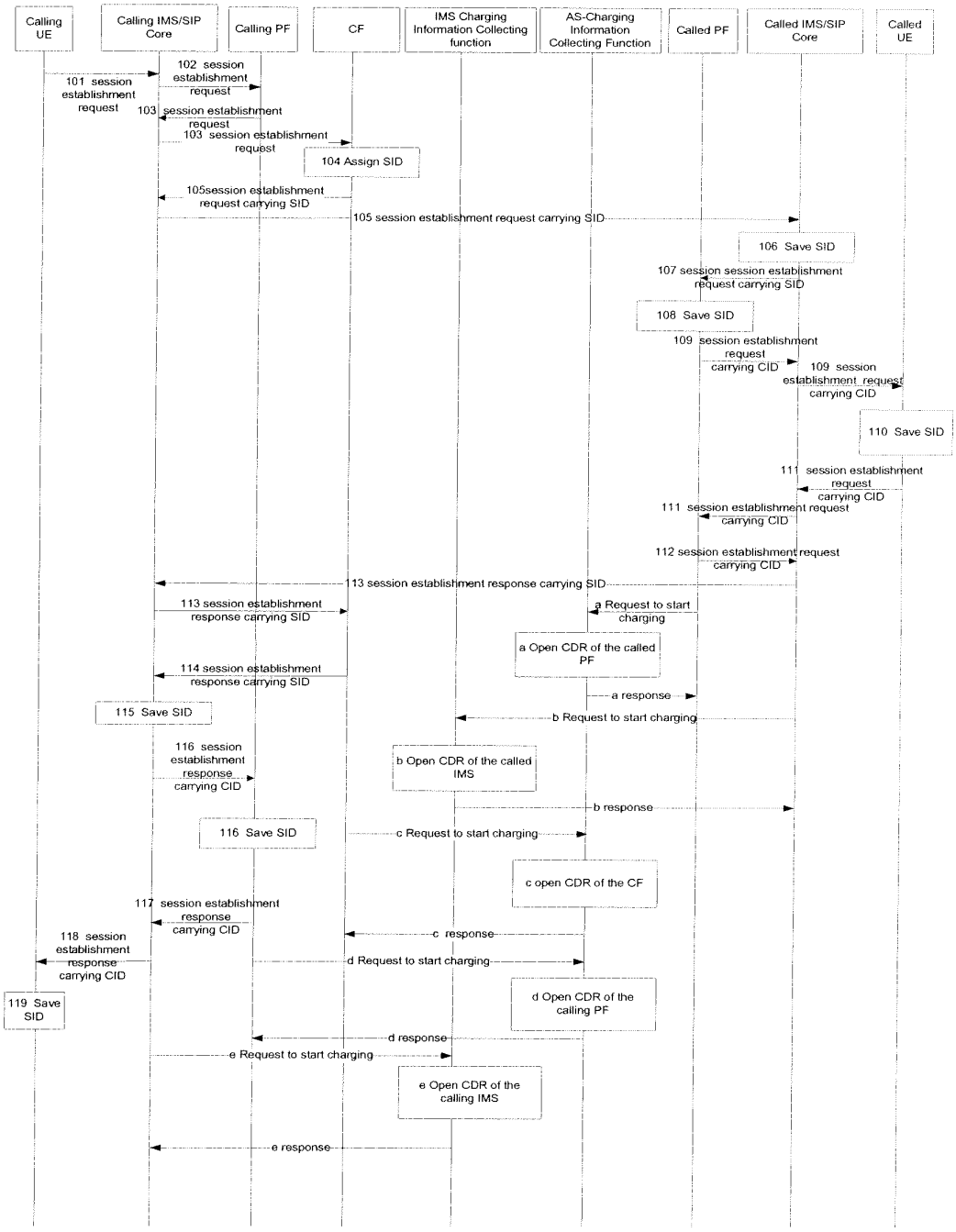

Calling UE
Calling IMS/SIP Core
Calling PF
CF
IMS Charging Information Collecting function
AS-Charging Information Collecting Function
Called PF
Called IMS/SIP Core
Called UE
101 session establishment request
102 session establishment request
103 session establishment request
103 session establishment request
104 Assign SID
105session establishment request carrying SID
105 session establishment request carrying SID
106 Save SID
107 session session establishment request carrying SID
108 Save SID
109 session establishment request carrying CID
109 session establishment request carrying CID
110 Save SID
111 session establishment request carrying CID
111 session establishment request carrying CID
112 session establishment request carrying CID
113 session establishment response carrying SID
113 session establishment response carrying SID
a Request to start charging
a Open CDR of the called PF
114 session establishment response carrying SID
a response
115 Save SID
b Request to start charging
116 session establishment response carrying CID
b Open CDR of the called IMS
b response
116 Save SID
c Request to start charging
c open CDR of the CF
117 session establishment response carrying CID
c response
118 session establishment response carrying CID
d Request to start charging
d Open CDR of the calling PF
119 Save SID
d response
e Request to start charging
e Open CDR of the calling IMS
e response

Fig. 1

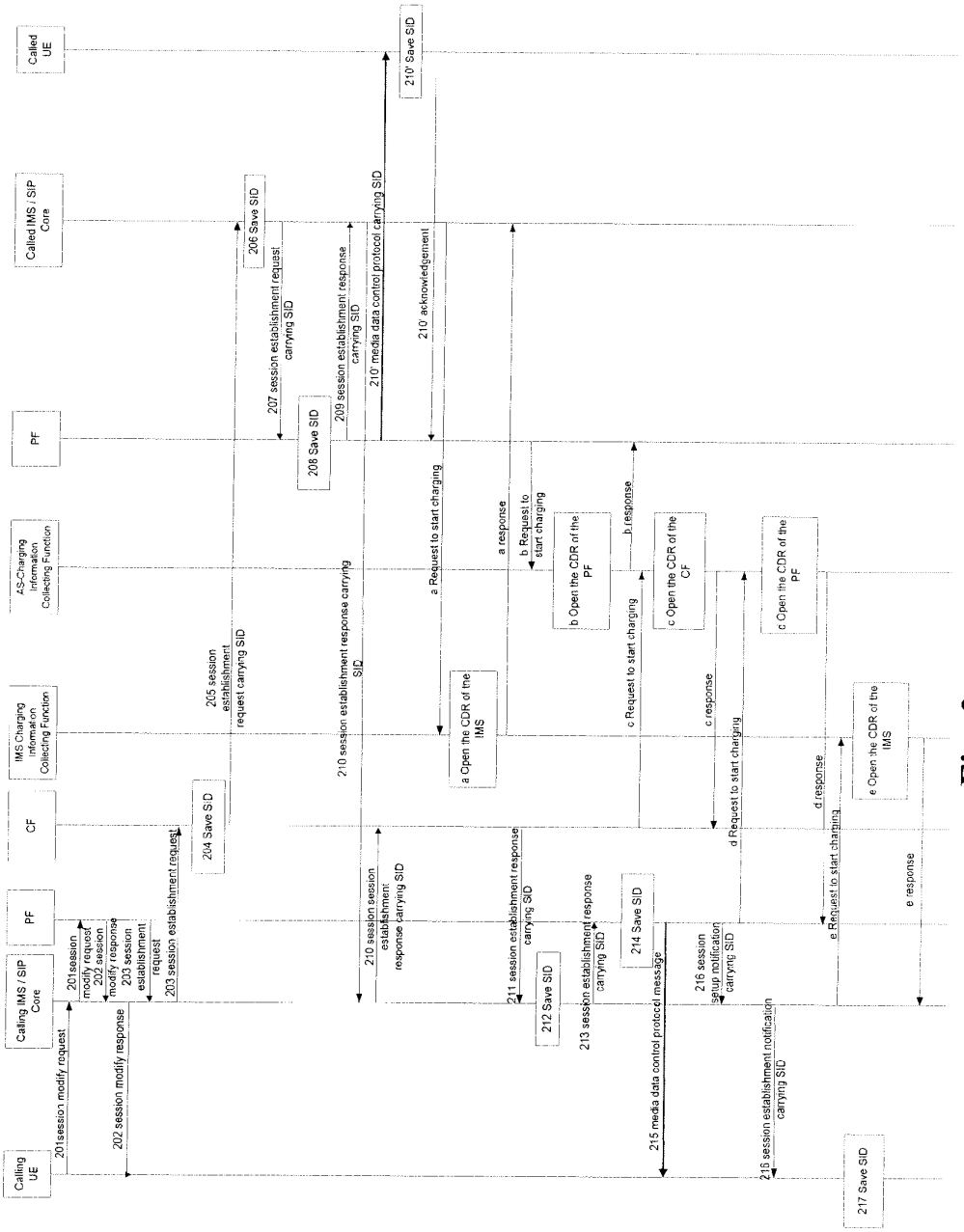

Calling UE
Calling IMS / SIP Core
PF
CF
IMS Charging Information Collecting Function
AS-Charging Information Collecting Function
PF
Called IMS / SIP Core
Called UE
201 session modify request
202 session modify response
201 session modify request
202 session modify response
203 session establishment request
203 session establishment request
204 Save SID
205 session establishment request carrying SID
206 Save SID
207 session establishment request carrying SID
208 Save SID
209 session establishment response carrying SID
210' media data control protocol carrying SID
210' Save SID
210' acknowledgement
210 session establishment response carrying SID
a Open the CDR of the IMS
a Request to start charging
a response
b Request to start charging
b Open the CDR of the PF
b response
c Request to start charging
c Open the CDR of the CF
c response
d Request to start charging
d response
e Request to start charging
e Open the CDR of the IMS
e response
211 session establishment response carrying SID
212 Save SID
213 session establishment response carrying SID
214 Save SID
215 media data control protocol message
216 session setup notification carrying SID
216 session establishment notification carrying SID
217 Save SID

Fig. 2

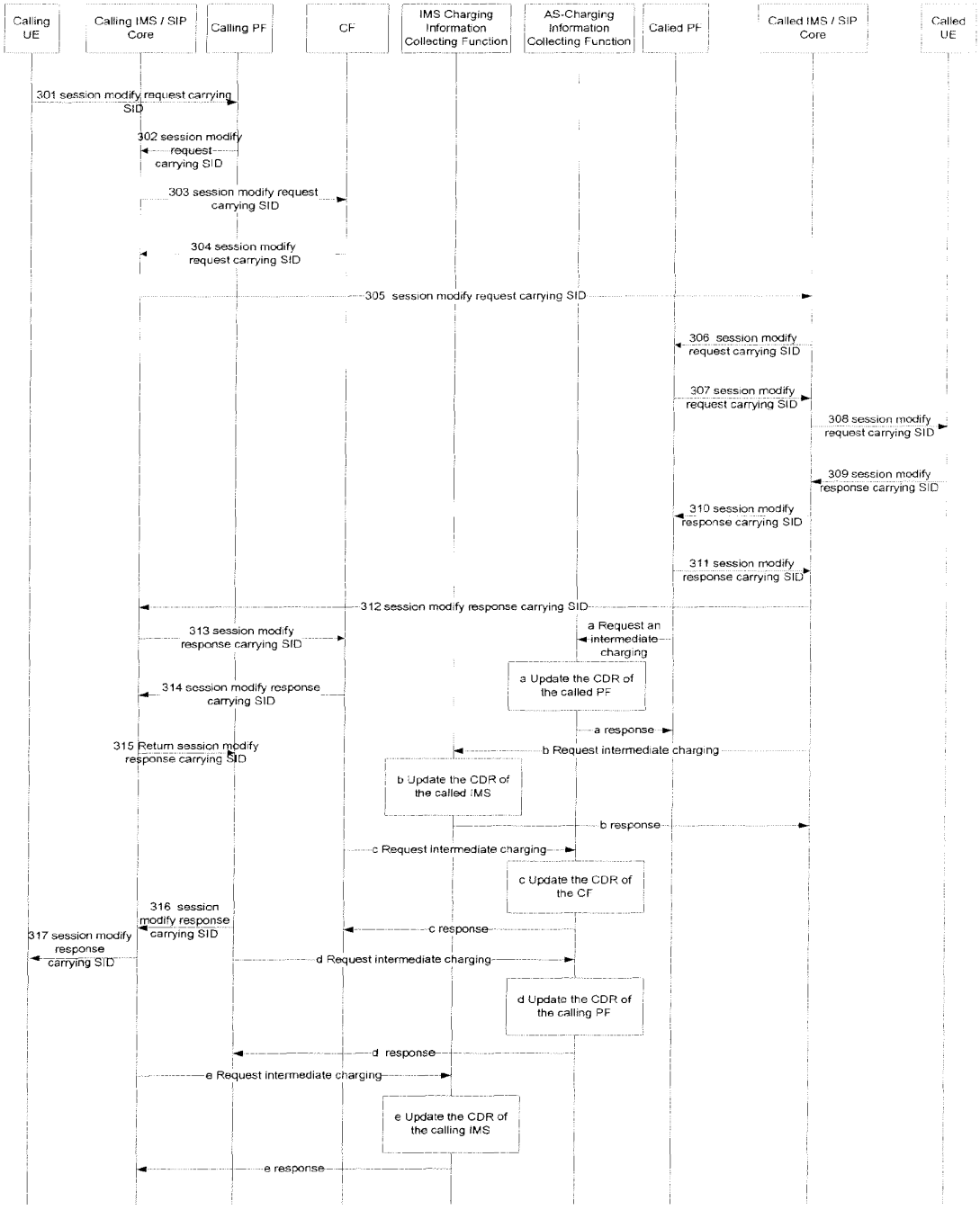

Calling UE
Calling IMS / SIP Core
Calling PF
CF
IMS Charging Information Collecting Function
AS-Charging Information Collecting Function
Called PF
Called IMS / SIP Core
Called UE
301 session modify request carrying SID
302 session modify request carrying SID
303 session modify request carrying SID
304 session modify request carrying SID
305 session modify request carrying SID
306 session modify request carrying SID
307 session modify request carrying SID
308 session modify request carrying SID
309 session modify response carrying SID
310 session modify response carrying SID
311 session modify response carrying SID
312 session modify response carrying SID
313 session modify response carrying SID
a Request an intermediate charging
a Update the CDR of the called PF
314 session modify response carrying SID
a response
315 Return session modify response carrying SID
b Request intermediate charging
b Update the CDR of the called IMS
b response
c Request intermediate charging
c Update the CDR of the CF
316 session modify response carrying SID
c response
317 session modify response carrying SID
d Request intermediate charging
d Update the CDR of the calling PF
d response
e Request intermediate charging
e Update the CDR of the calling IMS
e response

Fig. 3

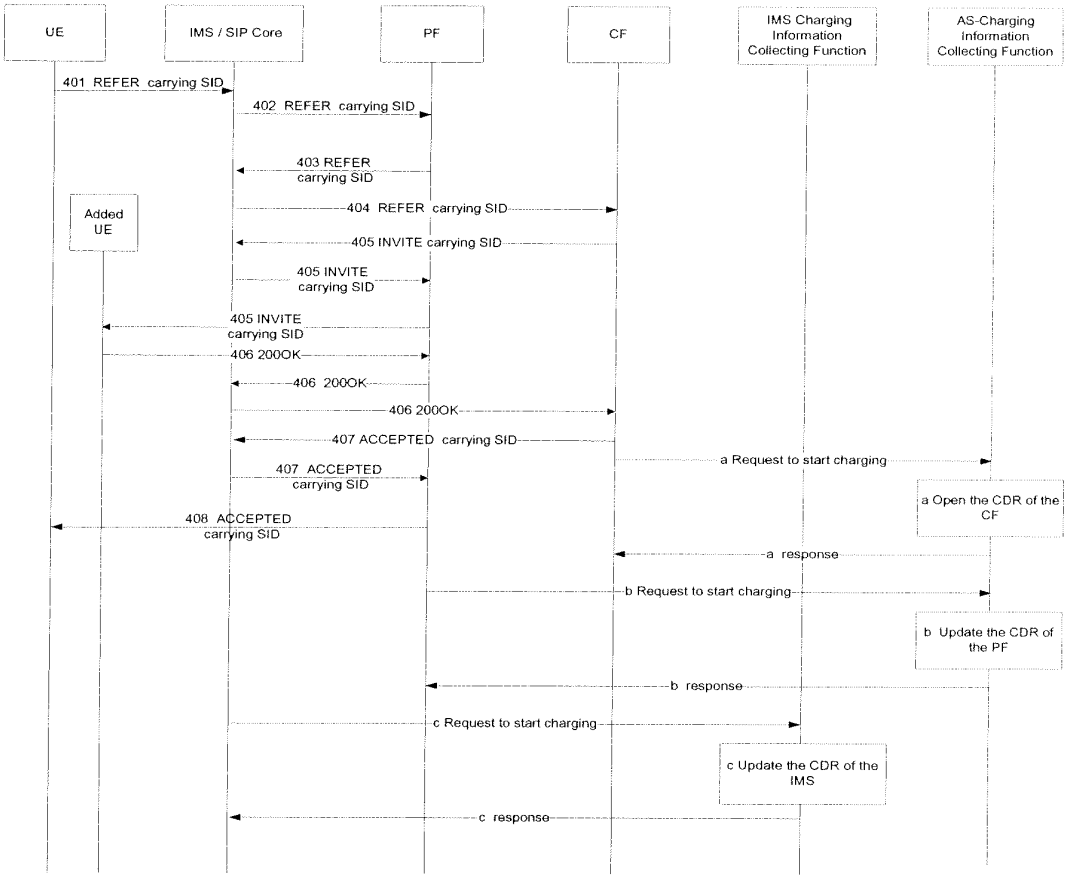

UE
IMS / SIP Core
PF
CF
IMS Charging Information Collecting Function
AS-Charging Information Collecting Function
401 REFER carrying SID
402 REFER carrying SID
403 REFER carrying SID
404 REFER carrying SID
Added UE
405 INVITE carrying SID
405 INVITE carrying SID
405 INVITE carrying SID
406 200OK
406 200OK
406 200OK
407 ACCEPTED carrying SID
a Request to start charging
407 ACCEPTED carrying SID
a Open the CDR of the CF
408 ACCEPTED carrying SID
a response
b Request to start charging
b Update the CDR of the PF
b response
c Request to start charging
c Update the CDR of the IMS
c response

Fig. 4

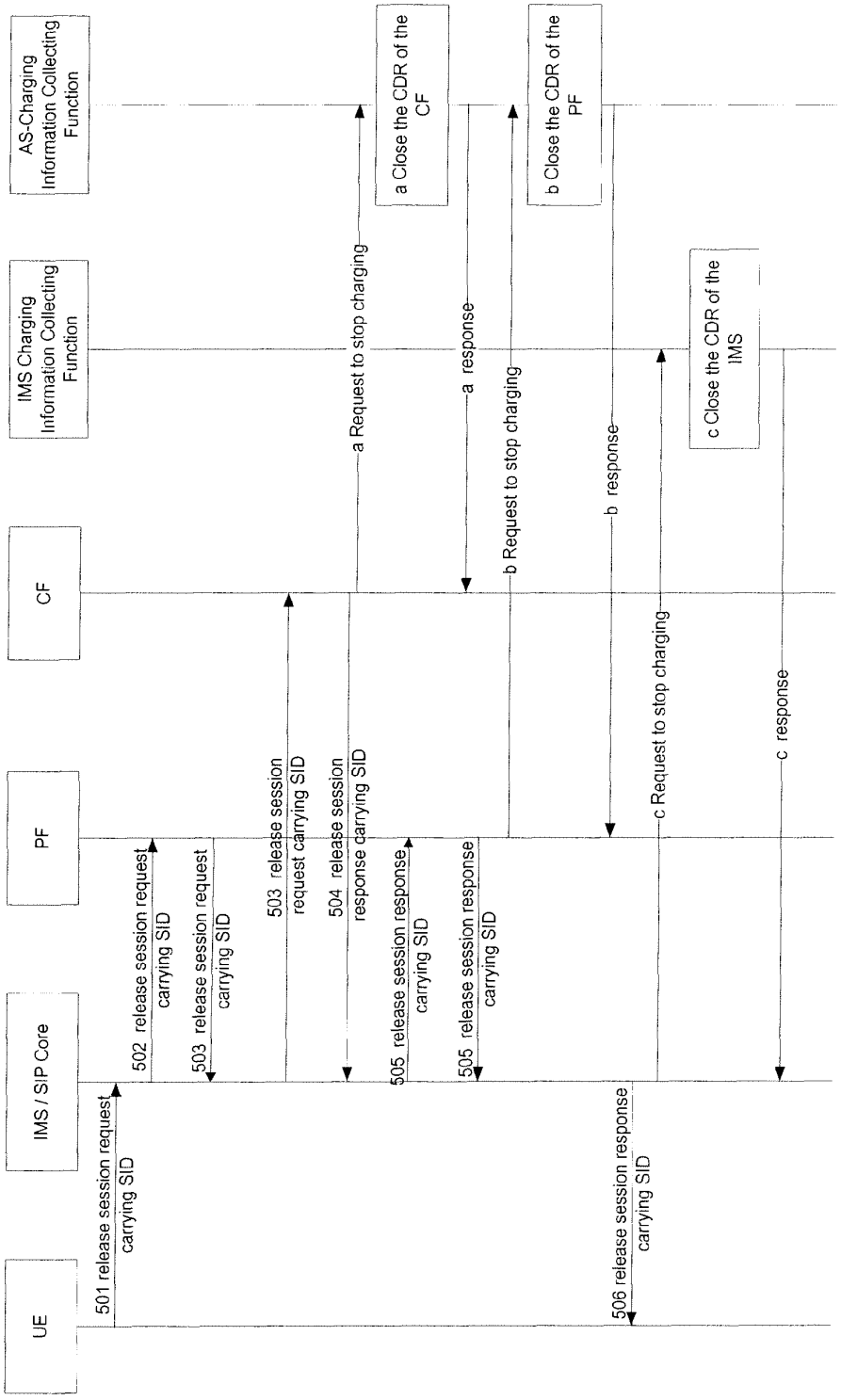

UE
IMS / SIP Core
PF
CF
IMS Charging Information Collecting Function
AS-Charging Information Collecting Function
501 release session request carrying SID
502 release session request carrying SID
503 release session request carrying SID
503 release session request carrying SID
504 release session response carrying SID
505 release session response carrying SID
505 release session response carrying SID
506 release session response carrying SID
a Request to stop charging
a response
a Close the CDR of the CF
b Request to stop charging
b response
b Close the CDR of the PF
c Request to stop charging
c response
c Close the CDR of the IMS

Fig. 5

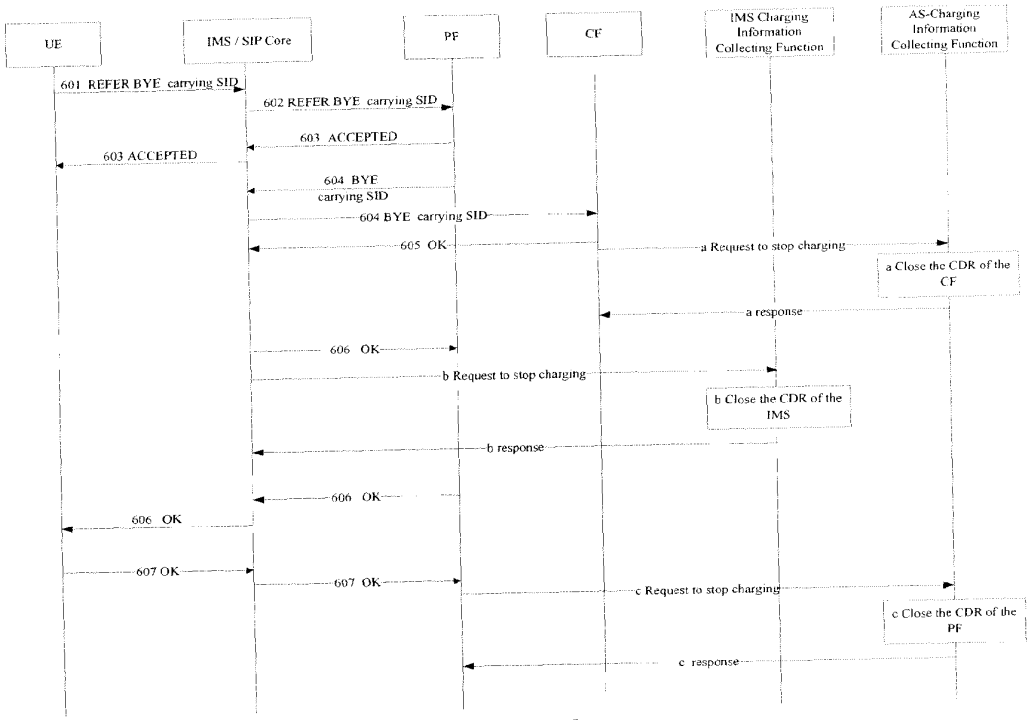

UE
IMS / SIP Core
PF
CF
IMS Charging Information Collecting Function
AS-Charging Information Collecting Function
601 REFER BYE carrying SID
602 REFER BYE carrying SID
603 ACCEPTED
603 ACCEPTED
604 BYE carrying SID
604 BYE carrying SID
605 OK
a Request to stop charging
a Close the CDR of the CF
a response
606 OK
b Request to stop charging
b Close the CDR of the IMS
b response
606 OK
606 OK
607 OK
607 OK
c Request to stop charging
c Close the CDR of the PF
c response

Fig. 6

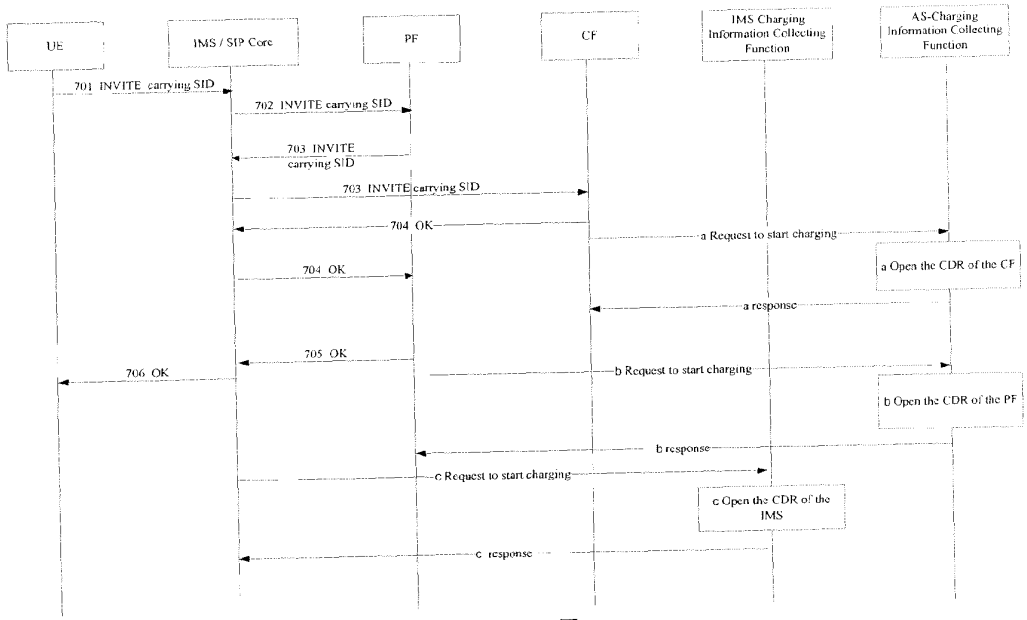

UE
IMS / SIP Core
PF
CF
IMS Charging Information Collecting Function
AS-Charging Information Collecting Function
701 INVITE carrying SID
702 INVITE carrying SID
703 INVITE carrying SID
703 INVITE carrying SID
704 OK
a Request to start charging
a Open the CDR of the CF
704 OK
a response
705 OK
706 OK
b Request to start charging
b Open the CDR of the PF
b response
c Request to start charging
c Open the CDR of the IMS
c response

Fig. 7

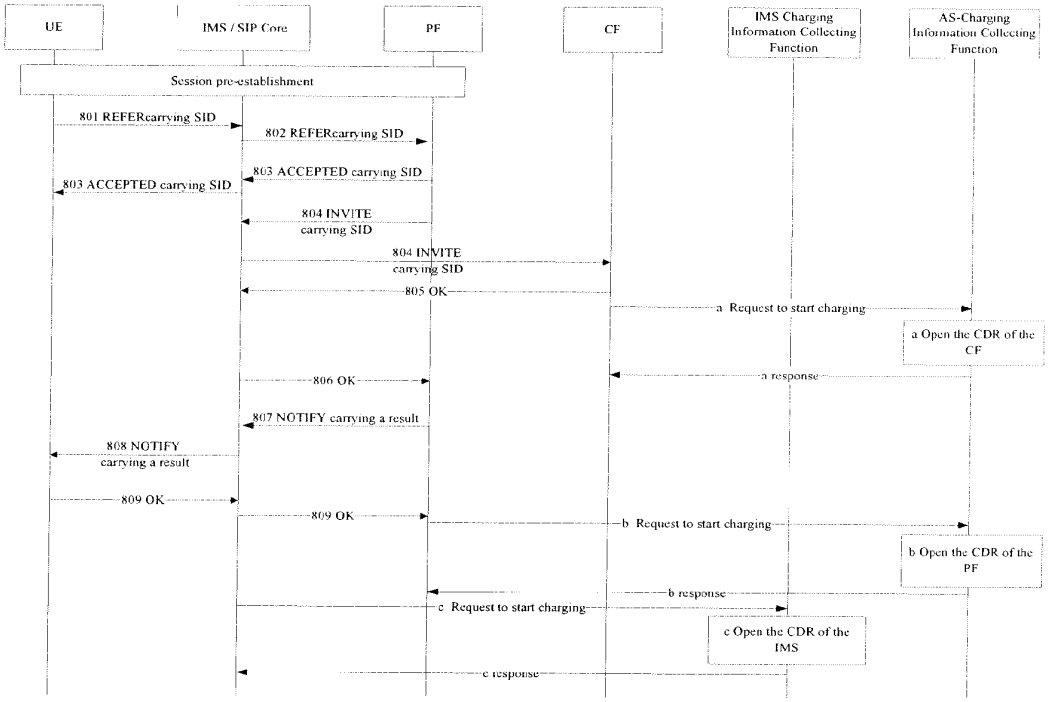

UE
IMS / SIP Core
PF
CF
IMS Charging Information Collecting Function
AS-Charging Information Collecting Function
Session pre-establishment
801 REFERcarrying SID
802 REFERcarrying SID
803 ACCEPTED carrying SID
803 ACCEPTED carrying SID
804 INVITE carrying SID
804 INVITE carrying SID
805 OK
a Request to start charging
a Open the CDR of the CF
a response
806 OK
807 NOTIFY carrying a result
808 NOTIFY carrying a result
809 OK
809 OK
b Request to start charging
b Open the CDR of the PF
b response
c Request to start charging
c Open the CDR of the IMS
c response

Fig. 8

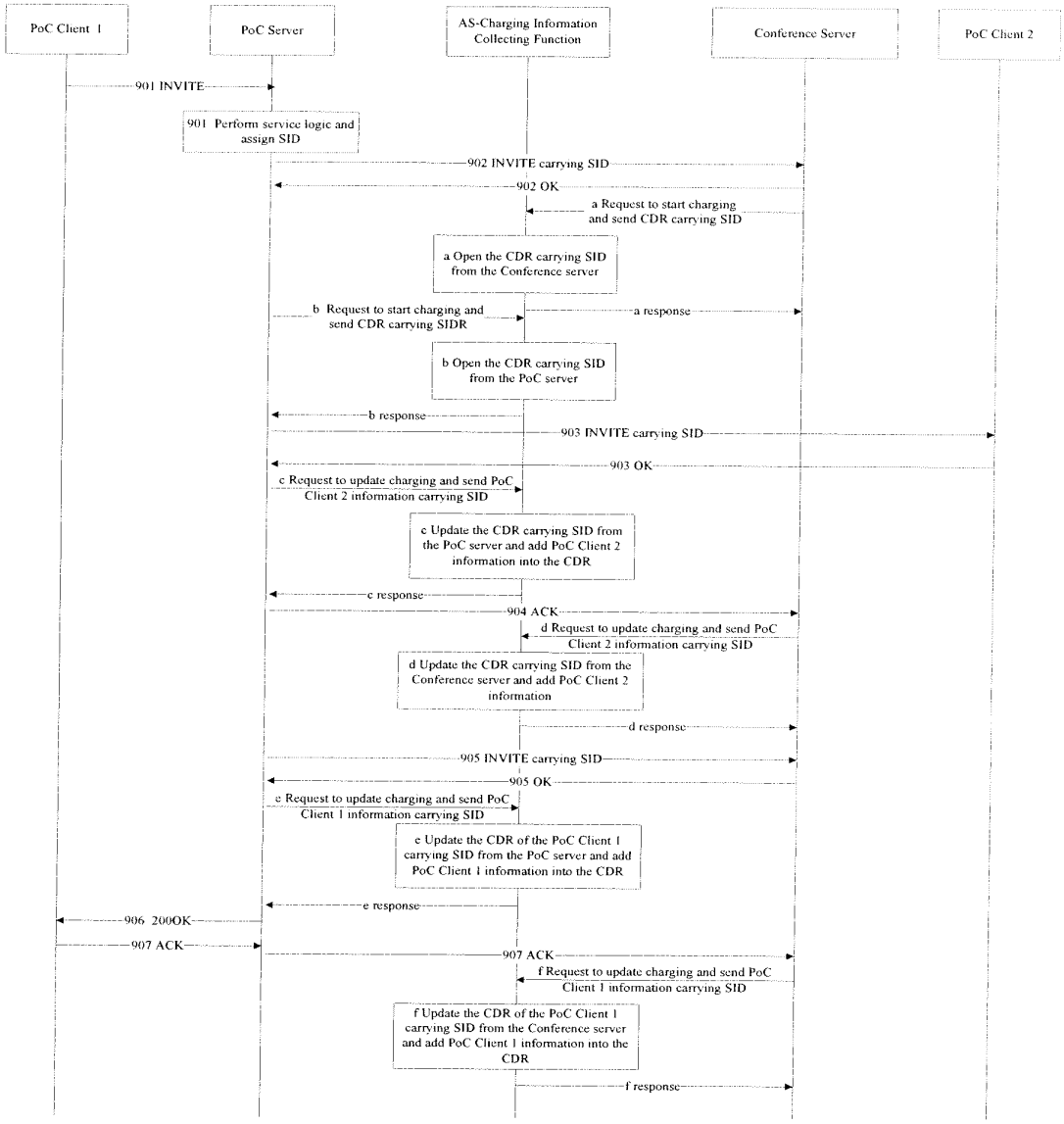


Fig. 9

EX1002 - Page 876

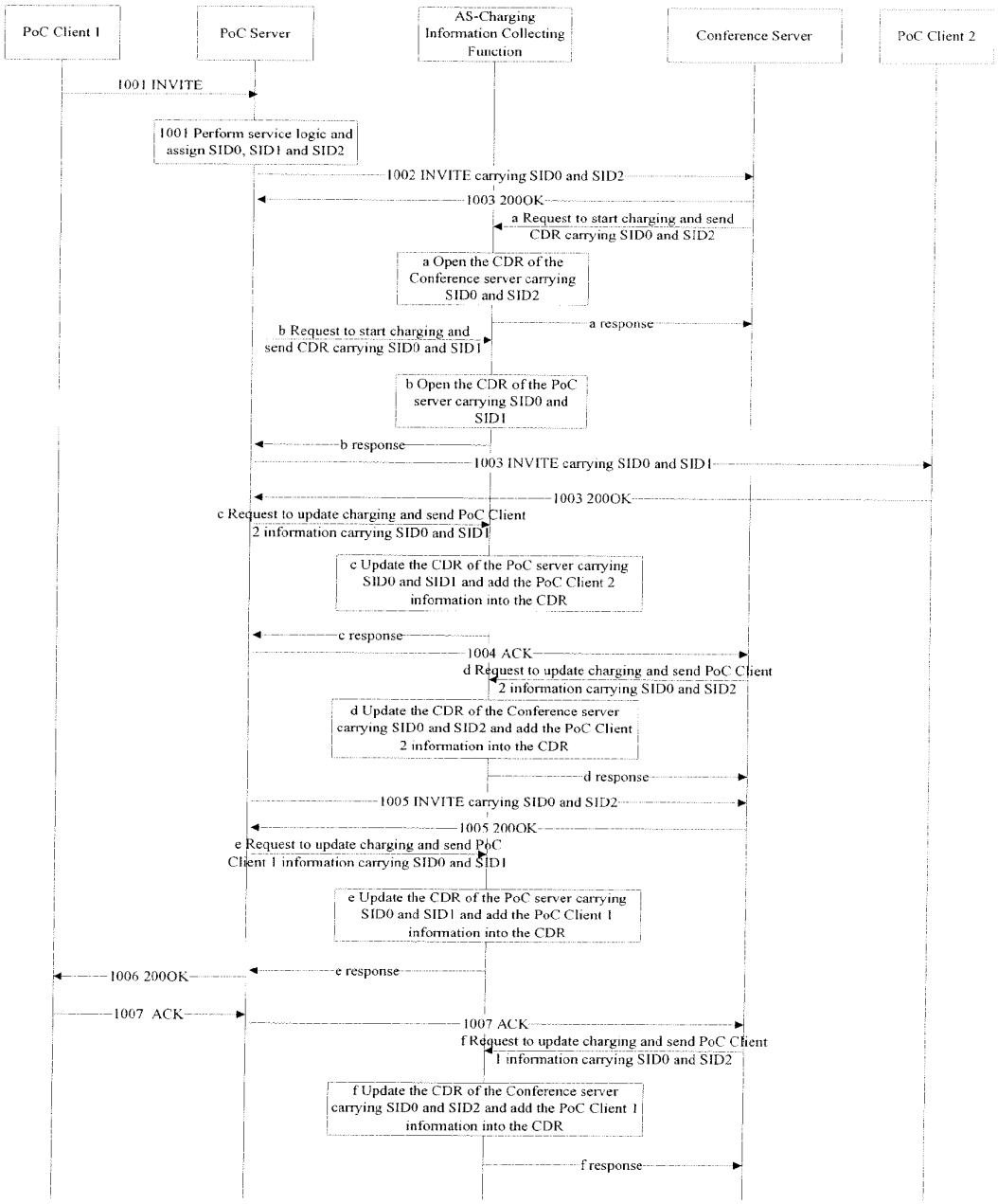

PoC Client 1
PoC Server
AS-Charging Information Collecting Function
Conference Server
PoC Client 2
1001 INVITE
1001 Perform service logic and assign SID0, SID1 and SID2
1002 INVITE carrying SID0 and SID2
1003 200OK
a Request to start charging and send CDR carrying SID0 and SID2
a Open the CDR of the Conference server carrying SID0 and SID2
a response
b Request to start charging and send CDR carrying SID0 and SID1
b Open the CDR of the PoC server carrying SID0 and SID1
b response
1003 INVITE carrying SID0 and SID1
1003 200OK
c Request to update charging and send PoC Client 2 information carrying SID0 and SID1
c Update the CDR of the PoC server carrying SID0 and SID1 and add the PoC Client 2 information into the CDR
c response
1004 ACK
d Request to update charging and send PoC Client 2 information carrying SID0 and SID2
d Update the CDR of the Conference server carrying SID0 and SID2 and add the PoC Client 2 information into the CDR
d response
1005 INVITE carrying SID0 and SID2
1005 200OK
e Request to update charging and send PoC Client 1 information carrying SID0 and SID1
e Update the CDR of the PoC server carrying SID0 and SID1 and add the PoC Client 1 information into the CDR
1006 200OK
e response
1007 ACK
1007 ACK
f Request to update charging and send PoC Client 1 information carrying SID0 and SID2
f Update the CDR of the Conference server carrying SID0 and SID2 and add the PoC Client 1 information into the CDR
f response

Fig. 10

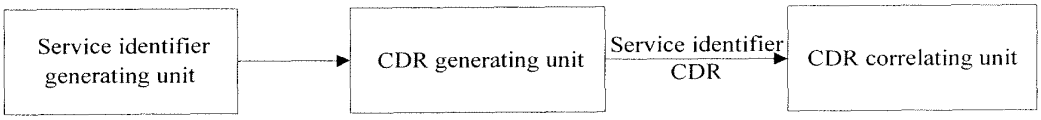

Service identifier generating unit
CDR generating unit
Service identifier
CDR
CDR correlating unit

Fig. 11

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2007/001048

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/14(2006.01)i

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 H04L 12/-; H04M 15/-; G06Q10/-

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)

CNPAT WPI EPODOC PAJ: service, charg+, money, bill, fee, cost, associat+, relat+, corresponding, flag, ID, identification, indicator, mark, identifier, identity, distribut+, assign, communicat+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN1267414A (NOKIA NETWORKS OY [FI]) 20 September 2000(20.09.2000) see claims 1,7and figure 3A	1-2, 15-16, 21, 24-25
A		3-14, 17-20, 22-23
A	CN1643888A (ERICSSON TELEFON AB L M [SE]) 20 July 2005(20.07.2005) see whole document	1-25
A	US2004255025A1 (RICAGNI GIUSEPPE [IT]) 16 December 2004(16.12.2004) see whole document	1-25

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&"document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 June 2007 (26.06.2007)	**12 Jul. 2007 (12.07.2007)**
Name and mailing address of the ISA/CN The State Intellectual Property Office, the P.R.China 6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China 100088 Facsimile No. 86-10-62019451	Authorized officer ZHAO,Weihua Telephone No. (86-10)62085024

Form PCT/ISA /210 (second sheet) (April 2007)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2007/001048

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN1267414A	20.09.2000	FI981031A	15.01.1999
		WO9907108A2	11.02.1999
		AU8443398A	22.02.1999
		NO20000170A	13.03.2000
		EP1005737A2	07.06.2000
		US6240091B1	29.05.2001
		JP2001512926T	28.08.2001
CN1643888A	20.07.2005	EP1345402A1	17.09.2003
		WO03077528A1	18.09.2003
		AU2003210373A	22.09.2003
		EP1483893A1	08.12.2004
		JP2005520405T	07.07.2005
		US2005176404A1	11.08.2005
		AT311719T	15.12.2005
		DE60302559D	05.01.2006
		ES2252682T	16.05.2006
US2004255025A1	16.12.2004	None	

Form PCT/ISA /210 (patent family annex) (April 2007)

Electronic Patent Application Fee Transmittal

Application Number:	15217538
Filing Date:	22-Jul-2016
Title of Invention:	MOBILE DEVICE AND METHOD WITH SECURE NETWORK MESSAGING FOR AUTHORIZED COMPONENTS
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Filer:	James E. Harris/Ann Taylor
Attorney Docket Number:	RALEP007C11C3C2C2

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
SUBMISSION- INFORMATION DISCLOSURE STMT	2806	1	90	90
		Total in USD ($)		**90**

Electronic Acknowledgement Receipt	
EFS ID:	27023650
Application Number:	15217538
International Application Number:	
Confirmation Number:	3305
Title of Invention:	MOBILE DEVICE AND METHOD WITH SECURE NETWORK MESSAGING FOR AUTHORIZED COMPONENTS
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:	RALEP007C11C3C2C2
Receipt Date:	23-SEP-2016
Filing Date:	22-JUL-2016
Time Stamp:	19:14:41
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$90
RAM confirmation Number	5665
Deposit Account	505876
Authorized User	Taylor, Ann
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 CFR 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 CFR 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 CFR 1.19 (Document supply fees)

Charge any Additional Fees required under 37 CFR 1.20 (Post Issuance fees)

Charge any Additional Fees required under 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	Information Disclosure Statement (IDS) Form (SB08)	P007C11C3C2C2_IDS1.pdf	1054726 d0f180f801e9eca92735f9948f00c49e1cbae830	no	6
Warnings:					
Information:					
2	Information Disclosure Statement (IDS) Form (SB08)	P007C11C3C2C2_IDS2.pdf	1054160 b7d5ac52510b263fb66140f327d7fbf8bf5c2f7c	no	4
Warnings:					
Information:					
3	Foreign Reference	2083.pdf	782462 2ce1ee70705ca2f54e4571f31517ddc96b1c19c4	no	8
Warnings:					
Information:					
4	Foreign Reference	2084.pdf	1397656 9e6a8957ad2e807f979431120ddbd1741e2acde7	no	57
Warnings:					
Information:					
5	Foreign Reference	2085.pdf	441333 e8defb411cdca2f87d3c0c97eae168e0c2960826	no	19
Warnings:					
Information:					
6	Foreign Reference	2087.pdf	922375 5370f148f48d4def4ad535f2c2b1762f0ca57119	no	47
Warnings:					
Information:					

7	Foreign Reference	2088.pdf	255944 b4b8ef7ddc1f98c4716aaed35917fdb84c9b e0fa	no	18
Warnings:					
Information:					
8	Foreign Reference	2089.pdf	172902 9025822de8f174376f282787af6b3524407b e5db	no	13
Warnings:					
Information:					
9	Foreign Reference	2090.pdf	643809 f84e3fb9347dd0d758241de1f737fa384a62 bebe	no	38
Warnings:					
Information:					
10	Fee Worksheet (SB06)	fee-info.pdf	30671 594f42831414fd8f9fa8a65f2e90fb6108795 9fc	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	6756038		

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

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

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

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
15/217,538	07/22/2016	3687	1530	RALEP007C11C3C2C2	14	2

CONFIRMATION NO. 3305

106963
Headwater Partners I LLC
1011 Pruitt Place
Tyler, TX 75703

CORRECTED FILING RECEIPT

OC000000088016018

Date Mailed: 09/26/2016

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

Inventor(s)

Gregory G. Raleigh, Woodside, CA;

Applicant(s)

Headwater Partners I 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 14/979,233 12/22/2015
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: 08/03/2016
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 15/217,538**
Projected Publication Date: 11/10/2016
Non-Publication Request: No
Early Publication Request: No
**** SMALL ENTITY ****
Title

MOBILE DEVICE AND METHOD WITH SECURE NETWORK MESSAGING FOR AUTHORIZED COMPONENTS

Preliminary Class

455

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.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

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

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

106963 7590 09/16/2016
Headwater Partners I 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 facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

Ann Taylor	(Depositor's name)
Ann Taylor	(Signature)
September 23, 2016	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/217,538	07/22/2016	Gregory G. Raleigh	RALEP007C11C3C2C2	3305

TITLE OF INVENTION: AUTOMATED DEVICE PROVISIONING AND ACTIVATION

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	12/16/2016

EXAMINER	ART UNIT	CLASS-SUBCLASS
RUDY, ANDREW J	3687	455-411000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

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

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

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

(A) NAME OF ASSIGNEE: Headwater Partners I LLC
(B) RESIDENCE: (CITY and STATE OR COUNTRY): 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. The following fee(s) are submitted:
☒ Issue Fee
☐ Publication Fee (No small entity discount permitted)
☐ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
☐ A check is enclosed.
☐ Payment by credit card. Form PTO-2038 is attached.
☒ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number 505876 (enclose an extra copy of this form).

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

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

Authorized Signature _____ Date September 23 2016
Typed or printed name James E. Harris Registration No. 40013

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

Electronic Patent Application Fee Transmittal

Application Number:	15217538
Filing Date:	22-Jul-2016
Title of Invention:	MOBILE DEVICE AND METHOD WITH SECURE NETWORK MESSAGING FOR AUTHORIZED COMPONENTS
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Filer:	James E. Harris/Ann Taylor
Attorney Docket Number:	RALEP007C11C3C2C2

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
UTILITY APPL ISSUE FEE	2501	1	480	480

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

Electronic Acknowledgement Receipt	
EFS ID:	27028229
Application Number:	15217538
International Application Number:	
Confirmation Number:	3305
Title of Invention:	MOBILE DEVICE AND METHOD WITH SECURE NETWORK MESSAGING FOR AUTHORIZED COMPONENTS
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:	RALEP007C11C3C2C2
Receipt Date:	26-SEP-2016
Filing Date:	22-JUL-2016
Time Stamp:	11:57:12
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$480
RAM confirmation Number	11133
Deposit Account	505876
Authorized User	Taylor, Ann
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 CFR 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 CFR 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 CFR 1.19 (Document supply fees)

Charge any Additional Fees required under 37 CFR 1.20 (Post Issuance fees)

Charge any Additional Fees required under 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)	P007C11C3C2C2_IssueFee.pdf	384249 4e9676499bb36868ea800b2cc3cf326c85f21859	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30746 9df9d8598bbd45f5adef774a73431b2fd5783db4	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	414995		

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 NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/217,538	07/22/2016	Gregory G. Raleigh	RALEP007C11C3C2C2	3305

106963 7590 10/07/2016

Headwater Partners I LLC
1011 Pruitt Place
Tyler, TX 75703

EXAMINER	
RUDY, ANDREW J	

ART UNIT	PAPER NUMBER
3687	

NOTIFICATION DATE	DELIVERY MODE
10/07/2016	ELECTRONIC

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

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

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

patent@headwaterllc.com

UNITED STATES DEPARTMENT OF COMMERCE
U.S. Patent and Trademark Office
Address : COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPLICATION NO./ CONTROL NO.	FILING DATE	FIRST NAMED INVENTOR / PATENT IN REEXAMINATION	ATTORNEY DOCKET NO.
15/217,538	22 July, 2016	RALEIGH, GREGORY G.	RALEP007C11C3C2C2

Headwater Partners I LLC
1011 Pruitt Place
Tyler, TX 75703

EXAMINER	
ANDREW JOSEPH RUDY	
ART UNIT	**PAPER**
3687	20160930

DATE MAILED:

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

Commissioner for Patents

Applicant's two Information Disclosure Statements (IDS's) submitted September 23, 2016 have been reviewed. Note the attached IDS's. The claims remain allowed.

/ANDREW JOSEPH RUDY/
Primary Examiner
Art Unit: 3687

PTO-90C (Rev.04-03)

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	15217538
Filing Date	2016-07-22
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP007C11C3C2C2

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	5617539	A	1997-04-01	Ludwig et al.	
	2	6601040	B1	2003-07-29	Kolls, H. Brock	
	3	6636721	B2	2003-10-21	Threadgill et al.	
	4	6959393	B2	2005-10-25	Hollis et al.	
	5	7177919	B1	2007-02-13	Truong et al.	
	6	7369856	B2	2008-05-06	Ovadia, Shlomo	
	7	7428750	B1	2008-09-23	Dunn et al.	
	8	7486658	B2	2009-02-03	Kumar, Rajneesh	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3C2C2

	9	7599714	B2	2009-10-06	Kuzminskiy, Alexandr	
	10	8943551	B2	2015-01-27	Ganapathy et al.	
	11	7610047	B2	2009-10-27	Hicks III et al.	
	12	7643411	B2	2010-01-05	Andreasen et al.	
	13	7719966	B2	2010-05-18	Luft et al.	
	14	7979069	B2	2011-07-12	Hupp et al.	
	15	8132256	B2	2012-03-06	Bari, Farooq	
	16	8145194	B2	2012-03-27	Yoshikawa et al.	
	17	8194581	B1	2012-06-05	Schroeder et al.	
	18	8380247	B2	2013-02-19	Engstrom	
	19	8418168	B2	2013-04-09	Tyhurst et al.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3C2C2

	20	8494559	B1	2013-07-23	Malmi	
	21	8543814	B2	2013-09-24	Laitinen et al.	
	22	9413546	B2	2016-08-09	Meier et al.	
	23	8719397	B2	2014-05-06	Levi et al.	
	24	8787249	B2	2014-07-22	Giaretta et al.	
	25	8838752	B2	2014-09-16	Lor et al.	
	26	8855620	B2	2014-10-07	Sievers et al.	
	27	8862751	B2	2014-10-14	Faccin 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

EFS Web 2.1.17

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3C2C2

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	/Andrew Joseph Rudy/	Date Considered	09/29/2016

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

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

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	15217538
Filing Date	2016-07-22
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP007C11C3C2C2

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	20070130283	A1	2007-06-07	Klein 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	1545114	EP	A1	2005-06-22	Alcatel		
	2	1887732	EP	A1	2008-02-13	Huawei Technologies Co., Ltd.		
	3	2007065	EP	A1	2008-12-24	Huawei Technologies Co., Ltd.		

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15217538
	Filing Date	2016-07-22
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C11C3C2C2

	4	2002067616	WO	A1	2002-08-29	Sonera Oyj		
	5	2003017063	WO	A2	2003-02-27	Apogee Networks		
	6	2003017065	WO	A2	2003-02-27	Apogee Networks		
	7	2007120310	WO		2007-10-25	Qualcomm 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

EXAMINER SIGNATURE

Examiner Signature	/Andrew Joseph Rudy/	Date Considered	09/29/2016

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

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

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15217538	RALEIGH, GREGORY G.
	Examiner	**Art Unit**
	ANDREW J RUDY	3687

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

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	2														
~~13~~	14														
3	3														
4	4														
5	5														
6	6														
7	7														
8	8														
9	9														
10	10														
11	11														
12	12														
~~12~~ 2	13														
14	15														

Change(s) applied
to document,
/R.L./
9/23/2016

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	14	
/ANDREW JOSEPH RUDY/ Primary Examiner.Art Unit 3687	9/12/2016	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	25

U.S. Patent and Trademark Office Part of Paper No. 20160912

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.
15/217,538	11/08/2016	9491564	RALEP007C11C3C2C2	3305

106963 7590 10/19/2016

Headwater Partners I 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 0 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

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

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

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

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

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

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
15/217,538	07/22/2016	Gregory G. Raleigh	RALEP007C11C3C2C2

CONFIRMATION NO. 3305

106963
Headwater Partners I LLC
1011 Pruitt Place
Tyler, TX 75703

PUBLICATION NOTICE

OC000000087134105

Title:MOBILE DEVICE AND METHOD WITH SECURE NETWORK MESSAGING FOR AUTHORIZED COMPONENTS

Publication No.US-2016-0330567-A1
Publication Date:11/10/2016

NOTICE OF PUBLICATION OF APPLICATION

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

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

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

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

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

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