PTO/AIA/15 (07-12)
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.

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No.	RALEP007C3
First Inventor	Raleigh, Gregory G.
Title	AUTOMATED DEVICE PROVISIONING AND ACTIVATION
Express Mail Label No.	n/a

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

1. ☑ **Fee Transmittal Form.** (PTO/SB/17 or equivalent)
2. ☑ **Applicant claims small entity status.** See 37 CFR 1.27.
3. ☑ **Specification.** [*Total Pages* 249] Both the claims and abstract must start on a new page *(For information on the preferred arrangement, see MPEP § 608.01(a))*
4. ☑ **Drawing(s).** (*35 U.S.C. 113*) [*Total Sheets* 106]
5. **Inventor's Oath or Declaration.** [*Total Sheets* 1] *(including substitute statements under 37 CFR 1.64 and assignments serving as an oath or declaration under 37 CFR 1.63(e))*
   a. ☑ Newly executed (original or copy)
   b. ☐ A copy from a prior application (37 CFR 1.63(d))
6. ☑ **Application Data Sheet.** **See Note below.* See 37 CFR 1.76 (PTO/AIA/14 or equivalent)
7. ☐ **CD-ROM or CD-R.** in duplicate, large table or Computer Program *(Appendix)*
   ☐ Landscape Table on CD
8. **Nucleotide and/or Amino Acid Sequence Submission.** *(if applicable, items a. – c. are required)*
   a. ☐ Computer Readable Form (CRF)
   b. ☐ Specification Sequence Listing on:
      i. ☐ CD-ROM or CD-R (2 copies); or
      ii. ☐ Paper
   c. ☐ Statements verifying identity of above copies

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

ACCOMPANYING APPLICATION PARTS

9. ☐ **Assignment Papers.** (cover sheet & document(s)) Name of Assignee
10. ☐ **37 CFR 3.73(c) Statement.** ☐ **Power of Attorney.** *(when there is an assignee)*
11. ☐ **English Translation Document.** *(if applicable)*
12. ☐ **Information Disclosure Statement.** (PTO/SB/08 or PTO-1449) ☐ Copies of citations attached
13. ☐ **Preliminary Amendment.**
14. ☐ **Return Receipt Postcard.** *(MPEP § 503) (Should be specifically itemized)*
15. ☐ **Certified Copy of Priority Document(s).** *(if foreign priority is claimed)*
16. ☐ **Nonpublication Request.** Under 35 U.S.C. 122(b)(2)(B)(i). Applicant must attach form PTO/SB/35 or equivalent.
17. ☑ **Other:** Certification and Request for Prioritized Examination Under 37 CFR 1.102(e) (TrackOne)

***Note:** (1) Benefit claims under 37 CFR 1.78 and foreign priority claims under 1.55 **must** be included in an Application Data Sheet (ADS).
(2) For applications filed under 35 U.S.C. 111, the application must contain an ADS specifying the applicant if the applicant is an assignee, person to whom the inventor is under an obligation to assign, or person who otherwise shows sufficient proprietary interest in the matter. See 37 CFR 1.46(b).

18. CORRESPONDENCE ADDRESS

☑ The address associated with Customer Number: 106963 *OR* ☐ Correspondence address below

Name					
Address					
City		State		Zip Code	
Country		Telephone		Email	

Signature		Date	December 4, 2012
Name (Print/Type)	Krista S. Jacobsen	Registration No. (Attorney/Agent)	59374

This collection of information is required by 37 CFR 1.53(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: 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/14 (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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	RALEP007C3
	Application Number	
Title of Invention	AUTOMATED DEVICE PROVISIONING AND ACTIVATION	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor 1 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Gregory	G.	Raleigh	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Woodside	State/Province	CA	Country of Residence i	US

Mailing Address of Inventor:

Address 1	131 Fox Hollow Road		
Address 2			
City	Woodside	State/Province	CA
Postal Code	94062	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	RALEP007C3	Small Entity Status Claimed	☒
Application Type	Nonprovisional		
Subject Matter			
Suggested Class (if any)		Sub Class (if any)	
Suggested Technology Center (if any)			
Total Number of Drawing Sheets (if any)	106	Suggested Figure for Publication (if any)	

PTO/AIA/14 (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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	RALEP007C3
	Application Number	
Title of Invention	AUTOMATED DEVICE PROVISIONING AND ACTIVATION	

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	106963		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	Continuation of	12/380780	2009-03-02
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
12/380780	non provisional of	61/206354	2009-01-28
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
12/380780	non provisional of	61/206944	2009-02-04
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
12/380780	non provisional of	61/207393	2009-02-10
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
12/380780	non provisional of	61/207739	2009-02-13

PTO/AIA/14 (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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	RALEP007C3
	Application Number	
Title of Invention	AUTOMATED DEVICE PROVISIONING AND ACTIVATION	

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button. Add

Foreign Priority Information:

This section allows for the applicant to claim benefit of foreign priority and to identify any prior foreign application for which priority is not claimed. 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(a).

Remove

Application Number	Country i	Filing Date (YYYY-MM-DD)	Priority Claimed
			○ Yes ◉ No

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button. Add

Authorization to Permit Access:

☒ Authorization to Permit Access to the Instant Application by the Participating Offices

If checked, the undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the instant patent application is filed access to the instant patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the instant patent application is filed to have access to the instant patent application.

In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the instant patent application with respect to: 1) the instant patent application-as-filed; 2) any foreign application to which the instant patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the instant patent application; and 3) any U.S. application-as-filed from which benefit is sought in the instant patent application.

In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date of filing this Authorization.

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

PTO/AIA/14 (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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	RALEP007C3
	Application Number	
Title of Invention	AUTOMATED DEVICE PROVISIONING AND ACTIVATION	

Applicant 1

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.

Remove

◉ Assignee	○ Legal Representative under 35 U.S.C. 117
○ 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 Assignee is an Organization check here. ☒

Organization Name	Headwater Partners I LLC

Mailing Address Information:

Address 1	350 Marine Parkway, Suite 300		
Address 2			
City	Redwood Shores	**State/Province**	CA
Country [i]	US	Postal Code	94065
Phone Number	650-217-2798	Fax Number	
Email Address	patent@headwaterllc.com		

Additional Applicant Data may be generated within this form by selecting the Add button. Add

Signature:

Remove

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

Signature	/Krista S. Jacobsen/			Date (YYYY-MM-DD)	2012-12-04
First Name	Krista S.	Last Name	Jacobsen	Registration Number	59374

Additional Signature may be generated within this form by selecting the Add button. Add

PTO/AIA/14 (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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	RALEP007C3
	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 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.

IPR2025-01571
Apple EX1002 Page 7

Attorney Docket No. RALEP007C3

APPLICATION FOR UNITED STATES PATENT

AUTOMATED DEVICE PROVISIONING AND ACTIVATION

By Inventor:

Gregory G. Raleigh
Woodside, CA
A Citizen of the United States

Assignee: Headwater Partners I LLC

HEADWATER PARTNERS I LLC
350 Marine Parkway, Suite 300
Redwood Shores, CA 94065
Telephone (650) 517-2798

CROSS REFERENCE TO OTHER APPLICATIONS

[0001] This application is a continuation of Application No. 12/380,780 (Attorney Docket No. RALEP007), entitled AUTOMATED DEVICE PROVISIONING AND ACTIVATION, filed March 2, 2009, which is incorporated herein by reference for all purposes. Application No. 12/380,780 (Attorney Docket No. RALEP007), entitled AUTOMATED DEVICE PROVISIONING AND ACTIVATION, filed March 2, 2009, claims the benefit of provisional Application No. 61/206,354 (Attorney Docket No. RALEP001+), entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD, filed January 28, 2009, provisional Application No. 61/206,944 (Attorney Docket No. RALEP002+), entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD, filed February 4, 2009, provisional Application No. 61/207,393 (Attorney Docket No. RALEP003+), entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD filed February 10, 2009, and provisional Application No. 61/207,739 (Attorney Docket No. RALEP004+), entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD filed February 13, 2009, all of which are incorporated herein by reference for all purposes.

IPR2025-01571
Apple EX1002 Page 9

BACKGROUND OF THE INVENTION

[0002] With the advent of mass market digital communications and content distribution, many access networks such as wireless networks, cable networks and DSL (Digital Subscriber Line) networks are pressed for user capacity, with, for example, EVDO (Evolution-Data Optimized), HSPA (High Speed Packet Access), LTE (Long Term Evolution), WiMax (Worldwide Interoperability for Microwave Access), and Wi-Fi (Wireless Fidelity) wireless networks increasingly becoming user capacity constrained. Although wireless network capacity will increase with new higher capacity wireless radio access technologies, such as MIMO (Multiple-Input Multiple-Output), and with more frequency spectrum being deployed in the future, these capacity gains are likely to be less than what is required to meet growing digital networking demand.

[0003] Similarly, although wire line access networks, such as cable and DSL, can have higher average capacity per user, wire line user service consumption habits are trending toward very high bandwidth applications that can quickly consume the available capacity and degrade overall network service experience. Because some components of service provider costs go up with increasing bandwidth, this trend will also negatively impact service provider profits.

IPR2025-01571
Apple EX1002 Page 10

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] Various embodiments of the invention are disclosed in the following detailed description and the accompanying drawings.

[0005] FIG. 1 illustrates a simplified (e.g., "flattened") network architecture in accordance with some embodiments.

[0006] FIG. 2 illustrates another simplified (e.g., "flattened") network architecture including an MVNO (Mobile Virtual Network Operator) relationship in accordance with some embodiments.

[0007] FIG. 3 illustrates another simplified (e.g., "flattened") network architecture including two central providers in accordance with some embodiments.

[0008] FIG. 4 illustrates a network architecture including a Universal Mobile Telecommunications System (UMTS) overlay configuration in accordance with some embodiments.

[0009] FIG. 5 illustrates a network architecture including an Evolution Data Optimized (EVDO) overlay configuration in accordance with some embodiments.

[0010] FIG. 6 illustrates a network architecture including a 4G LTE and Wi-Fi overlay configuration in accordance with some embodiments.

[0011] FIG. 7 illustrates a network architecture including a WiMax and Wi-Fi overlay configuration in accordance with some embodiments.

[0012] FIG. 8 illustrates another simplified (e.g., "flattened") network architecture including multiple wireless access networks (e.g., 3G and 4G Wireless Wide Area Networks (WWANs)) and multiple wire line networks (e.g., Data Over Cable Service Interface Specification (DOCSIS) and Digital Subscriber Line Access Multiplexer (DSLAM) wire line networks) in accordance with some embodiments.

IPR2025-01571
Apple EX1002 Page 11

[0013] FIG. 9 illustrates a hardware diagram of a device that includes a service processor in accordance with some embodiments.

[0014] FIG. 10 illustrates another hardware diagram of a device that includes a service processor in accordance with some embodiments.

[0015] FIG. 11 illustrates another hardware diagram of a device that includes a service processor in accordance with some embodiments.

[0016] FIG. 12 illustrates another hardware diagram of a device that includes a service processor in accordance with some embodiments.

[0017] FIG. 13 illustrates another hardware diagram of a device that includes a service processor implemented in external memory of a System On Chip (SOC) in accordance with some embodiments.

[0018] FIG. 14 illustrates another hardware diagram of a device that includes a service processor implemented in external memory of a System On Chip (SOC) in accordance with some embodiments.

[0019] FIGS. 15A through 15F illustrate hardware diagrams of a device that include a service processor and a bus structure extension using intermediate modem or networking device combinations in accordance with various embodiments.

[0020] FIG. 16 is a functional diagram illustrating a device based service processor and a service controller in accordance with some embodiments.

[0021] FIG. 17 is another functional diagram illustrating the device based service processor and the service controller in accordance with some embodiments.

[0022] FIG. 18 is another functional diagram illustrating the device based service processor and the service controller in which the service processor controls the policy implementation for multiple access network modems and technologies in accordance with some embodiments.

IPR2025-01571
Apple EX1002 Page 12

[0023] FIG. 19 is another functional diagram illustrating the service processor and the service controller in accordance with some embodiments.

[0024] FIG. 20 is another functional diagram illustrating the service processor and the service controller in accordance with some embodiments.

[0025] FIG. 21 is another functional diagram illustrating the service processor and the service controller in accordance with some embodiments.

[0026] FIGS. 22A and 22B provide tables summarizing various service processor agents (and/or components/functions implemented in software and/or hardware) in accordance with some embodiments.

[0027] FIG. 23 provides a table summarizing various service controller server elements (and/or components/functions implemented in software and/or hardware) in accordance with some embodiments.

[0028] FIG. 24 is a functional diagram illustrating the service control device link of the service processor and the service control service link of the service controller in accordance with some embodiments.

[0029] FIG. 25 is a functional diagram illustrating framing structure of a service processor communication frame and a service controller communication frame in accordance with some embodiments.

[0030] FIGS. 26A through 26H provide tables summarizing various service processor heartbeat functions and parameters in accordance with some embodiments.

[0031] FIGS. 27A through 27P provide tables summarizing various device based service policy implementation verification techniques in accordance with some embodiments.

[0032] FIGS. 28A through 28E provide tables summarizing various techniques for protecting the device based service policy from compromise in accordance with some embodiments.

IPR2025-01571
Apple EX1002 Page 13

[0033] FIG. 29 is a functional diagram illustrating a device communications stack that allows for implementing verifiable traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments.

[0034] FIG. 30 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments.

[0035] FIG. 31 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments.

[0036] FIG. 32 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments.

[0037] FIG. 33 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments.

[0038] FIG. 34 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments.

[0039] FIG. 35 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments.

[0040] FIG. 36 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments.

[0041] FIG. 37 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments.

IPR2025-01571
Apple EX1002 Page 14

[0042] FIG. 38 is a functional diagram illustrating a device service processor packet processing flow in accordance with some embodiments.

[0043] FIG. 39 is another functional diagram illustrating the device service processor packet processing flow in accordance with some embodiments.

[0044] FIG. 40 is another functional diagram illustrating the device service processor packet processing flow in accordance with some embodiments.

[0045] FIG. 41 provides a table summarizing various privacy levels for service history reporting in accordance with some embodiments.

[0046] FIGS. 42A through 42J provide tables summarizing various service policy control commands in accordance with some embodiments.

[0047] FIGS. 43A through 43B are flow diagrams illustrating a flow diagram for a service processor authorization sequence as shown in FIG. 43A and a flow diagram for a service controller authorization sequence as shown in FIG. 43B in accordance with some embodiments.

[0048] FIGS. 44A through 44B are flow diagrams illustrating a flow diagram for a service processor activation sequence as shown in FIG. 44A and a flow diagram for a service controller activation sequence as shown in FIG. 44B in accordance with some embodiments.

[0049] FIGS. 45A through 45B are flow diagrams illustrating a flow diagram for a service processor access control sequence as shown in FIG. 45A and a flow diagram for a service controller access control sequence as shown in FIG. 45B in accordance with some embodiments.

[0050] FIG. 46 is a functional diagram illustrating open, decentralized, device based mobile commerce transactions in accordance with some embodiments.

[0051] FIGS. 47A through 47B are transactional diagrams illustrating open, decentralized, device based mobile commerce transactions in accordance with some embodiments.

IPR2025-01571
Apple EX1002 Page 15

[0052] FIG. 48 illustrates a network architecture including a service controller device control system and a service controller analysis and management system in accordance with some embodiments.

[0053] FIG. 49 illustrates a network architecture for an open developer platform for virtual service provider (VSP) partitioning in accordance with some embodiments.

[0054] FIG. 50 illustrates a network architecture including a billing to service controller interface for accommodating minimum changes in existing central billing, AAA and/or other network components in accordance with some embodiments.

[0055] FIG. 51 illustrates a network architecture for locating service controller device control functions with AAA and network service usage functions in accordance with some embodiments.

[0056] FIG. 52 illustrates a network architecture for locating service controller device control functions in the access transport network in accordance with some embodiments.

[0057] FIG. 53 illustrates a network architecture for locating service controller device control functions in the radio access network in accordance with some embodiments.

[0058] FIG. 54 illustrates a network architecture for locating service controller device control functions with AAA and network service usage including deep packet inspection functions in accordance with some embodiments.

[0059] FIG. 55 illustrates another network architecture for locating service controller device control functions with AAA and network service usage including deep packet inspection functions in accordance with some embodiments.

[0060] FIG. 56 illustrates a 4G/3G/2G DPI/DPC enabled gateway in accordance with some embodiments.

[0061] FIG. 57 illustrates a network architecture including the VSP workstation server in communication with the 4G/3G/2G DPI/DPC gateways in accordance with some embodiments.

IPR2025-01571
Apple EX1002 Page 16

[0062] FIG. 58 illustrates another 4G/3G/2G DPI/DPC enabled gateway in accordance with some embodiments.

[0063] FIG. 59 illustrates another network architecture including the VSP workstation server in communication with the 4G/3G/2G DPI/DPC gateways in accordance with some embodiments.

[0064] FIG. 60 illustrates a 4G/3G/2G DPI/DPC enabled gateway and service controller device control system in accordance with some embodiments.

[0065] FIG. 61 illustrates another network architecture including the VSP workstation server in communication with the 4G/3G/2G DPI/DPC gateways in accordance with some embodiments.

[0066] FIG. 62 illustrates another 4G/3G/2G DPI/DPC enabled gateway and service controller device control system in accordance with some embodiments.

[0067] FIG. 63 illustrates another network architecture including the VSP workstation server in communication with the 4G/3G/2G DPI/DPC gateways in accordance with some embodiments.

[0068] FIG. 64 illustrates another network architecture including a system located in the manufacturing or distribution chain for the device that provides the device provisioning or partial provisioning, and any pre-activation required for the device to later activate on the network in accordance with some embodiments.

IPR2025-01571
Apple EX1002 Page 17

DETAILED DESCRIPTION

[0069] The invention can be implemented in numerous ways, including as a process; an apparatus; a system; a composition of matter; a computer program product embodied on a computer readable storage medium; and/or a processor, such as a processor configured to execute instructions stored on and/or provided by a memory coupled to the processor. In this specification, these implementations, or any other form that the invention may take, may be referred to as techniques. In general, the order of the steps of disclosed processes may be altered within the scope of the invention. Unless stated otherwise, a component such as a processor or a memory described as being configured to perform a task may be implemented as a general component that is temporarily configured to perform the task at a given time or a specific component that is manufactured to perform the task. As used herein, the term "processor" refers to one or more devices, circuits, and/or processing cores configured to process data, such as computer program instructions.

[0070] A detailed description of one or more embodiments of the invention is provided below along with accompanying figures that illustrate the principles of the invention. The invention is described in connection with such embodiments, but the invention is not limited to any embodiment. The scope of the invention is limited only by the claims and the invention encompasses numerous alternatives, modifications and equivalents. Numerous specific details are set forth in the following description in order to provide a thorough understanding of the invention. These details are provided for the purpose of example and the invention may be practiced according to the claims without some or all of these specific details. For the purpose of clarity, technical material that is known in the technical fields related to the invention has not been described in detail so that the invention is not unnecessarily obscured.

[0071] With the development and increasing proliferation of mass market digital communications and content distribution, communication network capacity gains are being outpaced by growing digital networking demand. For example, some industry experts project average wireless device usage of four devices per subscriber, with a mixture of general purpose devices like smart phones and computers along with special purpose devices like music players, electronic readers, connected (e.g., networked) cameras and connected gaming devices. In

IPR2025-01571
Apple EX1002 Page 18

addition, wire line user service consumption habits are trending toward very high bandwidth applications that can quickly consume the available capacity and degrade overall network service experience if not efficiently managed. Because some components of service provider costs go up with increasing bandwidth, this trend will also negatively impact service provider profits.

[0072] There is a need for a communication system and method that provides for flexible service plans and management of user network services to provide consumer choice of more refined service plan offerings and efficient management of network capacity.

[0073] Also, it is becoming increasingly important to more deeply manage the level of services delivered to networked devices to provide cost effective services that match growing digital networking usage patterns. For example, access providers can move away from only billing for basic access and move toward billing for higher level service delivery with example services including rich Internet access and email, application based billing, content distribution, entertainment activities, information or content subscription or gaming. In addition, a growing number of new special purpose and general purpose networked devices are fueling demand for new service plans, for example, tailored to the new device usage models (e.g., a special service plan for an e-book reader device).

[0074] As network capabilities grow and new networked device offerings grow, access network service providers will realize increasing value in opening up their networks to allow innovation and expanded offerings for network service consumers. However, opening up the networks to provide efficient third party definition of alternative service and billing models requires more flexible service and billing policy management solutions. For example, machine to machine applications such as telemetry, surveillance, shipment tracking and two way power control systems are example new applications that would require new offerings to make such available to network service customers. The need to customize service offerings for these new applications requires more efficient methods for defining, testing and launching new services with more refined control of service functions and service costs. In some embodiments, this means billing for different types of service elements, such as total traffic, content downloads, application usage, information or content subscription services, people or asset tracking services, real time machine to machine information or electronic commerce transactions.

IPR2025-01571
Apple EX1002 Page 19

[0075] In some embodiments, network user capacity is increased and user service costs are reduced by managing and billing for service consumption in a more refined manner (e.g., to satisfy network neutrality requirements). By managing service consumption in a user friendly manner, the overall service capacity required to satisfy the user device needs can be tailored more closely to the needs of a given user thereby reducing user service costs and increasing service provider profits. For example, managing service usage while maintaining user satisfaction includes service usage policy implementation and policy management to identify, manage and bill for service usage categories, such as total traffic consumption, content downloads, application usage, information or content subscription services, electronic commerce transactions, people or asset tracking services or machine to machine networking services. As described herein, service activity is used to refer to any service usage or traffic usage that can be associated with, for example, an application; a network communication end point, such as an address, uniform resource locator (URL) or other identifier with which the device is communicating; a traffic content type; a transaction where content or other material, information or goods are transacted, purchased, reserved, ordered or exchanged; a download, upload or file transfer; email, text, SMS, IMS or other messaging activity or usage; VOIP services; video services; a device usage event that generates a billing event; service usage associated with a bill by account activity (also referred to as billing by account) as described herein; device location; device service usage patterns, device user interface (UI) discovery patterns, content usage patterns or other characterizations of device usage; or other categories of user or device activity that can be identified, monitored, recorded, reported, controlled or processed in accordance with a set of verifiable service control policies. As will be apparent to one of ordinary skill in the art in view of the embodiments described herein, some embodiments identify various service activities for the purpose of decomposing overall service usage into finer sub-categories of activities that can be verifiably monitored, categorized, cataloged, reported, controlled, monetized and used for end user notification in a manner that results in superior optimization of the service capabilities for various levels of service cost or for various types of devices or groups. In some embodiments, it will be apparent to one of ordinary skill in the art that the terms service activity or service usage are associated with categorizing and possibly monitoring or controlling data traffic, application usage, communication with certain network end points, or transactions, and it will also be apparent that in some embodiments the term service activity is

IPR2025-01571
Apple EX1002 Page 20

intended to include one or more of the broader aspects listed above. The shortened term service usage can be used interchangeably with service activity, but neither term is intended in general to exclude any aspect of the other. In some cases, where the terms service usage or service activity are used, more specific descriptors such as traffic usage, application usage, website usage, and other service usage examples are also used to provide more specific examples or focus in on a particular element of the more encompassing terms.

[0076] In some embodiments, employing this level of service categorization and control is accomplished in a manner that satisfies user preferences. In some embodiments, employing this level of service categorization and control is accomplished in a manner that also satisfies government rules or regulations regarding open access, for example, network neutrality requirements. In some embodiments, service management solutions that also collect and/or report user or device service usage or service activity behavior to determine how best to meet the user's simultaneous desires for service quality and lower service costs are disclosed. For example, such monitoring and reporting are accomplished in a manner that includes approval by the user and in a manner that also protects the privacy of user information and service usage behavior or service activity history.

[0077] In some embodiments, a system and method is disclosed for increasing network user capacity for wireless networks in the face of increasing service demand per user by providing for a greater number of base stations, also sometimes referred to as access points, base terminals, terminal nodes or other well known acronyms, to be more easily and/or more cost effectively deployed. For example, to simplify the process of deploying base stations, the installation complexity and the network infrastructure required for the base station to obtain backhaul service to the various networks that users desire to connect with are reduced.

[0078] In some embodiments, dense base station deployments are simplified by reducing the requirement to aggregate or concentrate the base station traffic through a specific dedicated core network infrastructure, so that the base stations connect to the desired user networks through a more diverse set of local loop, back bone and core routing options. This approach also reduces network infrastructure equipment, installation and maintenance costs. In some embodiments, this is accomplished by distributing the network traffic policy implementation and

IPR2025-01571
Apple EX1002 Page 21

control away from the core network by providing for more control for service policy implementation and management on the end user device and, in some embodiments, in the end user device with respect to certain service policies and the network (e.g., control plane servers) with respect to other service policies. For example, this approach facilitates connecting the base stations directly to the local loop Internet with a minimum of specific dedicated networking infrastructure.

[0079] In some embodiments, service and transaction billing event capture and logging are distributed to the device. For example, providing service and transaction billing event capture and logging at the device provides a greater capability to monitor, classify and control deeper aspects of service usage or service activity at the device as compared to the relatively less capability for the same in the network infrastructure (e.g., for certain traffic flows, such as encrypted traffic flows). Furthermore, billing at the device provides for very specialized with many different billing and service plans for different device and service usage or service activity scenario combinations without the problem of attempting to propagate and manage many different deep packet inspection (DPI) and traffic shaping profiles in the networking equipment infrastructure. For example, service billing at the device can provide for more sophisticated, more specialized and more scalable billing and service plans.

[0080] Another form of billing that needs improvement is electronic commerce transaction billing with device assisted central billing. Today, most central billing and content distribution models require either centralized content distribution maintained by the central service provider or central billing authority, or a centralized ecommerce website or portal traffic aggregation system controlled by the central service provider or central billing provider, or both. In such systems, content and transaction providers such as media providers, application developers, entertainment providers, transaction website providers and others must adapt their mainstream electronic offering and commerce systems, such as shopping experience websites, to fit within the various proprietary customized infrastructure and content storage solutions for ecommerce markets, such as BREW® (Binary Runtime Environment for Wireless from Qualcomm® Inc.), Symbian OS (from Symbian Software Ltd) and Apple iPhone 3G App Store (from Apple Inc.). This approach requires a large amount of unnecessary custom interface development and stifles open market creativity for HTTP, WAP or portal/widget based shopping

IPR2025-01571
Apple EX1002 Page 22

destinations and experiences. As disclosed below, a superior approach includes device based transaction billing for an open ecosystem in which a central billing provider provides users and ecommerce transaction providers with a central billing solution and experience that does not require extensive custom development or ecommerce infrastructure interfacing.

[0081] In some embodiments, products that incorporate device assisted service policy implementation, network services and service profiles (e.g., a service profile includes a set of one or more service policy settings for the device for a service on the network) are disclosed, as described below. For example, aspects of the service policy (e.g., a set of policies/policy settings for the device for network services, typically referring to lower level settings, such as access control settings, traffic control settings, billing system settings, user notification settings, user privacy settings, user preference settings, authentication settings and admission control settings) that are moved out of the core network and into the end user device include, for example, certain lower level service policy implementations, service usage or service activity monitoring and reporting including, for example, privacy filtering, customer resource management monitoring and reporting including, for example, privacy filtering, adaptive service policy control, service network access control services, service network authentication services, service network admission control services, service billing, transaction billing, simplified service activation and sign up, user service usage or service activity notification and service preference feedback and other service capabilities.

[0082] As discussed below, product designs that move certain aspects of one or more of these service profile or service policy implementation elements into the device provide several advantageous solutions to the needs described above. For example, benefits of certain embodiments include the ability to manage or bill for a richer and more varied set of network services, better manage overall network capacity, better manage end user access costs, simplify user or new device service activation, simplify development and deployment of new devices with new service plans (e.g., service profile and billing/costs information associated with that service profile), equip central service providers with more effective open access networks for new third party solutions, simplify the equipment and processes necessary to deploy wireless base stations and simplify the core networking equipment required to deploy certain access networks.

IPR2025-01571
Apple EX1002 Page 23

[0083] As discussed below, there are two network types that are discussed: a central provider network and a service provider network. The central provider network generally refers to the access network required to connect the device to other networks. The central provider network generally includes the physical layer, the Media Access Control (MAC) and the various networking functions that can be implemented to perform authentication, authorization and access control, and to route traffic to a network that connects to the control plane servers, as discussed below. The service provider network generally refers to the network that includes the control plane servers. In some embodiments, a central provider network and a service provider network are the same, and in some embodiments, they are different. In some embodiments, the owner or manager of the central provider network and the owner or manager of the service provider network are the same, and in some embodiments, they are different.

[0084] In some embodiments, control of the device service policies is accomplished with a set of service control plane servers that reside in the access network or any network that can be reached by the device. This server based control plane architecture provides for a highly efficient means of enabling third party control of services and billing, such as for central carrier open development programs or Mobile Virtual Network Operator (MVNO) relationships. As device processing and memory capacity expands, moving to this distributed service policy processing architecture also becomes more efficient and economical. In some embodiments, several aspects of user privacy and desired network neutrality are provided by enabling user control of certain aspects of device based service usage or service activity reporting, traffic reporting, service policy control and customer resource management (CRM) reporting.

[0085] In many access networks, such as wireless access networks, bandwidth capacity is a valuable resource in the face of the increasing popularity of devices, applications and content types that consume more bandwidth. To maintain reasonable service profit margins, a typical present service provider practice is to charge enough per user for access to make service plans profitable for the higher bandwidth users. However, this is not an optimal situation for users who desire to pay less for lower bandwidth service usage or service activity scenarios.

[0086] Accordingly, in some embodiments, a range of service plan pricing can be enabled that also maintains service profitability for the service provider, for example, by

IPR2025-01571
Apple EX1002 Page 24

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

IPR2025-01571
Apple EX1002 Page 25

implementations ranging from examples such as free ambient services that are perhaps sponsored by transaction revenues and/or bill by account sponsored service partner revenues, to intermediately priced plans for basic access services for mass market user devices or machine to machine communication devices, to more expensive plans with very high levels of service usage or service activity limits or no limits at all. Several bill by account embodiments also provide for the cataloging of service usage that is not a direct benefit to end users but is needed for basic maintenance of the device control channels and access network connection, so that the maintenance traffic service cost can be removed from the user billing or billed to non-user accounts used to track or account for such service costs. These embodiments and others result in a service usage or service activity control capability that provides more attractive device and service alternatives to end users while maintaining profitability for service providers and their partners.

[0087] In some embodiments, the above described various embodiments for device based service policy and/or service profile communications control are implemented using network based service control, for example, for satisfying various network neutrality and/or privacy requirements, based on indication(s) received from the device (e.g., user input provided using the device UI using the service processor) and network based service control (e.g., using a DPI service monitor or DPC policy implementation and/or other network elements).

[0088] In some embodiments, a virtual network overlay includes a device service processor, a network service controller and a control plane communication link to manage various aspects of device based network service policy implementation. In some embodiments, the virtual network overlay networking solution is applied to an existing hierarchical network (e.g., for wireless services), and in some embodiments, is applied to simplify or flatten the network architecture as will be further described below. In some embodiments, the large majority of the complex data path network processing required to implement the richer service management objectives of existing hierarchical networks (e.g., for wireless services) are moved into the device, leaving less data path processing required in the edge network and in some cases even less in the core network. Because the control plane traffic between the service control servers and the device agents that implement service policies can be several orders of magnitude slower than the data plane traffic, service control server network placement and back-haul

IPR2025-01571
Apple EX1002 Page 26

infrastructure is much less performance sensitive than the data plane network. In some embodiments, as described further below, this architecture can be overlaid onto all the important existing access network architectures used today. In some embodiments, this architecture can be employed to greatly simplify core access network routing and data plane traffic forwarding and management. For example, in the case of wireless networks, the incorporation of device assisted service policy implementation architectures can result in base stations that directly connect to the Internet local loop and the data traffic does not need to be concentrated into a dedicated core network. This results, for example, in a large reduction in backhaul cost, core network cost and maintenance cost. These cost savings can be re-deployed to purchase and install more base stations with smaller cells, which results in higher data capacity for the access network leading to better user experience, more useful applications and lower service costs. This flattened networking architecture also results in latency reduction as fewer routes are needed to move traffic through the Internet. In some embodiments, the present invention provides the necessary teaching to enable this powerful transformation of centralized network service architectures to a more distributed device based service architectures.

[0089] Device based billing can be compromised, hacked and/or spoofed in many different ways. Merely determining that billing reports are being received from the device, that the device agent software is present and properly configured (e.g., the billing agent is present and properly configured) is insufficient and easily spoofed (e.g., by spoofing the agent itself, providing spoofed billing reports using a spoofed billing agent or providing spoofed agent configurations). Accordingly, in some embodiments, verifiable device assisted and/or network based service policy implementation is provided. For example, verifiable service usage and/or service usage billing can be provided as described herein with respect to various embodiments.

[0090] While much of the below discussion and embodiments described below focus on paid service networks, those of ordinary skill in the art will appreciate that many of the embodiments also apply to other networks, such as enterprise networks. For example, the same device assisted network services that create access control services, ambient activation services and other service profiles can be used by corporate IT managers to create a controlled cost service policy network for corporate mobile devices. As another example, embodiments described below for providing end user service control can also allow a service provider to offer

IPR2025-01571
Apple EX1002 Page 27

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.

[0091] **Network Architecture for Device Assisted/Based Service Control**

[0092] 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.

[0093] 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

IPR2025-01571
Apple EX1002 Page 28

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.

[0094] 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

IPR2025-01571
Apple EX1002 Page 29

a simple example and many other selection criteria are possible in the network selection embodiment as discussed further below.

[0095] Network Based Service Usage Monitoring for Verification and Other Purposes

[0096] 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

IPR2025-01571
Apple EX1002 Page 30

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.

[0097] 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.

[0098] 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

IPR2025-01571
Apple EX1002 Page 31

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.

[0099] 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

IPR2025-01571
Apple EX1002 Page 32

(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.

[00100] 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.

[00101] 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.

IPR2025-01571
Apple EX1002 Page 33

[00102] 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.

[00103] 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.

[00104] 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

IPR2025-01571
Apple EX1002 Page 34

(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.

[00105] 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.

[00106] 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.

IPR2025-01571
Apple EX1002 Page 35

[00107] 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.

[00108] 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

IPR2025-01571
Apple EX1002 Page 36

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.

[00109] 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.

[00110] 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.

IPR2025-01571
Apple EX1002 Page 37

[00111] 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.

[00112] 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

IPR2025-01571
Apple EX1002 Page 38

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.

[00113] 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.

[00114] 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.

IPR2025-01571
Apple EX1002 Page 39

[00115] 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.

[00116] 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

IPR2025-01571
Apple EX1002 Page 40

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.

[00117] 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.

[00118] 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

IPR2025-01571
Apple EX1002 Page 41

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.

[00119] 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

IPR2025-01571
Apple EX1002 Page 42

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.

[00120] 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.

[00121] 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.

[00122] 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

IPR2025-01571
Apple EX1002 Page 43

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.

[00123] 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.

[00124] 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.

IPR2025-01571
Apple EX1002 Page 44

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.

[00125] 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.

IPR2025-01571
Apple EX1002 Page 45

[00126] 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.

[00127] 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

IPR2025-01571
Apple EX1002 Page 46

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.

[00128] 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.

[00129] 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).

[00130] 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

IPR2025-01571
Apple EX1002 Page 47

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.

[00131] 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).

[00132] **Service Processor Configurations for Devices**

[00133] 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

IPR2025-01571
Apple EX1002 Page 48

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).

[00134] 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

IPR2025-01571
Apple EX1002 Page 49

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.

[00135] 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.

[00136] 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.

IPR2025-01571
Apple EX1002 Page 50

[00137] 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.

[00138] 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.

IPR2025-01571
Apple EX1002 Page 51

[00139] 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.

[00140] **Service Processor Implemented on a Communications Modem**

[00141] 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.

[00142] 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

IPR2025-01571
Apple EX1002 Page 52

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.

[00143] 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).

[00144] 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

IPR2025-01571
Apple EX1002 Page 53

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.

[00145] 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,

IPR2025-01571
Apple EX1002 Page 54

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.

[00146] 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.

[00147] 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.

[00148] 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

IPR2025-01571
Apple EX1002 Page 55

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.

[00149] 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.

[00150] 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.

[00151] 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

IPR2025-01571
Apple EX1002 Page 56

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.

[00152] **Service Processor Configurations for Intermediate Networking Devices**

[00153] 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.

[00154] 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

IPR2025-01571
Apple EX1002 Page 57

Wi-Fi data to the WWAN access network without implementing any portion of the service processor 115 as shown in FIG. 15B (1). 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.

[00155] 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

IPR2025-01571
Apple EX1002 Page 58

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.

[00156] 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.

[00157] 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

IPR2025-01571
Apple EX1002 Page 59

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.

[00158] 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.

[00159] 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

IPR2025-01571
Apple EX1002 Page 60

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.

[00160] 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.

[00161] 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

IPR2025-01571
Apple EX1002 Page 61

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.

[00162] 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.

[00163] 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

IPR2025-01571
Apple EX1002 Page 62

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.

[00164] 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.

[00165] 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.

IPR2025-01571
Apple EX1002 Page 63

[00166] **Service Processor and Service Controller for Verifiable Service Monitoring, Notification and Control**

[00167] 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.

[00168] 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

IPR2025-01571
Apple EX1002 Page 64

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.

[00169] 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.

[00170] 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.

IPR2025-01571
Apple EX1002 Page 65

[00171] 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.

[00172] 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

IPR2025-01571
Apple EX1002 Page 66

Network) services, other forms of IP layer encryption and/or another link layer encryption technique.

[00173] 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.

[00174] 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.

[00175] 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).

[00176] 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

IPR2025-01571
Apple EX1002 Page 67

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.

[00177] 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.

[00178] 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.

IPR2025-01571
Apple EX1002 Page 68

[00179] 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).

[00180] 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

IPR2025-01571
Apple EX1002 Page 69

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.

[00181] 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.

[00182] 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.

IPR2025-01571
Apple EX1002 Page 70

[00183] 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.

[00184] 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.

[00185] 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

IPR2025-01571
Apple EX1002 Page 71

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.

[00186] 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

IPR2025-01571
Apple EX1002 Page 72

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.

[00187] 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.

[00188] 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

IPR2025-01571
Apple EX1002 Page 73

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.

[00189] 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.

[00190] 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

IPR2025-01571
Apple EX1002 Page 74

usage monitoring verification tests, service usage billing verification tests and/or transaction billing verification tests.

[00191] 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

IPR2025-01571
Apple EX1002 Page 75

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.

[00192] 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.

[00193] 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.

[00194] 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

IPR2025-01571
Apple EX1002 Page 76

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.

[00195] 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.

[00196] 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.

[00197] 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

IPR2025-01571
Apple EX1002 Page 77

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.

[00198] 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

IPR2025-01571
Apple EX1002 Page 78

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.

[00199] 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.

[00200] 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).

[00201] 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.

[00202] 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

IPR2025-01571
Apple EX1002 Page 79

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.

[00203] 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).

IPR2025-01571
Apple EX1002 Page 80

[00204] 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).

[00205] 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.

[00206] In some embodiments, various lower level service policy implementation embodiments are combined with a higher level set of service policy supervision functions to

IPR2025-01571
Apple EX1002 Page 81

provide device assisted verifiable network access control, authentication and authorization services.

[00207] 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 101 to determine if the device has been used in a manner that is out of plan for the service plan associated with the device 101, 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.

[00208] 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

IPR2025-01571
Apple EX1002 Page 82

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.

[00209] 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.

[00210] 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.

[00211] 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

IPR2025-01571
Apple EX1002 Page 83

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.

[00212] 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.

[00213] 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

IPR2025-01571
Apple EX1002 Page 84

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.

[00214] 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.

[00215] 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.

IPR2025-01571
Apple EX1002 Page 85

[00216] 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.

[00217] 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.

[00218] 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.

IPR2025-01571
Apple EX1002 Page 86

[00219] 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.

[00220] 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

IPR2025-01571
Apple EX1002 Page 87

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.

[00221] 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.

[00222] 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

IPR2025-01571
Apple EX1002 Page 88

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).

[00223] 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.

[00224] 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.

[00225] 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,

IPR2025-01571
Apple EX1002 Page 89

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.

[00226] 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

IPR2025-01571
Apple EX1002 Page 90

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.

[00227] In some embodiments, the service monitor agent 1696 monitors application usage (e.g., which application the user executes on the device 101, 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 101. 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 101. In some embodiments, the service monitor agent 1696 monitors GPS/location information for the device 101. 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 101 such as GPS/location information. As described herein, in some embodiments, the user of the device 101 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).

[00228] 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

IPR2025-01571
Apple EX1002 Page 91

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.

[00229] 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,

IPR2025-01571
Apple EX1002 Page 92

including, for example, the policy control agent 1692 implementing an higher layer of service control to achieve a higher level objective as discussed herein.

[00230] 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.

[00231] 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.

[00232] 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

IPR2025-01571
Apple EX1002 Page 93

interacts with transaction servers (e.g., open content transaction partner sites 134) to conduct ecommerce transactions with central billing 1619.

[00233] 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 101. In some embodiments, a service usage counter monitors service usage including data usage to/from the device 101 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 101. In some embodiments, the service usage counter periodically, or in response to a request, synchronizes the service usage counter on the device 101 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 101 allows the service processor 115

IPR2025-01571
Apple EX1002 Page 94

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 101 in their monitored service data usage count.

[00234] 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 101 (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).

[00235] 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.

[00236] 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

IPR2025-01571
Apple EX1002 Page 95

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.

[00237] 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.

[00238] 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,

IPR2025-01571
Apple EX1002 Page 96

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.

[00239] 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,

IPR2025-01571
Apple EX1002 Page 97

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.

[00240] 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.

[00241] 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

IPR2025-01571
Apple EX1002 Page 98

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).

[00242] 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 101. 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.

[00243] 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 101) 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.

[00244] 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

IPR2025-01571
Apple EX1002 Page 99

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.

[00245] 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

IPR2025-01571
Apple EX1002 Page 100

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).

[00246] 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 101), 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.

[00247] 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

IPR2025-01571
Apple EX1002 Page 101

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.

[00248] 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

IPR2025-01571
Apple EX1002 Page 102

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.

[00249] 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.

[00250] 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

IPR2025-01571
Apple EX1002 Page 103

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.

[00251] 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.

[00252] 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

IPR2025-01571
Apple EX1002 Page 104

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.

[00253] 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.

[00254] 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

IPR2025-01571
Apple EX1002 Page 105

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.

[00255] 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

IPR2025-01571
Apple EX1002 Page 106

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.

[00256] 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.

[00257] 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

IPR2025-01571
Apple EX1002 Page 107

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.

[00258] 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

IPR2025-01571
Apple EX1002 Page 108

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.

[00259] 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

IPR2025-01571
Apple EX1002 Page 109

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).

[00260] 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.

[00261] 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

IPR2025-01571
Apple EX1002 Page 110

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.

[00262] 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.

[00263] 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

IPR2025-01571
Apple EX1002 Page 111

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.

[00264] 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.

[00265] 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.

[00266] 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

IPR2025-01571
Apple EX1002 Page 112

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.

[00267] 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.

[00268] 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.

[00269] 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

IPR2025-01571
Apple EX1002 Page 113

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.

[00270] 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

IPR2025-01571
Apple EX1002 Page 114

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.

[00271] 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

IPR2025-01571
Apple EX1002 Page 115

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.

[00272] 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).

[00273] 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

IPR2025-01571
Apple EX1002 Page 116

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.

[00274] 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

IPR2025-01571
Apple EX1002 Page 117

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.

[00275] 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

IPR2025-01571
Apple EX1002 Page 118

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).

[00276] 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.

[00277] 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.

[00278] 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

IPR2025-01571
Apple EX1002 Page 119

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.

[00279] 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.

IPR2025-01571
Apple EX1002 Page 120

[00280] 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.

[00281] 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.

[00282] 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

IPR2025-01571
Apple EX1002 Page 121

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.

[00283] 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.

[00284] 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.

[00285] 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.

IPR2025-01571
Apple EX1002 Page 122

[00286] 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.

[00287] 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).

[00288] 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.

IPR2025-01571
Apple EX1002 Page 123

[00289] 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.

[00290] **Establishing Coordinated Service and Verification Policies for Service Processor, Service Controller and Network Functions**

[00291] 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

IPR2025-01571
Apple EX1002 Page 124

apparatus. As an example, such embodiments can be applied in overlay applications as discussed below.

[00292] 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).

[00293] 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

IPR2025-01571
Apple EX1002 Page 125

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.

[00294] 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.

[00295] 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.

[00296] 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

IPR2025-01571
Apple EX1002 Page 126

embodiments associated with service activation or the virtual service provider apparatus embodiments, as described herein).

[00297] 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.

[00298] 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.

[00299] 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

IPR2025-01571
Apple EX1002 Page 127

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.

[00300] 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.

[00301] 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

IPR2025-01571
Apple EX1002 Page 128

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.

[00302] 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).

[00303] 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).

[00304] 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

IPR2025-01571
Apple EX1002 Page 129

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.

[00305] 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.

[00306] 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.

IPR2025-01571
Apple EX1002 Page 130

[00307] 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.

[00308] 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

IPR2025-01571
Apple EX1002 Page 131

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.

[00309] 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.

[00310] 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.

IPR2025-01571
Apple EX1002 Page 132

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.

[00311] 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.

[00312] 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

IPR2025-01571
Apple EX1002 Page 133

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.

[00313] 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.

[00314] 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

IPR2025-01571
Apple EX1002 Page 134

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.

[00315] 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.

IPR2025-01571
Apple EX1002 Page 135

[00316] 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.

[00317] 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.

[00318] 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,

IPR2025-01571
Apple EX1002 Page 136

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.

[00319] 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.

[00320] 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.

[00321] **Service Control Device Link and Continuous Heartbeat Authentication**

[00322] 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

IPR2025-01571
Apple EX1002 Page 137

or data packet framing mechanisms (e.g., IPV6), running a more conventional VPN or IPSEC channel, and/or using an independent access network connection.

[00323] 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

IPR2025-01571
Apple EX1002 Page 138

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.

[00324] 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

IPR2025-01571
Apple EX1002 Page 139

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.

[00325] 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

IPR2025-01571
Apple EX1002 Page 140

as using additional and/or fewer elements/functions or other design choices for providing such secure communications).

[00326] 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.

[00327] 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

IPR2025-01571
Apple EX1002 Page 141

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.

[00328] 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.

[00329] 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.

[00330] 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

IPR2025-01571
Apple EX1002 Page 142

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.

[00331] **Device Assisted Service Control and Traffic Control**

[00332] 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.

[00333] 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

IPR2025-01571
Apple EX1002 Page 143

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.

[00334] 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

IPR2025-01571
Apple EX1002 Page 144

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.

[00335] 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).

[00336] 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,

IPR2025-01571
Apple EX1002 Page 145

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

IPR2025-01571
Apple EX1002 Page 146

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.

[00337] 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

IPR2025-01571
Apple EX1002 Page 147

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.

[00338] 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).

[00339] 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

IPR2025-01571
Apple EX1002 Page 148

control integrity agent is in communication with the service monitor agent via the agent communications bus 1630, as also shown.

[00340] 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.

[00341] 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

IPR2025-01571
Apple EX1002 Page 149

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.

[00342] The embodiments depicted in FIG. 30 and other figures generally require enhancements to conventional device networking communication stack processing. For

IPR2025-01571
Apple EX1002 Page 150

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.

[00343] 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.

[00344] 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

IPR2025-01571
Apple EX1002 Page 151

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.

[00345] 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

IPR2025-01571
Apple EX1002 Page 152

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.

[00346] 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.

[00347] 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

IPR2025-01571
Apple EX1002 Page 153

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.

[00348] 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.

[00349] 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

IPR2025-01571
Apple EX1002 Page 154

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.

[00350] 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.

[00351] 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

IPR2025-01571
Apple EX1002 Page 155

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.

[00352] 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.

[00353] 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).

[00354] 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.

IPR2025-01571
Apple EX1002 Page 156

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.

[00355] 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.

[00356] 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

IPR2025-01571
Apple EX1002 Page 157

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.

[00357] 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.

[00358] 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.

IPR2025-01571
Apple EX1002 Page 158

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.

[00359] 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.

[00360] 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

IPR2025-01571
Apple EX1002 Page 159

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.

[00361] 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.

[00362] 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

IPR2025-01571
Apple EX1002 Page 160

one of ordinary skill in the art and not all the processing steps and flow sequences are described herein.

[00363] 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.

[00364] 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.

[00365] 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

IPR2025-01571
Apple EX1002 Page 161

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.

[00366] 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

IPR2025-01571
Apple EX1002 Page 162

burst jitter) can be adjusted so that the access network downstream MAC and/or PHY efficiencies are optimized.

[00367] 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.

[00368] 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.

IPR2025-01571
Apple EX1002 Page 163

39 (e.g., of a less feature rich device service processor embodiment, such as one similar to that depicted in FIG. 32).

[00369] 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).

[00370] 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.

[00371] 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.

[00372] 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

IPR2025-01571
Apple EX1002 Page 164

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.

[00373] 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.

[00374] 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.

[00375] 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

IPR2025-01571
Apple EX1002 Page 165

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.

[00376] 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.

[00377] 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.

[00378] 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,

IPR2025-01571
Apple EX1002 Page 166

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.

[00379] 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.

[00380] 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.

IPR2025-01571
Apple EX1002 Page 167

[00381] 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.

[00382] **Open Content Distribution and Transaction System**

[00383] 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.

[00384] 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

IPR2025-01571
Apple EX1002 Page 168

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.

[00385] 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

IPR2025-01571
Apple EX1002 Page 169

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.

[00386] 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).

[00387] 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

IPR2025-01571
Apple EX1002 Page 170

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.

[00388] 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

IPR2025-01571
Apple EX1002 Page 171

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.

[00389] **Design and Testing for Service Control**

[00390] 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.

[00391] 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

IPR2025-01571
Apple EX1002 Page 172

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.

[00392] 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.

[00393] 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

IPR2025-01571
Apple EX1002 Page 173

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

IPR2025-01571
Apple EX1002 Page 174

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.

[00394] 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.

[00395] 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

IPR2025-01571
Apple EX1002 Page 175

MVNO or VSP. For example, this allows for new services to be more efficiently and more effectively developed, tested and proliferated.

[00396] 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.

[00397] **Virtual Service Provider for Service Control**

[00398] 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.

[00399] 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

IPR2025-01571
Apple EX1002 Page 176

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.

[00400] 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.

[00401] 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

IPR2025-01571
Apple EX1002 Page 177

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.

[00402] 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).

[00403] 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

IPR2025-01571
Apple EX1002 Page 178

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.

[00404] **Open Development System for Access Services – SDK**

[00405] 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

IPR2025-01571
Apple EX1002 Page 179

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.

[00406] 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

IPR2025-01571
Apple EX1002 Page 180

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.

IPR2025-01571
Apple EX1002 Page 181

[00407] 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).

[00408] 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.

[00409] **Interface Server Overlay for Billing/IPDR Feed Mediation**

[00410] 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

IPR2025-01571
Apple EX1002 Page 182

system 123 to efficiently communicate with the service controller (e.g., service controller device control system 4825).

[00411] 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.

[00412] 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.

IPR2025-01571
Apple EX1002 Page 183

[00413] 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.

[00414] 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.

[00415] 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

IPR2025-01571
Apple EX1002 Page 184

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.

[00416] 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.

[00417] 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.

[00418] **Integrated Service Control**

[00419] 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.

[00420] 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).

IPR2025-01571
Apple EX1002 Page 185

[00421] 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).

[00422] **Ambient Services**

[00423] 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.

[00424] 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

IPR2025-01571
Apple EX1002 Page 186

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.

[00425] 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.

[00426] 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

IPR2025-01571
Apple EX1002 Page 187

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).

[00427] 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

IPR2025-01571
Apple EX1002 Page 188

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.

[00428] 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.

[00429] 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

IPR2025-01571
Apple EX1002 Page 189

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.

[00430] **Network Based Service Monitoring, Notification and Control**

[00431] 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.

[00432] 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

IPR2025-01571
Apple EX1002 Page 190

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.

[00433] 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.

[00434] 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

IPR2025-01571
Apple EX1002 Page 191

(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.

[00435] 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.

[00436] 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

IPR2025-01571
Apple EX1002 Page 192

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.

[00437] 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.

[00438] 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

IPR2025-01571
Apple EX1002 Page 193

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).

[00439] 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

IPR2025-01571
Apple EX1002 Page 194

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.

[00440] 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

IPR2025-01571
Apple EX1002 Page 195

the user can be notified, or the service can be controlled or throttled if the user has selected a control or throttling option.

[00441] 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.

[00442] 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

IPR2025-01571
Apple EX1002 Page 196

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.

[00443] 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

IPR2025-01571
Apple EX1002 Page 197

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.

[00444] 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.

[00445] 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.

[00446] 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.

[00447] 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.

IPR2025-01571
Apple EX1002 Page 198

[00448] 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.

[00449] 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.

IPR2025-01571
Apple EX1002 Page 199

[00450] 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.

[00451] 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

IPR2025-01571
Apple EX1002 Page 200

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.

[00452] 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).

[00453] 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.

[00454] 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

IPR2025-01571
Apple EX1002 Page 201

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.

[00455] 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.

[00456] 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

IPR2025-01571
Apple EX1002 Page 202

conjunction with the service controller device control system 6225 without assistance from the service processors 115.

[00457] 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.

[00458] 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.

[00459] **Provisioning and Activation**

[00460] 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.

[00461] 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

IPR2025-01571
Apple EX1002 Page 203

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.

[00462] 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).

[00463] 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

IPR2025-01571
Apple EX1002 Page 204

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.

[00464] 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.

[00465] 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

IPR2025-01571
Apple EX1002 Page 205

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

IPR2025-01571
Apple EX1002 Page 206

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.

[00466] 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

IPR2025-01571
Apple EX1002 Page 207

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.

[00467] 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.

[00468] 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

IPR2025-01571
Apple EX1002 Page 208

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).

[00469] 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,

IPR2025-01571
Apple EX1002 Page 209

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.

[00470] 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.

[00471] 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.

[00472] 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

IPR2025-01571
Apple EX1002 Page 210

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.

[00473] 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.

[00474] 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.

[00475] 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

IPR2025-01571
Apple EX1002 Page 211

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.

[00476] 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

IPR2025-01571
Apple EX1002 Page 212

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.

[00477] 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.

[00478] 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

IPR2025-01571
Apple EX1002 Page 213

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.

[00479] 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.

[00480] 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

IPR2025-01571
Apple EX1002 Page 214

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.

[00481] 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

IPR2025-01571
Apple EX1002 Page 215

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).

[00482] 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

IPR2025-01571
Apple EX1002 Page 216

used/required to provision the device or service is generated at the time the partial credentials are determined rather than beforehand.

[00483] 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.

[00484] 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

IPR2025-01571
Apple EX1002 Page 217

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.

[00485] 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.

IPR2025-01571
Apple EX1002 Page 218

[00486] 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.

[00487] 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.

[00488] 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

IPR2025-01571
Apple EX1002 Page 219

access the network, then one or more reserve sets can be drawn upon to gain access to the network.

[00489] 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.

[00490] 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

IPR2025-01571
Apple EX1002 Page 220

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.

[00491] 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

IPR2025-01571
Apple EX1002 Page 221

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.

[00492] 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.

IPR2025-01571
Apple EX1002 Page 222

[00493] 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.

[00494] 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.

IPR2025-01571
Apple EX1002 Page 223

[00495] 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.

[00496] 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

IPR2025-01571
Apple EX1002 Page 224

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.

[00497] 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.

[00498] 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

IPR2025-01571
Apple EX1002 Page 225

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.

[00499] 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.

[00500] 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

IPR2025-01571
Apple EX1002 Page 226

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.

[00501] 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.

[00502] 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

IPR2025-01571
Apple EX1002 Page 227

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.

[00503] 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.

IPR2025-01571
Apple EX1002 Page 228

[00504] 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.

[00505] 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.

[00506] 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

IPR2025-01571
Apple EX1002 Page 229

device based software and/or hardware element), and the credentials are, in some cases, also communicated to the various network equipment elements.

[00507] 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.

[00508] 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.

[00509] 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

IPR2025-01571
Apple EX1002 Page 230

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.

[00510] 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.

[00511] 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

IPR2025-01571
Apple EX1002 Page 231

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.

[00512] 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.

IPR2025-01571
Apple EX1002 Page 232

[00513] 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.

[00514] 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.

[00515] **Verifiable Device Assisted Services For Intermediate Networking Devices**

[00516] 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.

IPR2025-01571
Apple EX1002 Page 233

[00517] 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.

[00518] 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

IPR2025-01571
Apple EX1002 Page 234

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.

[00519] 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.

[00520] 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

IPR2025-01571
Apple EX1002 Page 235

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.

[00521] 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.

[00522] 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

IPR2025-01571
Apple EX1002 Page 236

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.

[00523] 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.

[00524] 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

IPR2025-01571
Apple EX1002 Page 237

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.

[00525] 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.

IPR2025-01571
Apple EX1002 Page 238

[00526] 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.

[00527] 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.

[00528] 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

IPR2025-01571
Apple EX1002 Page 239

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.

[00529] 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.

[00530] 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.

[00531] 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

IPR2025-01571
Apple EX1002 Page 240

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.

[00532] 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.

IPR2025-01571
Apple EX1002 Page 241

[00533] 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.

[00534] 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 a end point device identifier, user identifier, end point device group identifier, and/or user group identifier.

[00535] 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

IPR2025-01571
Apple EX1002 Page 242

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.

[00536] 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.

[00537] 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

IPR2025-01571
Apple EX1002 Page 243

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.

[00538] 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.

[00539] 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.

[00540] 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.

IPR2025-01571
Apple EX1002 Page 244

[00541] 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.

[00542] 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.

[00543] 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.

IPR2025-01571
Apple EX1002 Page 245

[00544] 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.

[00545] 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 indentifying 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.

IPR2025-01571
Apple EX1002 Page 246

[00546] 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 a 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.

[00547] 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.

[00548] 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

IPR2025-01571
Apple EX1002 Page 247

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.

[00549] 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.

[00550] WHAT IS CLAIMED IS:

IPR2025-01571
Apple EX1002 Page 248

CLAIMS

1. A method performed by a network system, the method comprising:

providing a plurality of service control links to a plurality of end-user devices communicatively coupled to the network system, each service control link secured by an encryption protocol, a particular service control link of the plurality of service control links supporting control-plane communications between the network system and a particular end-user device of the plurality of end-user devices over one or more wireless access networks;

receiving a server message from a particular server of a plurality of servers communicatively coupled to the network system, the server message comprising message payload and information identifying a particular device agent of a plurality of device agents on the particular end-user device;

generating an encrypted message comprising the message payload and an identifier configured to assist in delivering at least a portion of the message payload to the particular device agent on the particular end-user device; and

sending the encrypted message to the particular end-user device over the particular service control link.

2. The method of claim 1, wherein the particular server comprises a service usage history server, a policy management server, an access control integrity server, a network traffic analysis server, a beta test server, a service download control server, a billing event server, an activation server, a transaction server, an authentication server, or a content management server.

3. The method of claim 1, wherein the message payload comprises information associated with a service usage or cost.

4. The method of claim 3, wherein the information associated with a service usage or cost comprises one or more of a service usage value, a projected service usage value, a service usage plan limit, a projected service usage overage warning, a projected

IPR2025-01571
Apple EX1002 Page 249

service cost overage warning, a service plan period time duration, a service plan time remaining before end of period, and information about a service overage.

5. The method of claim 1, wherein the message payload is based, at least in part, on a user preference.

6. The method of claim 1, wherein the message payload comprises a service offer, an advertisement, or a transaction offer.

7. The method of claim 1, wherein the message payload comprises a device agent instruction, a setting, an agent configuration, or a software update for the particular device agent.

8. The method of claim 1, wherein the message payload comprises information associated with software or a media file.

9. The method of claim 1, wherein the message payload comprises information associated with a service policy.

10. The method of claim 1, wherein the message payload comprises an indication of additional data or information available to the particular device agent.

11. The method of claim 1, wherein the message payload is configured to assist in causing the particular end-user device to present, through a user interface, information associated with the message payload.

12. The method of claim 1, wherein the server message is a first server message, and wherein the message payload is a first message payload, and wherein the information identifying the particular device agent of the plurality of device agents on the particular end-user device is first information, and wherein the identifier configured to assist the particular end-user device in delivering at least a portion of the message payload to the particular device agent is a first identifier, and further comprising

IPR2025-01571
Apple EX1002 Page 250

receiving a second server message from the particular server or from another server of the plurality of servers communicatively coupled to the network system, the second server message comprising second message payload and second information identifying a second device agent on the particular end-user device, the second device agent being the particular device agent or another device agent of the plurality of device agents on the particular end-user device, and wherein the encrypted message further comprises the second message payload and a second identifier configured to assist in delivering at least a portion of the second message payload to the second device agent.

13. The method of claim 1, wherein the server message is a first server message, and wherein the particular server is a first server, and wherein the message payload is first message payload, and wherein the particular device agent is a first device agent, and wherein the encrypted message is a first encrypted message, and wherein the agent identifier is a first agent identifier, and further comprising:

receiving a second server message from a second server of the plurality of servers, the second server message comprising second message payload and information identifying a second device agent of the plurality of device agents on the particular end-user device;

generating a second encrypted message comprising the second message payload and a second agent identifier configured to assist the particular end-user device in delivering the second message payload to the second device agent; and

sending the second encrypted message to the particular end-user device over the particular service control link.

14. The method of claim 1, wherein the particular service control link supports asynchronous transmissions by the network system.

IPR2025-01571
Apple EX1002 Page 251

15. The method of claim 1, further comprising sending a credential, a certificate, or a token to the particular end-user device or obtaining the credential, the certificate, or the token from the particular end-user device during a service authorization sequence.

16. The method of claim 15, wherein the credential comprises one or more of a phone number, an identification number, a security signature, a security credential, a subscriber identity module (SIM) identifier, a mobile equipment identifier (MEID), and a device identifier.

17. The method of claim 1, wherein the particular device agent comprises software.

18. The method of claim 1, further comprising:

triggering a transmission to maintain the particular service control link when a time since sending the encrypted message to the particular end-user device would otherwise cause the particular service control link to terminate, and

determining when to send the encrypted message to the particular end-user device.

19. The method of claim 1, wherein the sending the encrypted message to the particular end-user device over the particular service control link is not based on whether the particular device agent is running on the particular end-user device.

20. The method of claim 1, wherein at least one of the plurality of servers comprises a content transaction server configured to provide an electronic commerce offering and transaction platform to the particular end-user device.

21. The method of claim 20, further comprising including one or more third party transaction bills on a central provider bill.

22. The method of claim 1, wherein a transmission over the particular service control link is within an ambient service.

IPR2025-01571
Apple EX1002 Page 252

23. The method of claim 1, wherein the plurality of service control links enables a particular server of the plurality of servers to push the message payload to a selected one of the plurality of device agents on any one of the plurality of end-user devices.

24. The method of claim 1, wherein the particular service control link is configured to support control-plane communications using an Internet protocol.

25. The method of claim 1, wherein providing the plurality of service control links to the plurality of end-user devices comprises providing the plurality of service control links to a plurality of service control device link agents, each service control device link agent on one of the plurality of end-user devices, a particular service control device link agent on the particular end-user device for delivering agent messages over an agent communication bus to at least one of the plurality of device agents on the particular end-user device.

26. The method of claim 25, wherein the encrypted message is a first encrypted message, and wherein the identifier is configured to assist the particular service control device link agent in generating a second encrypted message for delivery to the particular device agent, the second encrypted message comprising the at least a portion of the message payload.

27. A network system comprising:

means for providing a plurality of service control links to a plurality of end-user devices communicatively coupled to the network system, each service control link secured by an encryption protocol, a particular service control link of the plurality of service control links supporting control-plane communications between the network system and a particular end-user device of the plurality of end-user devices over one or more wireless access networks;

means for receiving a server message from a particular server of a plurality of servers communicatively coupled to the network system, the server message

IPR2025-01571
Apple EX1002 Page 253

comprising message payload and information identifying a particular device agent of a plurality of device agents on the particular end-user device;

means for generating an encrypted message comprising the message payload and an identifier configured to assist in delivering at least a portion of the message payload to the particular device agent on the particular end-user device; and

means for sending the encrypted message to the particular end-user device over the particular service control link.

28. A non-transitory computer-readable storage medium storing program code for causing a computer to execute a method comprising:

providing a plurality of service control links to a plurality of end-user devices communicatively coupled to the computer, each service control link secured by an encryption protocol, a particular service control link of the plurality of service control links supporting control-plane communications between the computer and a particular end-user device of the plurality of end-user devices over one or more wireless access networks;

receiving a server message from a particular server of a plurality of servers communicatively coupled to the computer, the server message comprising message payload and information identifying a particular device agent of a plurality of device agents on the particular end-user device;

generating an encrypted message comprising the message payload and an identifier configured to assist in delivering at least a portion of the message payload to the particular device agent on the particular end-user device; and

sending the encrypted message to the particular end-user device over the particular service control link.

29. The non-transitory computer-readable storage medium recited in claim 28, wherein providing the plurality of service control links to the plurality of end-user devices comprises providing the plurality of service control links to a plurality of service control device link agents, each service control device link agent on a different one of

IPR2025-01571
Apple EX1002 Page 254

the plurality of end-user devices, a particular service control device link agent on the particular end-user device for delivering agent messages over an agent communication bus to at least one of the plurality of device agents on the particular end-user device.

30. The non-transitory computer-readable storage medium recited in claim 28, wherein the message payload is configured to assist in causing the particular end-user device to present, through a user interface, information associated with the message payload.

IPR2025-01571
Apple EX1002 Page 255

ABSTRACT

A method, and a computer-readable medium storing program code for causing a computer to execute the method, comprising providing a plurality of links to a plurality of end-user devices communicatively coupled to a network system, a particular link of the plurality of links supporting control-plane communications between the network system and a particular end-user device of the plurality of end-user devices over one or more wireless access networks; receiving a message from a server communicatively coupled to the network system, the message comprising payload and information identifying a particular device agent of a plurality of device agents on the particular end-user device; generating an encrypted message comprising the payload and an identifier configured to assist in delivering at least a portion of the payload to the particular device agent on the particular end-user device; and sending the encrypted message to the particular end-user device over the particular link.

IPR2025-01571
Apple EX1002 Page 256

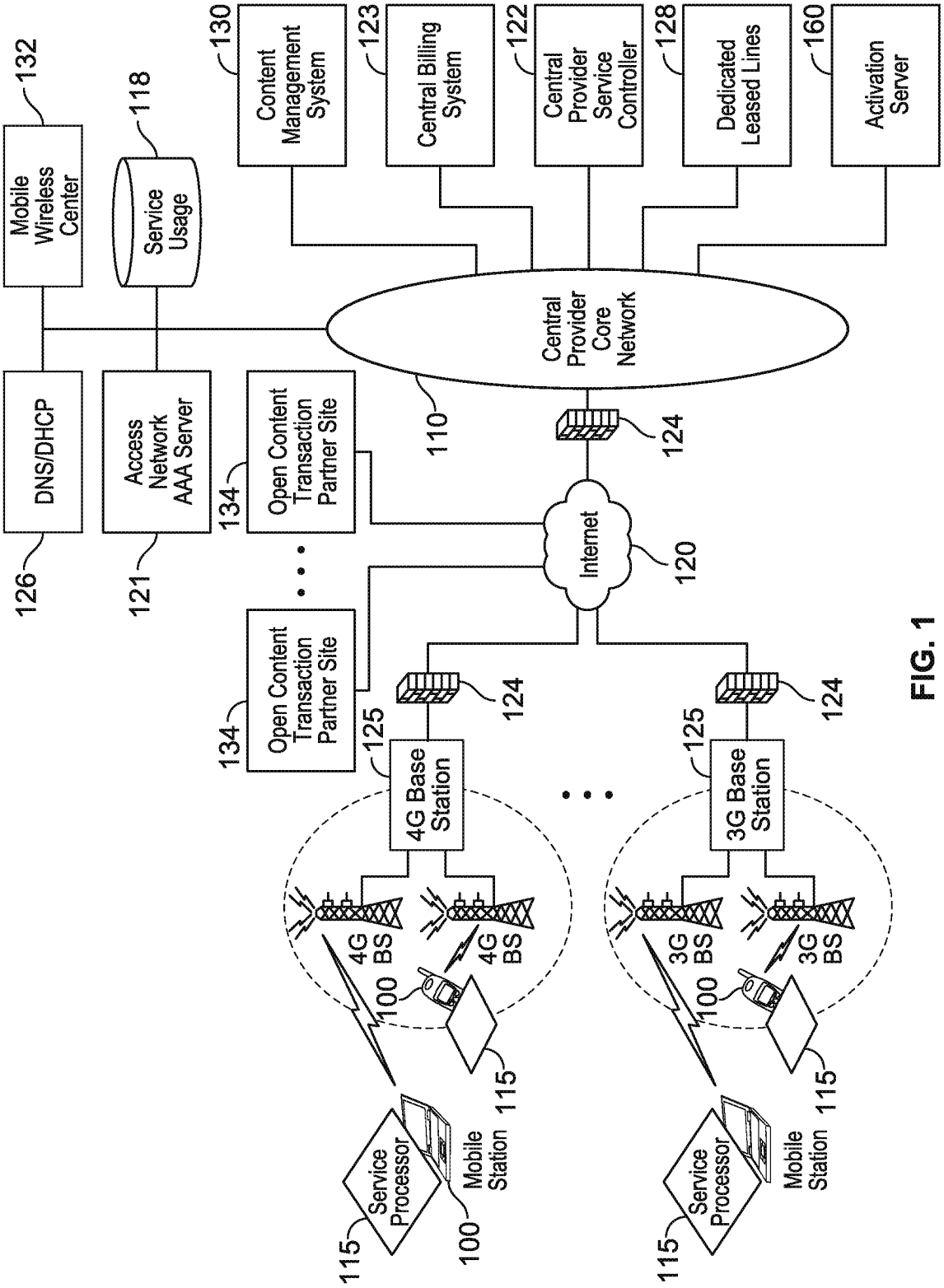

Content Management System
130
Central Billing System
123
Central Provider Service Controller
122
Dedicated Leased Lines
128
Activation Server
160
Mobile Wireless Center
132
Service Usage
118
Central Provider Core Network
110
DNS/DHCP
126
Access Network AAA Server
121
Open Content Transaction Partner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

FIG. 1

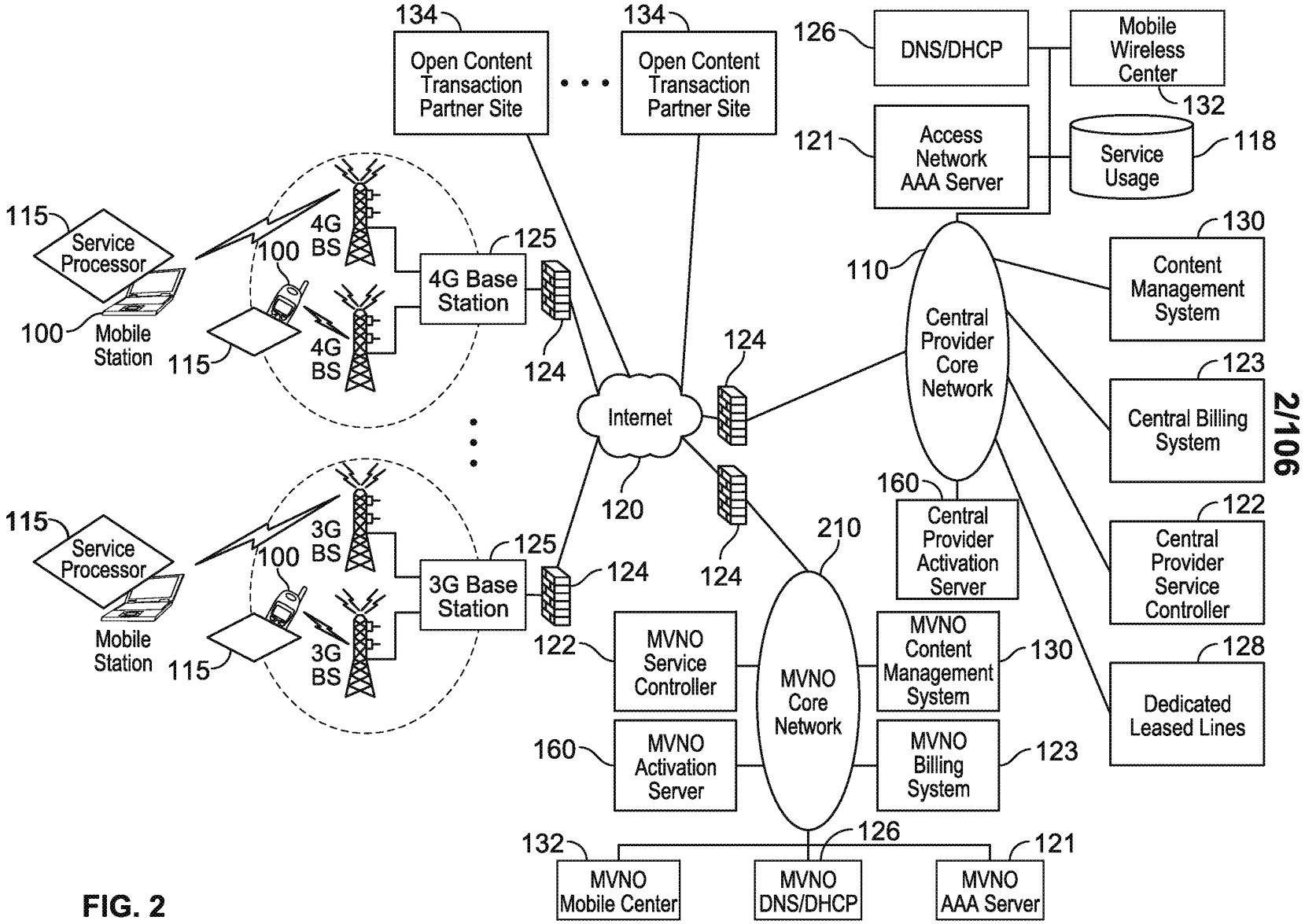


FIG. 2

2/106

IPR2025-01571
Apple EX1002 Page 258

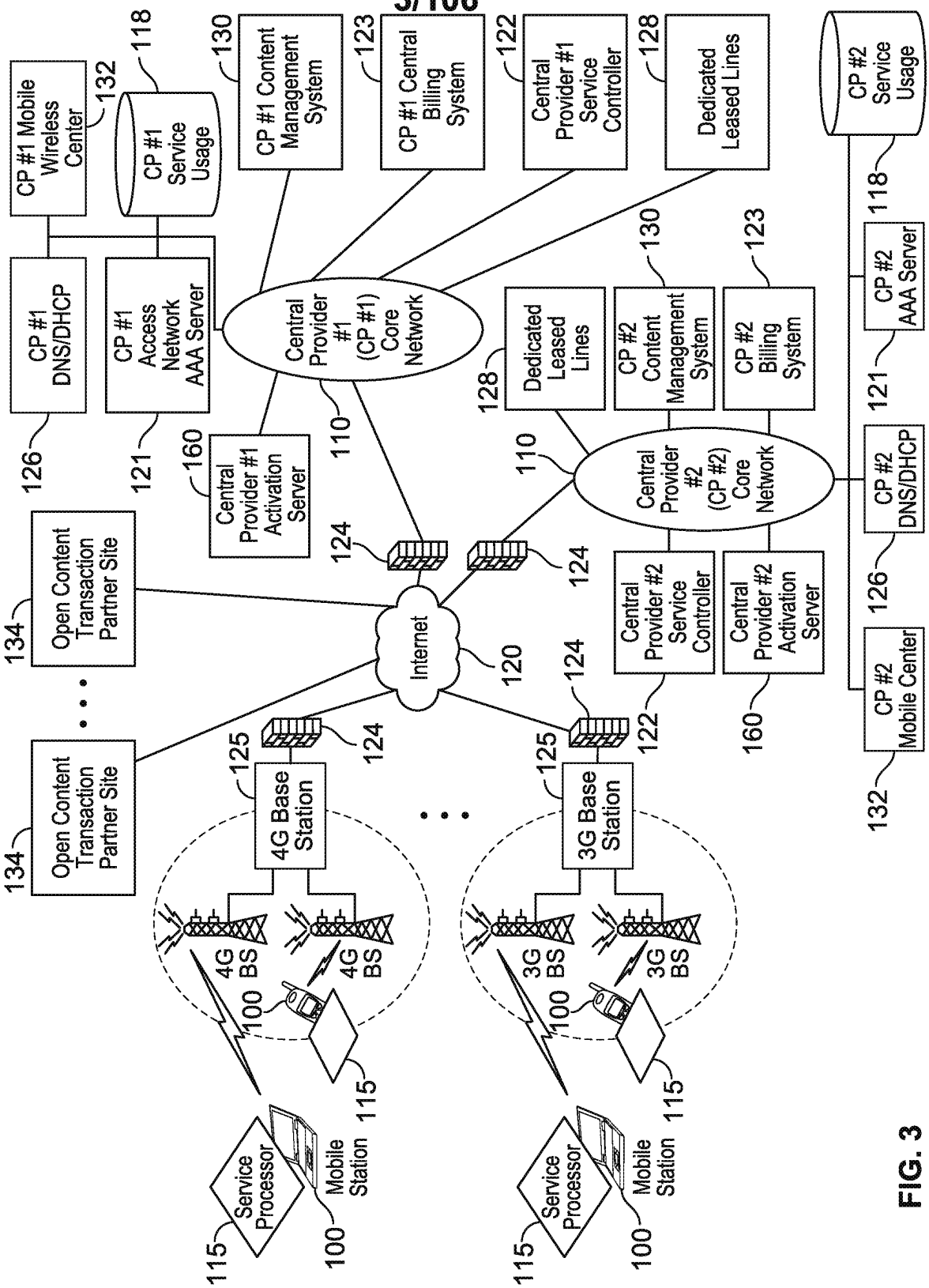

CP #1 Mobile Wireless Center
132
CP #1 Service Usage
118
CP #1 Content Management System
130
CP #1 Central Billing System
123
Central Provider #1 Service Controller
122
Dedicated Leased Lines
128
CP #2 Service Usage
CP #1 DNS/DHCP
126
CP #1 Access Network AAA Server
121
Central Provider #1 Activation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

FIG. 3

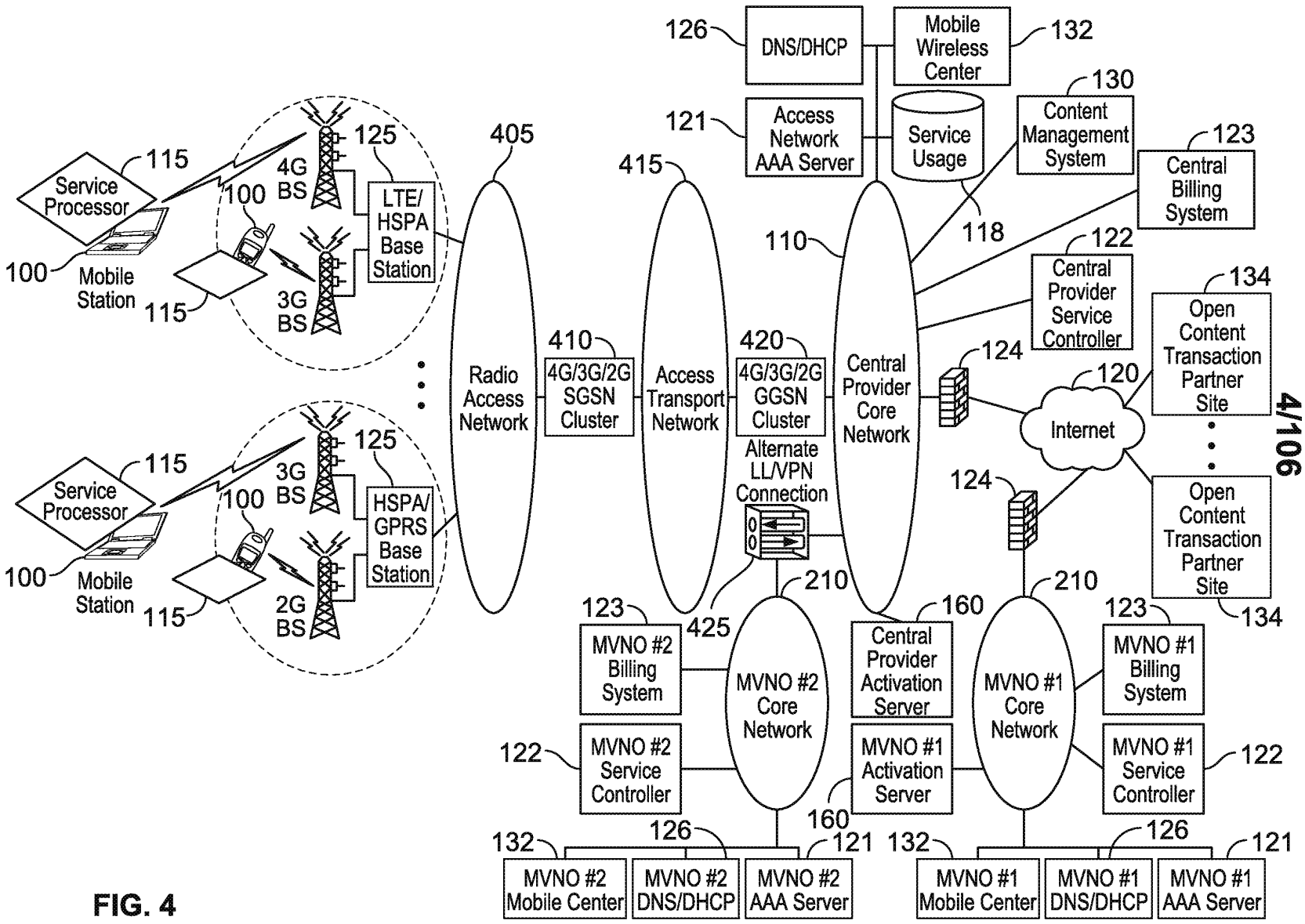


FIG. 4

IPR2025-01571
Apple EX1002 Page 260

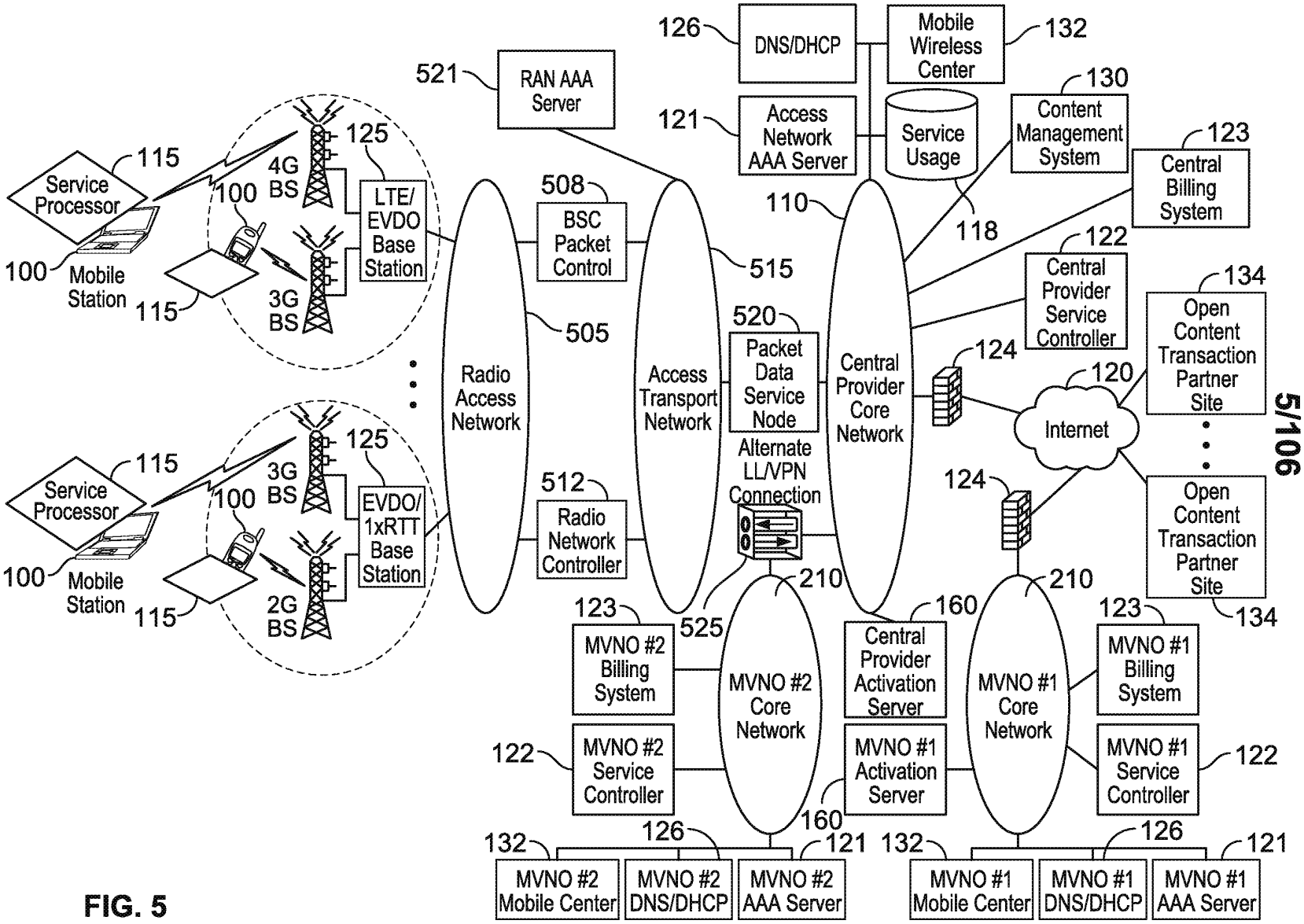


FIG. 5

IPR2025-01571
Apple EX1002 Page 261

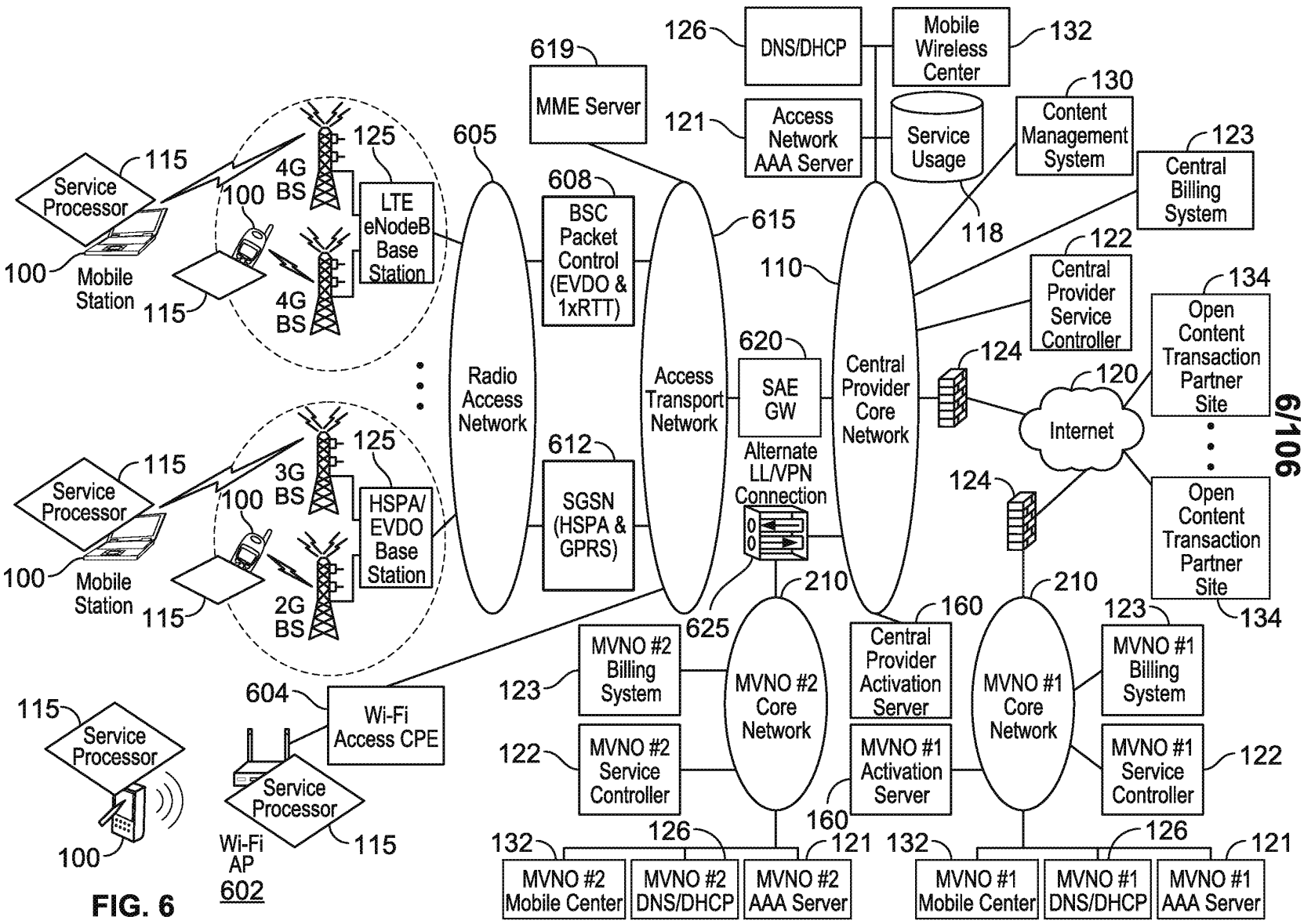


FIG. 6

6/106

IPR2025-01571
Apple EX1002 Page 262

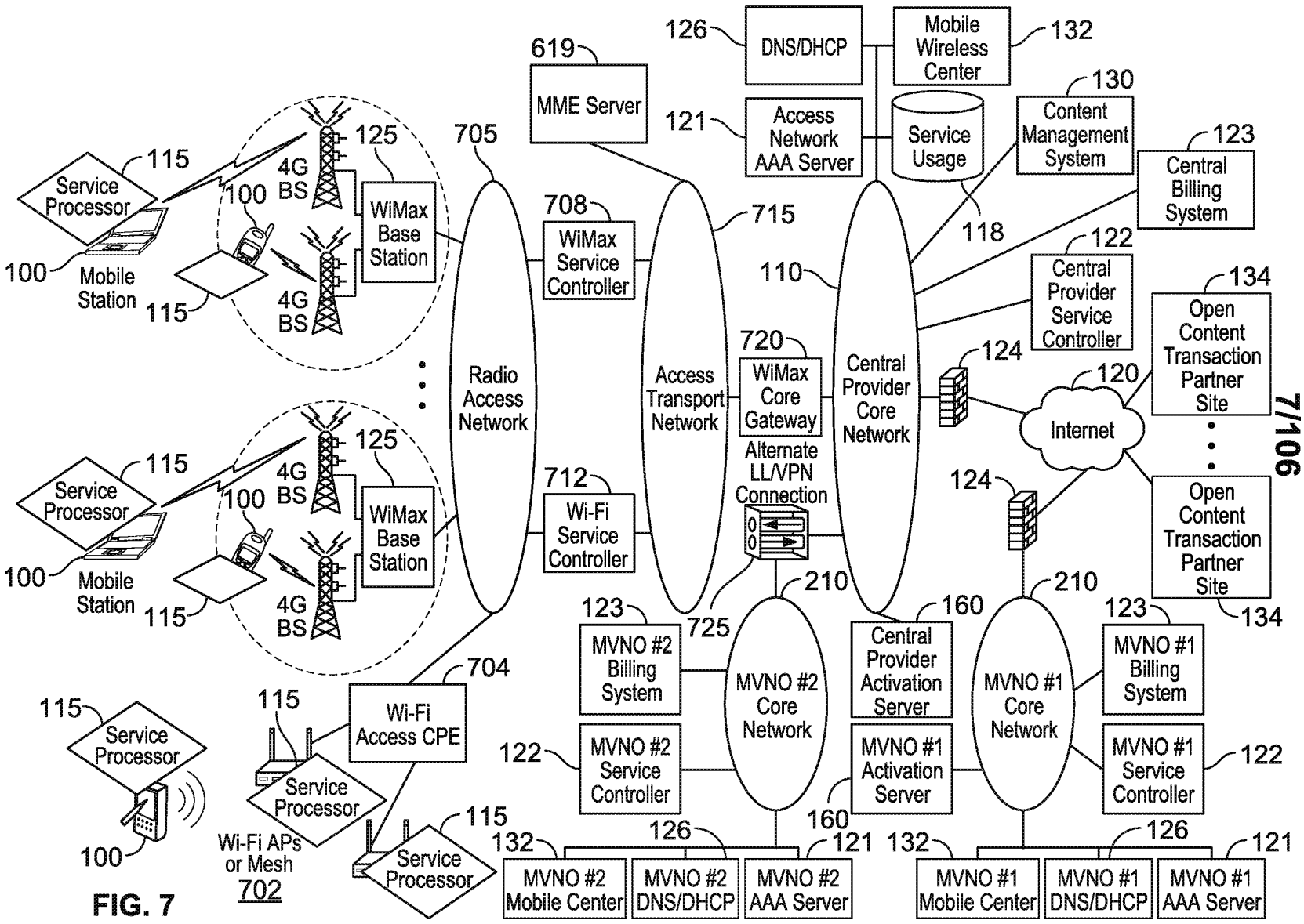


FIG. 7

7/106

IPR2025-01571
Apple EX1002 Page 263

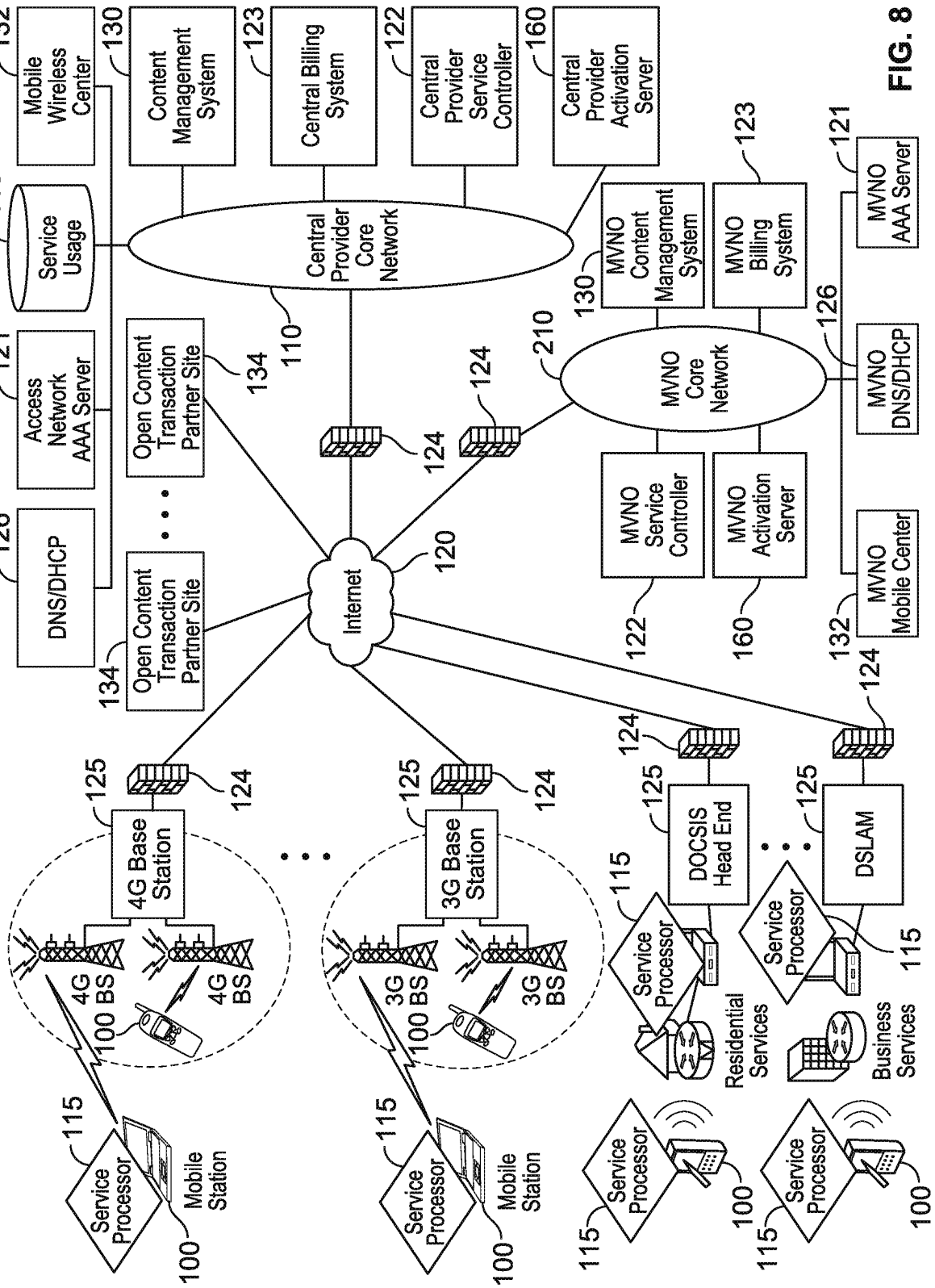

Mobile Wireless Center
132
Content Management System
130
Central Billing System
123
Central Provider Service Controller
122
Central Provider Activation Server
160
Service Usage
118
Central Provider Core Network
110
Access Network AAA Server
121
Open Content Transaction Partner Site
134
DNS/DHCP
126
Internet
120
MVNO Content Management System
MVNO Billing System
MVNO AAA Server
MVNO Core Network
210
MVNO DNS/DHCP
MVNO Service Controller
MVNO Activation Server
MVNO Mobile Center
4G Base Station
3G Base Station
4G BS
3G BS
100 BS
DOCSIS Head End
DSLAM
Service Processor
Mobile Station
Residential Services
Business Services
125
124
115
100

FIG. 8

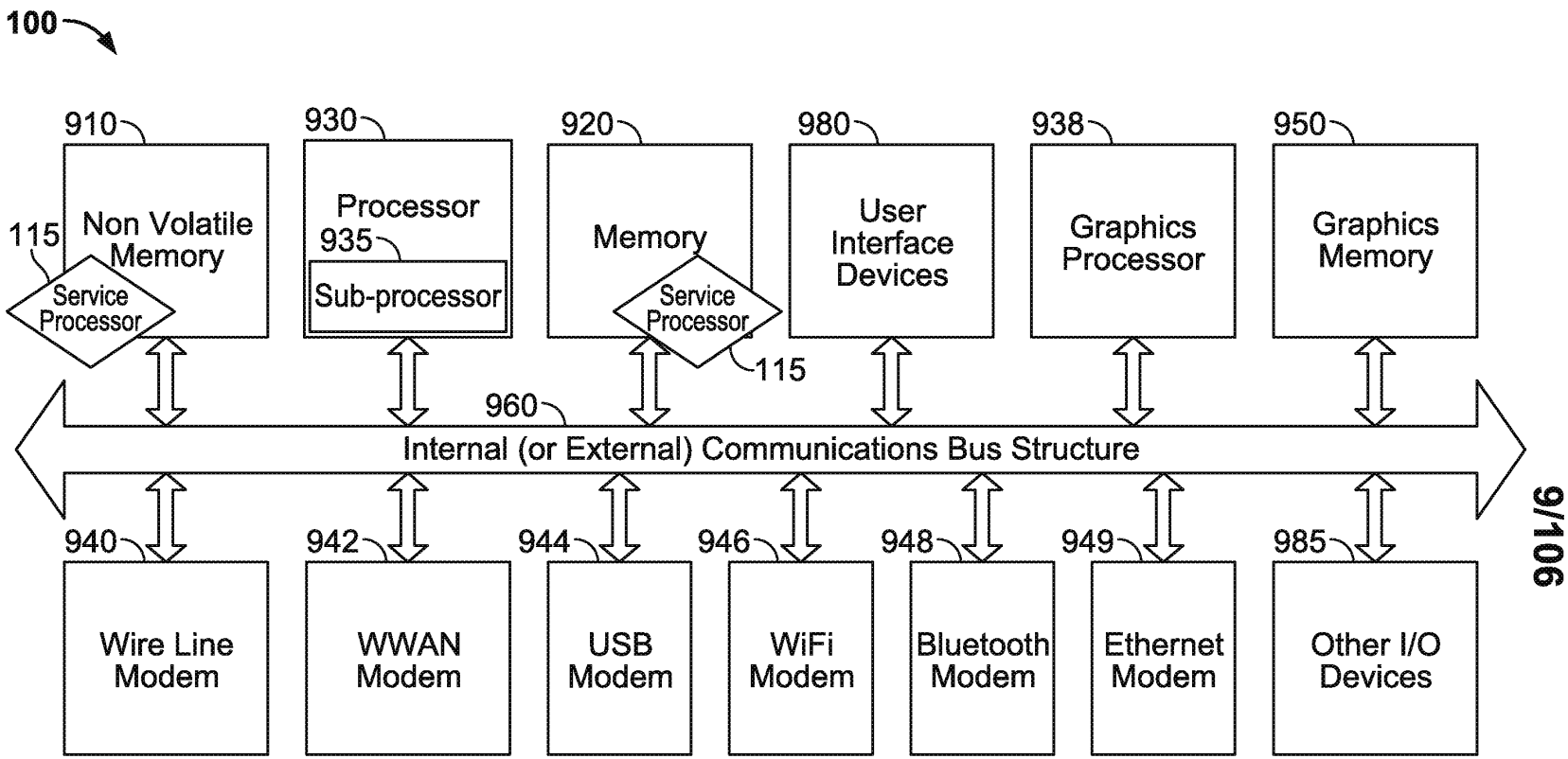


FIG. 9

IPR2025-01571
Apple EX1002 Page 265

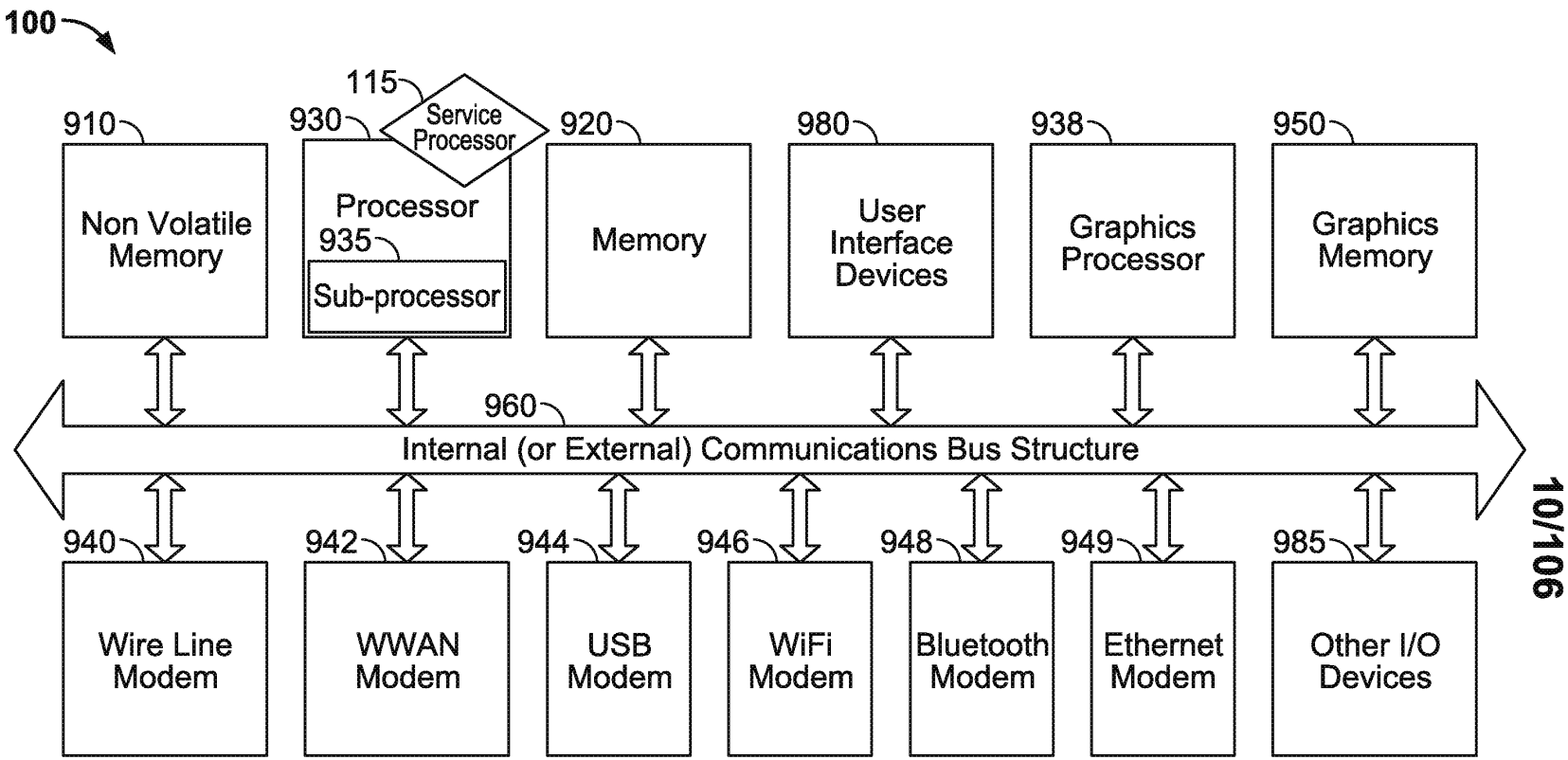


FIG. 10

IPR2025-01571
Apple EX1002 Page 266

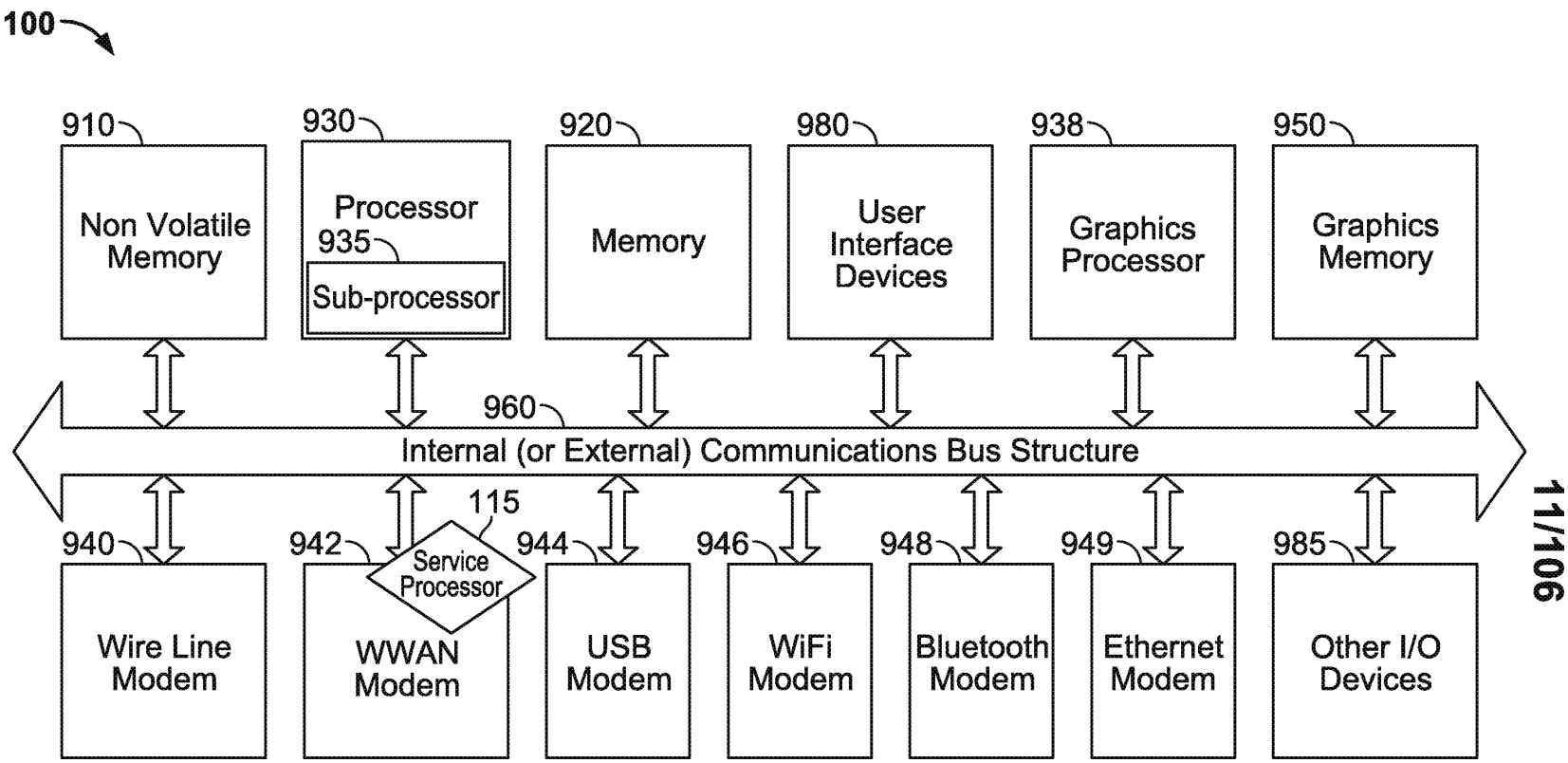


FIG. 11

IPR2025-01571
Apple EX1002 Page 267

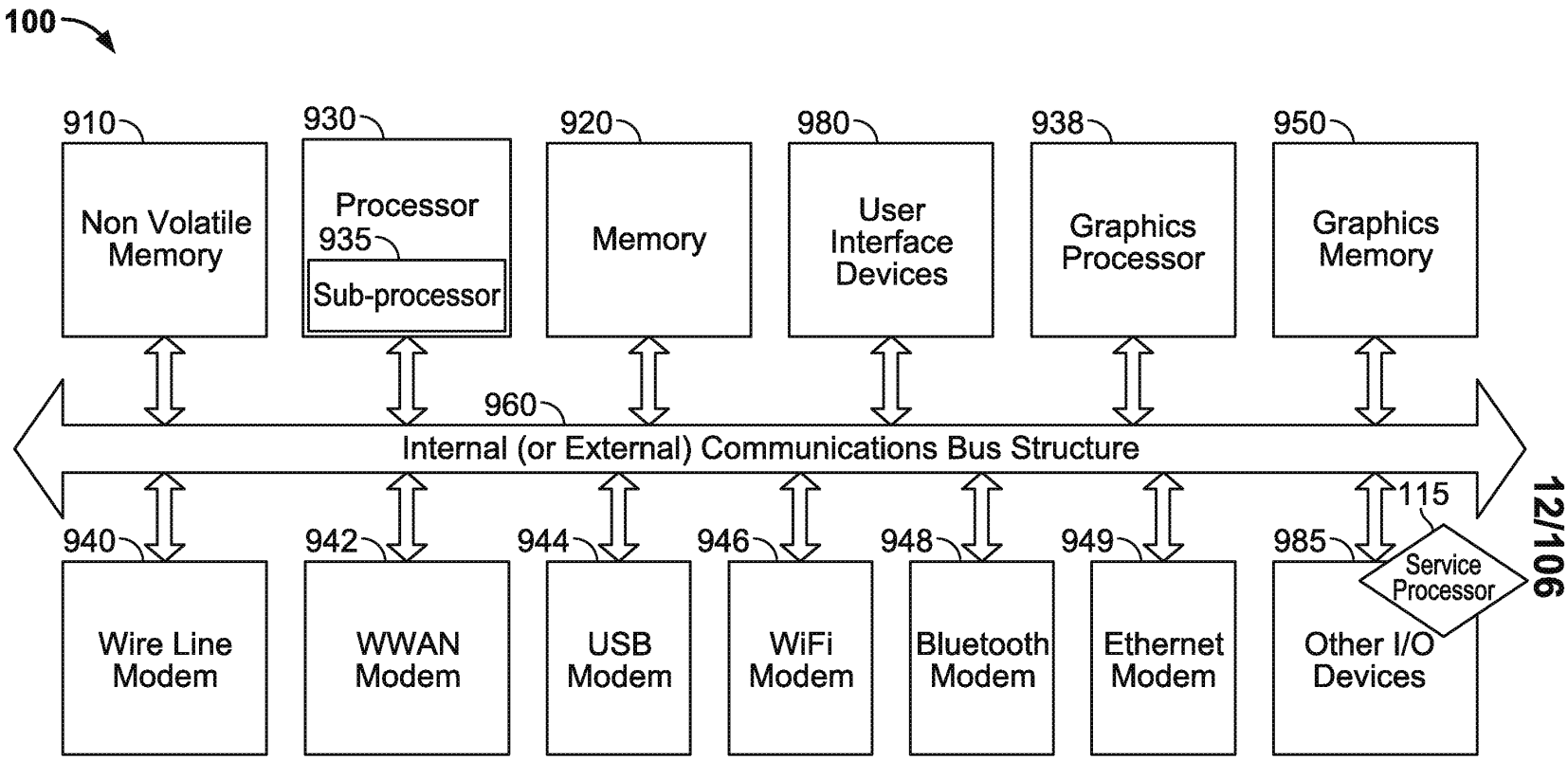


FIG. 12

IPR2025-01571
Apple EX1002 Page 268

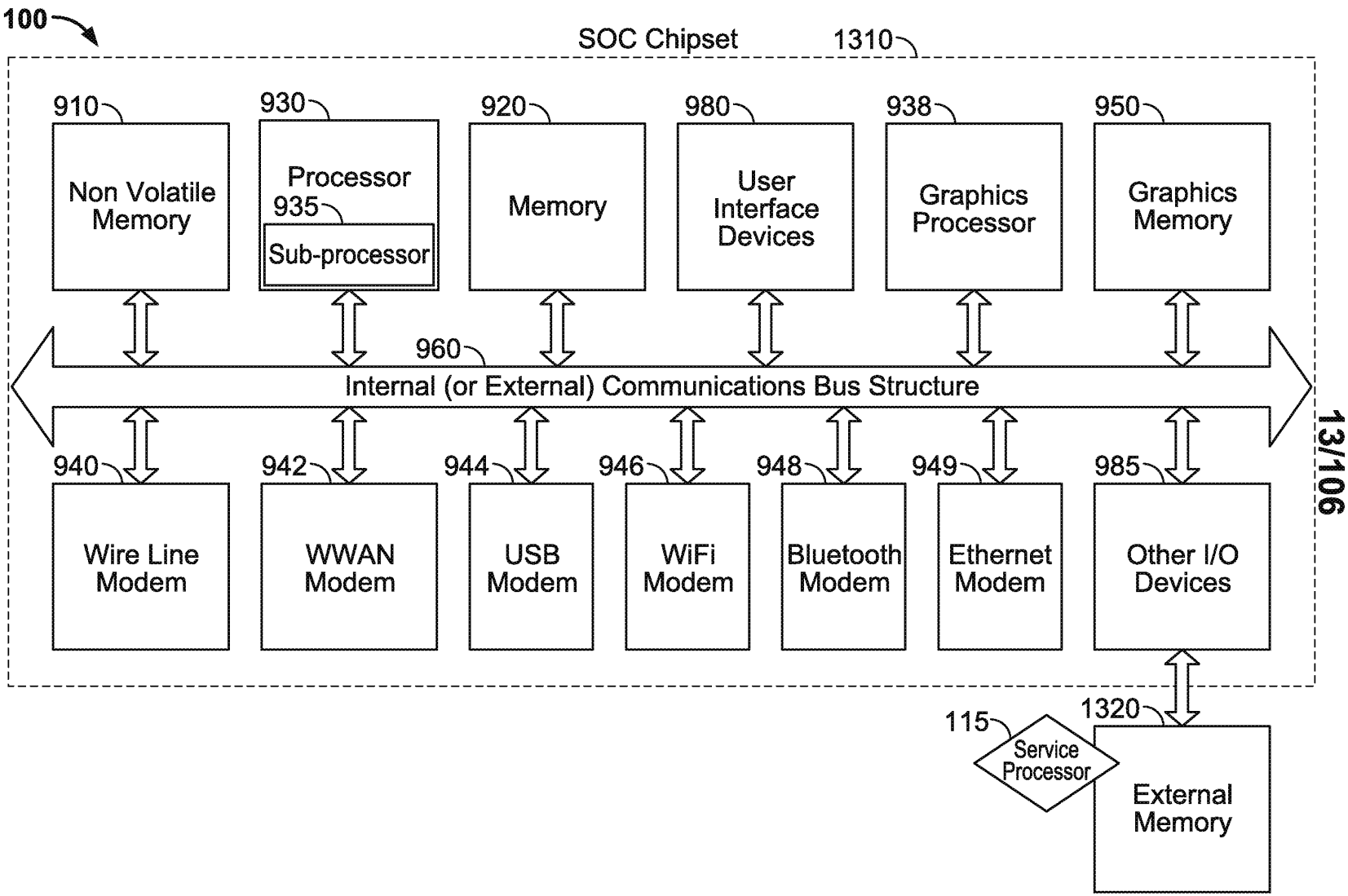


FIG. 13

IPR2025-01571
Apple EX1002 Page 269

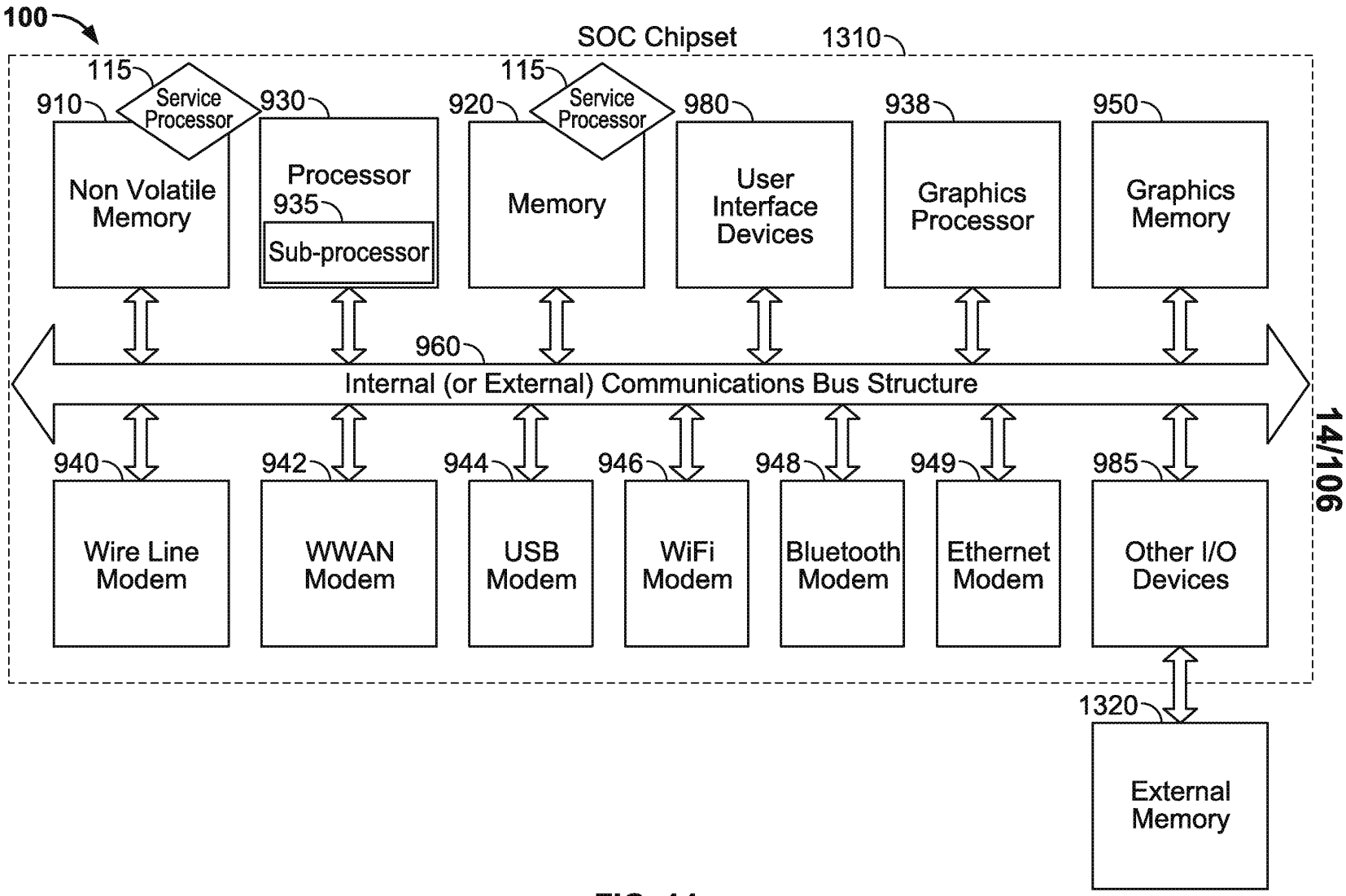


FIG. 14

IPR2025-01571
Apple EX1002 Page 270

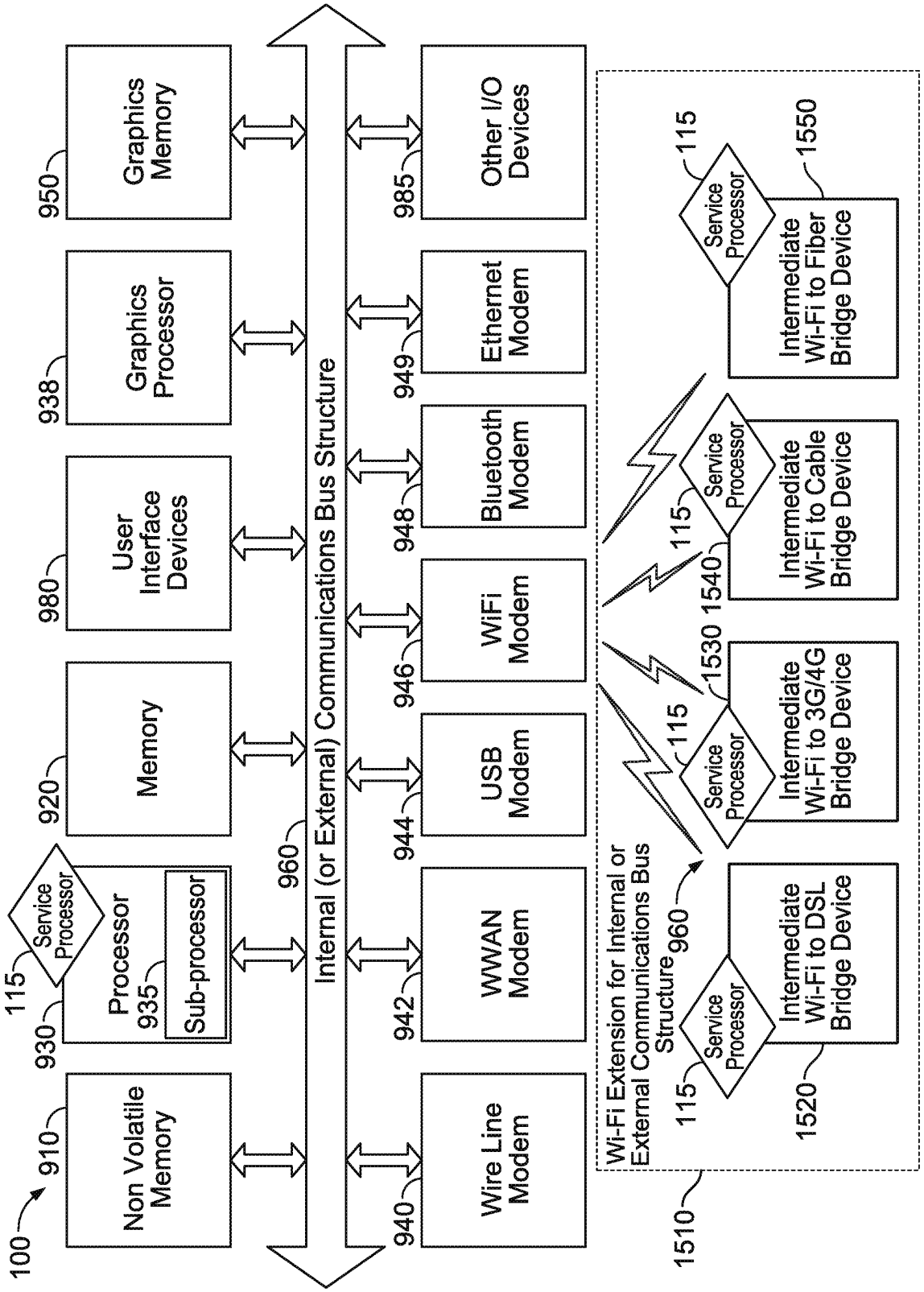

100
910
Non Volatile Memory
930
Processor
935
Sub-processor
115
Service Processor
920
Memory
980
User Interface Devices
938
Graphics Processor
950
Graphics Memory
960
Internal (or External) Communications Bus Structure
940
Wire Line Modem
942
WWAN Modem
944
USB Modem
946
WiFi Modem
948
Bluetooth Modem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

FIG. 15A

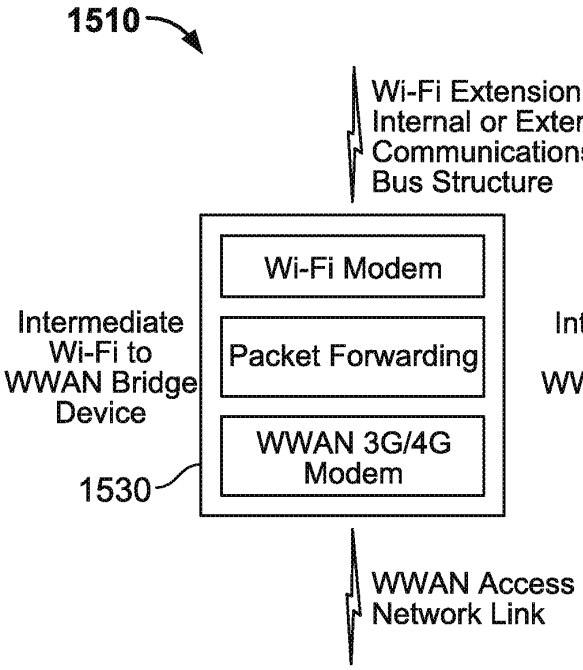


FIG. 15B

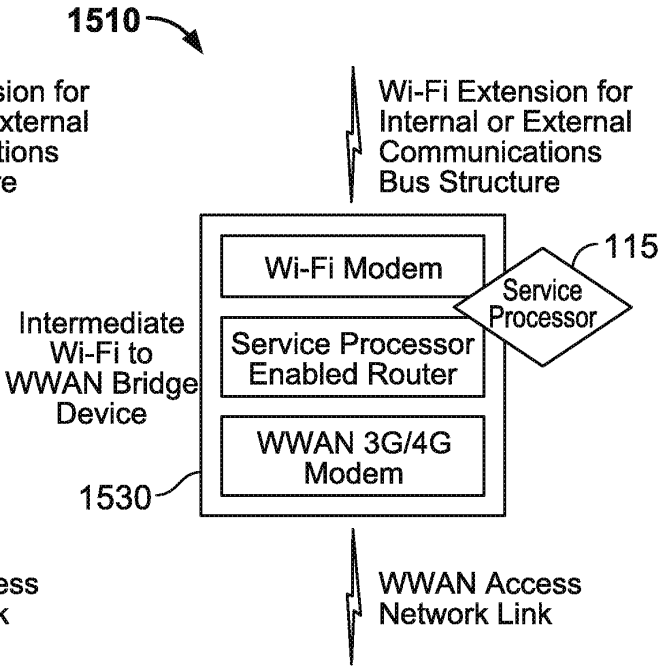


FIG. 15C

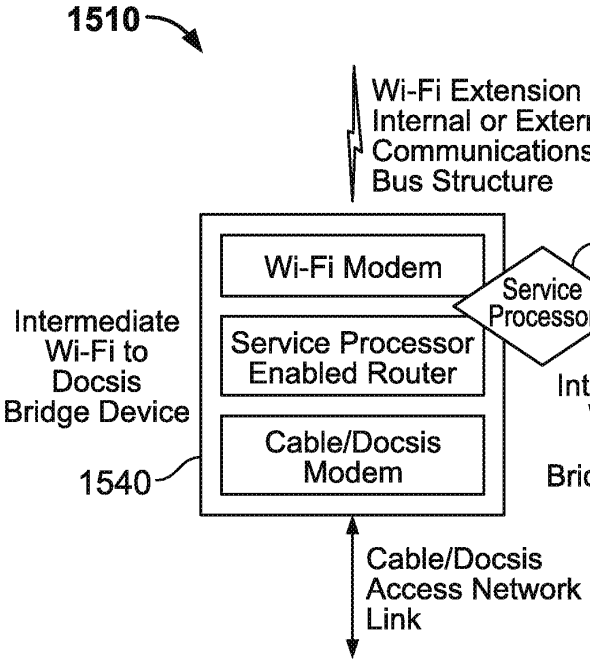


FIG. 15D

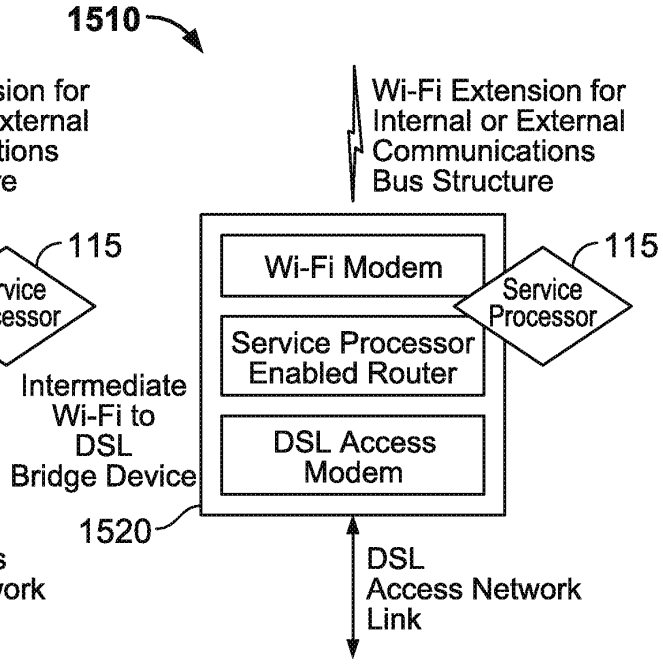


FIG. 15E

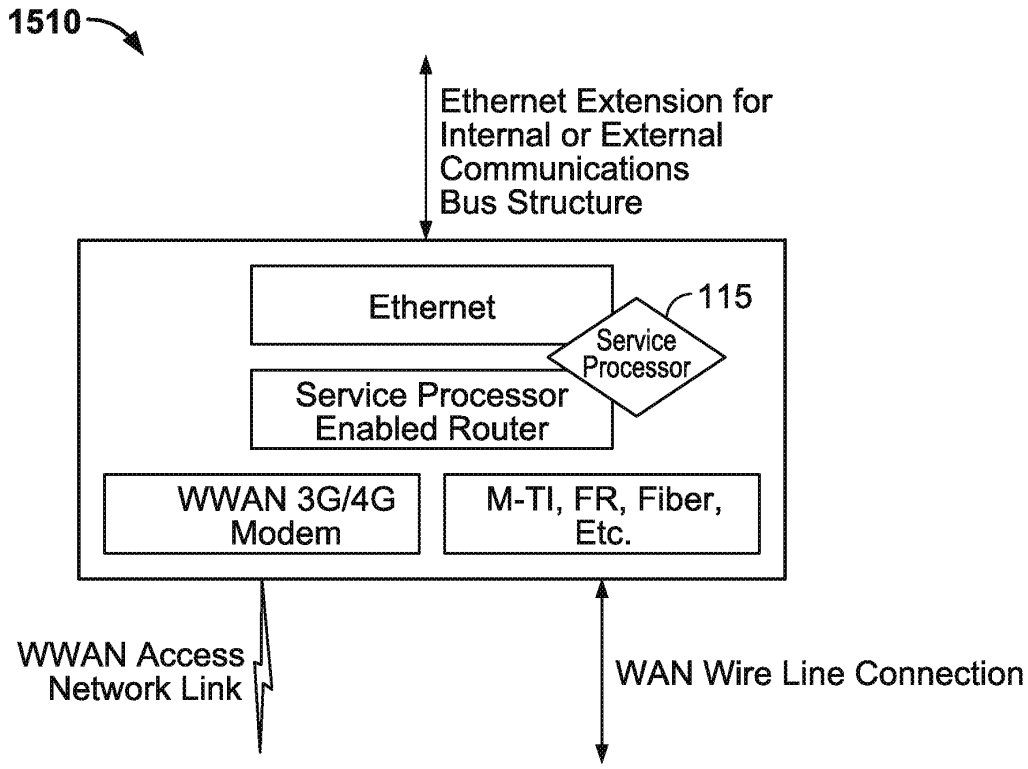

1510
Ethernet Extension for Internal or External Communications Bus Structure
Ethernet
115
Service Processor
Service Processor Enabled Router
WWAN 3G/4G Modem
M-TI, FR, Fiber, Etc.
WWAN Access Network Link
WAN Wire Line Connection

FIG. 15F

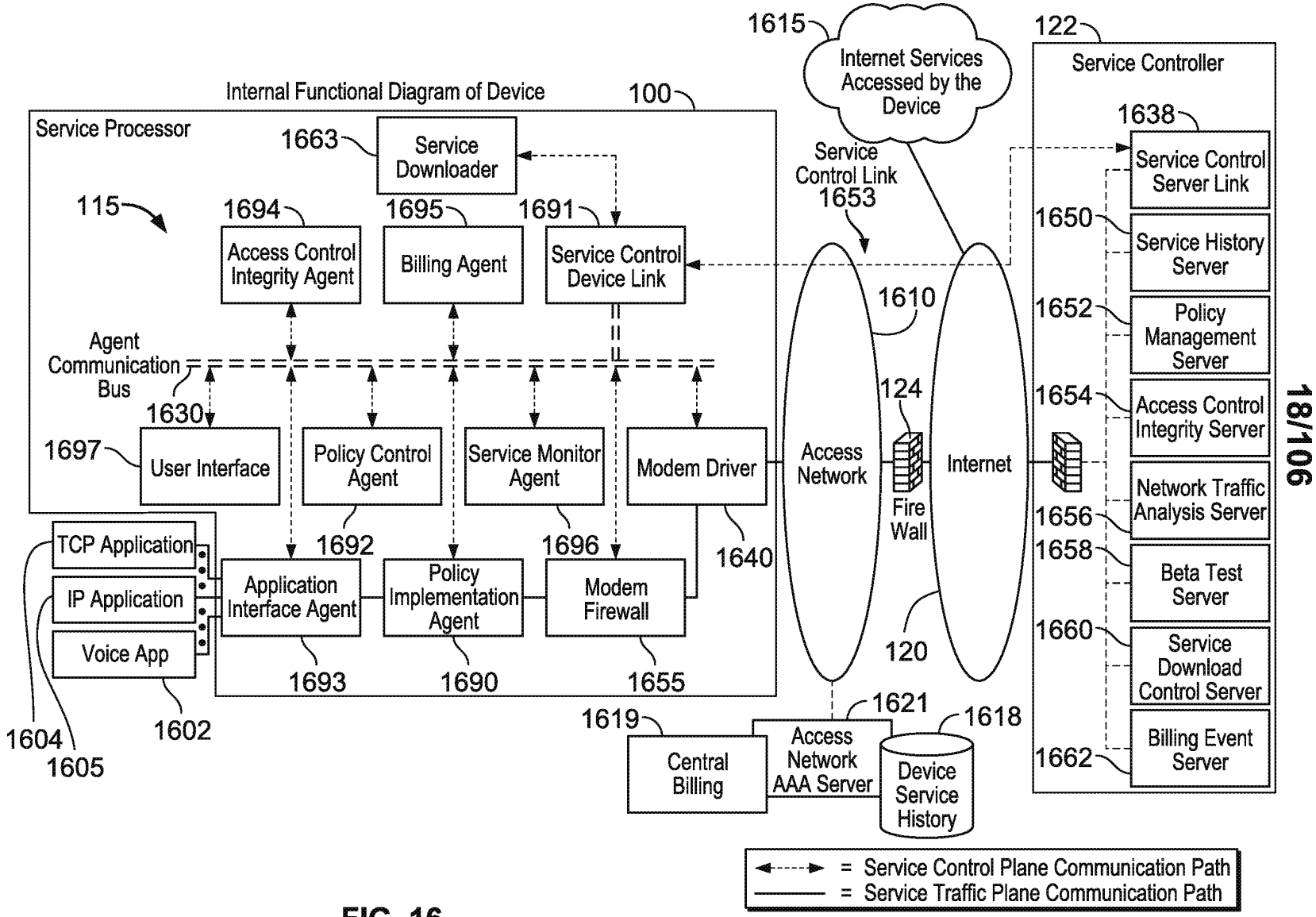


FIG. 16

IPR2025-01571
Apple EX1002 Page 274

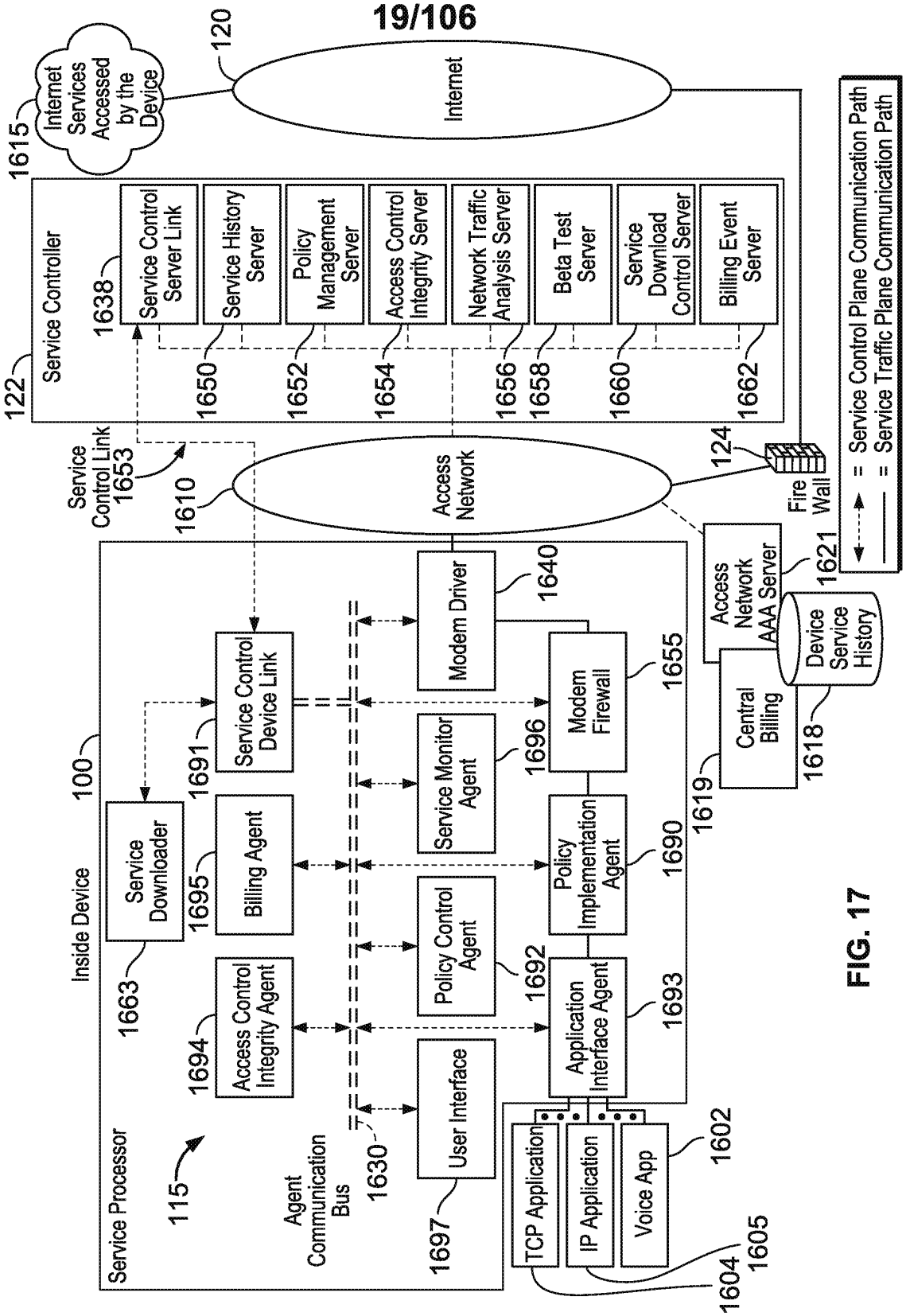

Internet Services Accessed by the Device
1615
120
Internet
Service Controller
122
1638
Service Control Server Link
Service History Server
Policy Management Server
Access Control Integrity Server
Network Traffic Analysis Server
Beta Test Server
Service Download Control Server
Billing Event Server
1650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

FIG. 17

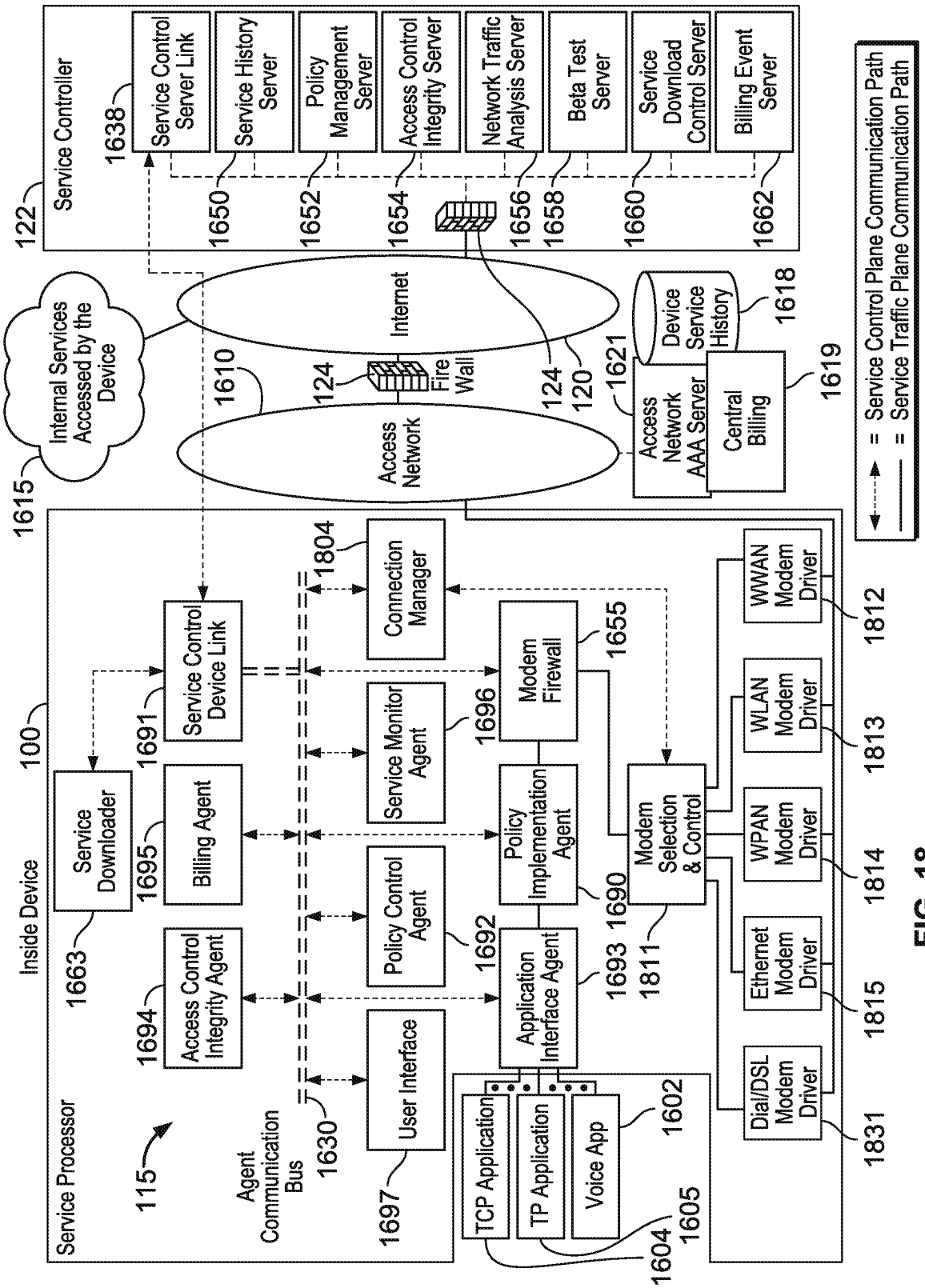

Service Controller
122
1638
Service Control Server Link
Service History Server
Policy Management Server
Access Control Integrity Server
Network Traffic Analysis Server
Beta Test Server
Service Download Control Server
Billing Event Server
1650
1652
1654
1656
1658
1660
1662
Internal Services Accessed by the Device
1615
Internet
Fire Wall
124
120
1610
Access Network
Access Network AAA Server
1621
Device Service History
1618
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
Access Control Integrity Agent
1694
User Interface
1697
Service Control Device Link
1691
Service Monitor Agent
1696
Policy Control Agent
1692
Policy Implementation Agent
1690
Application Interface Agent
1693
Connection Manager
1804
Modem Firewall
1655
Modem Selection & Control
1811
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

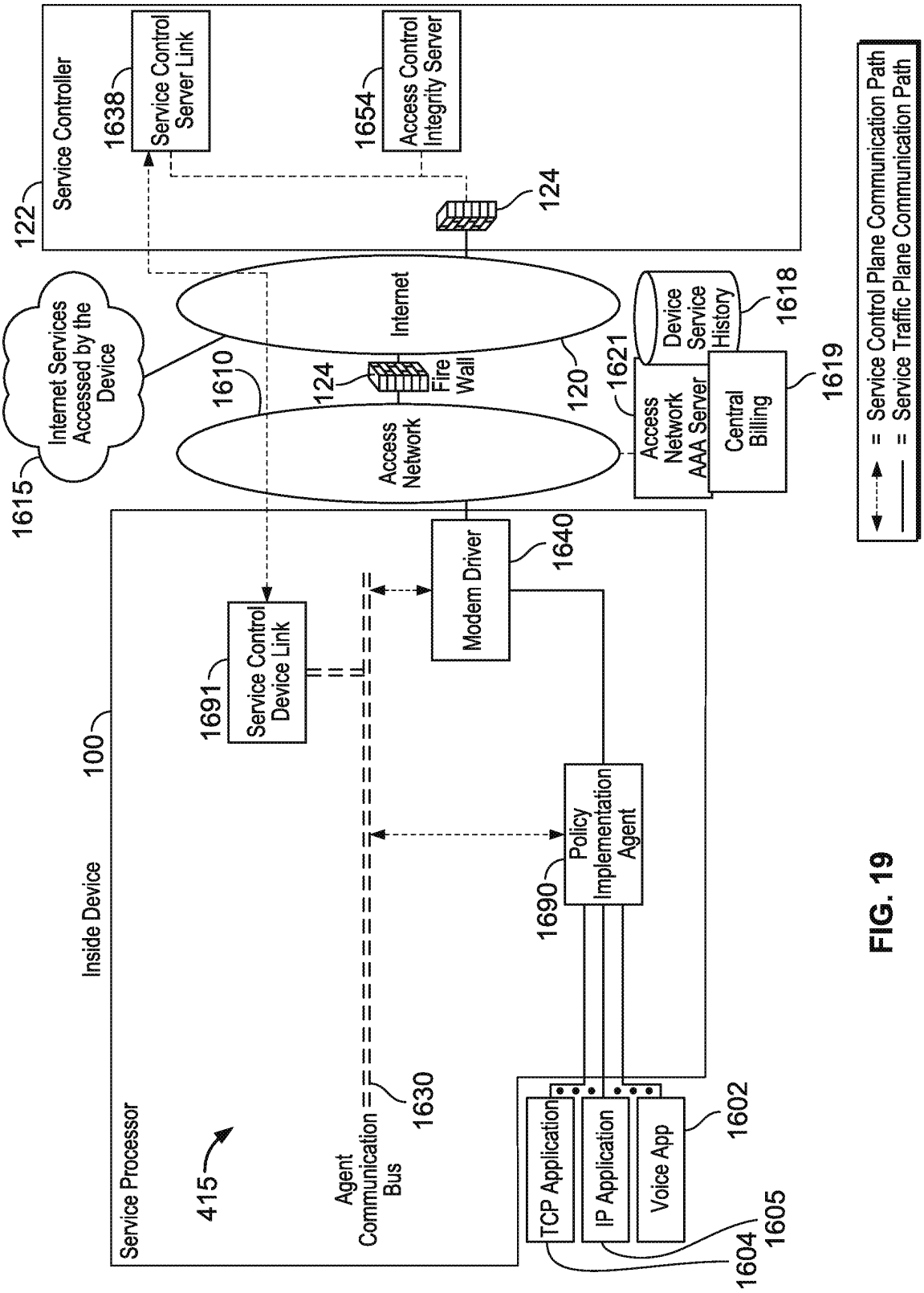

Service Controller
122
Service Control Server Link
1638
Access Control Integrity Server
1654
124
Internet Services Accessed by the Device
1615
Internet
1610
124
Fire Wall
120
Access Network
1621
Device Service History
1618
Access Network AAA Server
Central Billing
1619
= Service Control Plane Communication Path
= Service Traffic Plane Communication Path
Inside Device
100
Service Processor
415
Service Control Device Link
1691
Modem Driver
1640
Policy Implementation Agent
1690
Agent Communication Bus
1630
TCP Application
IP Application
Voice App
1602
1604
1605

FIG. 19

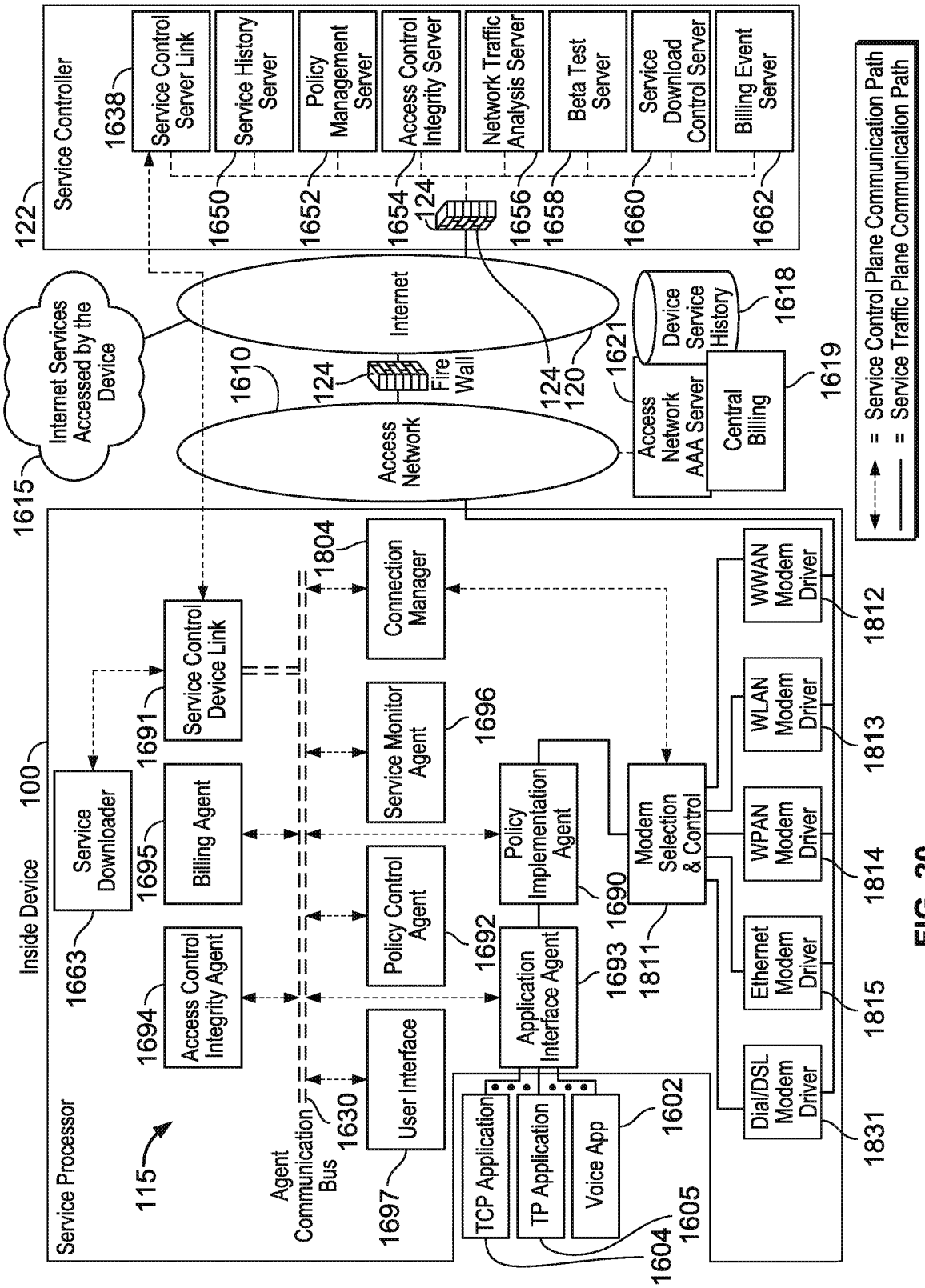

Service Controller
122
Service Control Server Link
Service History Server
Policy Management Server
Access Control Integrity Server
Network Traffic Analysis Server
Beta Test Server
Service Download Control Server
Billing Event Server
1638
1650
1652
1654
1656
1658
1660
1662
124
Internet
Fire Wall
Access Network
1610
1615
Internet Services Accessed by the Device
120
1621
Device Service History
1618
Access Network AAA Server
Central Billing
1619
= Service Control Plane Communication Path
= Service Traffic Plane Communication Path
Inside Device
100
Service Processor
115
Service Downloader
1663
Billing Agent
1695
Service Control Device Link
1691
Service Monitor Agent
1696
Connection Manager
1804
Access Control Integrity Agent
1694
Policy Control Agent
1692
Policy Implementation Agent
1690
Modem Selection & Control
1811
Application Interface Agent
1693
User Interface
1697
1630
Agent Communication Bus
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. 20

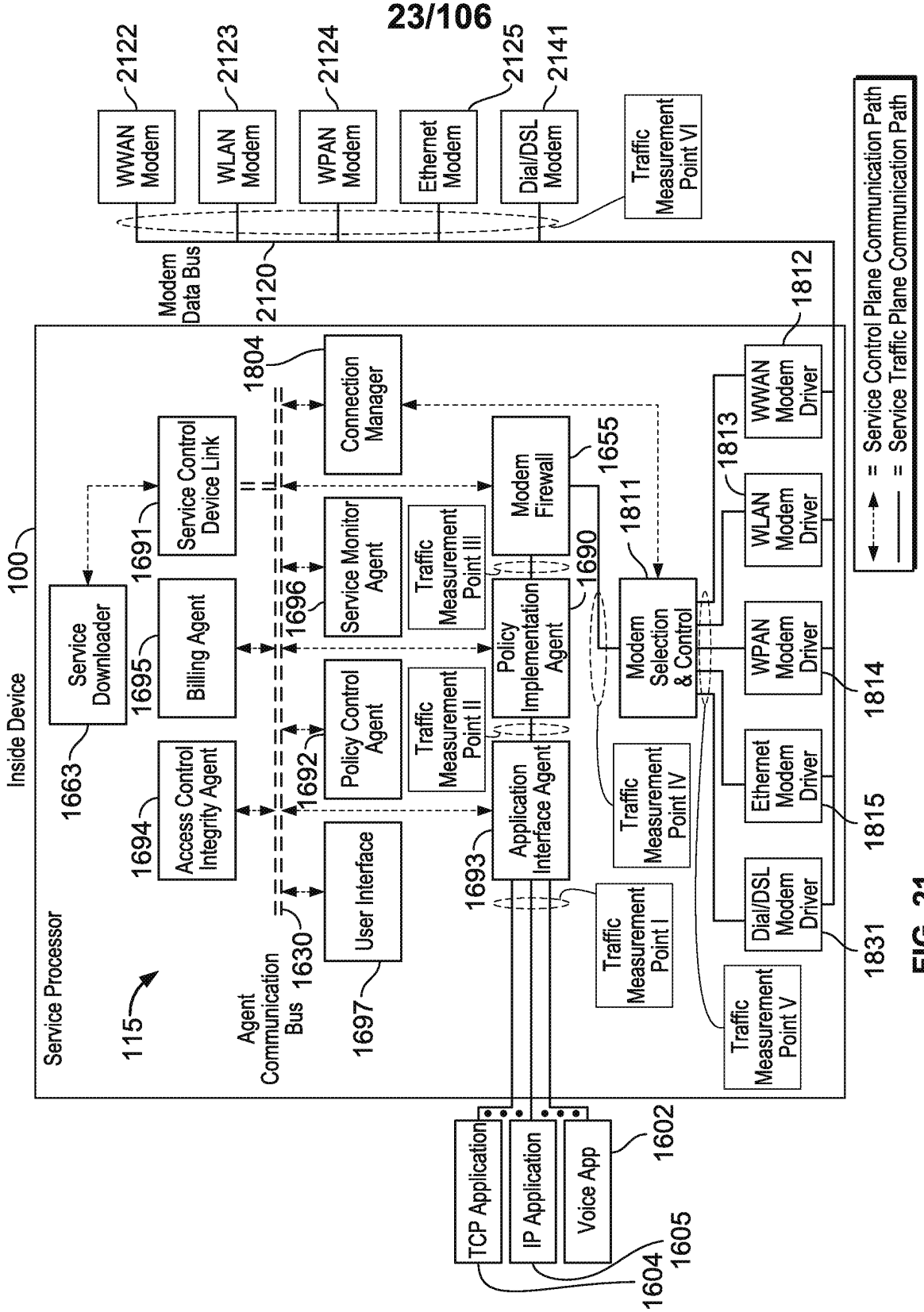

Inside Device
100
Service Processor
115
Agent Communication Bus
1630
Modem Data Bus
2120
WWAN Modem
2122
WLAN Modem
2123
WPAN Modem
2124
Ethernet Modem
2125
Dial/DSL Modem
2141
Traffic Measurement Point VI
Service Downloader
1663
Billing Agent
1695
Access Control Integrity Agent
1694
User Interface
1697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

FIG. 21

Service Processor 115 Embodiment	Partial Summary of Embodiment Functions
Service Control Device Link 1691	Device side control plane link for connecting Service Processor 415 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 490.
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 497 to provide the user with service plan options, accept service plan selections, provide notification on service usage levels, provide options on service usage control policy, accept choices on service usage policy, provide transaction options or accept transaction choices. In some embodiments, interacts with Transaction Servers 134 to conduct ecommerce transactions with central billing.

FIG. 22A

User Interface Agent 1697	Provide service interface to users.
Service Downloader 1663	Provides a download function to install or update service software elements on the device.
Connection Manager 1804	Provides a control and supervision function for one or more modem drivers or modems that connect to an access network.
Modem Selection and Control 1811	Selects the access network connection.
Modem Drivers 1831, 1815, 1814, 1813, 1812	Converts data traffic into modem bus traffic for one or more modems.
Modems 2141, 2125, 2124, 2123, 2122	Connects the device to one or more networks.

FIG. 22B

Service Controller 122 Element	Partial Summary of Embodiment Functions
Service Control Server Link 1638	Network side control plane link for connecting Service Controller 422 Service Processor 415 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 415.
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 421 and the Service Monitor Agent 496. 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 415, provides service usage updates to the Service Processor 415, 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

IPR2025-01571
Apple EX1002 Page 282

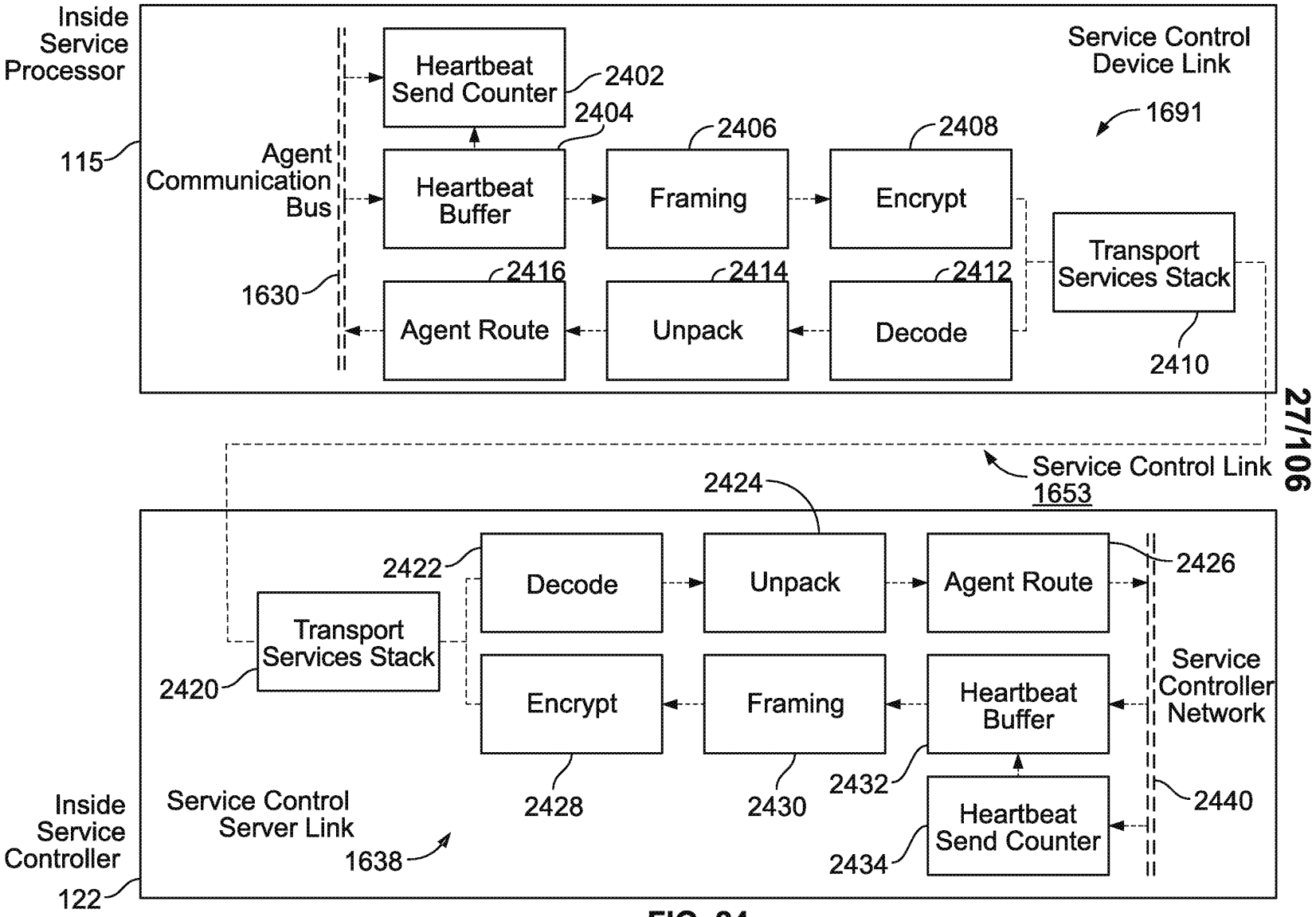


FIG. 24

IPR2025-01571
Apple EX1002 Page 283

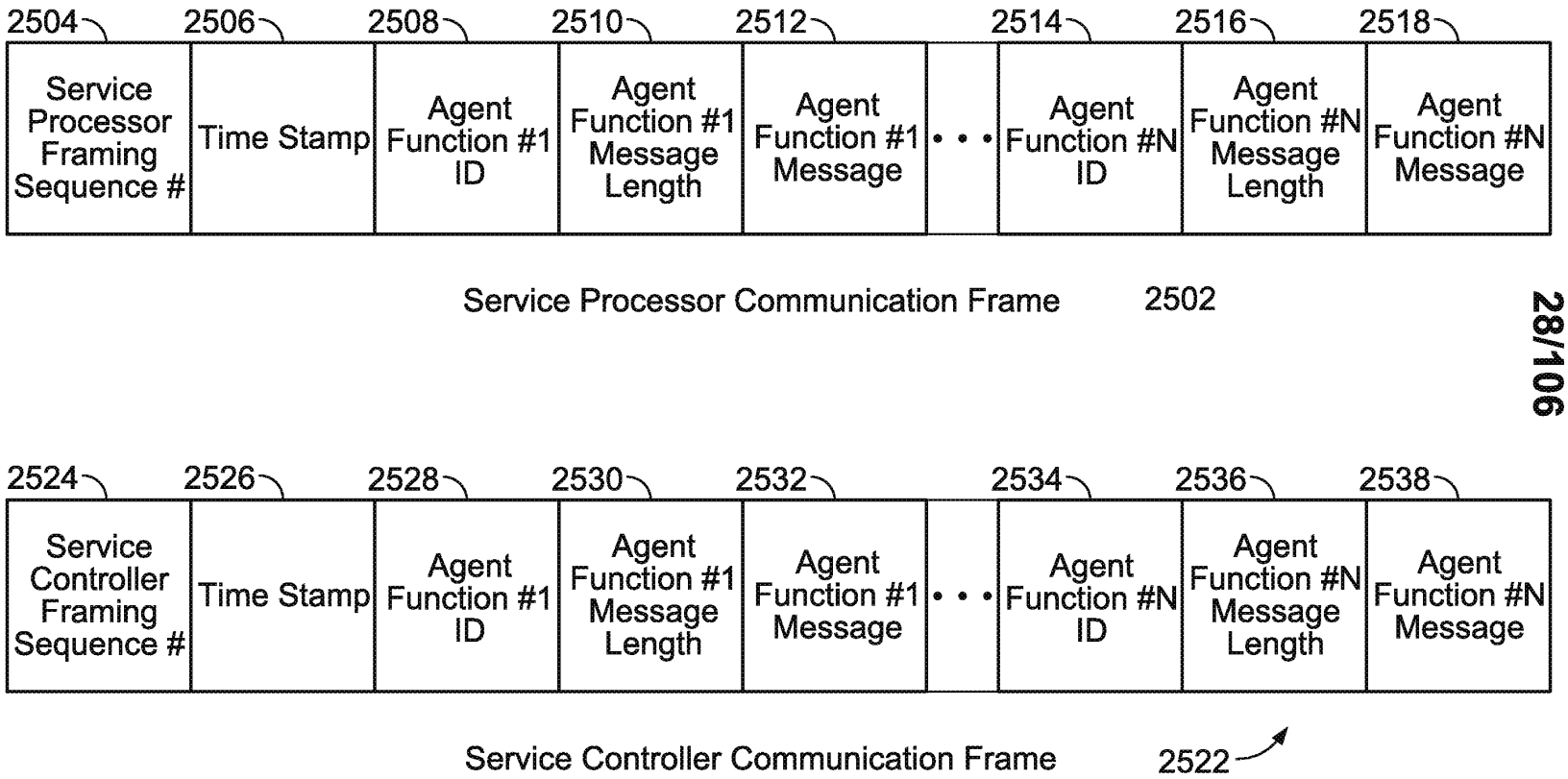


FIG. 25

IPR2025-01571
Apple EX1002 Page 284

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

IPR2025-01571
Apple EX1002 Page 285

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

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

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

	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

IPR2025-01571
Apple EX1002 Page 291

		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

IPR2025-01571
Apple EX1002 Page 292

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

FIG. 27A

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

FIG. 27B

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

FIG. 27C

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

FIG. 27D

IPR2025-01571
Apple EX1002 Page 296

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

FIG. 27E

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

FIG. 27F

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

FIG. 27G

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

FIG. 27H

		the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.
Verify activation tracking system presence, configuration or operation	Activation tracking service is not present, is not providing scheduled network activity reporting, or is exhibiting erroneous reports.	In some embodiments the response is to place the device ID. on a list of devices suspected of having activation tracking functions that have been tampered with for the purpose of central provider billing reconciliation. In some embodiments, install a new copy of the activation tracking service agent software either from a locally stored device copy or a network download. In some embodiments where authorization exists to manage device software and some aspects of service tracking, run further checks on device service integrity such as agent query-response. In some embodiments where authorization exists to manage a device access service connection, send error message to device UI, suspend device or place device on quarantine route. In some embodiments send error message to human interface for troubleshooting.
Verify device standing or service plan standing	No service plan on record or device not authorized	In some embodiments, if device is not yet activated with a service plan, provide UI with activation sequence. In some embodiments, if device is not authorized for service on one of the networks controlled by the Service

FIG. 27I

IPR2025-01571
Apple EX1002 Page 301

		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

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

		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

IPR2025-01571
Apple EX1002 Page 305

		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

		quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.
Verify user standing	User does not respond with proper response to UI query such as request for ID., password or biometric input. This process may be part of handling a suspected error.	In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis. In some embodiments, the user may be asked to acknowledge a service overage notification and/or to also provide a password, biometric signature, hardware key or other mechanism to verify the service overage acknowledgment.
Agent communications log	Unauthorized communications with one or more agents is detected	In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control.

FIG. 27O

		In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.

FIG. 27P

Service Policy Implementation Tamper or Error Protection Techniques	Example Error Trigger Criteria	Example Error Responses
Detect or block device networking activity that is potentially harmful for the operation of Service Processor.	Network activity is observed in service monitor reports that fit known patterns that indicated harmful software may be present on device.	Initiate or install and initiate eradication software. Block traffic from the suspect entity. In some embodiments if software can not be eradicated or blocked, then send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.
Detect or block unauthorized Service Processor software from being loaded.	Access Control Integrity Agent discovers software that is on a known malicious list.	Same as above.
Detect or block unauthorized access of protected Service Processor software or hardware memory.	Unauthorized access is detected, memory contents are corrupted or unresponsive.	Identify the entity that has gained access to the Service Processor if possible and eradicate. In some embodiments repair any compromised agents with dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code . In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.
Detect or block unauthorized communication with Service Processor software or hardware.	Unauthorized communication is detected.	Identify the entity that has gained access to the Service Processor if possible and eradicate. In some embodiments repair any compromised agents with dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code . In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.

FIG. 28A

IPR2025-01571
Apple EX1002 Page 309

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

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

IPR2025-01571
Apple EX1002 Page 311

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

FIG. 28D

Agent communication log	Unauthorized communication is discovered with one or more agents	Same as above.
Encrypted agent code for downloads	Agent download is found to have incorrect or absent encryption or signature	Same as above.
Secure downloader memory	Unauthorized access to or storage in secure downloader memory is discovered	Same as above.

FIG. 28E

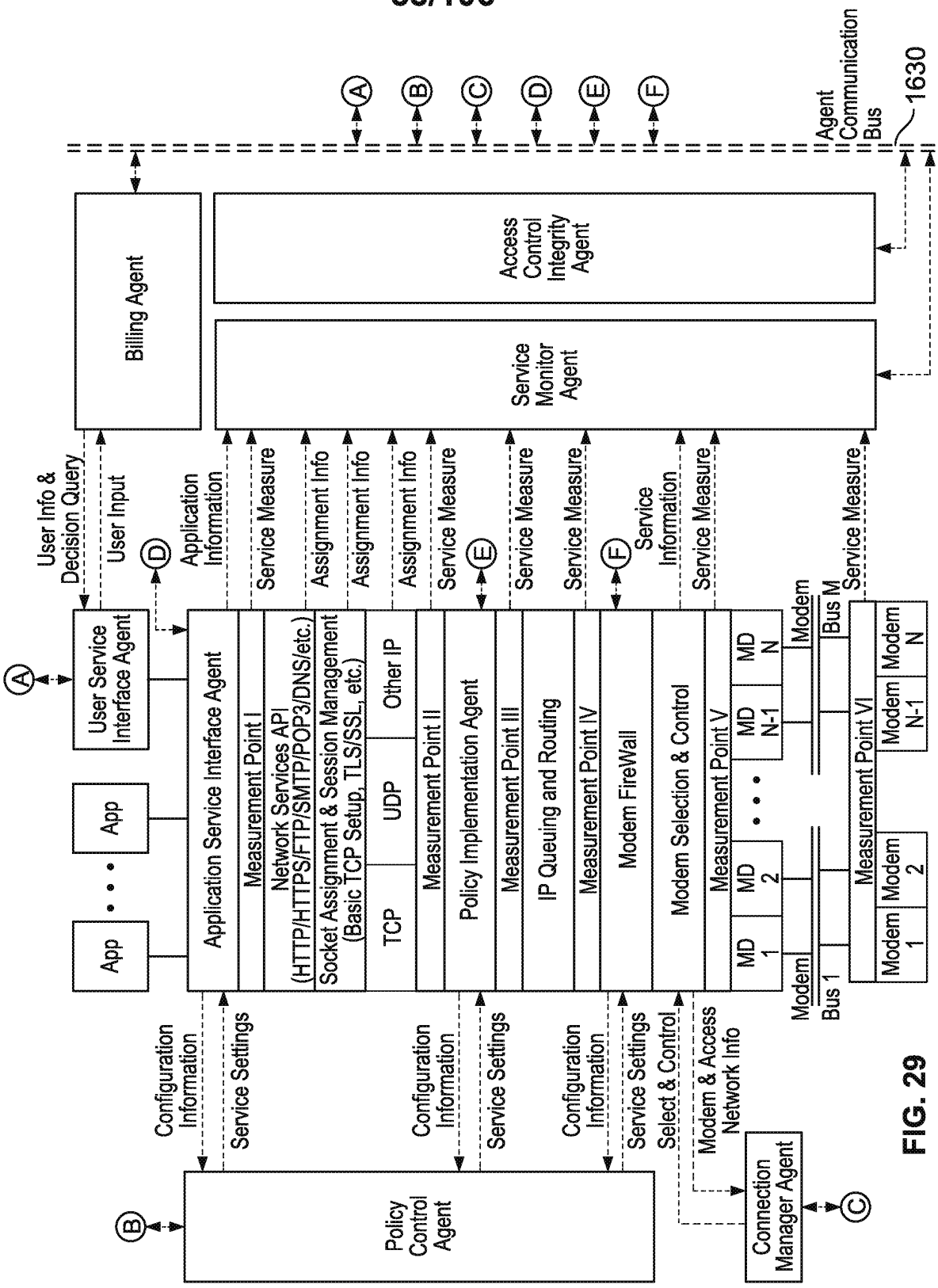

Billing Agent
Access Control Integrity Agent
Service Monitor Agent
Agent Communication Bus
1630
A
B
C
D
E
F
User Info & Decision Query
User Input
Application Information
Service Measure
Assignment Info
Service Information
User Service Interface Agent
App
App
Application Service Interface Agent
Measurement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

FIG. 29

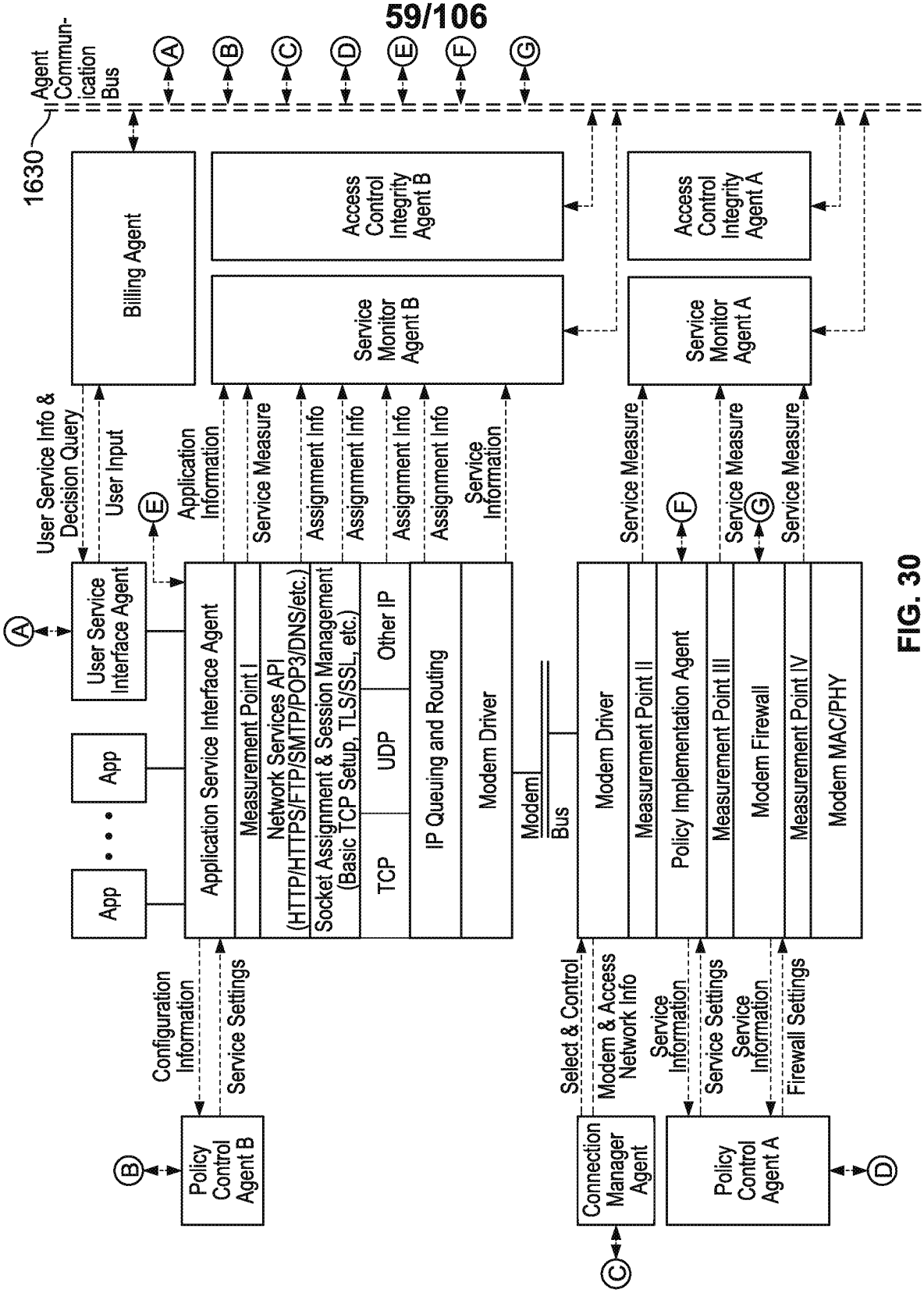

1630
Agent Communication Bus
A
B
C
D
E
F
G
Billing Agent
Access Control Integrity Agent B
Service Monitor Agent B
Access Control Integrity Agent A
Service Monitor Agent A
User Service Info & Decision Query
User Input
Application Information
Service Measure
Assignment Info
Service Information
User Service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

FIG. 30

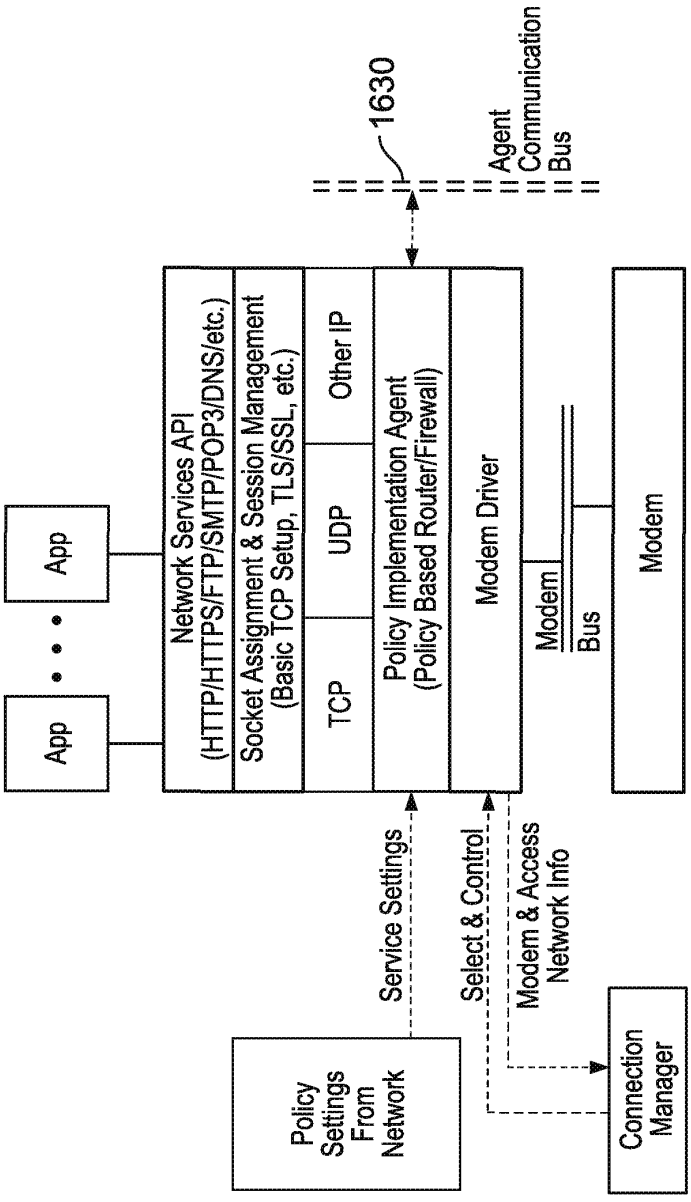

App
App
Network Services API
(HTTP/HTTPS/FTP/SMTP/POP3/DNS/etc.)
Socket Assignment & Session Management
(Basic TCP Setup, TLS/SSL, etc.)
TCP
UDP
Other IP
Policy Implementation Agent
(Policy Based Router/Firewall)
Modem Driver
Modem
Bus
Modem
1630
Agent
Communication
Bus
Service Settings
Select & Control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

FIG. 31

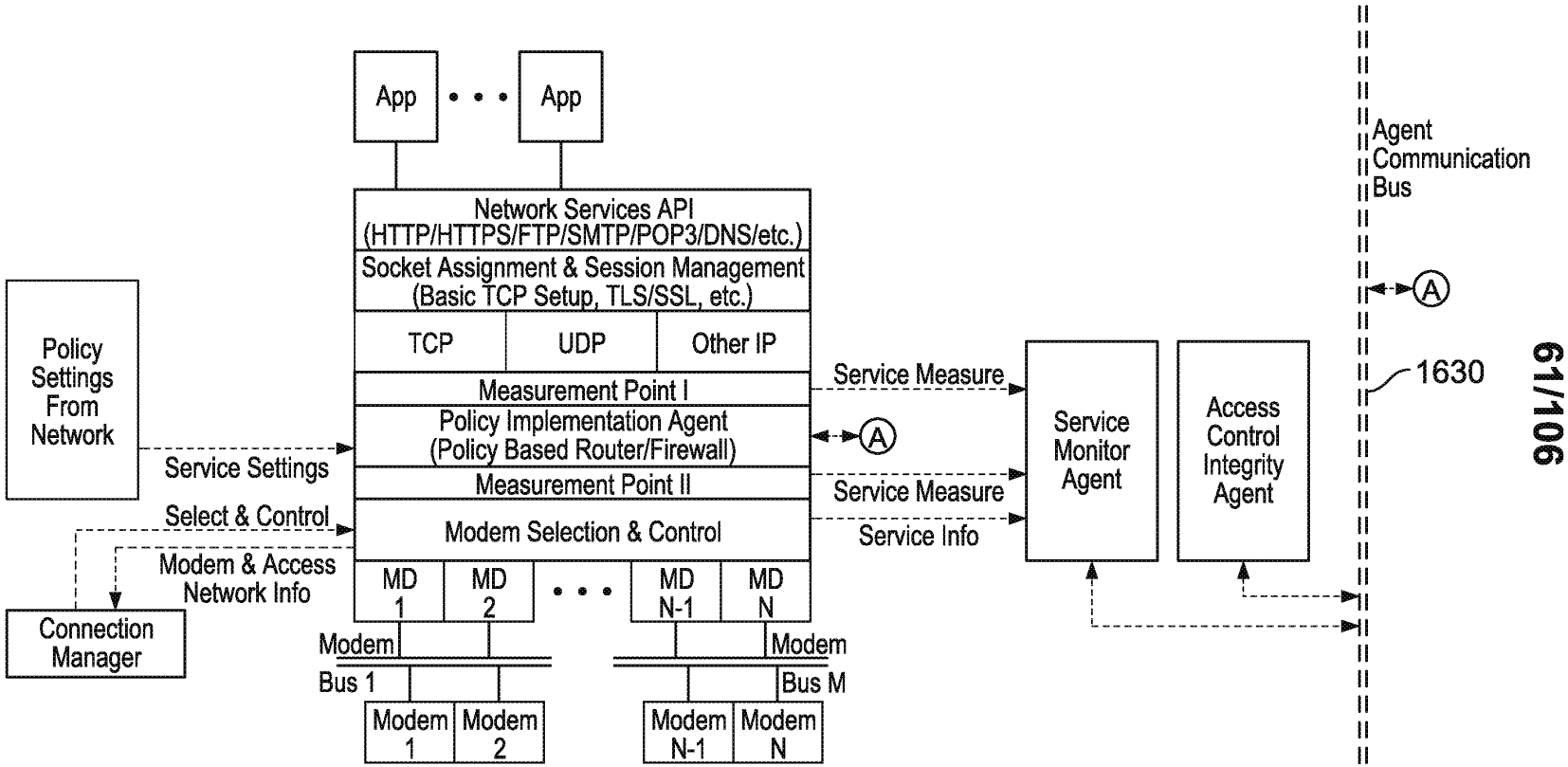


FIG. 32

IPR2025-01571
Apple EX1002 Page 317

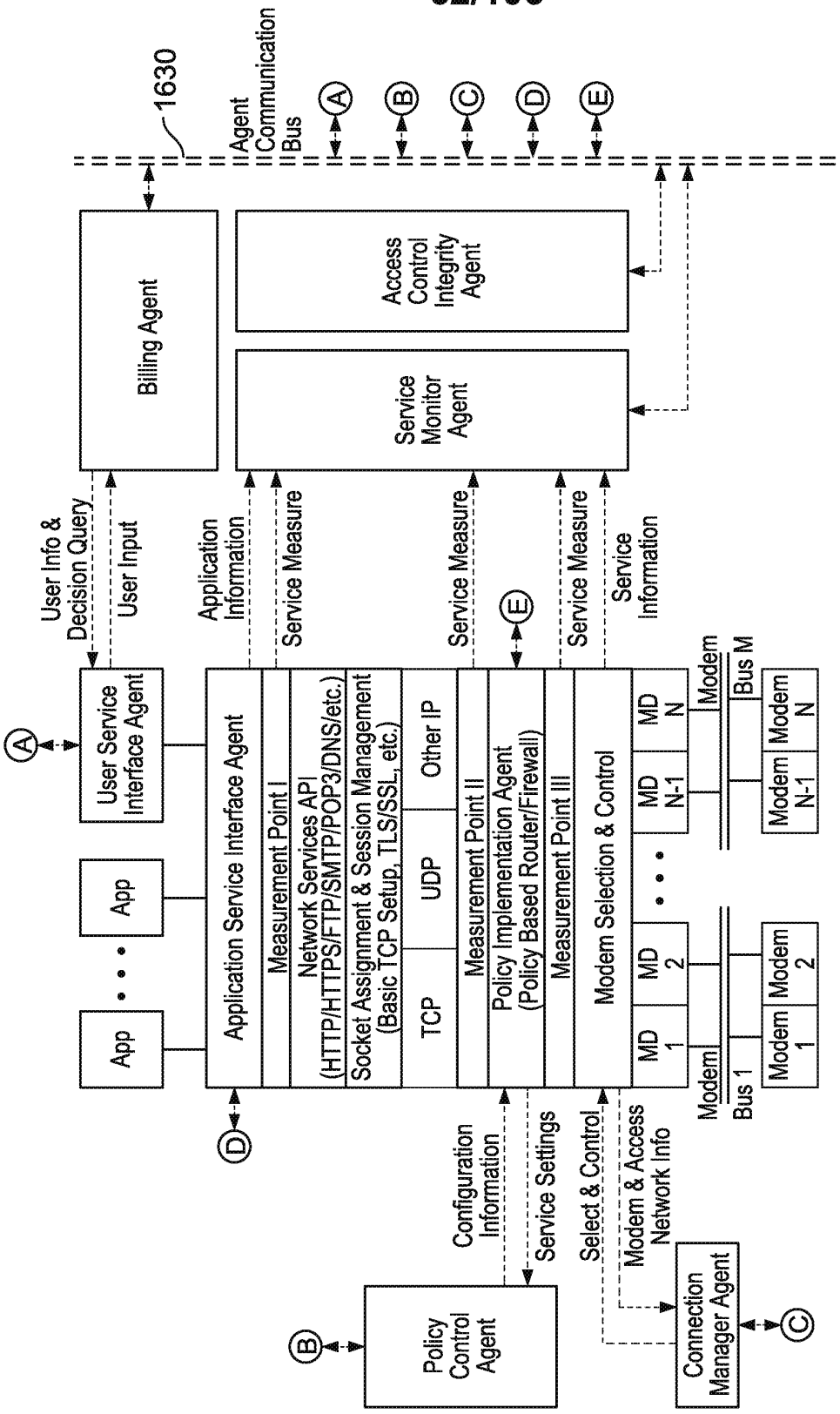

1630
Agent Communication Bus
A
B
C
D
E
Billing Agent
Access Control Integrity Agent
Service Monitor Agent
User Info & Decision Query
User Input
Application Information
Service Measure
Service Measure
Service Measure
Service Information
User Service Interface Agent
App
App
Application Service Interface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

FIG. 33

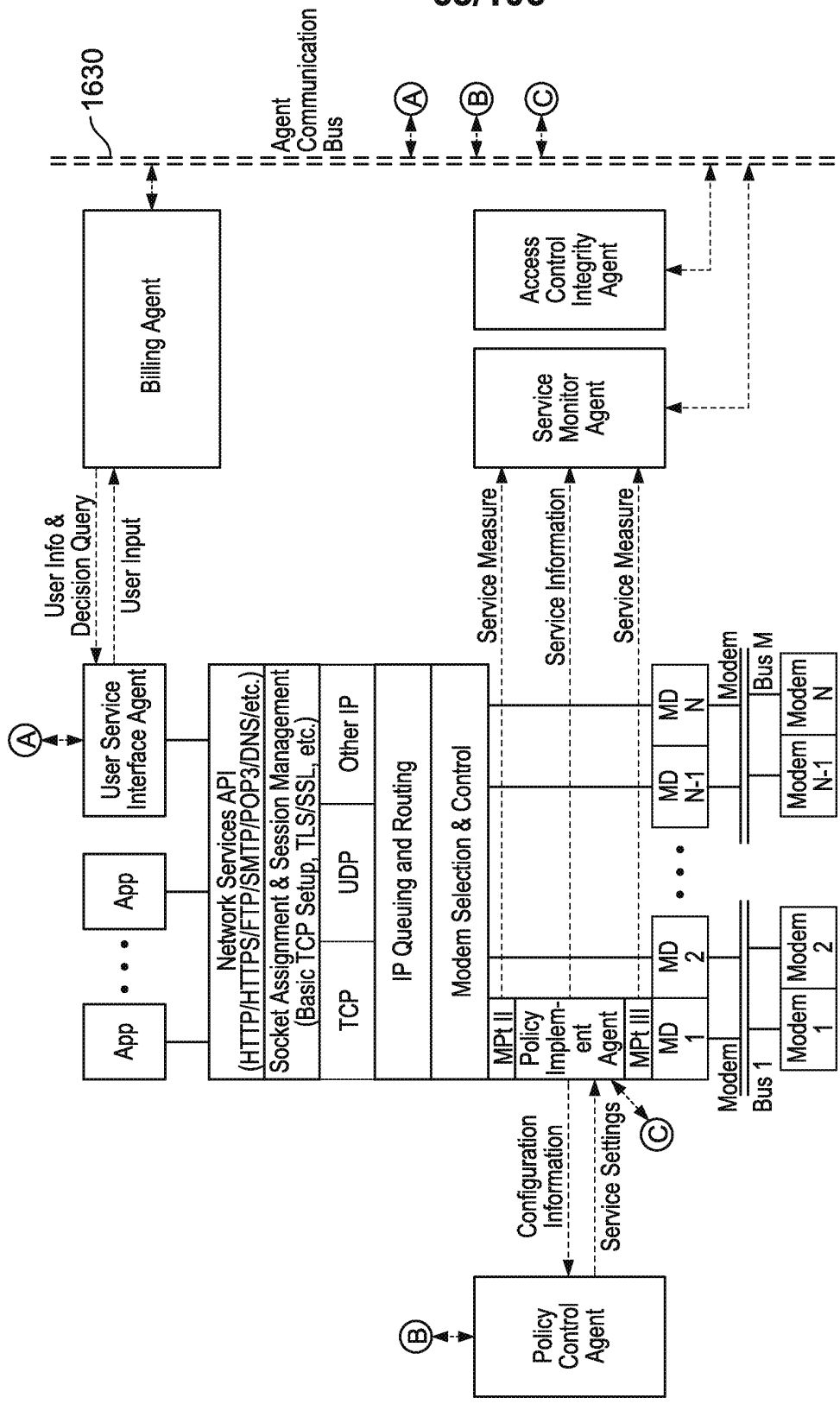

1630
Agent Communication Bus
A
B
C
Billing Agent
Access Control Integrity Agent
Service Monitor Agent
User Info & Decision Query
User Input
Service Measure
Service Information
Service Measure
User Service Interface Agent
App
App
Network Services API (HTTP/HTTPS/FTP/SMTP/POP3/DNS/etc.)
Socket Assignment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

FIG. 34

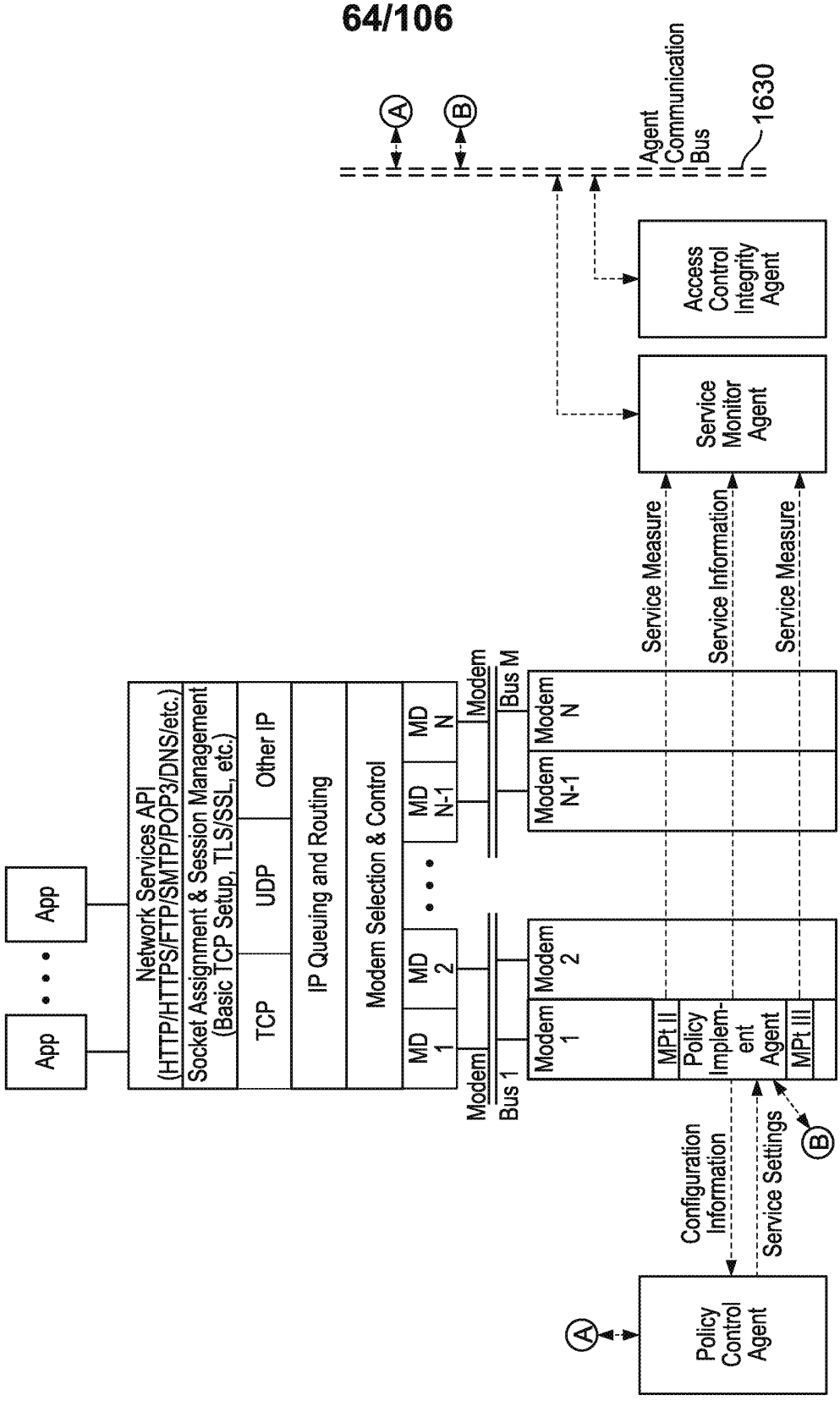

App
App
Network Services API
(HTTP/HTTPS/FTP/SMTP/POP3/DNS/etc.)
Socket Assignment & Session Management
(Basic TCP Setup, TLS/SSL, etc.)
TCP
UDP
Other IP
IP Queuing and Routing
Modem Selection & Control
MD 1
MD 2
MD N-1
MD N
Modem Bus 1
Modem Bus M
Modem 1
Modem 2
Modem N-1
Modem N
MPt II
Policy Implem-ent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

FIG. 35

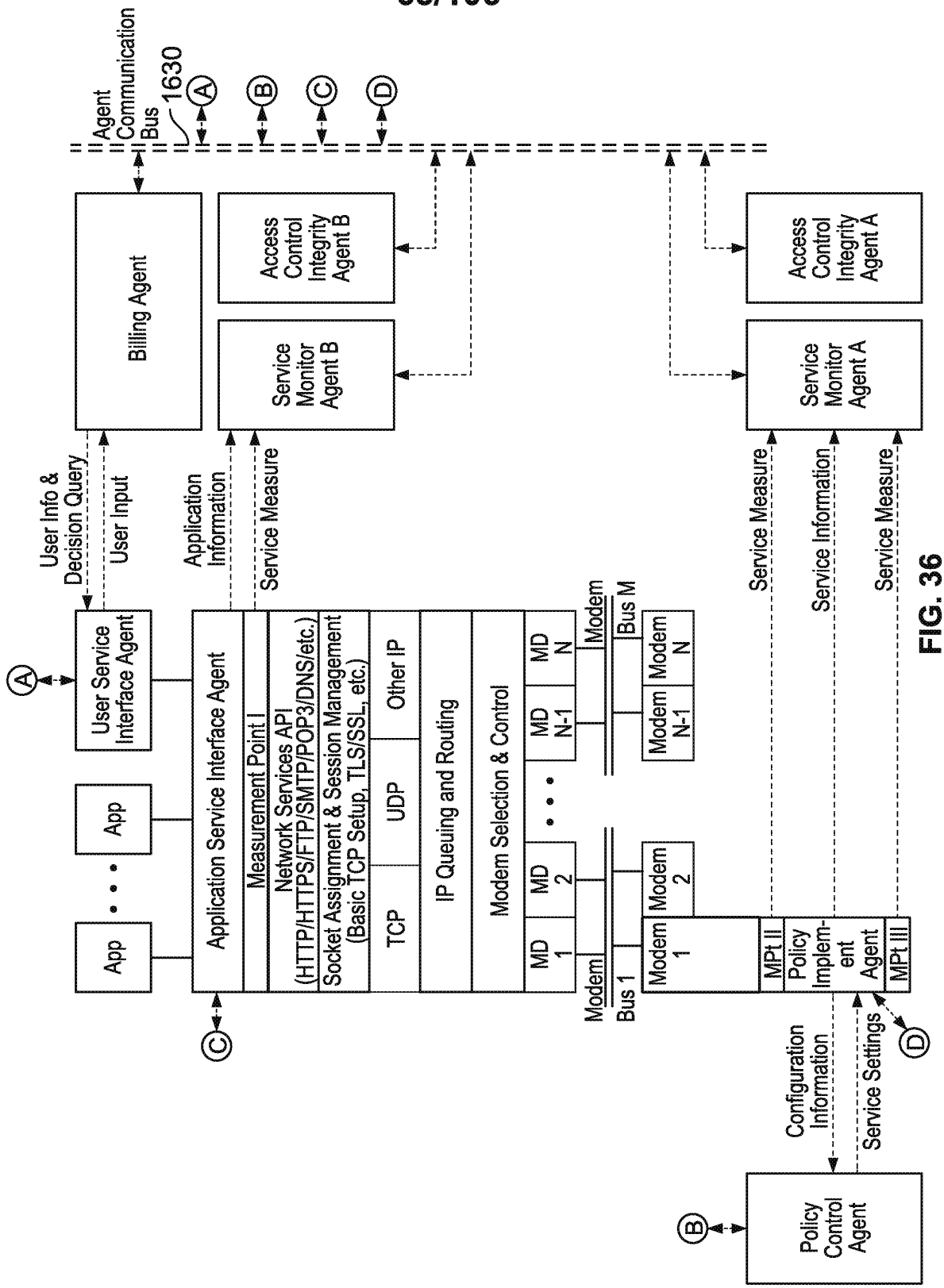

Agent Communication Bus
1630
A
B
C
D
Billing Agent
Access Control Integrity Agent B
Service Monitor Agent B
Access Control Integrity Agent A
Service Monitor Agent A
User Info & Decision Query
User Input
Application Information
Service Measure
Service Measure
Service Information
Service Measure
User Service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

FIG. 36

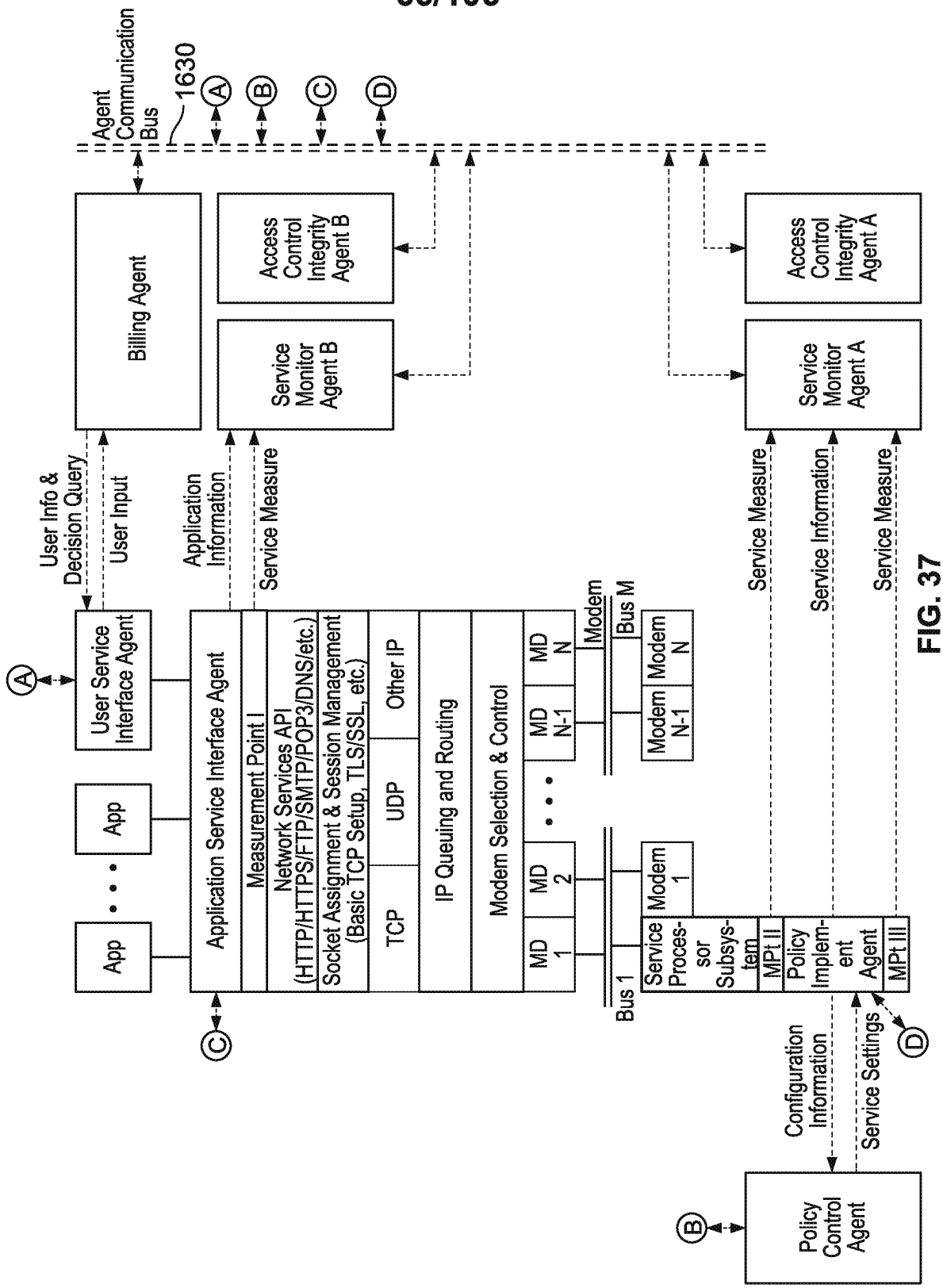

Agent Communication Bus
1630
A
B
C
D
Billing Agent
Access Control Integrity Agent B
Service Monitor Agent B
Access Control Integrity Agent A
Service Monitor Agent A
User Info & Decision Query
User Input
Application Information
Service Measure
Service Measure
Service Information
Service Measure
User Service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

FIG. 37

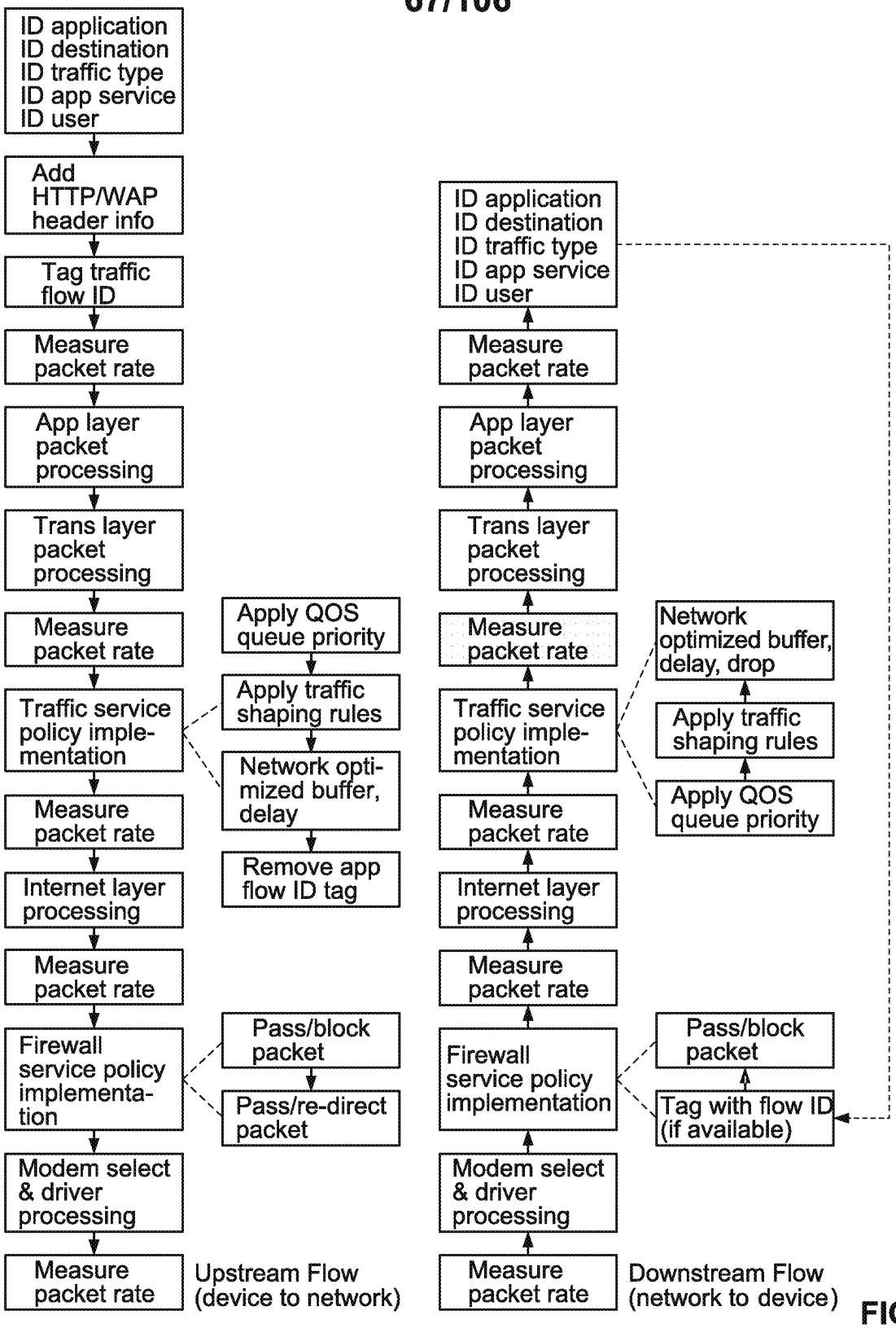

ID application
ID destination
ID traffic type
ID app service
ID user
Add HTTP/WAP header info
Tag traffic flow ID
Measure packet rate
App layer packet processing
Trans layer packet processing
Measure packet rate
Traffic service policy imple-mentation
Measure packet rate
Internet layer processing
Measure packet rate
Firewall service policy implementa-tion
Modem select & driver processing
Measure packet rate
Upstream Flow (device to network)
Apply QOS queue priority
Apply traffic shaping rules
Network opti-mized buffer, delay
Remove app flow ID tag
Pass/block packet
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
Measure packet rate
Firewall service policy implementation
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. 38

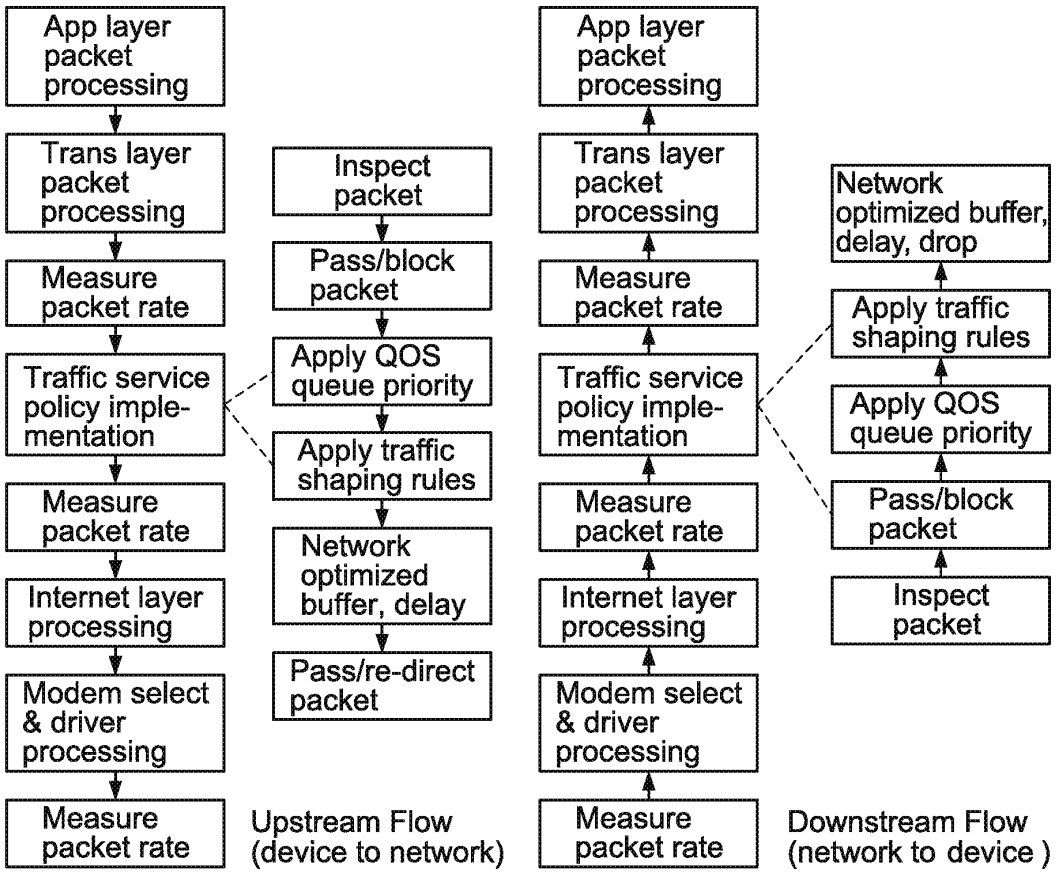

App layer packet processing
Trans layer packet processing
Measure packet rate
Traffic service policy imple-mentation
Measure packet rate
Internet layer processing
Modem select & driver processing
Measure packet rate
Upstream Flow (device to network)
Inspect packet
Pass/block packet
Apply QOS queue priority
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

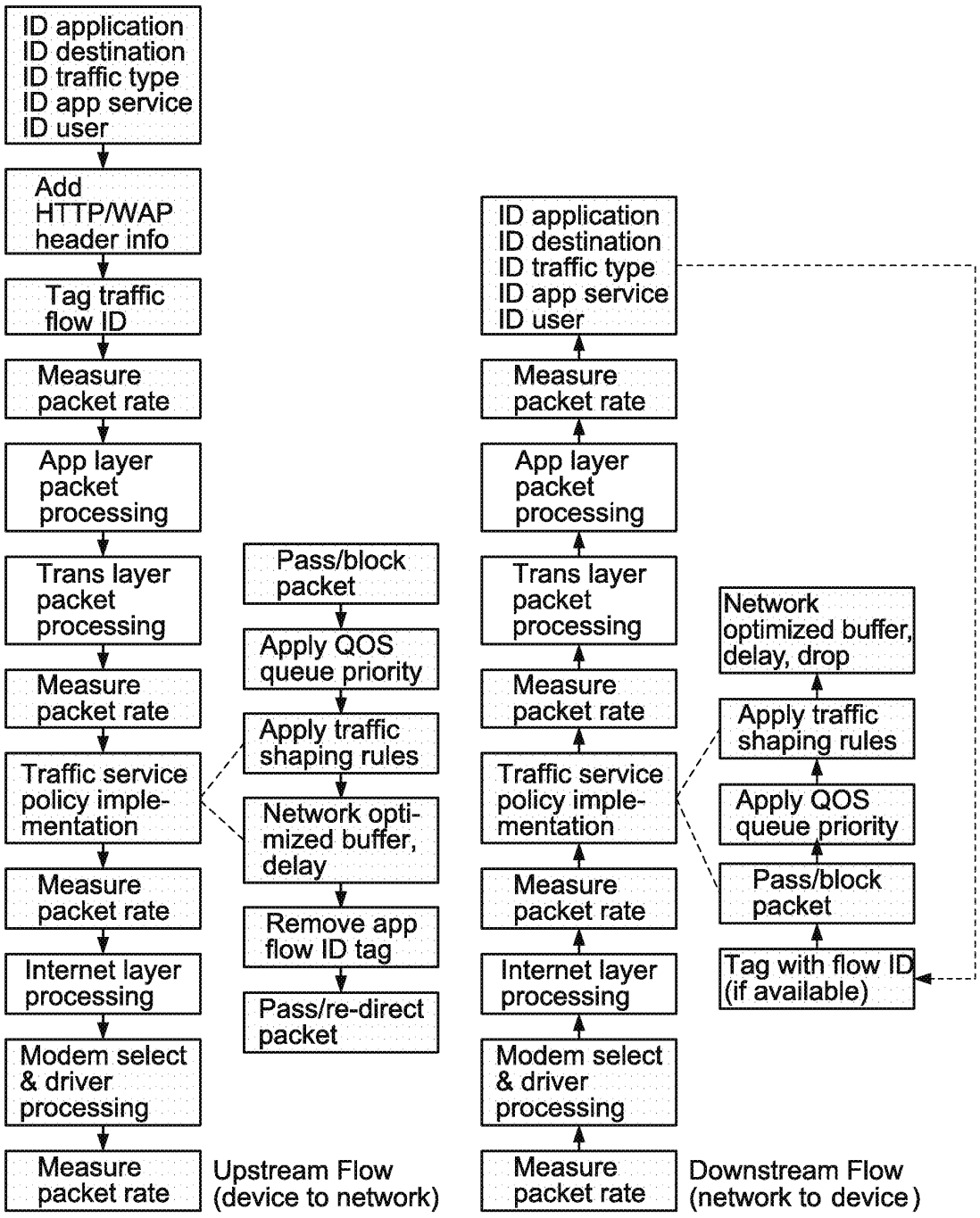

ID application
ID destination
ID traffic type
ID app service
ID user
Add HTTP/WAP header info
Tag traffic flow ID
Measure packet rate
App layer packet processing
Trans layer packet processing
Measure packet rate
Traffic service policy imple-mentation
Measure packet rate
Internet layer processing
Modem 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

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

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

FIG. 42B

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

FIG. 42C

	embodiment, the analyze traffic functionality is used to identify those service aspects that are causing the majority of the service plan usage, and then each of those service plan aspects are limited using the successive limitation functionality, with the service level limitations being based on the traffic usage patterns and specific application scenarios for each service aspect. For example, in some embodiments the service aspects that are creating the most service usage are subjected to more service level limitation than service aspects that are creating less service usage. Service usage may be defined as usage of a raw service measurement such as total data consumption, files downloaded or time spent on network, or it may be translated into an economic measure using the lookup service cost functionality. In some embodiments, the period of time elapsed in the service accounting period is taken into account in determining…	
Synchronize service usage counters	Synchronizes service usage counters on device from time to time to minimize service accounting errors between the device data base and the central billing data base. In some embodiments this is a part of the Service Processor heartbeat communication system that need not happen every heartbeat. In some embodiments this occurs with a request for update by the device to the central billing system or to a server function in the Service Processor	Provided for in the basic service agreement.
Lookup service cost	Provides a data base of service usage vs. cost for each type of service offered on the device. Provides for a lookup function of service cost.	Same as above.
Convert service usage to service cost	Uses the service cost vs. usage lookup function to transform one or more service usage aspects to one or more service cost aspect. One example embodiment provides a service cost measure for one specific aspect of service usage, for example total data consumed over a period of time. Another example embodiment provides a total service cost measure for all service usage over a period of time.	Same as above.
Notify user of service overage	Sends a notification message or screen to the UI to inform the user that the one or more aspects of service usage has exceeded the specified limits of one or more service plans. In some embodiments, the user notice is a pop-up window and in some embodiments there is a continuous display on a small gauge in main screen.	Same as above.
Project service usage	Uses the analyze traffic functionality and projects an estimate of what the traffic usage will be at the end of a service plan measurement interval if the service usage does not change. In some embodiments the projected service usage is made based on assuming the average service usage per unit time in the present service plan measurement interval does not change for the remainder of the service plan measurement interval.	Same as above

FIG. 42D

Notify user of service cost overage	Performs a service cost estimate based on one or more aspects of service usage and informs the user that the one or more aspects of service cost has exceeded the specified limits of a service plan. In some embodiments, the user notice is a pop-up window and in some embodiments there is a continuous display on a small gauge in main screen.	Provided for in the basic service agreement.
Notify user of usage behavior likely to run over service usage limit	Uses the project service usage functionality to determine if the service usage is projected to go beyond the service plan limit, notifies the user if the projected usage is over the service plan limit for the service plan measurement interval. In some embodiments, the user notice is a pop-up window and in some embodiments there is a continuous display on a small gauge in main screen. In some embodiments the projected service usage is made based on assuming the average service usage per unit time in the present service plan measurement interval does not change for the remainder of the service plan measurement interval.	Same as above.
Notify user of usage behavior likely to run over cost limit	Uses the project service usage functionality to determine if the service usage is projected to go beyond the service plan limit, uses convert service measure to service cost functionality to estimate the service cost of the projected service overage, notifies the user if the projected cost is over the service plan cost associated with the service plan service limit for the service plan measurement interval. In some embodiments, the user notice is a pop-up window and in some embodiments there is a continuous display on a small gauge in main screen. In some embodiments the projected cost is made based on assuming the average service usage per unit time in the present service plan measurement interval does not change for the remainder of the service plan measurement interval.	Same as above.
Project user service cost if usage behavior continues	Uses the project service usage functionality to determine if the service usage is projected to go beyond the service plan limit, uses convert service measure to service cost functionality to estimate the service cost of the projected service overage, notifies the user of what the projected cost will be if the service usage behavior remains the same. In some embodiments, the user notice is a pop-up window and in some embodiments there is a continuous display on a small gauge in main screen. In some embodiments the projected cost is made based on assuming the average service usage per unit time in the present service plan measurement interval does not change for the remainder of the service plan measurement interval.	Same as above.

FIG. 42E

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

FIG. 42F

Access control enable list	List of service usage activities that are enabled.	Authorization restricted to service controller, VSP or other network function with proper credentials to access the control data base.
Access control block list	List of service usage activities that are blocked.	Same as above.
User service control option UI	Provides the user with a list of options for how they would like to control service usage or service cost.	In some embodiments UI screens and scripts are defined by the UI agent software version and access to modifying this software is restricted to service controller, VSP or other network function with proper credentials to access the UI data base. Some embodiments call for the UI screens or UI screen content to be generated by the service controller, VSP or another network function (e.g. service usage notification gateway or billing system) and in this case access is restricted to service controller, VSP or other network function with proper credentials to access the UI pass through screens.
User service notification option preference	Provides the user with a list of options for how they would like service notification information to be displayed. In some embodiments provides the user with the option to turn off one or more aspects of service notification. In some embodiments the user is not allowed to turn off notification for service usage events that require user decision or acknowledgement.	In some embodiments UI screens and scripts are defined by the UI agent software version and access to modifying this software is restricted to service controller, VSP or other network function with proper credentials to access the UI data base. Some embodiments call for the UI screens or UI screen content to be generated by the service controller, VSP or another network function (e.g. service usage notification gateway or billing system) and in this case access is restricted to service controller, VSP or other network function with proper credentials to access the UI pass through screens.

FIG. 42G

User CRM or service usage monitoring filtering option preference	Filters the device and/or user information that is being collected before it is reported to the network to maintain the desired level of user privacy. In some embodiments the user defines preferences on user privacy that are used to define the filter settings.	In some embodiments this is not accessible by the network and only may be modified by the user. In other embodiments it may be read but not written by the network and in this case authorization is restricted to service controller, VSP or other network function with proper credentials to access the filter settings data base. In some embodiments the network is allowed to change the CRM filter settings and in this case Authorization restricted to service controller, VSP or other network function with proper credentials to access the CRM filter settings data base.
Service usage billing event record	A record of service usage billing events. In some embodiments this record is transmitted to the billing server or another network function to aid service billing or billing reconciliation.	In some embodiments authorization restricted to service controller, VSP or other network function with proper credentials to access the billing data base. In some embodiments the user is allowed to read but not write the data base.
Bill by account	The bill by account embodiments provide for service billing to accounts different than the main user account, for example tracking network device chatter that is not desired to be billed to the user, transaction partner access costs that are shared with or billed to the transaction partner, ambient service cost tracking, tracking temporary account costs, etc.	In some embodiments authorization restricted to service controller, VSP or other network function with proper credentials to access the billing data base. In some embodiments the user is allowed to read but not write the data base.
Central billing transaction and event recording	Billing event tracking and reporting associated with the central provider open billing embodiments. Some embodiments include generation of billing certificates or receipts. In some embodiments the device may serve as a billing feed.	In some embodiments authorization restricted to service controller, VSP or other network function with proper credentials to access the billing data base. In some embodiments the user is allowed to read but not write the data base.
Service owner registration or re-registration	Function that allows a portion of the device credentials to be programmed to indicated the VSP.	In some embodiments authorization to write the device is restricted with security signatures or other security methods to the VSP and possibly the central provider. Some embodiments involve provisions to report to a network function when the VSP settings are changed or the software is uninstalled. Other embodiments involve restoring VSP settings or software if removed.

FIG. 42H

Credentials swap	Function that provides for swapping of credentials, for example temporary credentials to permanent credentials.	Authorization restricted to service controller, VSP or other network function with proper credentials to access the credentials data base.
Account information swap	Function that provides for swapping the account information, for example temporary account to permanent account.	Authorization restricted to service controller, VSP or other network function with proper credentials to access the activation service profile data base.
Configure or re-configure service processor for new device service	Function that provides for service processor programming for all the information that defines the service profile, device credentials, VSP and other necessary parameters.	Authorization restricted to service controller, VSP or other network function with proper credentials to access the service profile data base.
Ambient service profile definition	Function that provides for service processor programming for all the information that defines the ambient service profile, device credentials, VSP and other necessary parameters.	Authorization restricted to service controller, VSP or other network function with proper credentials to access the ambient service profile data base.
Analyze service usage statistics	VSP function to analyzer service usage statistics for a device, defined group of devices, defined group of service plans or service profiles, defined group of users or other groupings.	Authorization typically restricted to service controller, VSP or other network entity with the credentials to access the service usage history data bases.
Dry lab test new service policy	Allows simulated testing of draft service profiles and/or service plans against device usage statistics for a defined group of devices or users or service profiles, or against simulated device service usage behavior. Some embodiments show the estimated profitability of proposed service profile and service plan. Some embodiments allow decomposition of the service usage statistics to identify the user group service usage activities that may be modified by changing the service usage control policies or made more profitable by changing the service plan billing policies.	Authorization typically restricted to service controller, VSP or other network entity with the credentials to access the service usage history data bases.
Beta test publishing system	Function that provides for service processor programming for all the information that defines the service profile device credentials, VSP and other necessary parameters for a beta test device group.	Authorization restricted to service controller, VSP or other network function with proper credentials to access the service profile data base.
Publish new service	Function that provides for service processor programming for all the information that defines the service profile, device credentials, VSP and other necessary parameters for a production device group.	Authorization restricted to service controller, VSP or other network function with proper credentials to access the service profile data base.

FIG. 42I

IPR2025-01571
Apple EX1002 Page 335

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

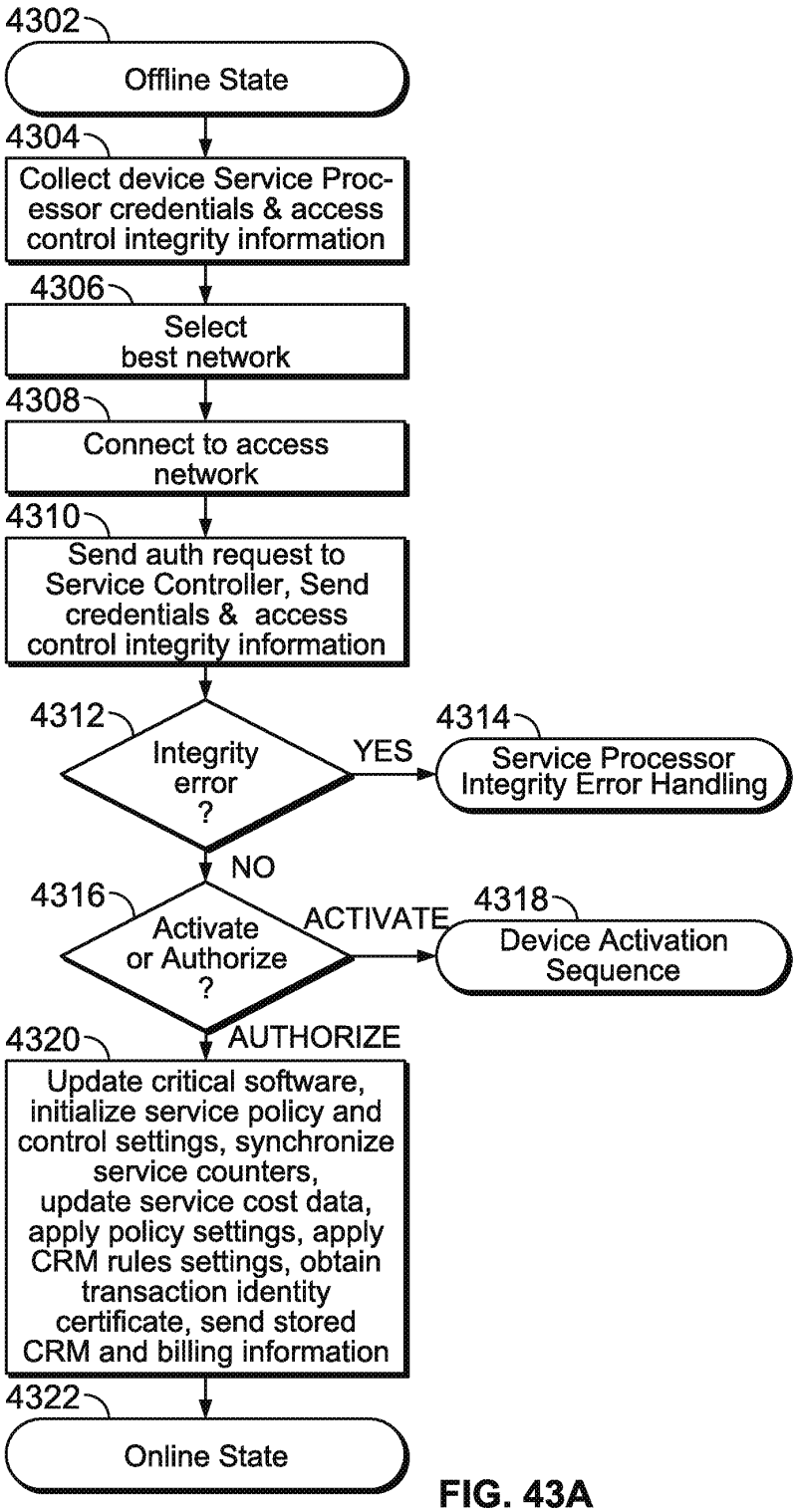


FIG. 43A

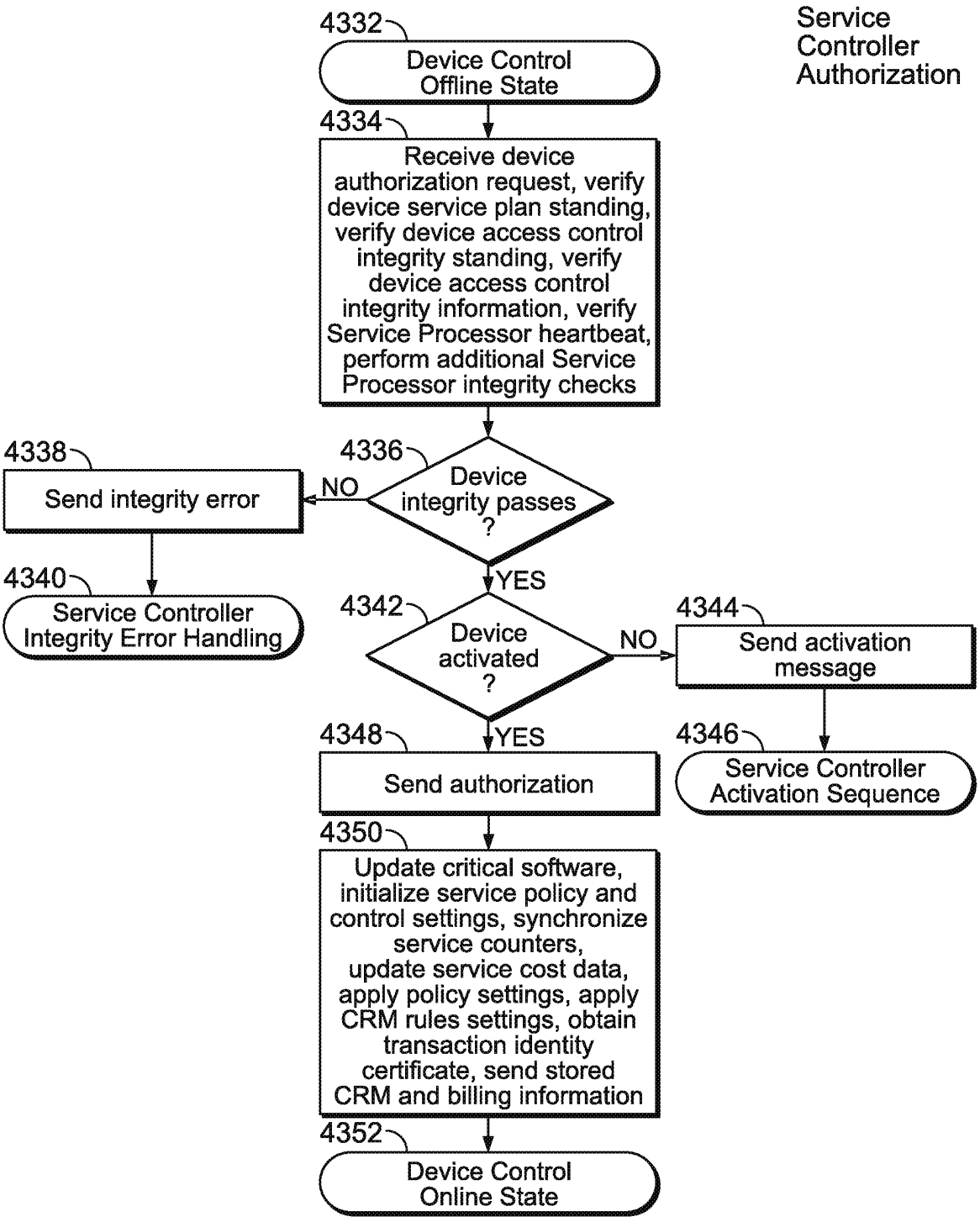

Service Controller Authorization
4332
Device Control Offline State
4334
Receive device authorization request, verify device service plan standing, verify device access control integrity standing, verify device access control integrity information, verify Service Processor heartbeat, perform additional 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

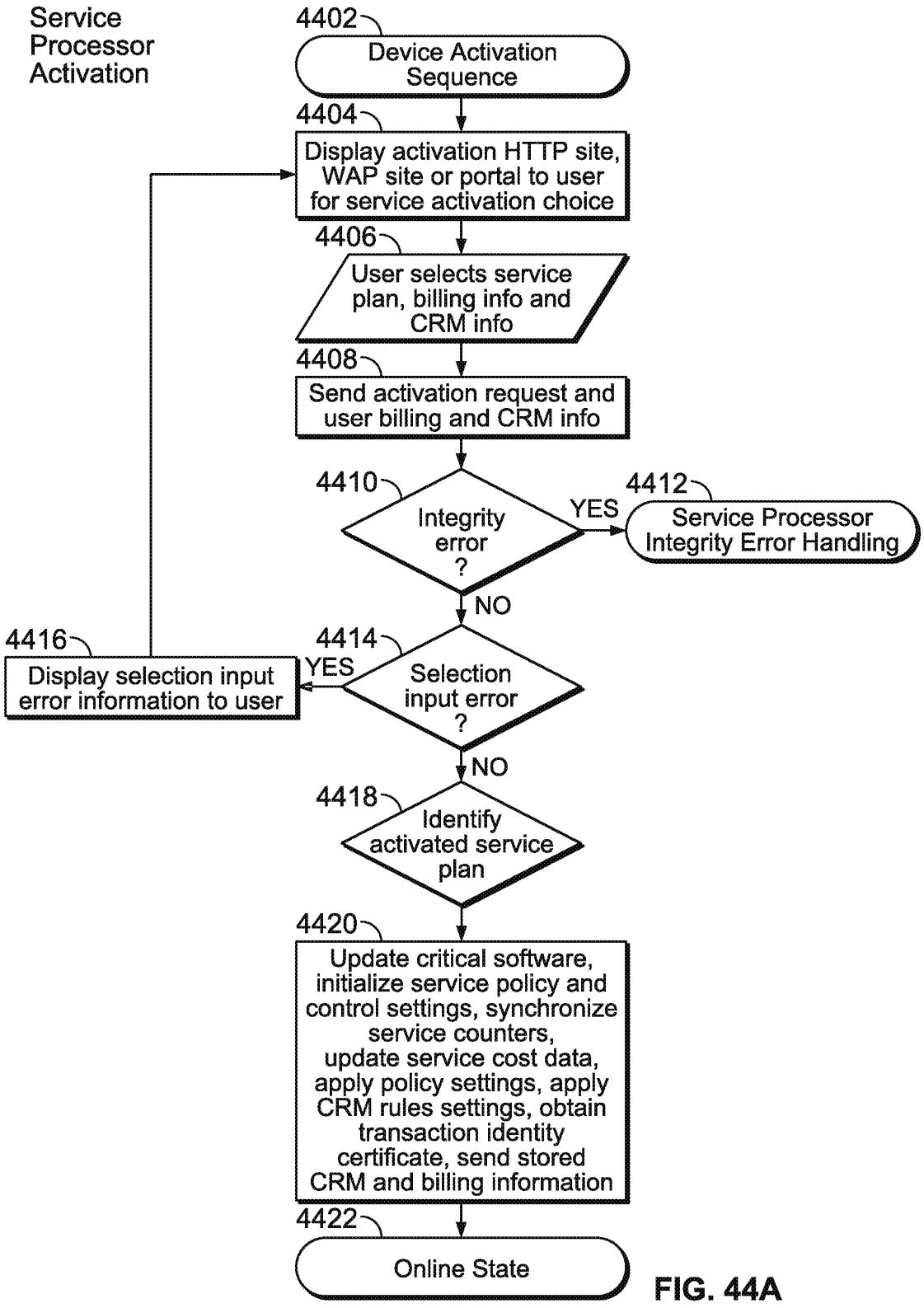

Service Processor Activation
4402
Device Activation Sequence
4404
Display activation HTTP site, WAP site or portal to user for service activation choice
4406
User selects service plan, billing info and CRM info
4408
Send activation request and user billing and CRM info
4410
Integrity error ?
YES
4412
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

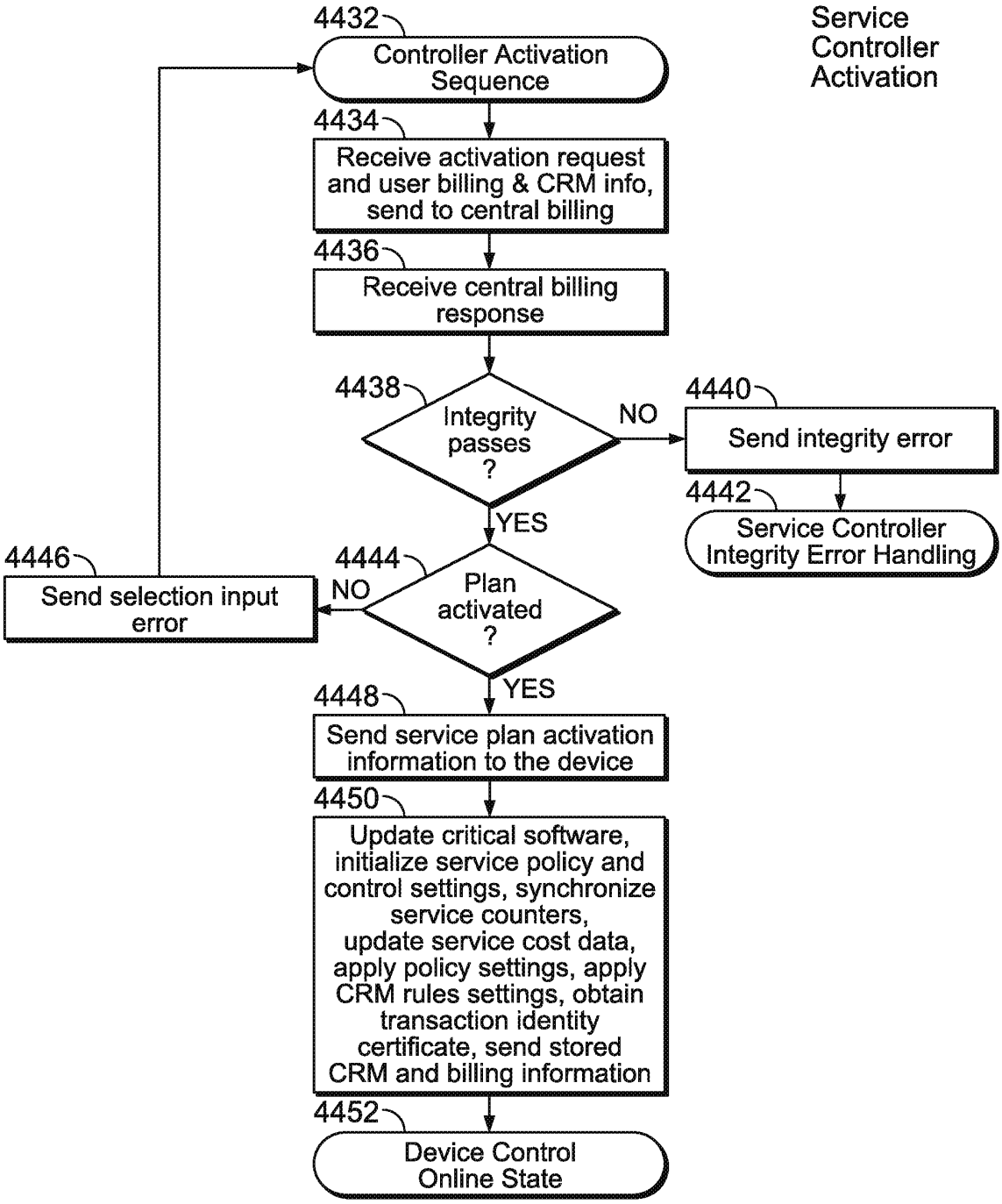

Service Controller Activation
4432
Controller Activation Sequence
4434
Receive activation request and user billing & CRM info, send to central billing
4436
Receive central billing response
4438
Integrity passes ?
NO
4440
Send integrity error
4442
Service Controller Integrity Error Handling
YES
4444
Plan 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

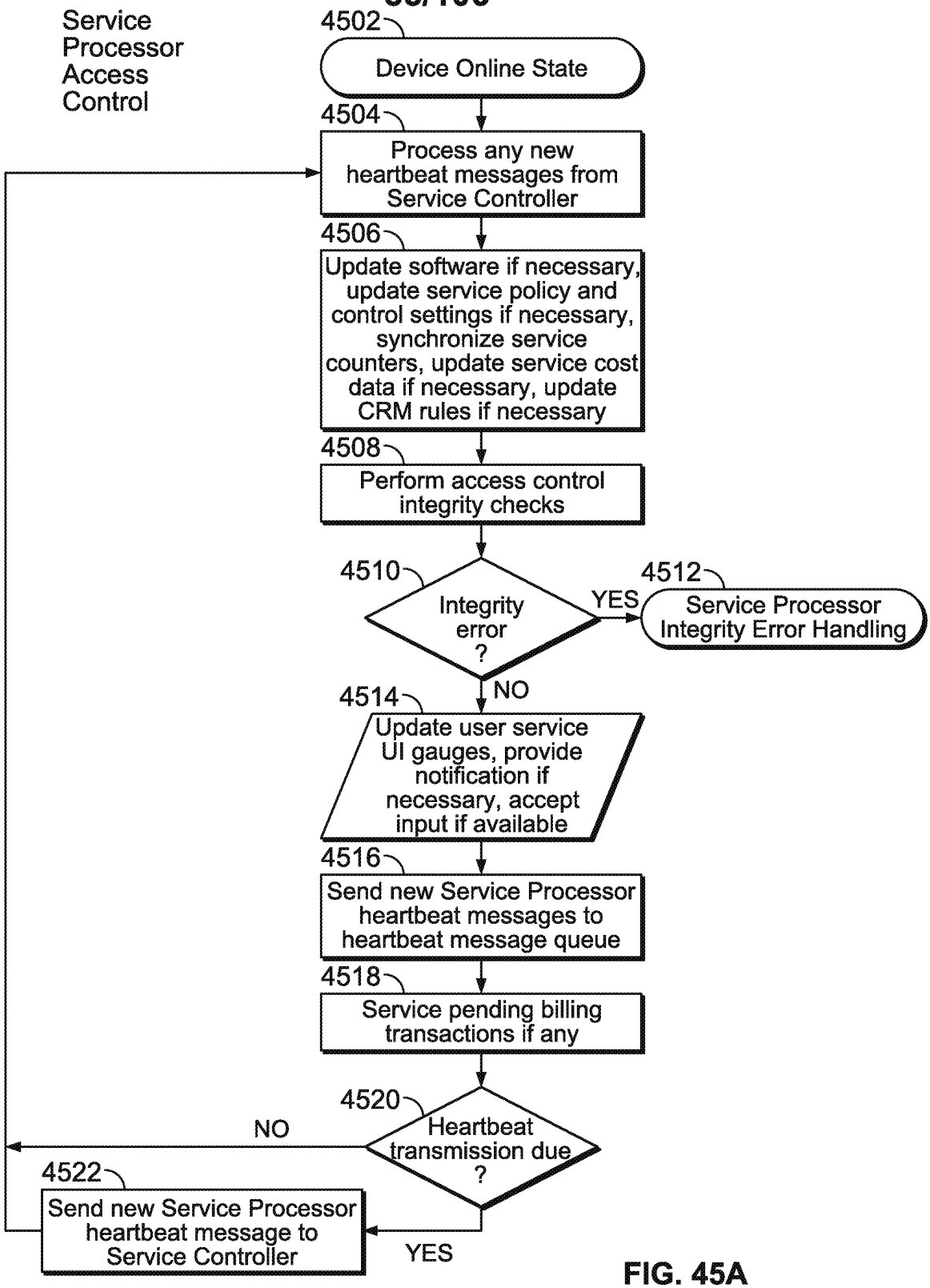

Service Processor Access Control
4502
Device Online State
4504
Process any new heartbeat messages from Service Controller
4506
Update software if necessary, update service policy and control settings if necessary, synchronize service counters, update service cost data if necessary, update CRM rules if 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

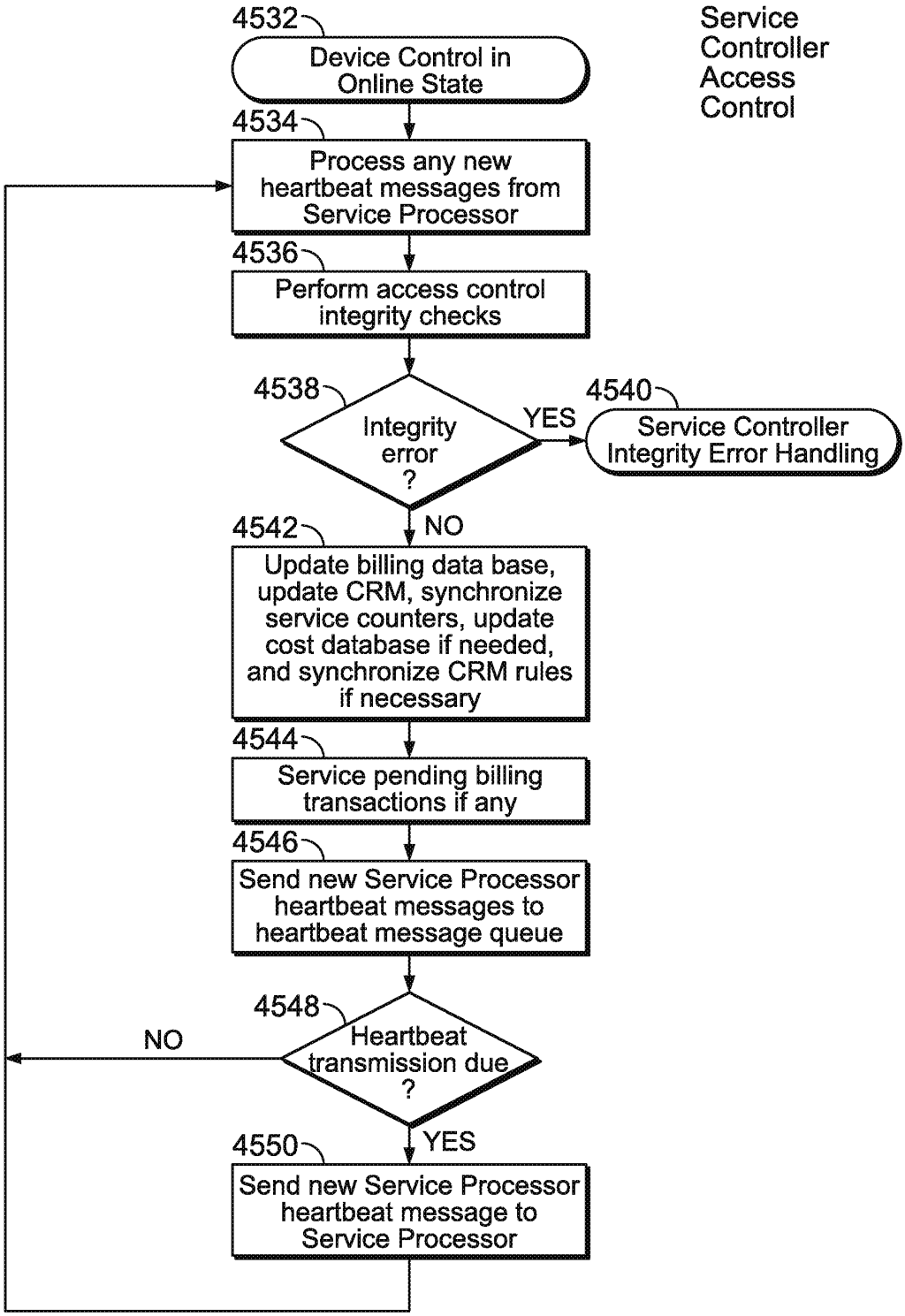

Service Controller Access Control
4532
Device Control in Online State
4534
Process any new heartbeat messages from Service Processor
4536
Perform access control integrity checks
4538
Integrity error ?
YES
4540
Service Controller Integrity Error Handling
NO
4542
Update billing data base, update CRM, synchronize 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

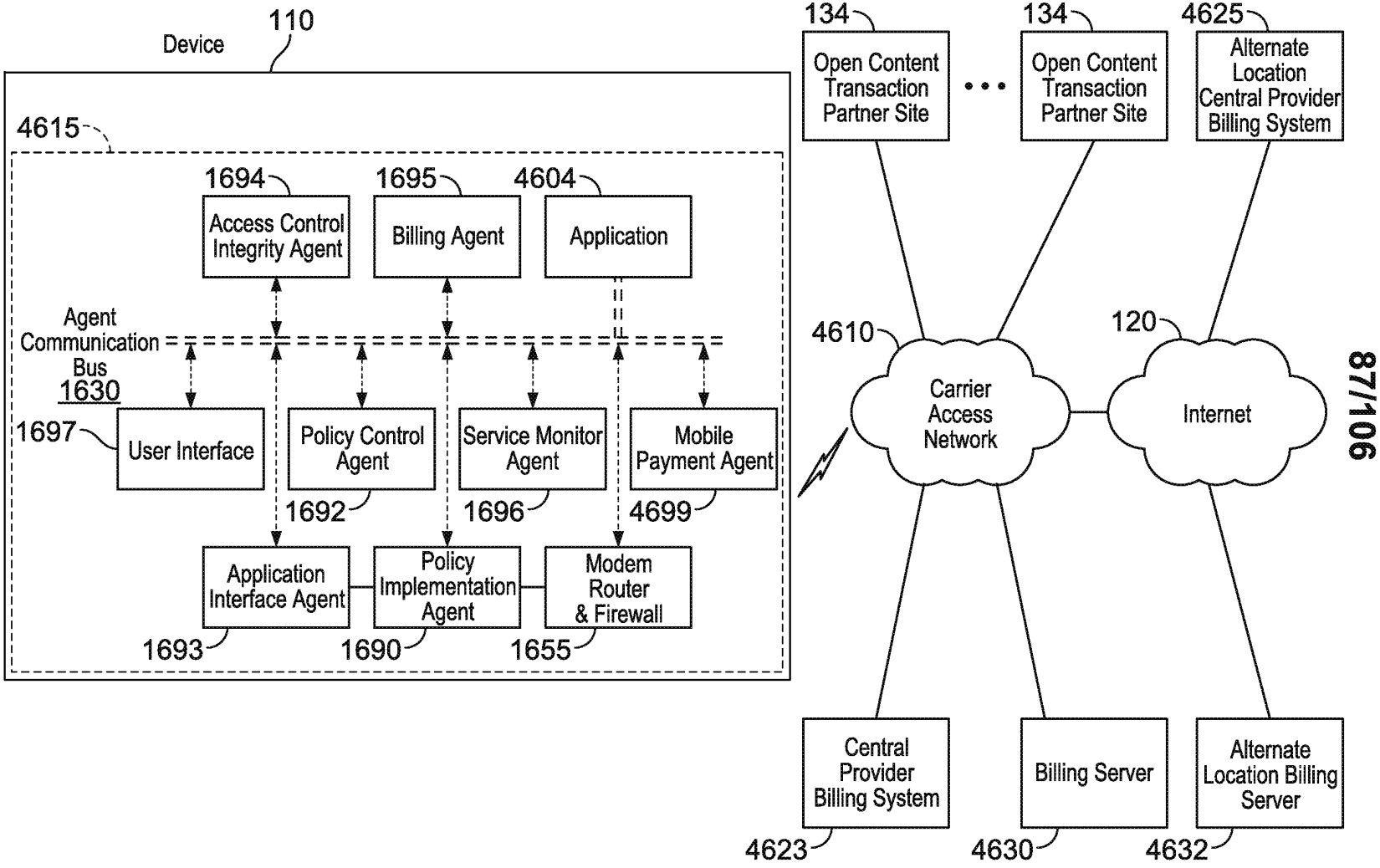


FIG. 46

IPR2025-01571
Apple EX1002 Page 343

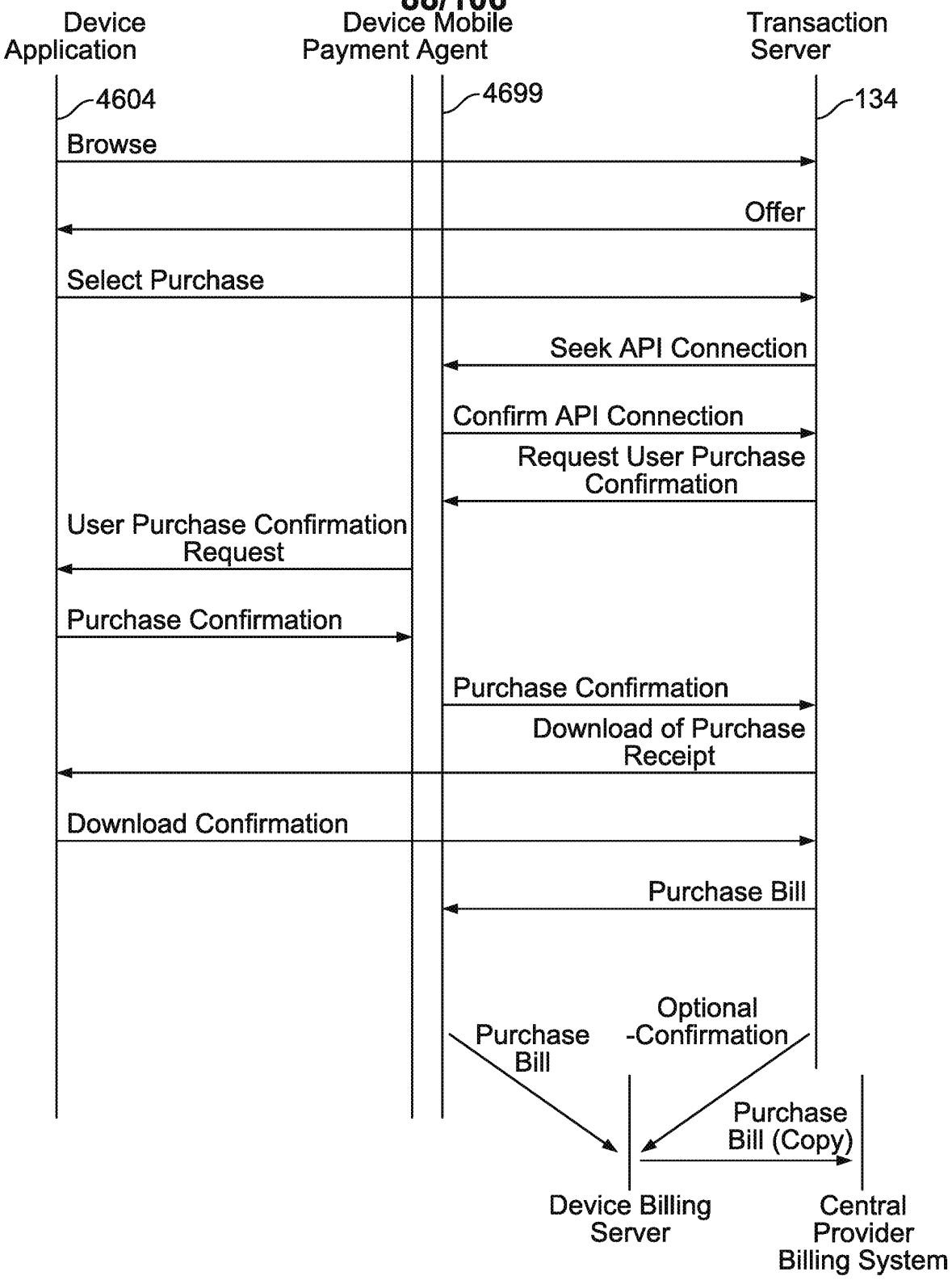

Device Application
Device Mobile Payment Agent
Transaction Server
4604
4699
134
Browse
Offer
Select Purchase
Seek API Connection
Confirm API Connection
Request User Purchase Confirmation
User Purchase Confirmation Request
Purchase Confirmation
Purchase Confirmation
Download of Purchase Receipt
Download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

FIG. 47A

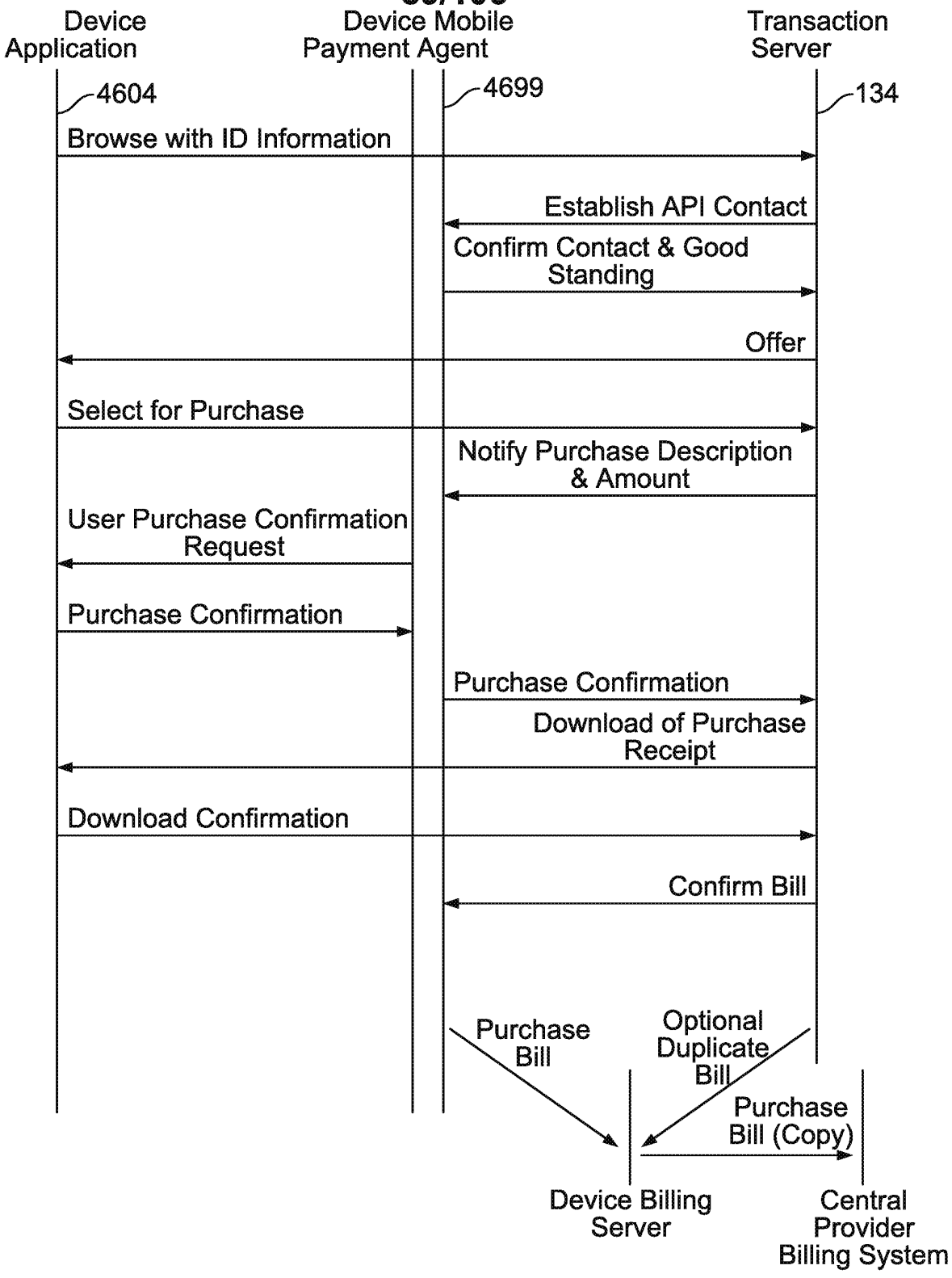

Device Application
Device Mobile Payment Agent
Transaction Server
4604
4699
134
Browse with ID Information
Establish API Contact
Confirm Contact & Good Standing
Offer
Select for Purchase
Notify Purchase Description & Amount
User Purchase Confirmation Request
Purchase Confirmation
Purchase Confirmation
Download of Purchase Receipt
Download Confirmation
Confirm Bill
Purchase Bill
Optional Duplicate Bill
Purchase Bill (Copy)
Device Billing Server
Central Provider Billing System

FIG. 47B

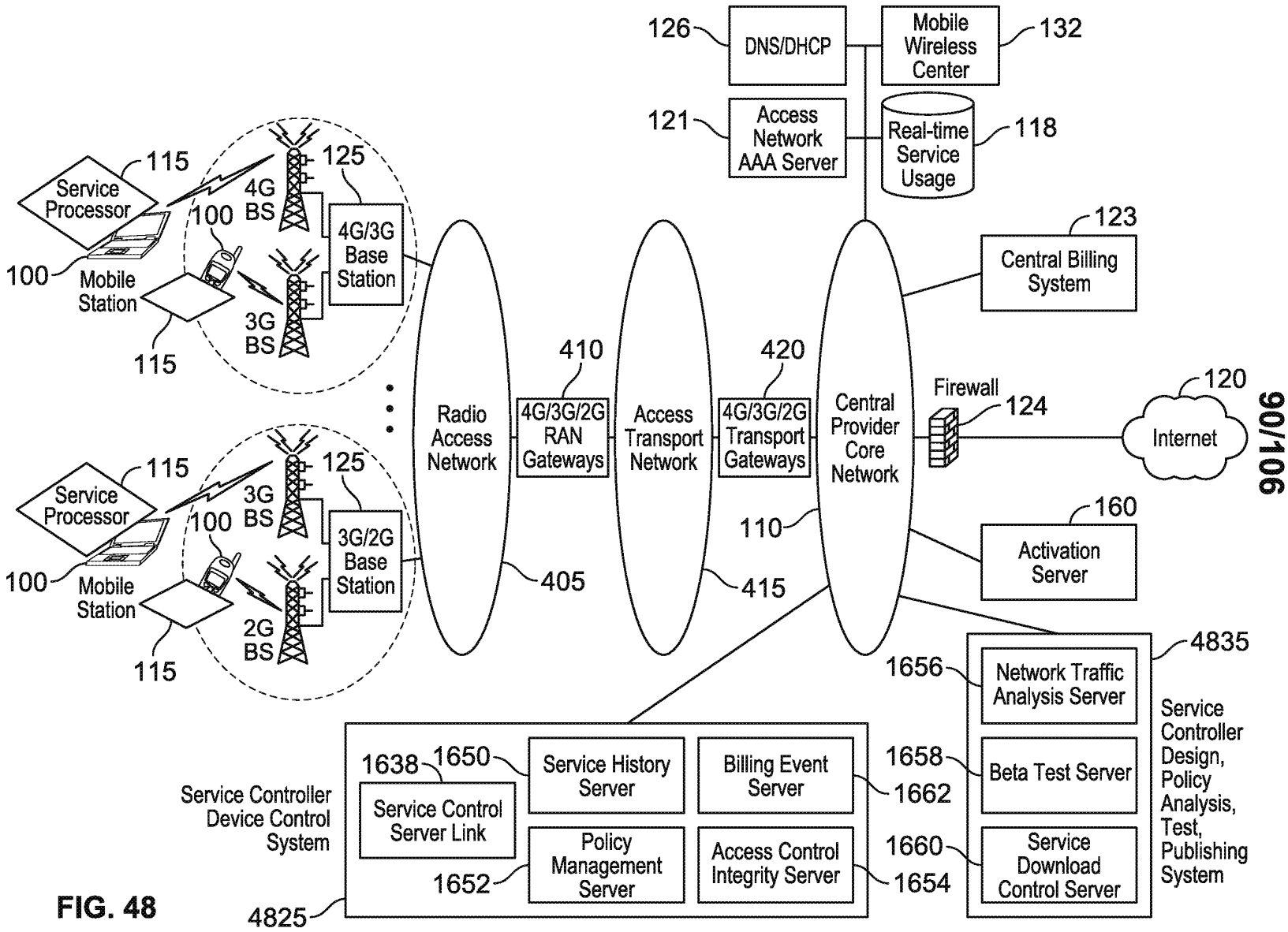


FIG. 48

IPR2025-01571
Apple EX1002 Page 346

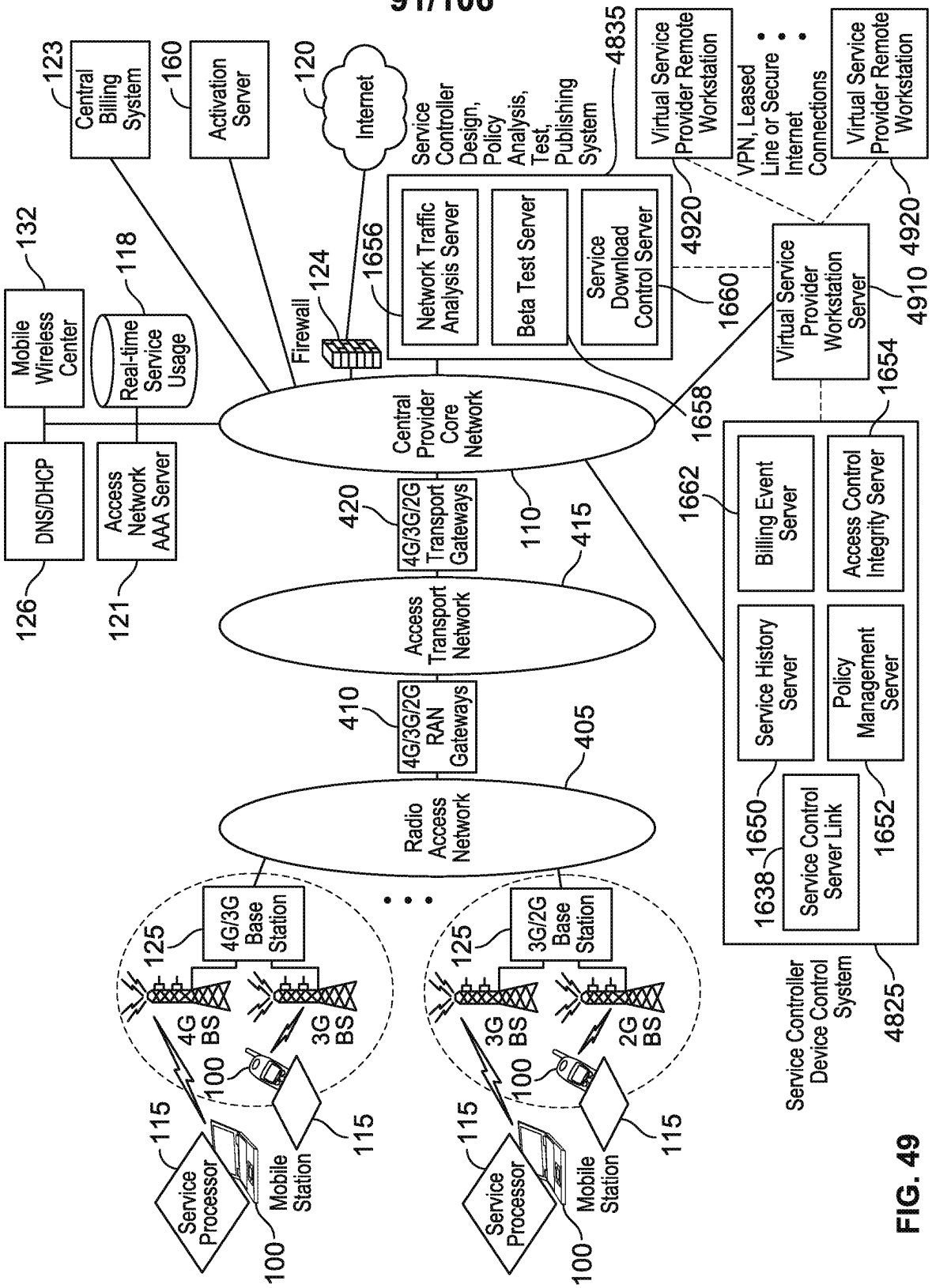

Central Billing System
123
Activation Server
160
Internet
120
Service Controller Design, Policy Analysis, Test, Publishing System
4835
Virtual Service Provider Remote Workstation
VPN, Leased Line or Secure Internet Connections
Virtual Service Provider Remote Workstation
Mobile Wireless Center
132
Real-time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

FIG. 49

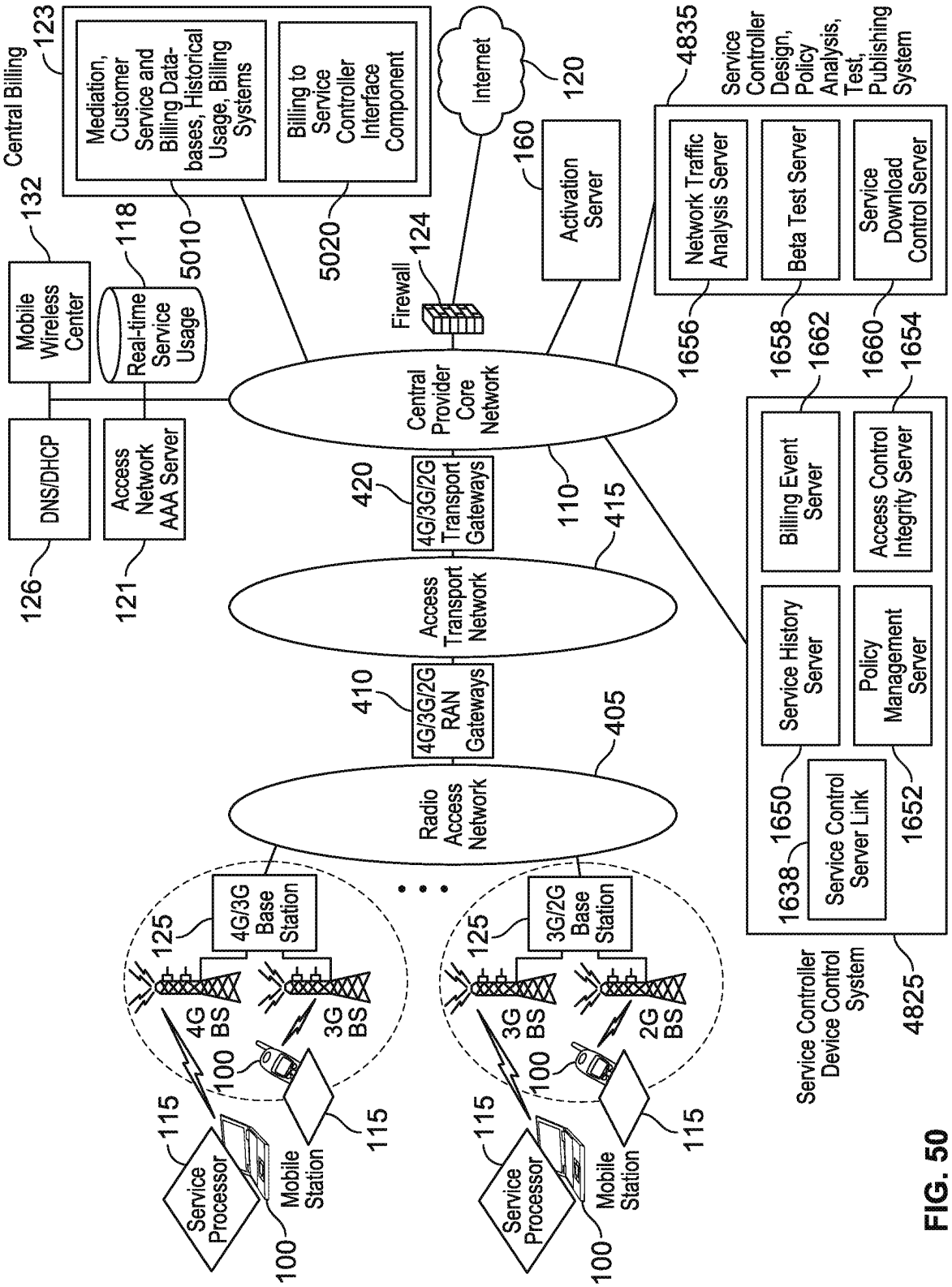

Central Billing
123
Mediation, Customer Service and Billing Data-bases, Historical Usage, Billing Systems
Billing to Service Controller Interface Component
Internet
120
Service Controller Design, Policy Analysis, Test, Publishing System
4835
Network Traffic Analysis Server
Beta Test Server
Service Download Control Server
1656
1658
1660
1662
1654
Activation Server
160
132
Mobile Wireless Center
118
Real-time Service Usage
5010
5020
Firewall
124
Central Provider Core Network
DNS/DHCP
126
Access Network AAA Server
121
420
4G/3G/2G Transport Gateways
110
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
115
100
Service Processor
Mobile Station

FIG. 50

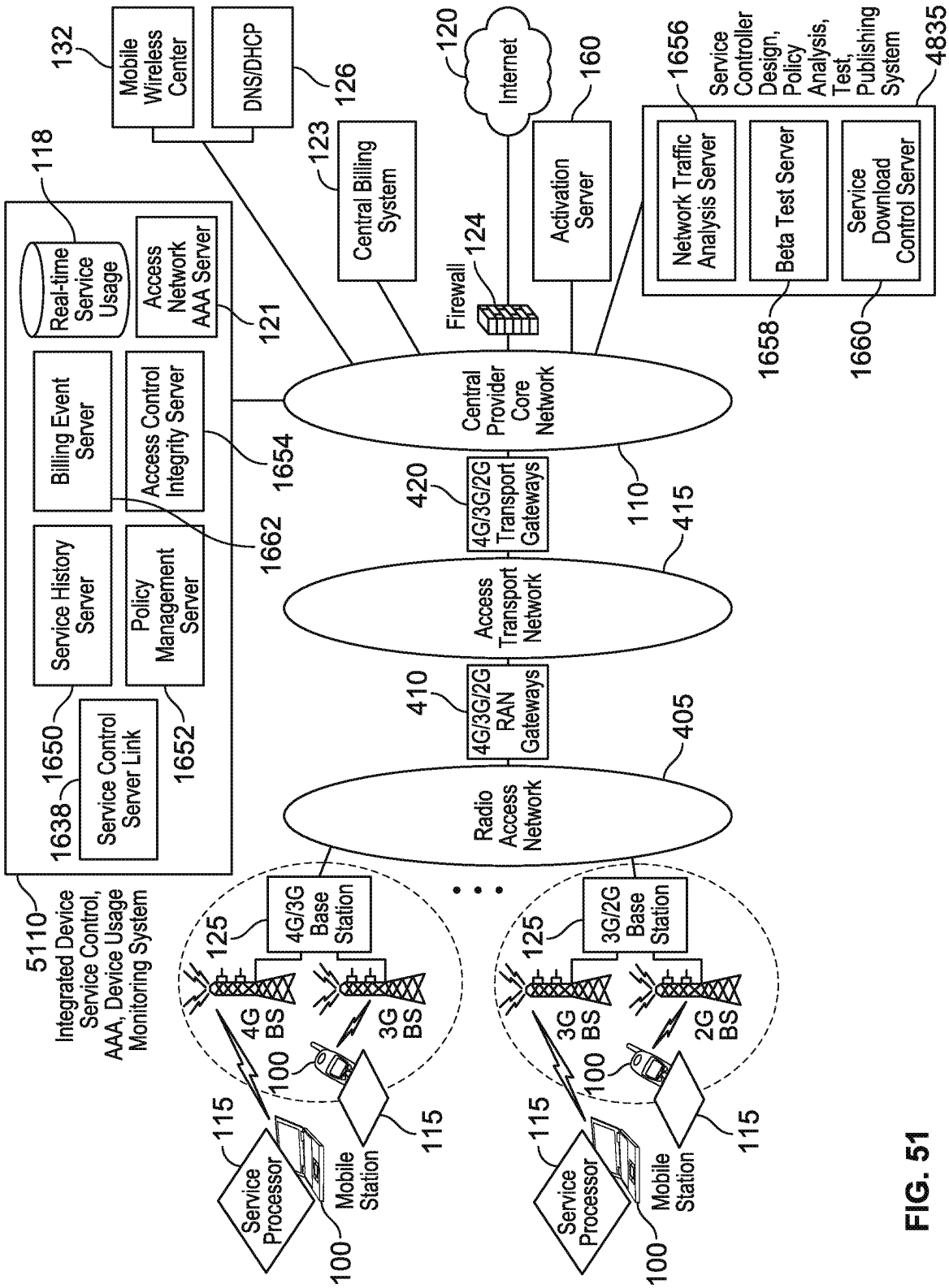

5110
Integrated Device Service Control, AAA, Device Usage Monitoring System
118
Real-time Service Usage
Access Network AAA Server
121
Billing Event Server
Access Control Integrity Server
1654
Service History Server
Policy Management Server
1662
1650
1652
1638
Service Control Server Link
132
Mobile Wireless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

FIG. 51

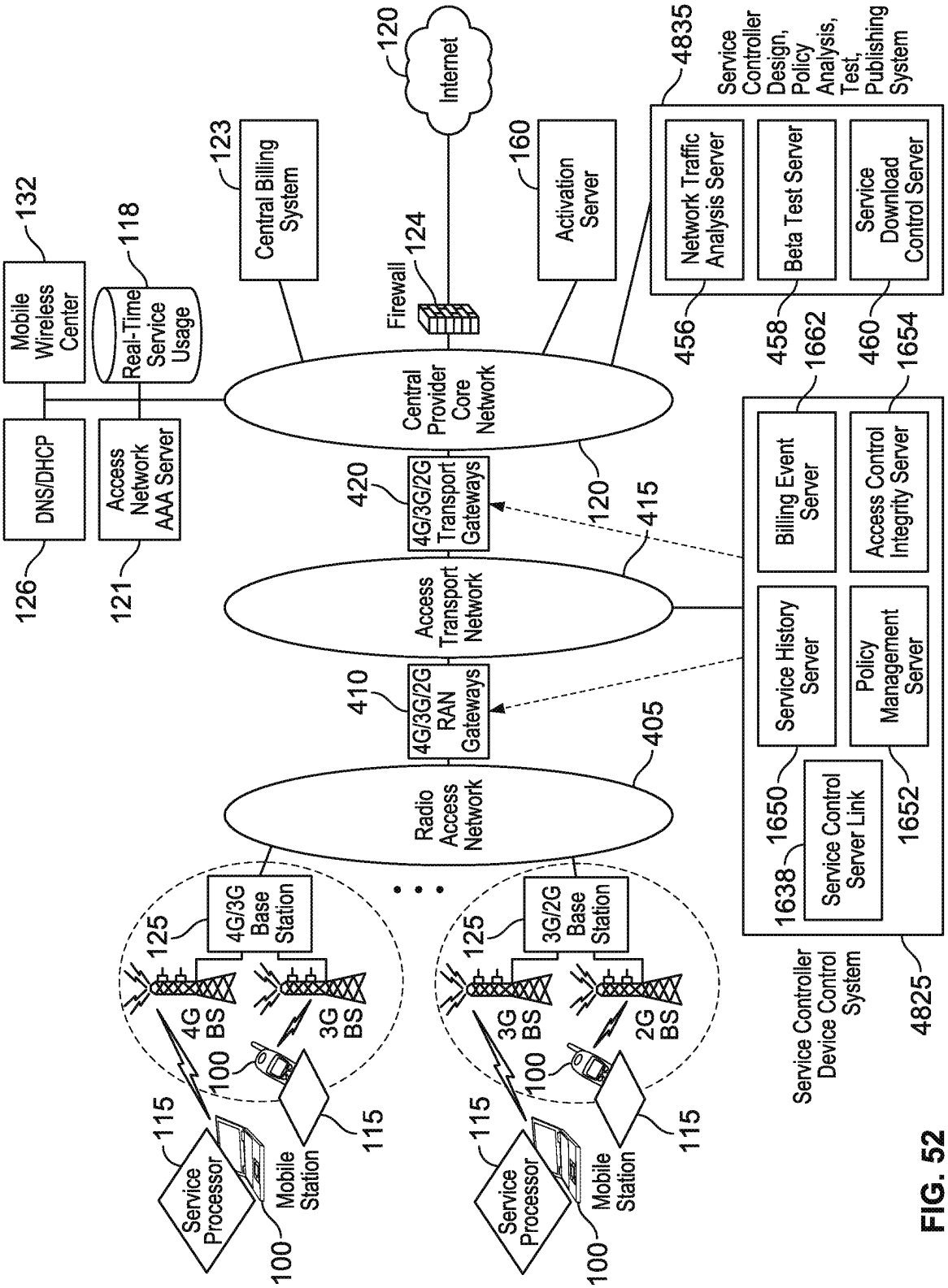

Mobile Wireless Center
132
Real-Time Service Usage
118
Central Billing System
123
Internet
120
Firewall
124
Activation Server
160
Service Controller Design, Policy Analysis, Test, Publishing System
4835
Network Traffic Analysis Server
Beta Test Server
Service Download Control Server
456
458
460
1662
1654
DNS/DHCP
126
Access Network AAA Server
121
Central Provider Core Network
120
4G/3G/2G Transport Gateways
420
415
Billing Event Server
Access Control Integrity Server
Access Transport Network
Service History Server
Policy Management Server
4G/3G/2G RAN Gateways
410
405
Radio Access Network
1650
1652
1638
Service Control Server Link
Service Controller Device Control System
4825
4G/3G Base Station
3G/2G Base Station
125
4G BS
3G BS
3G BS
2G BS
100
115
Service Processor
Mobile Station

FIG. 52

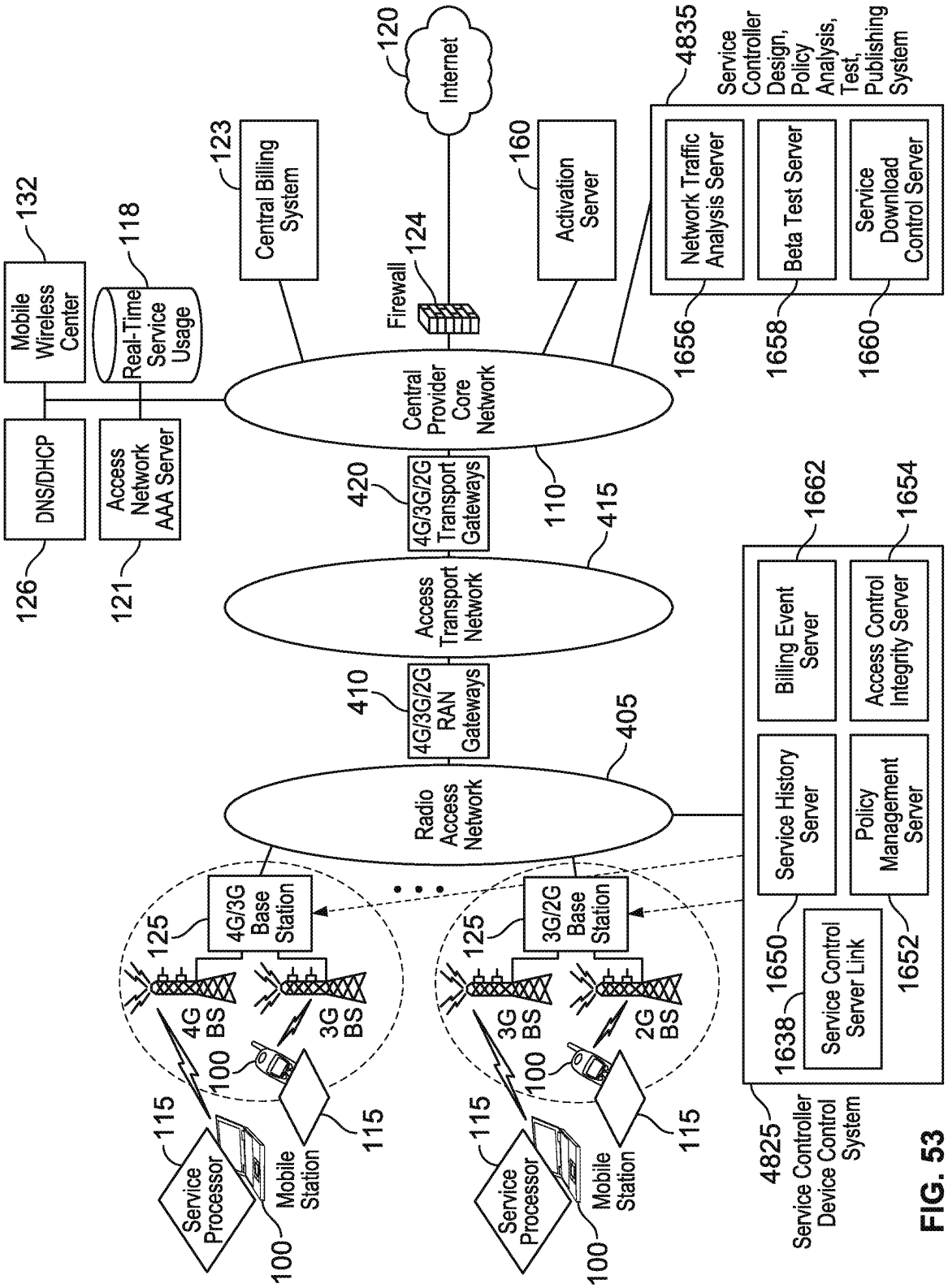

Mobile Wireless Center
132
DNS/DHCP
126
Real-Time Service Usage
118
Access Network AAA Server
121
Central Billing System
123
Internet
120
Firewall
124
Activation Server
160
Central Provider Core Network
110
Network Traffic Analysis Server
1656
Beta Test Server
1658
Service Download Control Server
1660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

FIG. 53

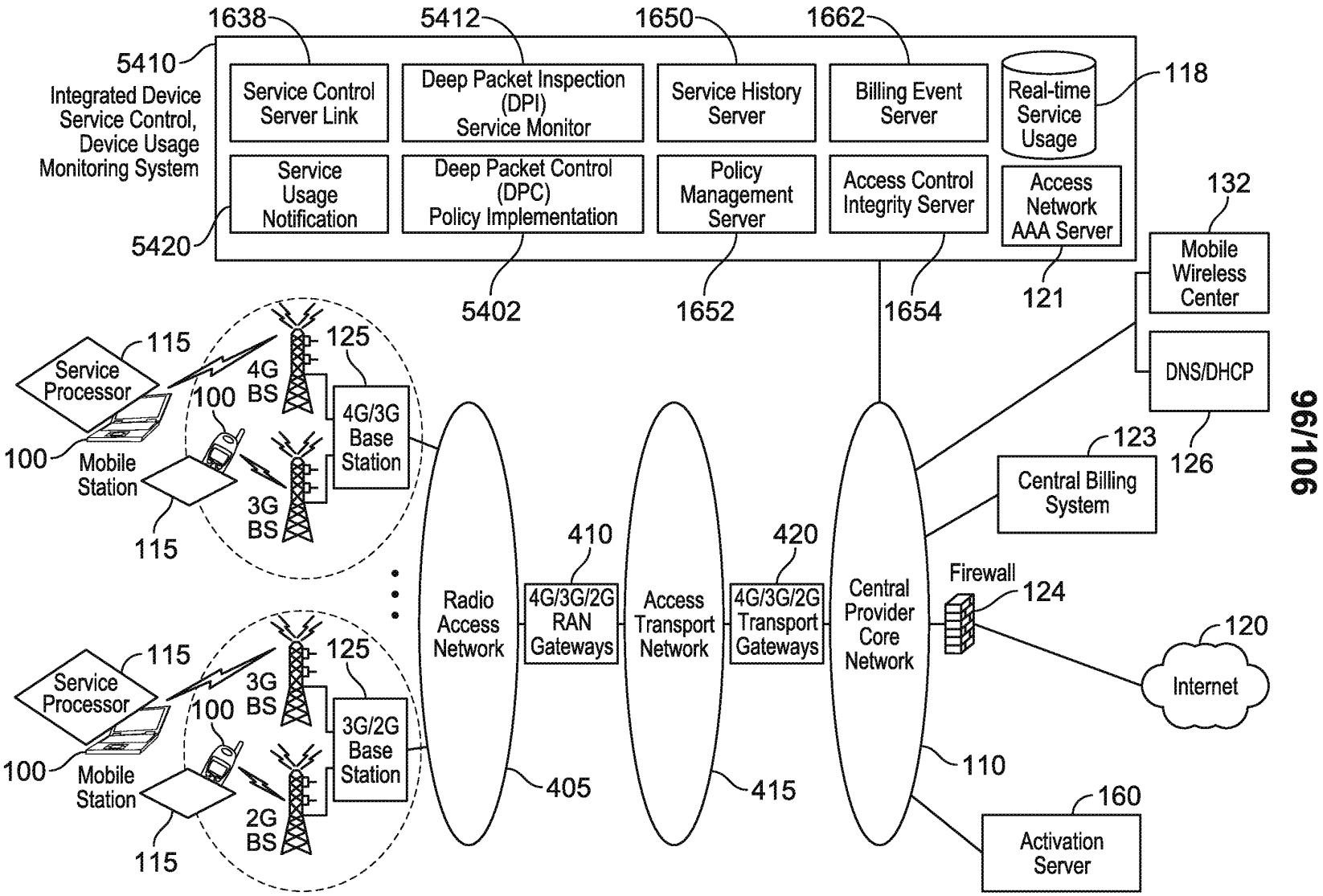


FIG. 54

IPR2025-01571
Apple EX1002 Page 352

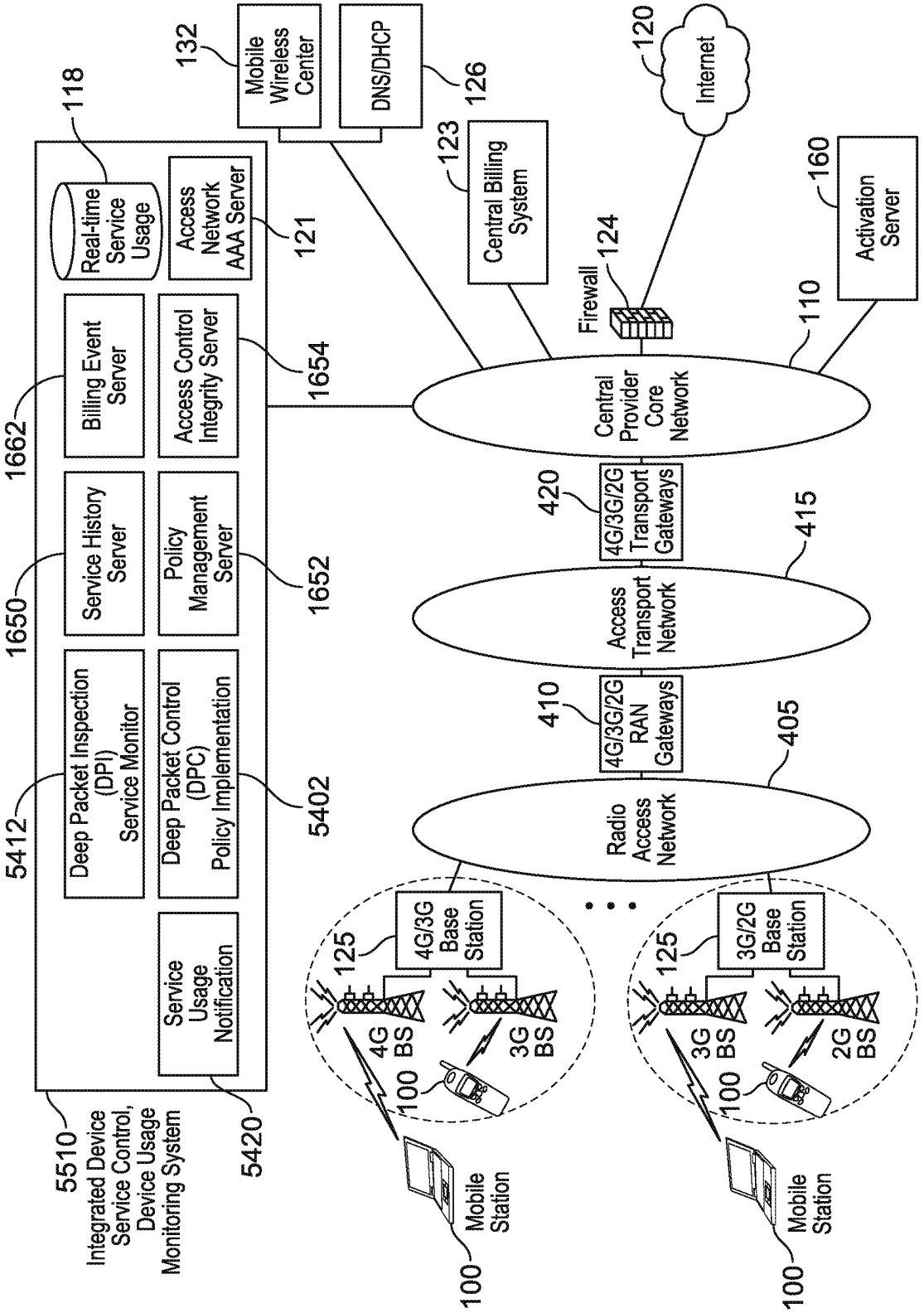

5510
Integrated Device Service Control, Device Usage Monitoring System
5420
5412
Deep Packet Inspection (DPI) Service Monitor
Service Usage Notification
1650
Service History Server
Deep Packet Control (DPC) Policy Implementation
5402
1662
Billing Event Server
Policy Management Server
1652
Access Control Integrity Server
1654
118
Real-time Service Usage
Access Network AAA Server
121
132
Mobile Wireless Center
DNS/DHCP
126
123
Central Billing System
Firewall
124
120
Internet
160
Activation Server
110
Central Provider Core Network
420
4G/3G/2G Transport Gateways
415
Access Transport Network
410
4G/3G/2G RAN Gateways
405
Radio Access Network
125
4G/3G Base Station
4G BS
3G BS
100
Mobile Station
125
3G/2G Base Station
3G BS
2G BS
100
Mobile Station

FIG. 55

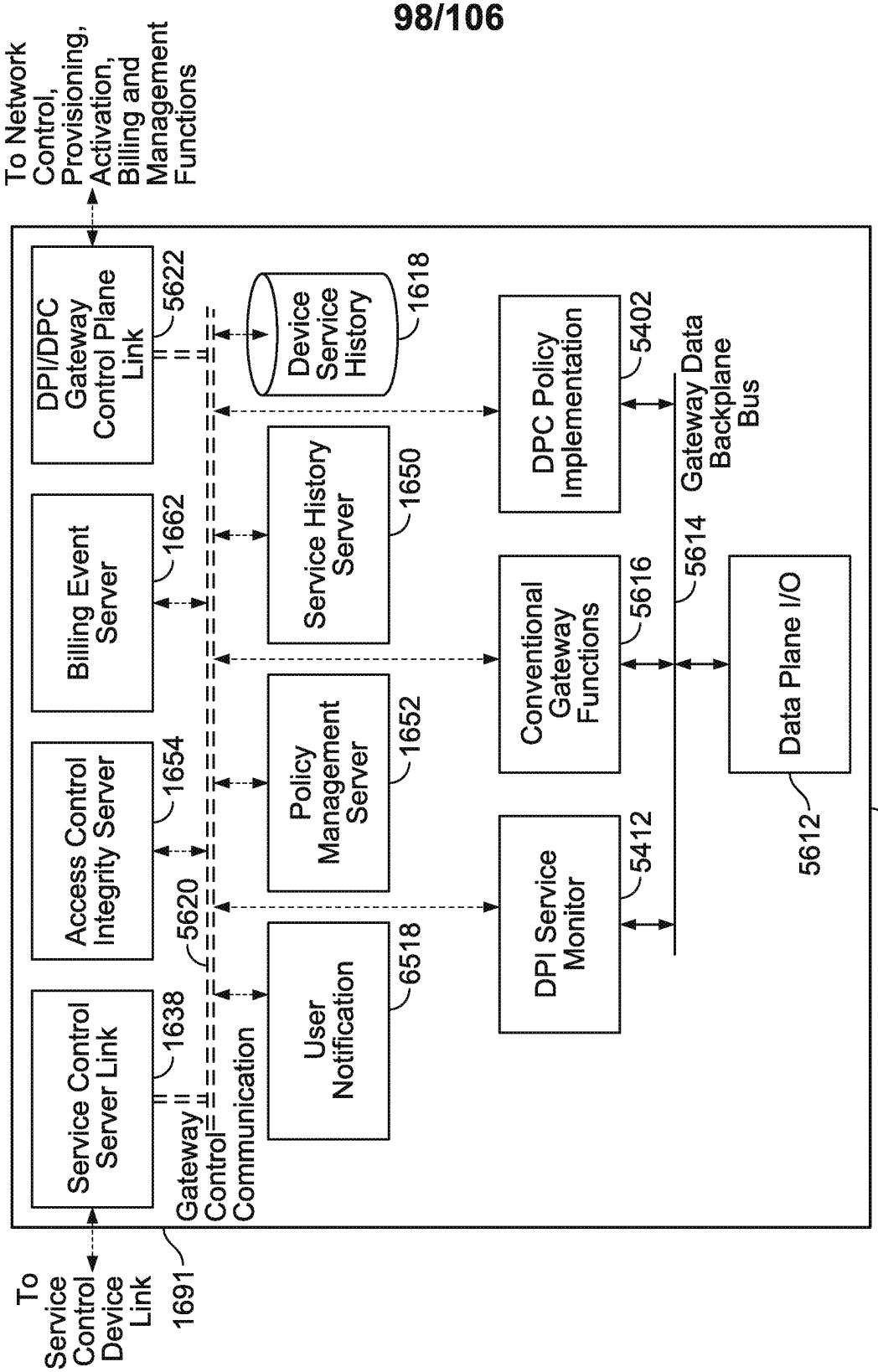

To Network Control, Provisioning, Activation, Billing and Management Functions
To Service Control Device Link
1691
Service Control Server Link
1638
Gateway Control Communication
5620
Access Control Integrity Server
1654
Billing Event Server
1662
DPI/DPC Gateway Control Plane Link
5622
Device Service History
1618
Service History Server
1650
Policy Management Server
1652
User Notification
6518
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
5610

FIG. 56

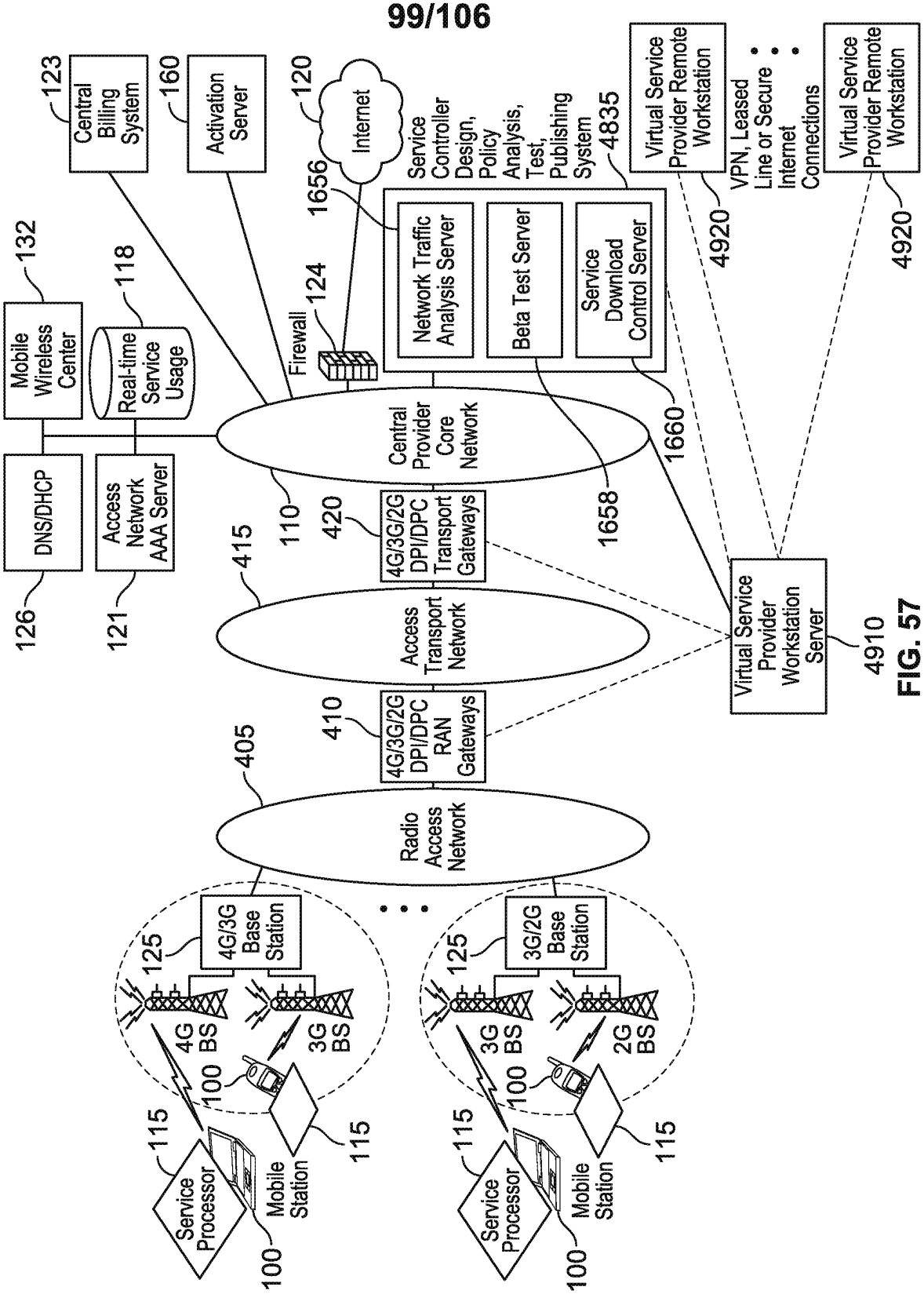

Central Billing System
123
Activation Server
160
Internet
120
Service Controller Design, Policy Analysis, Test, Publishing System
4835
Virtual Service Provider Remote Workstation
VPN, Leased Line or Secure Internet Connections
Virtual Service Provider Remote Workstation
4920
4920
1656
Network Traffic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

FIG. 57

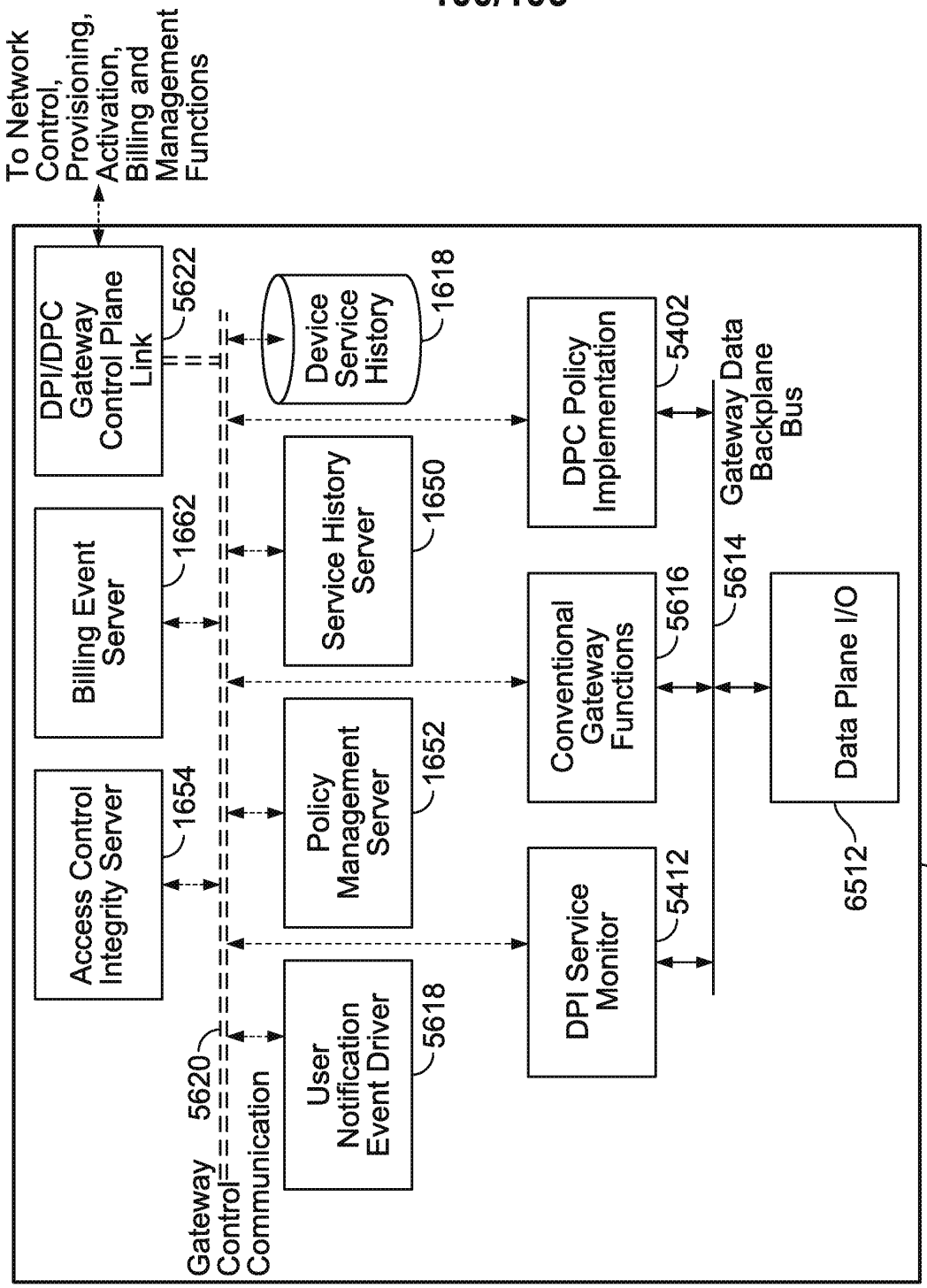

To Network Control, Provisioning, Activation, Billing and Management Functions
DPI/DPC Gateway Control Plane Link
5622
Device Service History
1618
Billing Event Server
1662
Service History Server
1650
DPC Policy Implementation
5402
Gateway Data Backplane Bus
Access Control Integrity Server
1654
Policy Management Server
1652
Conventional Gateway Functions
5616
5614
Data Plane I/O
User Notification Event Driver
5618
DPI Service Monitor
5412
6512
Gateway Control Communication
5620
4G/3G/2G DPI/DPC Gateway
5810

FIG. 58

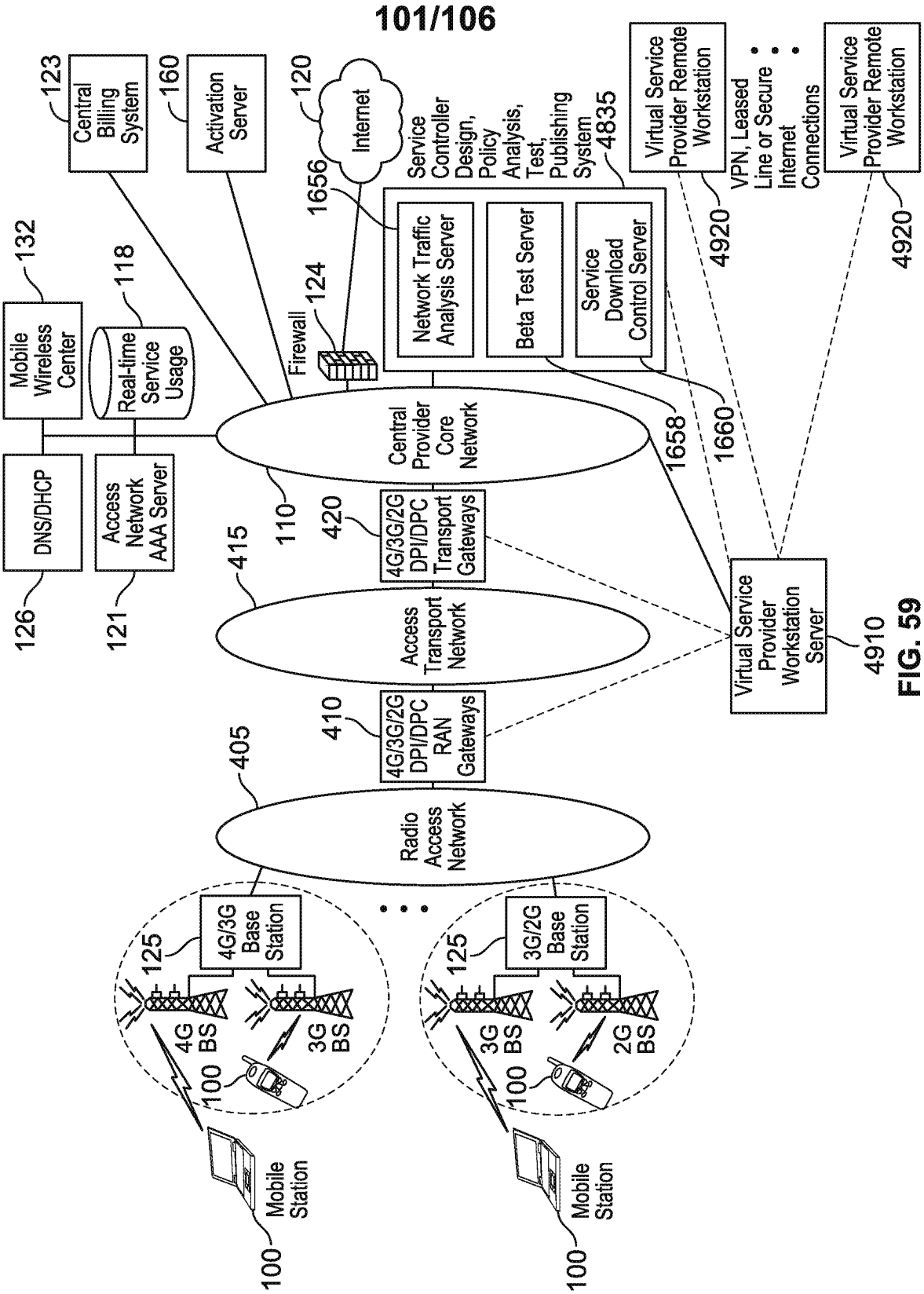

101/106
123
Central Billing System
160
Activation Server
120
Internet
Service Controller Design, Policy Analysis, Test, Publishing System
4835
Virtual Service Provider Remote Workstation
VPN, Leased Line or Secure Internet Connections
Virtual Service Provider Remote Workstation
4920
4920
1656
Network Traffic Analysis Server
Beta Test Server
Service Download Control Server
1658
1660
132
Mobile Wireless Center
118
Real-time Service Usage
Firewall
124
Central Provider Core Network
110
DNS/DHCP
126
Access Network AAA Server
121
420
4G/3G/2G DPI/DPC Transport Gateways
415
Access Transport Network
410
4G/3G/2G DPI/DPC RAN Gateways
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

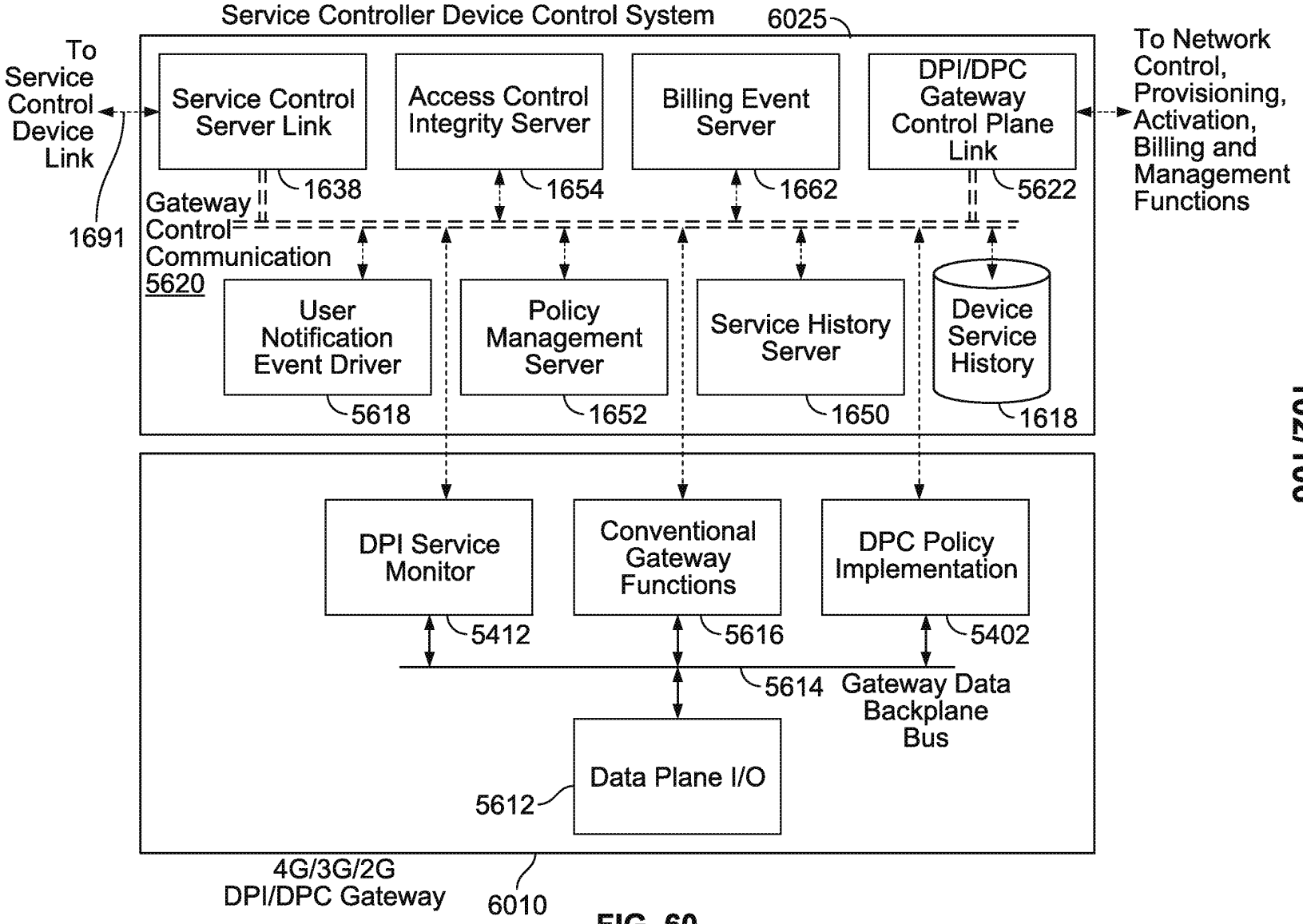


FIG. 60

IPR2025-01571
Apple EX1002 Page 358

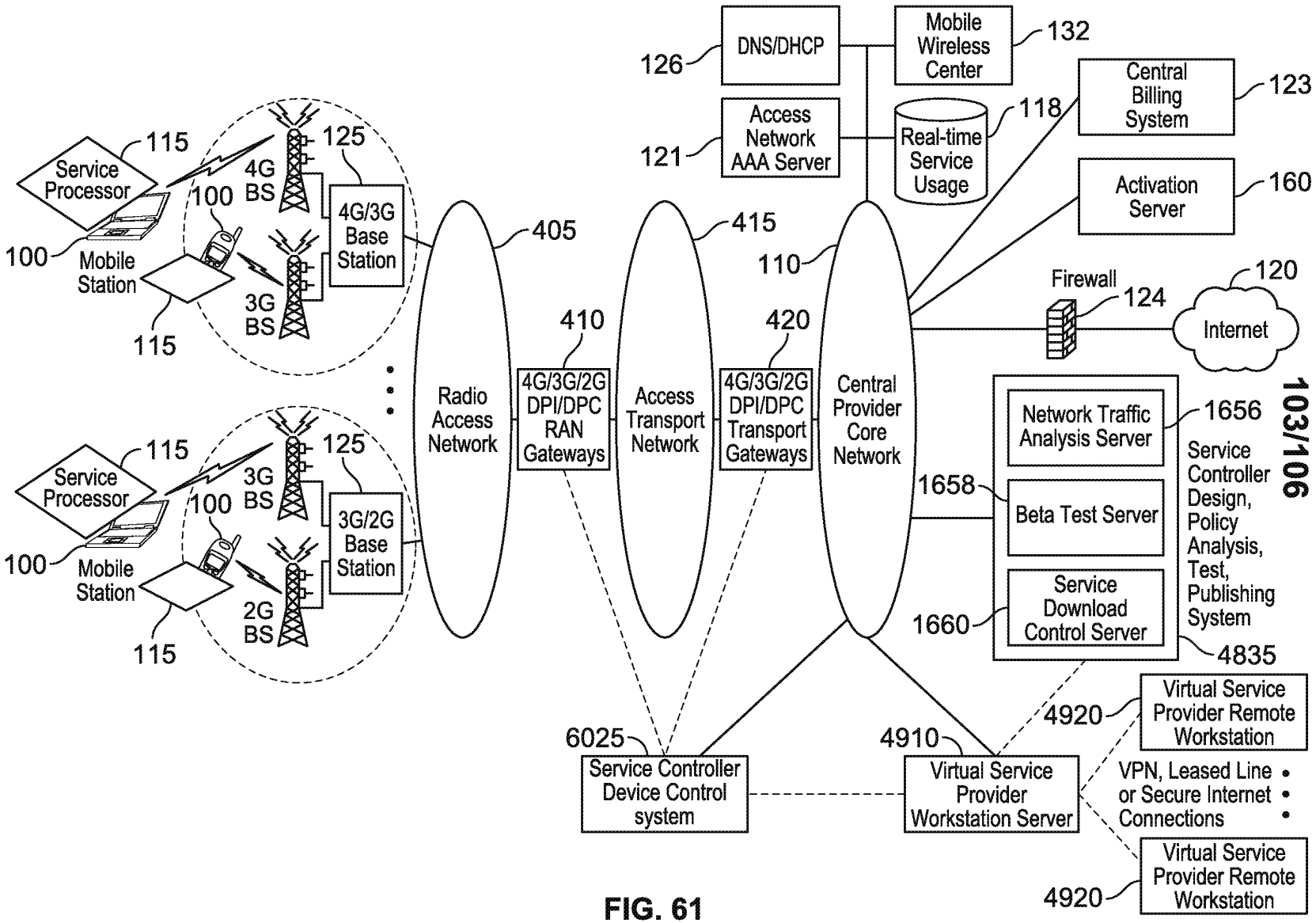


FIG. 61

IPR2025-01571
Apple EX1002 Page 359

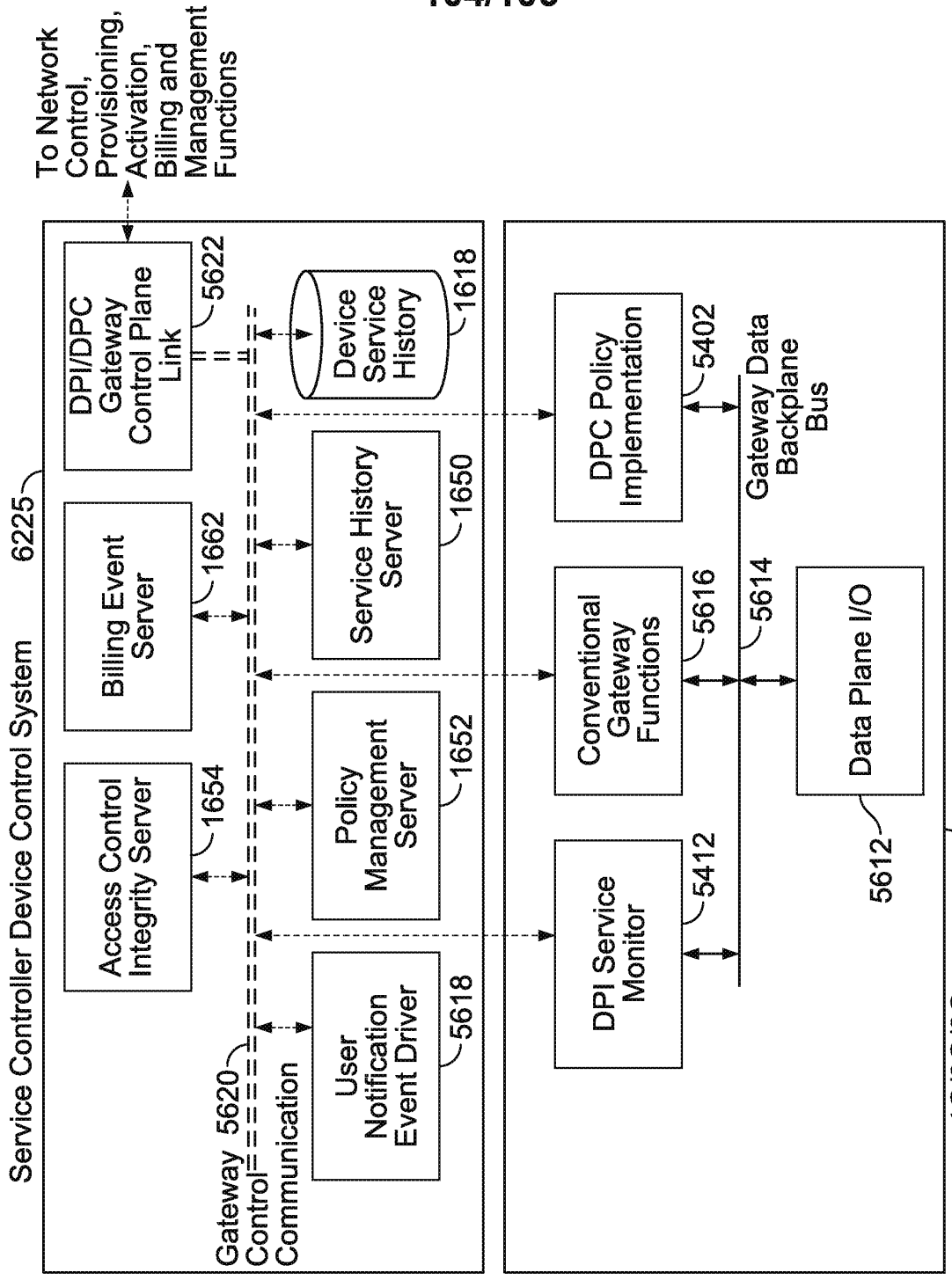

To Network Control, Provisioning, Activation, Billing and Management Functions
Service Controller Device Control System
6225
DPI/DPC Gateway Control Plane Link
5622
Billing Event Server
1662
Service History Server
1650
Device Service History
1618
Access Control Integrity Server
1654
Policy Management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

FIG. 62

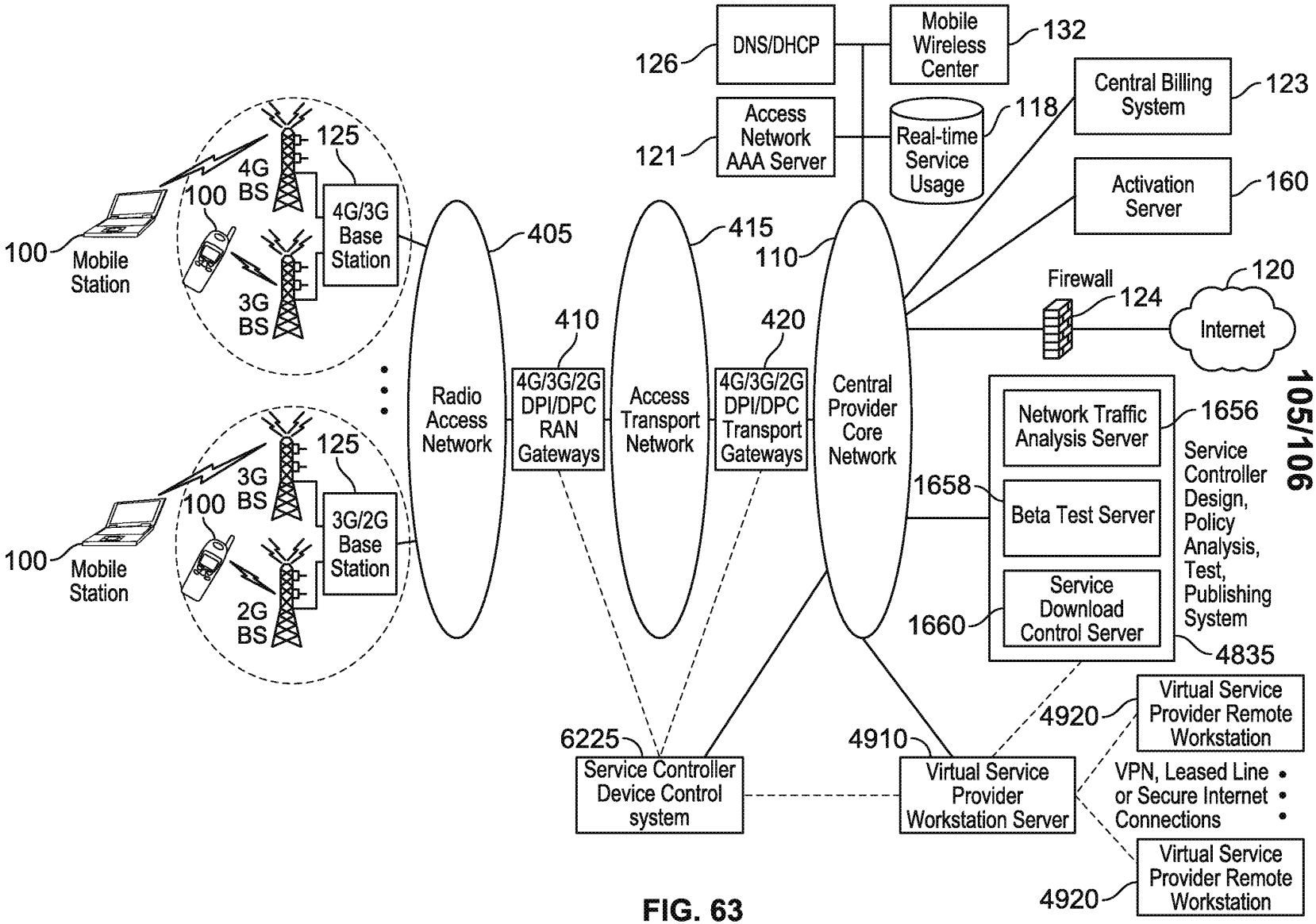


FIG. 63

IPR2025-01571
Apple EX1002 Page 361

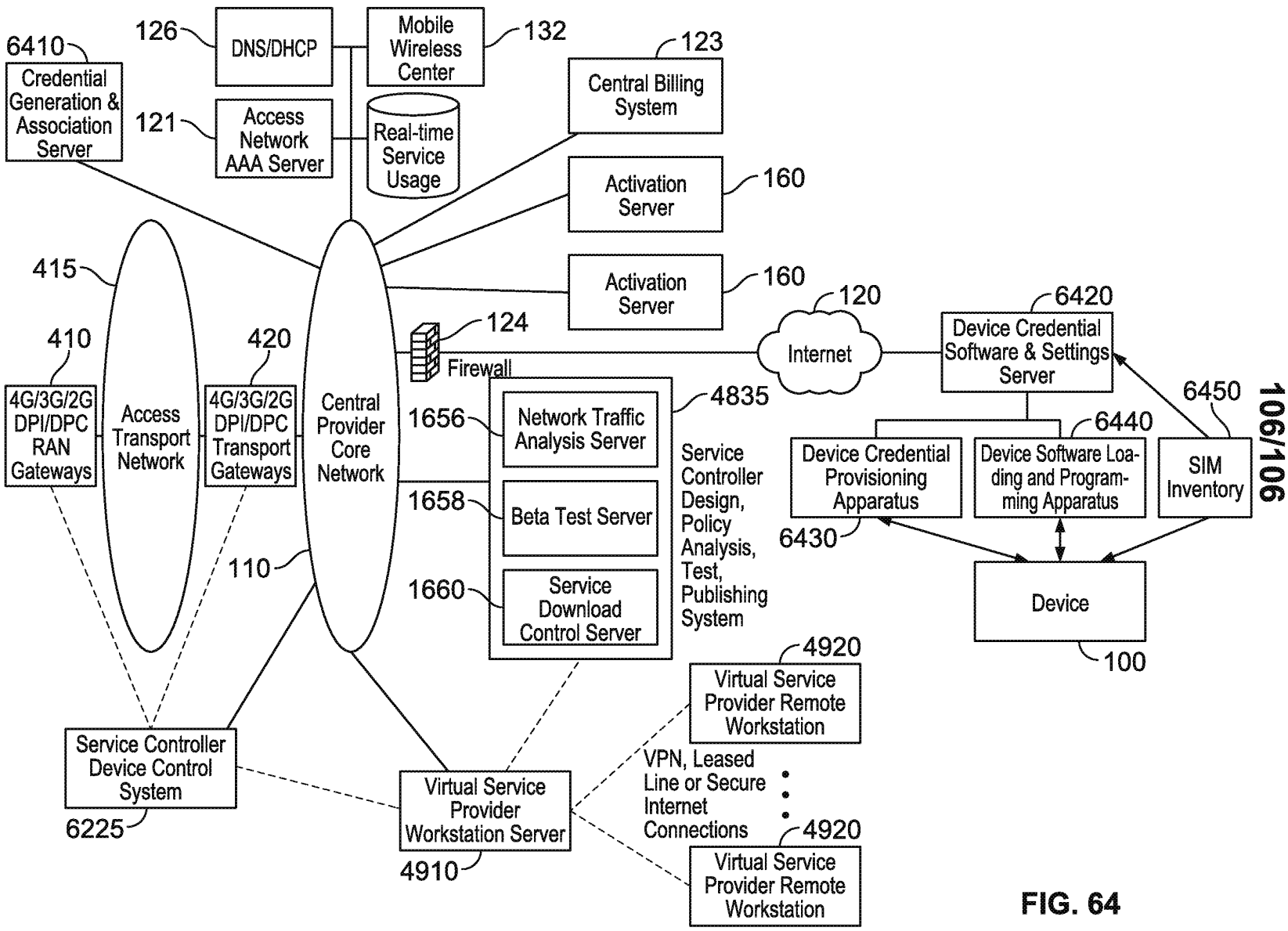


FIG. 64

IPR2025-01571
Apple EX1002 Page 362

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	AUTOMATED DEVICE PROVISIONING AND ACTIVATION

As the below named inventor, I hereby declare that:

This declaration is directed to:

- [■] The attached application, or
- [ ] United States application or PCT international application number _____

filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Gregory G. Raleigh Date (Optional) :_____

Signature: _____

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

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:	Krista Susan Jacobsen/Ann Taylor
Attorney Docket Number:	RALEP007C3
Filed as Small Entity	

Track I Prioritized Examination - Nonprovisional Application under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility filing Fee (Electronic filing)	4011	1	98	98
Utility Search Fee	2111	1	310	310
Utility Examination Fee	2311	1	125	125
Request for Prioritized Examination	2817	1	2400	2400
Pages:				
Utility Appl Size fee per 50 sheets >100	2081	4	160	640
Claims:				
Claims in excess of 20	2202	10	31	310

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous-Filing:				
Publ. Fee- early, voluntary, or normal	1504	1	300	300
Processing Fee, except for Provis. apps	1808	1	130	130
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**4313**

Electronic Acknowledgement Receipt	
EFS ID:	14384014
Application Number:	13705055
International Application Number:	
Confirmation Number:	3375
Title of Invention:	Automated Device Provisioning and Activation
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	Krista Susan Jacobsen/Ann Taylor
Filer Authorized By:	Krista Susan Jacobsen
Attorney Docket Number:	RALEP007C3
Receipt Date:	04-DEC-2012
Filing Date:	
Time Stamp:	19:57:52
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$4313
RAM confirmation Number	7320
Deposit Account	505876
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees) Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees) Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	TrackOne Request	TrackOneRequest.pdf	183120 2824168d3299333501d6d2568d53978df0fad848	no	2
Warnings:					
Information:					
2	Transmittal of New Application	P007C3Trans.pdf	352931 281f403f1920b99c5a4bad10b5b9585b24702ac4	no	1
Warnings:					
Information:					
3	Application Data Sheet	P007C3ADS.pdf	1400761 4de57ef7a862cd656bcbd5408f3de01e363ceaae	no	6
Warnings:					
Information:					
4		RALEP007C3APP.pdf	1217069 cfae338135d5e2e15a9c927c14e42583221bdc95	yes	249

Multipart Description/PDF files in .zip description

Document Description	Start	End
Specification	1	241
Claims	242	248
Abstract	249	249

Warnings:					
Information:					
5	Drawings-only black and white line drawings	Drawings.pdf	8130950 e65dd0d7bc05ea8b58bfa21e993141b11828ce44	no	106
Warnings:					
Information:					
6	Oath or Declaration filed	Declaration.pdf	64660 1550e5d3ba30a1301410b0897f909349c3536677	no	1
Warnings:					

Information:					
7	Fee Worksheet (SB06)	fee-info.pdf	42775 9ff5ab66227edbf65bf231fb806e9fcae2d4f031	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	11392266	

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.

Doc Code: TRACK1.REQ
Document Description: TrackOne Request

PTO/AIA/424 (09-12)

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

First Named Inventor:	Raleigh, Gregory G.	Nonprovisional Application Number (if known):	
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), the prioritized examination fee set forth in 37 CFR 1.17(c), and if not already paid, the publication fee set forth in 37 CFR 1.18(d) have been filed with the request. The basic filing fee, search fee, examination fee, and any required excess claims and application size fees are filed with the request or have been already been paid.

2. The application contains or is amended to contain no more than four independent claims and no more than thirty total claims, and no multiple dependent claims.

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. The executed inventor's oath or declaration is filed with the application. (37 CFR 1.63 and 1.64)

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 /Krista S. Jacobsen/	Date December 4, 2012
Name (Print/Typed) Krista S. Jacobsen	Practitioner Registration Number 59374

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, see below*.*

☐ *Total of _____ forms are submitted.

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.

IPR2025-01571
Apple EX1002 Page 370

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: RALEIGH, Gregory G. Application No.: 13/705,055 Filed: December 4, 2012 Title: Automated Device Provisioning and Activation	Examiner: Not yet assigned Art Unit: 2447 Confirmation No.: 3375

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

PRELIMINARY AMENDMENT

Dear Sir:

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 10.

IPR2025-01571
Apple EX1002 Page 371

AMENDMENTS TO THE SPECIFICATION

In the Abstract:

Please replace the abstract with the following:

-- A method comprising providing a plurality of links to a plurality of end-user devices communicatively coupled to a network system, a particular link of the plurality of links supporting control-plane communications between the network system and a particular end-user device of the plurality of end-user devices over one or more wireless access networks; receiving a message from a server communicatively coupled to the network system, the message comprising payload for delivery to the particular end-user device; generating an encrypted message comprising the payload and an identifier identifying a particular device agent of a plurality of device agents on the particular end-user device, the identifier configured to assist in delivering at least a portion of the payload to the particular device agent on the particular end-user device; and sending the encrypted message to the particular end-user device over the particular link. --

IPR2025-01571
Apple EX1002 Page 372

AMENDMENTS TO THE CLAIMS

Prior to examination, please amend the claims as provided by the following listing of claims, which will replace all previous versions and listings of claims in the application.

1. (Currently Amended) A method performed by a network system, the method comprising:

providing a plurality of service control links to a plurality of end-user devices communicatively coupled to the network system, each service control link secured by an encryption protocol, a particular service control link of the plurality of service control links supporting control-plane communications between the network system and a particular end-user device of the plurality of end-user devices over one or more wireless access networks;

receiving a server message from a particular server of a plurality of servers communicatively coupled to the network system, the server message comprising message payload **for delivery to** ~~**and information identifying a particular device agent of a plurality of device agents on**~~ the particular end-user device;

generating an encrypted message comprising the message payload and an identifier **identifying a particular device agent of a plurality of device agents on the particular end-user device, the identifier** configured to assist in delivering at least a portion of the message payload to the particular device agent on the particular end-user device; and

sending the encrypted message to the particular end-user device over the particular service control link.

2. (Original) The method of claim 1, wherein the particular server comprises a service usage history server, a policy management server, an access control integrity server, a network traffic analysis server, a beta test server, a service download control server, a billing event server, an activation server, a transaction server, an authentication server, or a content management server.

IPR2025-01571
Apple EX1002 Page 373

3. (Original) The method of claim 1, wherein the message payload comprises information associated with a service usage or cost.

4. (Currently amended) The method of claim 3, wherein the information associated with a service usage or cost comprises ~~**one or more of**~~ a service usage value, a projected service usage value, a service usage plan limit, a projected service usage overage warning, a projected service cost overage warning, a service plan period time duration, a service plan time remaining before end of period, **or** ~~**and**~~ information about a service overage.

5. (Original) The method of claim 1, wherein the message payload is based, at least in part, on a user preference.

6. (Original) The method of claim 1, wherein the message payload comprises a service offer, an advertisement, or a transaction offer.

7. (Original) The method of claim 1, wherein the message payload comprises a device agent instruction, a setting, an agent configuration, or a software update for the particular device agent.

8. (Original) The method of claim 1, wherein the message payload comprises information associated with software or a media file.

9. (Original) The method of claim 1, wherein the message payload comprises information associated with a service policy.

10. (Original) The method of claim 1, wherein the message payload comprises an indication of additional data or information available to the particular device agent.

IPR2025-01571
Apple EX1002 Page 374

11. (Original) The method of claim 1, wherein the message payload is configured to assist in causing the particular end-user device to present, through a user interface, information associated with the message payload.

12. (Currently amended) The method of claim 1, wherein the server message is a first server message, and wherein the message payload is a first message payload, and wherein the **identifier** ~~**information**~~ identifying the particular device agent of the plurality of device agents on the particular end-user device is **a** first **identifier** ~~**information**~~, ~~**and wherein the identifier configured to assist the particular end-user device in delivering at least a portion of the message payload to the particular device agent is a first identifier,**~~ and further comprising receiving a second server message from the particular server or from another server of the plurality of servers communicatively coupled to the network system, the second server message comprising second message payload ~~**and second information identifying a second device agent on the particular end-user device, the second device agent being the particular device agent or another device agent of the plurality of device agents on the particular end-user device**~~, and wherein the encrypted message further comprises the second message payload and a second identifier configured to assist in delivering at least a portion of the second message payload to **a** ~~**the**~~ second device agent **on the particular end-user device, the second device agent being the particular device agent or another device agent of the plurality of device agents on the particular end-user device**.

13. (Currently amended) The method of claim 1, wherein the server message is a first server message, and wherein the particular server is a first server, and wherein the message payload is first message payload, and wherein the particular device agent is a first device agent, and wherein the encrypted message is a first encrypted message, and wherein the ~~**agent**~~ identifier is a first ~~**agent**~~ identifier, and further comprising:

receiving a second server message from a second server of the plurality of servers, the second server message comprising second message payload ~~**and**~~

IPR2025-01571
Apple EX1002 Page 375

~~information identifying a second device agent of the plurality of device agents on the particular end-user device~~;

generating a second encrypted message comprising the second message payload and a second ~~agent~~ identifier configured to assist the particular end-user device in delivering the second message payload to **a** ~~the~~ second device agent **of the plurality of device agents on the particular end-user device**; and

sending the second encrypted message to the particular end-user device over the particular service control link.

14. (Original) The method of claim 1, wherein the particular service control link supports asynchronous transmissions by the network system.

15. (Original) The method of claim 1, further comprising sending a credential, a certificate, or a token to the particular end-user device or obtaining the credential, the certificate, or the token from the particular end-user device during a service authorization sequence.

16. (Currently amended) The method of claim 15, wherein the credential comprises ~~one or more of~~ a phone number, an identification number, a security signature, a security credential, a subscriber identity module (SIM) identifier, a mobile equipment identifier (MEID), **or** ~~and~~ a device identifier.

17. (Original) The method of claim 1, wherein the particular device agent comprises software.

18. (Original) The method of claim 1, further comprising:

triggering a transmission to maintain the particular service control link when a time since sending the encrypted message to the particular end-user device would otherwise cause the particular service control link to terminate, and

determining when to send the encrypted message to the particular end-user device.

IPR2025-01571
Apple EX1002 Page 376

19. (Original) The method of claim 1, wherein the sending the encrypted message to the particular end-user device over the particular service control link is not based on whether the particular device agent is running on the particular end-user device.

20. (Original) The method of claim 1, wherein at least one of the plurality of servers comprises a content transaction server configured to provide an electronic commerce offering and transaction platform to the particular end-user device.

21. (Original) The method of claim 20, further comprising including one or more third party transaction bills on a central provider bill.

22. (Currently amended) The method of claim 1, wherein a transmission over the particular service control link is within an ambient service**, the ambient service provided at no cost to a user or a subscriber associated with the particular end-user device**.

23. (Original) The method of claim 1, wherein the plurality of service control links enables a particular server of the plurality of servers to push the message payload to a selected one of the plurality of device agents on any one of the plurality of end-user devices.

24. (Original) The method of claim 1, wherein the particular service control link is configured to support control-plane communications using an Internet protocol.

25. (Original) The method of claim 1, wherein providing the plurality of service control links to the plurality of end-user devices comprises providing the plurality of service control links to a plurality of service control device link agents, each service control device link agent on one of the plurality of end-user devices, a particular service control device link agent on the particular end-user device for delivering agent messages over an agent communication bus to at least one of the plurality of device agents on the particular end-user device.

IPR2025-01571
Apple EX1002 Page 377

26. (Original) The method of claim 25, wherein the encrypted message is a first encrypted message, and wherein the identifier is configured to assist the particular service control device link agent in generating a second encrypted message for delivery to the particular device agent, the second encrypted message comprising the at least a portion of the message payload.

27. (Currently amended) A network system comprising:

means for providing a plurality of service control links to a plurality of end-user devices communicatively coupled to the network system, each service control link secured by an encryption protocol, a particular service control link of the plurality of service control links supporting control-plane communications between the network system and a particular end-user device of the plurality of end-user devices over one or more wireless access networks;

means for receiving a server message from a particular server of a plurality of servers communicatively coupled to the network system, the server message comprising message payload **~~and information identifying a particular device agent of a plurality of device agents on the particular end-user device~~**;

means for generating an encrypted message comprising the message payload and an identifier **identifying a particular device agent of a plurality of device agents on the particular end-user device, the identifier** configured to assist in delivering at least a portion of the message payload to the particular device agent on the particular end-user device; and

means for sending the encrypted message to the particular end-user device over the particular service control link.

28. (Currently amended) A non-transitory computer-readable storage medium storing program code for causing **one or more processors** **~~a computer~~** to execute a method comprising:

providing a plurality of service control links to a plurality of end-user devices communicatively coupled to the computer, each service control link secured

IPR2025-01571
Apple EX1002 Page 378

by an encryption protocol, a particular service control link of the plurality of service control links supporting control-plane communications between the computer and a particular end-user device of the plurality of end-user devices over one or more wireless access networks;

receiving a server message from a particular server of a plurality of servers communicatively coupled to the computer, the server message comprising message payload ~~**and information identifying a particular device agent of a plurality of device agents on the particular end-user device**~~;

generating an encrypted message comprising the message payload and an identifier **identifying a particular device agent of a plurality of device agents on the particular end-user device** configured to assist in delivering at least a portion of the message payload to the particular device agent on the particular end-user device; and

sending the encrypted message to the particular end-user device over the particular service control link.

29. (Original) The non-transitory computer-readable storage medium recited in claim 28, wherein providing the plurality of service control links to the plurality of end-user devices comprises providing the plurality of service control links to a plurality of service control device link agents, each service control device link agent on a different one of the plurality of end-user devices, a particular service control device link agent on the particular end-user device for delivering agent messages over an agent communication bus to at least one of the plurality of device agents on the particular end-user device.

30. (Original) The non-transitory computer-readable storage medium recited in claim 28, wherein the message payload is configured to assist in causing the particular end-user device to present, through a user interface, information associated with the message payload.

IPR2025-01571
Apple EX1002 Page 379

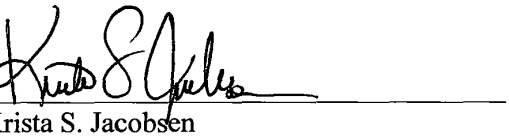
REMARKS

Claims 1-30 are pending. Claims 1, 4, 12, 13, 16, 22, 27, and 28 are being amended herein. No new matter is being added.

This preliminary amendment is presented before any office action. Thus, Applicant respectfully requests that the preliminary amendment provided herein be entered.

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.

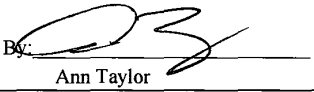
Respectfully submitted,

Date: December 11, 2012 By: 

Krista S. Jacobsen
Reg. No. 59,374
Head Counsel
Headwater Partners I LLC
350 Marine Parkway, Suite 300
Redwood Shores, CA 94065
(650) 517-2798

CERTIFICATE OF ELECTRONIC TRANSMISSION

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being filed electronically via EFS-Web addressed to the Commissioner for Patents on:

Date: Dec. 11, 2012 By: 
Ann Taylor

IPR2025-01571
Apple EX1002 Page 380

Electronic Acknowledgement Receipt	
EFS ID:	14442714
Application Number:	13705055
International Application Number:	
Confirmation Number:	3375
Title of Invention:	AUTOMATED DEVICE PROVISIONING AND ACTIVATION
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	Krista Susan Jacobsen/Ann Taylor
Filer Authorized By:	Krista Susan Jacobsen
Attorney Docket Number:	RALEP007C3
Receipt Date:	11-DEC-2012
Filing Date:	
Time Stamp:	21:05:46
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	Transmittal Letter	P007C3Trans.pdf	297409 56df6239bb1721493ee378487beb496c63b fe88d	no	1
Warnings:					
Information:					

2		P007C3PrelAmd.pdf	301094 52fc6a5229338d472c050df6b1e2d368fad95230	yes	10

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Preliminary Amendment	1	1
	Abstract	2	2
	Claims	3	9
	Applicant Arguments/Remarks Made in an Amendment	10	10

Warnings:	
Information:	
Total Files Size (in bytes):	598503

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.

Doc Code: TRAN.LET

Document Description: Transmittal Letter

PTO/SB/21 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission	11

Application Number	13/705,055
Filing Date	2012-12-04
First Named Inventor	Gregory G. Raleigh
Art Unit	2447 Conf. No. 3375
Examiner Name	not yet assigned
Attorney Docket Number	RALEP007C3

ENCLOSURES *(Check all that apply)*

- ☐ Fee Transmittal Form
  - ☐ Fee Attached
- ☑ Amendment/Reply
  - ☐ After Final
  - ☐ Affidavits/declaration(s)
- ☐ Extension of Time Request
- ☐ Express Abandonment Request
- ☐ Information Disclosure Statement
- ☐ Certified Copy of Priority Document(s)
- ☐ Reply to Missing Parts/ Incomplete Application
  - ☐ Reply to Missing Parts under 37 CFR 1.52 or 1.53
- ☐ Drawing(s)
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert to a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s) _____
  - ☐ Landscape Table on CD
- ☐ After Allowance Communication to TC
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☐ Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- ☐ Proprietary Information
- ☐ Status Letter
- ☐ Other Enclosure(s) (please Identify below):

Remarks

You are hereby authorized to charge any additional fee required or credit any overpayment to Deposit Account No. 50-5876.

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	Headwater Partners I LLC		
Signature			
Printed name	Krista S. Jacobsen		
Date	December 11, 2012	Reg. No.	59374

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature			
Typed or printed name	Ann Taylor	Date	December 11, 2012

This collection of information is required by 37 CFR 1.5. 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 and1.14. This collection is estimated to 2 hours 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/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
350 Marine Parkway, Suite 300
Redwood Shores, CA 94065 U.S.A.

A copy of this form, together with a statement under 37 CFR 3.73(c) (Form PTO/AIA/96 or equivalent) is required to be filed in each application in which this form is used. The statement under 37 CFR 3.73(c) may be completed by one of the practitioners appointed in this form, and must identify the application in which this Power of Attorney is to be filed.

SIGNATURE of Assignee of Record
The individual whose signature and title is supplied below is authorized to act on behalf of the assignee

Signature		Date	10-5-2012
Name	Gregory G. Raleigh	Telephone	650-517-2781
Title	Manager		

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.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Examiner:
Gregory G. Raleigh	Not yet assigned
Serial No. 13/705,055	Art Unit: 2447
Filed: December 4, 2012	Conf. No.: 3375

Title: Automated Device Provisioning and Activation

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

INFORMATION DISCLOSURE STATEMENT

Sir:

The references cited on attached form PTO/SB/08A are being called to the attention of the Examiner. Copies of the references are not enclosed.

In accordance with 37 CFR §1.98(d), copies of the references can be found in related U.S. Patent Application No. 12/380,780, filed March 2, 2009.

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.

IPR2025-01571
Apple EX1002 Page 385

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: December 12, 2012

By: _____

Krista S. Jacobsen
Reg. No. 59,374
Head Counsel
Headwater Partners I LLC
350 Marine Parkway, Suite 300
Redwood Shores, CA 94065
(650) 517-2798

CERTIFICATE OF ELECTRONIC TRANSMISSION

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being filed electronically via EFS-Web addressed to the Commissioner for Patents on:

Date: December 12, 2012 By: _____
Ann Taylor

IPR2025-01571
Apple EX1002 Page 386

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	13705055
Filing Date	2012-12-04
First Named Inventor	Raleigh, Gregory G.
Art Unit	2447
Examiner Name	not yet assigned
Attorney Docket Number	RALEP007C3

U.S.PATENTS

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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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.	

IPR2025-01571
Apple EX1002 Page 399

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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		2012-09-26	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

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

IPR2025-01571
Apple EX1002 Page 404

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

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.

FOREIGN PATENT DOCUMENTS

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	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		☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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		☐
	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.		☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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		☐
	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		☐

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

NON-PATENT LITERATURE DOCUMENTS

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

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	☐
	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	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	☐
	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	☐

IPR2025-01571
Apple EX1002 Page 409

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	☐

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

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.

IPR2025-01571
Apple EX1002 Page 410

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

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		Date (YYYY-MM-DD)	2012-12-12
Name/Print	Krista S. Jacobsen	Registration Number	59374

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.**

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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

U.S.PATENTS

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.

U.S.PATENT APPLICATION PUBLICATIONS

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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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.	

IPR2025-01571
Apple EX1002 Page 418

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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.	

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

FOREIGN PATENT DOCUMENTS

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

NON-PATENT LITERATURE DOCUMENTS

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

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

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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

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).

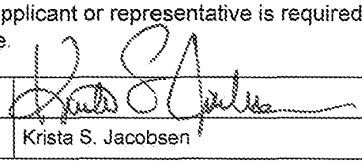
☐ See attached certification statement.

☐ 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		Date (YYYY-MM-DD)	2012-12-12
Name/Print	Krista S. Jacobsen	Registration Number	59374

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.**

Electronic Acknowledgement Receipt	
EFS ID:	14453565
Application Number:	13705055
International Application Number:	
Confirmation Number:	3375
Title of Invention:	AUTOMATED DEVICE PROVISIONING AND ACTIVATION
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	Krista Susan Jacobsen/Ann Taylor
Filer Authorized By:	Krista Susan Jacobsen
Attorney Docket Number:	RALEP007C3
Receipt Date:	12-DEC-2012
Filing Date:	
Time Stamp:	18:35:11
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal Letter	P007C3Trans.pdf	301102 2415db01272af5c3c59cc603a1cd975c257e974b	no	1
Warnings:					
Information:					

2	Assignee showing of ownership per 37 CFR 3.73.	P007C3Stmt.pdf	499551 87afd893266465b316631f059866ead10196c6fc	no	2
Warnings:					
Information:					
3	Power of Attorney	P007C3POA.pdf	65650 619528167e8b20bd6b9592faf4145906b3e637c7	no	1
Warnings:					
Information:					
4	Transmittal Letter	P007C3IDSLtr.pdf	312678 28a3a02ba4f8ea84283d5be29a36dd82d62e8d76	no	2
Warnings:					
Information:					
5	Information Disclosure Statement (IDS) Form (SB08)	P007C3IDS1.pdf	5072084 b5d352c0abd6d983dec48fd6f673003b3a0da453	no	25
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
6	Information Disclosure Statement (IDS) Form (SB08)	P007C3IDS2.pdf	4336849 4cb65fb62ee5ff6d4c0e8a78912f50e92ae402e0	no	22
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
		Total Files Size (in bytes):	10587914		

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.

Doc Code: TRAN.LET

Document Description: Transmittal Letter

PTO/SB/21 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission	53

Application Number	13/705,055
Filing Date	2012-12-04
First Named Inventor	Gregory G. Raleigh
Art Unit	2447 Conf. No. 3375
Examiner Name	not yet assigned
Attorney Docket Number	RALEP007C3

ENCLOSURES *(Check all that apply)*

- ☐ Fee Transmittal Form
  - ☐ Fee Attached
- ☐ Amendment/Reply
  - ☐ After Final
  - ☐ Affidavits/declaration(s)
- ☐ Extension of Time Request
- ☐ Express Abandonment Request
- ☑ Information Disclosure Statement
- ☐ Certified Copy of Priority Document(s)
- ☐ Reply to Missing Parts/ Incomplete Application
  - ☐ Reply to Missing Parts under 37 CFR 1.52 or 1.53
- ☐ Drawing(s)
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert to a Provisional Application
- ☑ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s) _____
  - ☐ Landscape Table on CD
- ☐ After Allowance Communication to TC
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☐ Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- ☐ Proprietary Information
- ☐ Status Letter
- ☑ Other Enclosure(s) (please Identify below):
  Statement Under 37 CFR 3.73(c)

Remarks

You are hereby authorized to charge any additional fee required or credit any overpayment to Deposit Account No. 50-5876.

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	Headwater Partners I, LLC		
Signature			
Printed name	Krista S. Jacobsen		
Date	December 12, 2012	Reg. No.	59374

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature			
Typed or printed name	Ann Taylor	Date	December 12, 2012

This collection of information is required by 37 CFR 1.5. 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 and1.14. This collection is estimated to 2 hours 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)

Applicant/Patent Owner: Gregory G. Raleigh

Application No./Patent No.: 13/705,055 Filed/Issue Date: December 4, 2012

Titled: Automated Device Provisioning and Activation

Headwater Partners I LLC, a limited liability corporation

(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 029429, Frame 0983, 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.

Signature	December 12, 2012 Date
Krista S. Jacobsen Printed or Typed Name	59374 Title or Registration Number

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 13/705,055

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	98		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	310		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	125		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	30 minus 20 =	* 10	x 31 =	310	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*	x 125 =	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).			640			
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	1483		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($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

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

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

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

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/705,055	12/04/2012	Gregory G. Raleigh	RALEP007C3

CONFIRMATION NO. 3375

106963
Headwater Partners I LLC
350 Marine Parkway, Suite 300
Redwood Shores, CA 94065

POA ACCEPTANCE LETTER

OC000000058433040

Date Mailed: 01/09/2013

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 12/12/2012.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

/eerido/

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
13/705,055	12/04/2012	2447	1783	RALEP007C3	30	3

CONFIRMATION NO. 3375

106963
Headwater Partners I LLC
350 Marine Parkway, Suite 300
Redwood Shores, CA 94065

FILING RECEIPT

OC000000058452943

Date Mailed: 01/09/2013

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

Inventor(s)

Gregory G. Raleigh, Woodside, CA;

Applicant(s)

Headwater Partners I LLC, Redwood Shores, CA

Assignment For Published Patent Application

Headwater Partners I LLC, Redwood Shores, CA

Power of Attorney: The patent practitioners associated with Customer Number 106963

Domestic Priority data as claimed by applicant

This application is a CON of 12/380,780 03/02/2009
which claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009

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

Permission to Access - A proper **Authorization to Permit Access to Application by Participating Offices** (PTO/SB/39 or its equivalent) has been received by the USPTO.

If Required, Foreign Filing License Granted: 01/02/2013

IPR2025-01571
Apple EX1002 Page 441

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/705,055**

Projected Publication Date: 04/18/2013

Non-Publication Request: No

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

AUTOMATED DEVICE PROVISIONING AND ACTIVATION

Preliminary Class

709

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

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

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

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

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

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

IPR2025-01571
Apple EX1002 Page 442

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

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

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

NOT GRANTED

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

SelectUSA

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

Headwater Partners I LLC
350 Marine Parkway, Suite 300
Redwood Shores CA 94065

MAILED
JAN 10 2013
OFFICE OF PETITIONS

Doc Code: TRACK1.GRANT

Decision Granting Request for Prioritized Examination (Track I or After RCE)	Application No.: 13/705,055

1. THE REQUEST FILED December 4, 2012 IS **GRANTED.**

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

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

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

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

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

/Brian W. Brown/
[*Signature*]

Petitions Examiner, Office of Petitions
(Title)

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	13705055
Filing Date	2012-12-04
First Named Inventor	Raleigh, Gregory G.
Art Unit	2447
Examiner Name	not yet assigned
Attorney Docket Number	RALEP007C3

U.S.PATENTS

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	7957020		2011-06-07	Mine, Ryuta et al.	
	2	7346410		2008-03-18	Uchiyama, Kenji	
	3	7167078		2007-01-23	Pourchot, Shawn C.	
	4	8102814		2012-01-24	Rahman, Shahriar I. et al.	
	5	7970350		2011-06-28	Sheynman, Arnold et al.	
	6	8094551		2012-01-10	Huber, Kurt Donald et al.	

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

U.S.PATENT APPLICATION PUBLICATIONS

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	1	20010053694		2001-12-20	Igarashi, Yoichiro et al.	
	2	20100041364		2010-02-18	Lott, Robert Wayne et al.	
	3	20100027469		2010-02-04	Gurajala, Ravindra Babu et al.	

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

FOREIGN PATENT DOCUMENTS

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

NON-PATENT LITERATURE DOCUMENTS

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

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.

EFS Web 2.1.17

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

[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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

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).

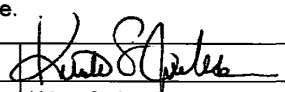
☐ See attached certification statement.

☐ 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		Date (YYYY-MM-DD)	2013-01-22
Name/Print	Krista S. Jacobsen	Registration Number	59374

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.**

Electronic Acknowledgement Receipt	
EFS ID:	14763936
Application Number:	13705055
International Application Number:	
Confirmation Number:	3375
Title of Invention:	AUTOMATED DEVICE PROVISIONING AND ACTIVATION
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	Krista Susan Jacobsen/Ann Taylor
Filer Authorized By:	Krista Susan Jacobsen
Attorney Docket Number:	RALEP007C3
Receipt Date:	22-JAN-2013
Filing Date:	04-DEC-2012
Time Stamp:	20:50:41
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	P007C3IDS.pdf	805746 43e4c6c573bbf8cca11202f98f84d6b2aeeb1fd0	no	4

Warnings:
Information:

This is not an USPTO supplied IDS fillable form	
Total Files Size (in bytes):	805746

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

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

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

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

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

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

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

Application Number	13705055
Filing Date	2012-12-04
First Named Inventor	Raleigh, Gregory G.
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP007C3

U.S.PATENTS

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	8135388		2012-03-13	Gailloux, Michael A. et al.	
	2	6947723		2005-09-20	Gurnani, Roger et al.	
	3	8350700		2013-01-08	Fast, Raymond D. et al.	
	4	8204190		2012-06-19	Bang, Jung-Hee et al.	
	5	7962622		2011-06-14	Friend, John et al.	
	6	7583964		2009-09-01	Wong, Gregory A.	
	7	7565141		2009-07-21	Macaluso, Anthony G.	
	8	7373179		2008-05-13	Stine, Ted et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C3

	9	7236780		2007-06-26	Benco, David S. et al.	
	10	7039403		2006-05-02	Wong, Gregory A.	
	11	7865182		2011-01-04	Macaluso, Anthony G.	
	12	8370477		2013-02-05	Short, Joel E. et al.	
	13	8364806		2013-01-29	Short, Joel E. et al.	
	14	8279067		2012-10-02	Berger, Thomas R. et al.	
	15	8213296		2012-07-03	Shannon, Frank M. et al.	
	16	8019868		2011-09-13	Rao, Goutham et al.	
	17	8005988		2011-08-23	Maes, Stephane H.	
	18	7978627		2011-07-12	Taylor, William Scott et al.	
	19	7711848		2010-05-04	Maes, Stephane H.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C3

	20	6782412		2004-08-24	Brophy, Kevin et al.	
	21	6081591		2000-06-27	Skoog, Frederick H.	
	22	6064878		2000-05-16	Denker, John Stewart et al.	
	23	7730123		2010-06-01	Erickson, Richard R. et al.	
	24	8024397		2011-09-20	Erickson, Richard R. et al.	
	25	8156206		2012-04-10	Kiley, Kevin J. et al.	
	26	8126722		2012-02-28	Robb, Terence Alan et al.	
	27	8291238		2012-10-16	GINTER, Karl L. et al.	
	28	8068824		2011-11-29	SHAN, Xueshan et al.	
	29	7228354		2007-06-05	CHAMBLISS, David Darden et al.	
	30	5283904		1994-02-01	CARSON, David G. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C3

	31	8208919		2012-06-26	KOTECHA, Lalit Ratilal	
	32	8185152		2012-05-22	GOLDNER, Alla	
	33	7844728		2010-11-30	ANDERSON, Thomas W. et al.	
	34	7873344		2011-01-18	BOWSER, Robert et al.	
	35	7856226		2010-12-21	WONG, Ellis L. et al.	
	36	7948952		2011-05-24	HURTTA, Tuija et al.	

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

U.S.PATENT APPLICATION PUBLICATIONS

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	20090299857		2009-12-03	Brubaker, Curtis M.	
	2	20090307746		2009-12-10	DI, Jinwen et al.	
	3	20050009499		2005-01-13	KOSTER, Karl	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C3

FOREIGN PATENT DOCUMENTS

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

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

NON-PATENT LITERATURE DOCUMENTS

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

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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C3

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		Date (YYYY-MM-DD)	2013-03-21
Name/Print	Krista S. Jacobsen	Registration Number	59374

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.**

Electronic Acknowledgement Receipt	
EFS ID:	15326754
Application Number:	13705055
International Application Number:	
Confirmation Number:	3375
Title of Invention:	AUTOMATED DEVICE PROVISIONING AND ACTIVATION
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	Krista Susan Jacobsen/Ann Taylor
Filer Authorized By:	Krista Susan Jacobsen
Attorney Docket Number:	RALEP007C3
Receipt Date:	21-MAR-2013
Filing Date:	04-DEC-2012
Time Stamp:	19:49:34
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	P007C3IDS.pdf	1199480 fb33b47774579148fe73c068de53e003f0a062af	no	6

Warnings:
Information:

This is not an USPTO supplied IDS fillable form	
Total Files Size (in bytes):	1199480

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

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

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

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/705,055	12/04/2012	Gregory G. Raleigh	RALEP007C03

CONFIRMATION NO. 3375

106963
Headwater Partners I LLC
350 Marine Parkway, Suite 300
Redwood Shores, CA 94065

PUBLICATION NOTICE

OC000000060546646

Title:AUTOMATED DEVICE PROVISIONING AND ACTIVATION

Publication No.US-2013-0096998-A1
Publication Date:04/18/2013

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

IPR2025-01571
Apple EX1002 Page 459

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	13705055
Filing Date	2012-12-04
First Named Inventor	Raleigh, Gregory G.
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP007C3

U.S.PATENTS

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	6754470		2004-06-22	Hendrickson, Keith et al.	
	2	8122128		2012-02-21	Burke, II, Robert M. et al.	
	3	8149823		2012-04-03	Turcan, Diane Brown et al.	
	4	8131256		2012-03-06	Martti, Jyrki et al.	
	5	6381316		2002-04-30	Joyce, Simon James et al.	
	6	7965983		2011-06-21	Swan, Tim et al.	
	7	8284740		2012-10-09	O'Connor, Dennis M.	
	8	8116223		2012-02-14	Tian, Dan et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C3

	9	6154738		2000-11-28	Call, Charles Gainor	
	10	8423016		2013-04-16	Buckley, Adrian et al.	

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

U.S.PATENT APPLICATION PUBLICATIONS

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	20110173678		2011-07-14	Kaippallimalil, John et al.	
	2	20080235511		2008-09-25	O'Brien, William G. et al.	
	3	20080240373		2008-10-02	Wilhelm, Robert D.	
	4	20100027559		2010-02-04	LIN, Hung-Ming et al.	
	5	20020116338		2002-08-22	Gonthier, Jean-Charles et al.	
	6	20070061878		2007-03-15	Hagiu, Costin et al.	
	7	20100020822		2010-01-28	Zerillo, Anthony J. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C3

	8	20040203755		2004-10-14	Brunet, Jeffrey et al.	
	9	20090172077		2009-07-02	Roxburgh, David et al.	
	10	20080051076		2008-02-28	O'Shaughnessy, John et al.	
	11	20080313730		2008-12-18	Iftimie, Sorin et al.	

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

FOREIGN PATENT DOCUMENTS

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	2006120558A1	WO		2006-11-16	Nokia Corp.		☐

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

NON-PATENT LITERATURE DOCUMENTS

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

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.

EFS Web 2.1.17

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C3

[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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C3

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		Date (YYYY-MM-DD)	2013-05-21
Name/Print	Krista S. Jacobsen	Registration Number	59374

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.**

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
16 November 2006 (16.11.2006)

PCT

(10) International Publication Number
WO 2006/120558 A1

(51) International Patent Classification:
G06Q 20/00 (2006.01) *H04M 15/00* (2006.01)

(21) International Application Number:
PCT/IB2006/001254

(22) International Filing Date: 4 May 2006 (04.05.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0509440.4 9 May 2005 (09.05.2005) GB
11/300,297 15 December 2005 (15.12.2005) US

(71) Applicant *(for all designated States except US)*: **NOKIA CORPORATION** [FI/FI]; Keilalahdentie 4, FIN-02150 Espoo (FI).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **MARTTI, Jyrki** [FI/FI]; Pohjantie 8-10 A 22, FIN-02100 Espoo (FI).

(74) Agents: **RUUSKANEN, Juha-Pekka** et al.; Page White & Farrer, Bedford House, John Street, London WC1N 2BF (GB).

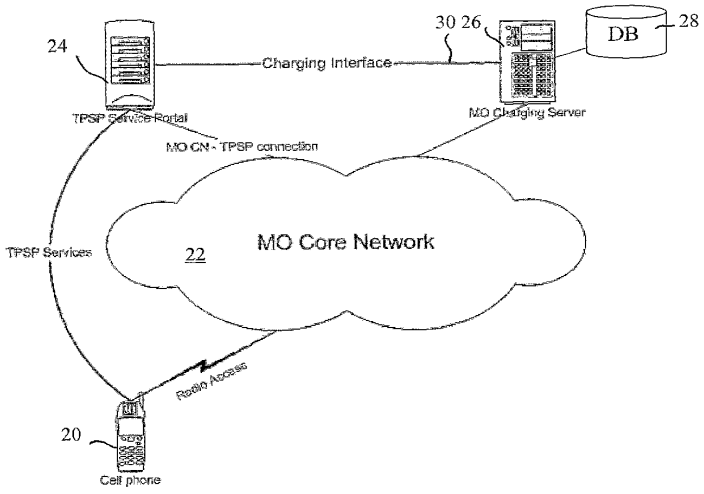
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *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: SERVICES IN A COMMUNICATION SYSTEM



(57) Abstract: A user device (20) is provided with information relating to a service wherein content is communicated to the user device via an access system provided by a communications network (22). In the method information regarding access charges from a charging entity (26) associated with the access system is provided to a service provider entity (24), where after an indication of total cost of the service covering content charges and the access charges is sent from the service provider entity to the user device. Alternatively, indication of the total costs can be sent directly to the user device from the charging entity.

WO 2006/120558 A1

IPR2025-01571
Apple EX1002 Page 465

SERVICES IN A COMMUNICATION SYSTEM

Field of the Invention

The present invention relates to services offered to end-users of a communication system, and more particularly, to services wherein content is delivered to user devices of the end-users.

Background of the Invention

A communication system is a facility which enables communication between two or more entities such as user terminal equipment (mobile or fixed) or other communication devices and/or network entities and other nodes associated with a communication system. The communication may comprise, for example, communication of voice, electronic mail (email), text messages, data, multimedia and so on. A communications system may also be used for providing users with services, typically for communication between users and service providers and for delivery of content data to the user devices. The content data delivery typically includes downloading of data from a remote node, such as a service provide server, via an access system of the communications system.

A communication system typically operates in accordance with a given standard or with a given set of specifications which set out what the various elements of a system are permitted to do and how that should be achieved. For example, the standard or specification may define if the user, or more precisely user equipment, is provided with access via a circuit switched bearer or a packet switched bearer, or both. Communication protocols and/or parameters which should be used for the access to the communication system are also typically defined. For example, the manner in which communication should be implemented between the user equipment and the

elements of the communication networks is typically based on a predefined communication protocol. In other words, a specific set of "rules" on which the communication can be based needs to be defined to enable the user equipment to communicate via the communication system.

Access for a user device to the communication system may be provided by a fixed line and/or wireless communication interface. An example of communication systems providing wireless access are public land mobile networks (PLMN). In a more detailed example the end-user may access the service via a GPRS (General Packet Radio Service) or another cellular wireless access system operated by a telephone operator. Other examples pf possible wireless access systems include various wireless local area networks (WLANs) and satellite based systems. Examples of communication systems providing fixed line access include public switched telephone networks (PSTN), cable networks, digital subscriber line (DSL) networks, and so on.

Content services can be provided by third party service providers (TPSP). The end-users can be subscribers of an operator, for example a fixed line operator or a mobile operator (MO), and commonly use an access network of a telecommunications system operator to contact the third party service provider's service portal. When a third party service provider (TPSP) provides a service to an end-user, it may need to indicate the price of the service to the end-user. The total cost of the service may need to be presented, for example, for customer service reasons. In some countries the cost may need to be indicated for legal reasons.

The third party service provider typically knows the price of the content which it delivers. However, if for example a downloadable game or other considerable data volume is delivered, the end-user may also need to pay for the access costs. The problem is that the third party service provider does not necessarily know what will the access charges be. For example, the third party service provider may not be aware of the access charges for a particular content download.

Arrangements wherein a charging interface is provided between a third party service provider (TPSP) and a mobile operator (MO) have been proposed. In a scenario a TPSP may use a charging interface to request charging information from the mobile operator whose subscriber the end-user is. However, the charging interface has not been designed for provision of information to the end-user relating to the total cost of a particular content download and it's delivery, for example via a GPRS access system. Instead, the cost that has typically been indicated to the end-user is the price of the content itself with a vague reference to additional access charges that may apply. This may not enable the end-user to get any realistic indication of the likely total costs, unless he or she is able to convert the volume of the content to be downloaded to the access charge costs applicable at that specific time. This may not satisfy legislative requirement of some countries where it might be required that the end-user must be given a substantially accurate indication of the total cost of the service.

Summary of the Invention

In accordance with an embodiment there is provided a method for providing a user device with information relating to a service wherein content associated with a service provided by a service provider is communicated to the user device via an access system provided by a communications network. In the method information regarding access charges of the access system is generated. Said information regarding access charges of the access system is then communicated together with content charges of the service provider to the user device.

Another embodiment provides a charging server comprising means for generating information regarding access charges of an access system of a communication network when content that is associated with a service provided by a service provider is communicated to a user device via the access system, and an interface for sending said information regarding

access charges of the access system for communication together with content charges of the service provider to the user device.

Another embodiment provides a service provider entity, comprising an interface for receiving information from a charging entity associated with an access system of a communication network relating to costs of the access system for communication of content that is associated with a service provided by the service provider entity to a user device via the access system, and means for sending information regarding access charges of the access system for communication together with content charges of the service provider to the user device.

The embodiments of the invention may provide an advantage in that making it easier for the end-users to make decisions on whether to buy a service or not. The embodiments may enable providing the user with an indication of the total service costs. Such an indication may make the available services more attractive for end-users. Charging services offered by the operators may also become more attractive for third party service providers.

Brief Description of the Drawings

For a better understanding of the present invention and how the same may be carried into effect, reference will now be made by way of example only to the accompanying drawings in which:

Figure 1 shows a schematic view of a communications system wherein the invention may be embodied;

Figure 2 shows a flowchart for operation in accordance with an embodiment of the present invention;

Figure 3 is a sequence diagram in accordance with an embodiment the invention.

Figure 4 shows signalling flows in accordance with an embodiment;

Figure 5 shows a flowchart for operation in accordance with an embodiment;

Figure 6 shows a flowchart for operation in accordance with a further embodiment.

Detailed Description of Embodiments of the Present Invention

To assist in understanding the invention, an explanation of a possible underlying communication system is given first with reference to elements of a cellular mobile communication network as defined by the third generation partnership project (3GPP). It is noted that although certain embodiments will now be described by way of example, with reference to the exemplifying architectures of a communication system comprising 3GPP mobile access networks and/or wireless local area networks, embodiments may be applied to any other suitable forms of communication systems than those illustrated and described herein.

A user device of an end-user may communicate data in association with various services based on an appropriate data communication protocol. In Figure 1 the services available for mobile user devices 20 (only one shown for clarity) are provided by a service provider portal 24. The portal may be provided by a server or any other appropriate data processing device capable of communicating with user devices. The services may be provided, for example, by means of the Internet Protocol (IP), and thus the portal 24 can be understood as, for example, denoting an Internet Protocol (IP) based device.

A mobile communication system 22 is typically arranged to serve a plurality of mobile user devices which have accessed wirelessly the access system. A core network part of the communication system is typically connected to a number of access networks, typically to base station systems. The base stations are arranged to transmit signals to and receive signals from a mobile user equipment, via respective wireless interfaces. Correspondingly, each mobile device is able to transmit signals to and receive signals from the base stations via the wireless interface. In a typical operation a mobile

communication network provides packet switched data transmission in the packet switched domain between a support node and mobile user equipment via the access system.

A non-limiting example of a possible mobile network is the 3rd generation cellular network wherein a mobile user device may connect to an access network by setting up a PDP (Packet Data Protocol) context through a GPRS (General Packet Radio Service) network. The GPRS service allows transmission of packet data between mobile communication devices and external data networks. In this case the mobile network 22 would be connected to external data networks, for example the Internet, via a gateway GPRS support node (GGSN). Each PDP context provides a communication pathway between a particular user and a gateway node of the network. Once the PDP context is established, it can typically carry multiple flows. Each flow normally represents, for example, a particular service and/or media component of a particular service. The PDP context therefore often represents a logical communication pathway for one or more flows across the network. To implement the PDP context between user equipment and a node, radio access bearers need to be established which commonly allow for data transfer for the user equipment. Another option to wirelessly access services is to set up an IPsec tunnel through a WLAN network that is then connected to a core communication network.

A mobile communication device within an access network may communicate with a radio network controller via radio network channels which are typically referred to as radio bearers. Each mobile device such as a mobile user equipment may have one or more radio channels open at any one time with the radio network controller. Any appropriate mobile device adapted for Internet protocol (IP) communication maybe used to connect to the network. For example, a user may access the cellular network by means of communication devices such as a personal computer, personal data assistant (PDA), mobile station (MS), portable computer, combinations thereof or the like.

The mobile communication device can be used for various tasks such as making and receiving phone calls, for receiving and sending data from and to a network and for experiencing, for example, multimedia or other content. The communication device is typically provided with a processor and memory for accomplishing these tasks. The operation of the user equipment may be controlled by means of a suitable user interface such as key pad, voice commands, touch sensitive screen or pad, combinations thereof or the like.

The following describes an exemplifying embodiment for charging of services provided by third party service providers utilizing bearer services offered by a mobile operator. The example is described with reference to Figure 1 wherein an end-user using a mobile terminal (MT) 20 is a subscriber to a mobile operator (MO) operating network 22. The end-user may request for services provided by a third party service provider (TPSP) portal 24.

Use of the services can be charged by the third party service provider by sending of charging requests to a charging server 26 hosting the end-user charging account. The mobile operator (MO) may be responsible for the operation of the communications network 22 and the charging server 26. The charging server 26 may be based on an existing charging server of an operator. In such case the server and/or system functionality thereof may need to be updated to support the new functionalities required by the embodiment.

An online charging web service interface 30 is provided between the third party service provider portal 24 and charging server 26. The charging interface may be provided by an external data network, for an Internet Protocol based network and/or via the communications network 22. The online charging interface 30 supports communication of indications associated with the costs of services. The third party service provider portal 24 may use the charging interface 30 to charge via operator based billing the end-users for the services the end-users are using. The online charging interface 30 can be used to indicate the charges that are applicable to a service provided to user devices in an access system associted with the charging server. This is

an important improvement on the prior art charging interfaces which have not been used for consideration how access charges, in addition to the content price, that relate to delivery of the content can be reported to the TPSP in order to provided the end-user with an indication of the total cost of the content download.

A database 28 is also provided for storing information needed to resolve the access changes for a specific service. The database may be hosted by the mobile operator, or any other appropriate party. The database 28 may be integrated with the server 26, or the server may be provided with an access thereto.

Figure 2 shows a flowchart for operation in accordance with an embodiment. In the embodiment a user of a user device is provided with information relating to the cost of using a service before he/she makes a definitive decision whether to order the service. In Figure 2 embodiment the service provider first sends a request for information about access charges to a charging entity associated with an access network of a communication system at step 100. This is not always necessary, and information about the access charges may also be provided to the service provider entity without a specific request, for example periodically. Information regarding access charges is communicated in step 102 from the charging entity to the service provider entity. Communication between the entities may occur via the interface 30 of Figure 1.

When generating the information, the charging entity may fetch relevant information from a database. The service provider entity may then generate an appropriate indication of total cost of the service covering content charges and the access charges, and send the indication to the user device at step 104. This communication may occur via the communication network 22.

The cost may then be displayed to the user, step 106. This preferably occurs before the service is taken into use at the user device, i.e. before the user has decided if he/she wants to use the service. The cost can be presented for the

end-user only for information, and the service provision is continued automatically, step 108. Alternatively, the end user may be asked to accept the cost, see step 110. In the latter case, if the cost are acceptable at step 112, the user may order the service by sending his acceptance, step 116. If the costs are not acceptable, the user does not respond at all, or sends a denial, and may not be charged, step 114.

There are various ways to support the providing of indications regarding the access charges from the content that is to be downloaded, if the service is ordered. According to a possibility the service provider 24 may request information regarding the access charges via the on-line charging interface 30. The charging web service provided by server 26 supports the relevant service interface and charging server functionality. The service interface is on the operator side of the connection, i.e. the charging interface is controlled by the operator. The TPSP can be seen as the client of the charging service. The charging interface can be used for all exchange of charging information between the service provider and the charging entity of the operator.

The signalling flow of Figure 3 shows operation in accordance with this embodiment in more detail. In the flow chart the solid lines present functionalities that are required by this embodiment and dashed lines describe functionalities that may be needed to support the particular communication environment, but are not necessary. Dotted lines are for information purposes only.

The end-user requests for a service, for example a game or other content, from a service provider by message 1. Optional messages 2 and 3 may be signalled for discovery of a charging web service interface (WSI) service, for example by using a functionality provided by the Project Liberty Alliance. A request 4 containing information about the service and the end-user is then sent from the service provider to the operator. Request 4 may contain information regarding the end-user, the requested service, volume of the content, the access bearer and so on. This message may also include various other parameters, such as information regarding rates, credit reservations,

credit deductions, credit checks, charging method and so on. The charging system can be made aware of what access bearer the terminal is using based on a service identifier or a correlation-identifier in the request that is received by the charging system. This can be, for example, a user identity or a dynamically defined service identity that is defined when the access is initiated.

The operator owned charging entity may then resolve at step 5 the costs of the access charges based on the received information and information stored in a database. At step 6 the charging entity may debit funds both for content and access charges from an end-user account, make a respective reservation or reservation on a user account. or take any other required action required for the actual charging.

A response message 7 may contain information regarding granted charging units and a specific field or parameter for indicating either the total const or at least the access charges for the service. The online charging interface mechanism can include to the response message the access charges that the service provider server can then add to the price of the content. According to an alternative the response can contain the total charges of the service, for example if the service is also rated by the operator.

The total charges or the access charge only caused by the download are then indicated to the service provider by message 7. The service provider may then indicate the price to the end-user by message 8.

In accordance with a possibility, in case the operator is also rating charge of the content, the mobile operator can indicate the costs of the service directly to the end-user through appropriate channels.

The end-user may then confirm that he/she is willing to use the service by message 9. The service is delivered by signalling 10. After completion of the service delivery the success thereof may be indicated to the TPSP by signalling 11.

In case of the first request towards the operators charging infrastructure only made a reservation of charging units, the reserved units can be committed in response to message 12.

According to another possibility the service provide is provided with a database that contains access charge rates for all its customers. This may be a more complicated to provide, because the service providers do not commonly define themselves what the access charges are. Thus even in this alternative the service provider needs to request information from the operator of the end-user. The end-user may also have different tariffs for the access charges depending the time of the day, so the service provider may need frequently update the information.

Further exemplifying embodiments will now be described with reference to Figures 4 to 6. In these embodiments a user device 20 is involved, at least to a degree, in generation of the total charge information. The involvement of the user device 20 may be provided in various ways. For example, the user device may be made aware of the access charges incurred for data traffic. This information may come from the access network 22. The access charge information available at the user device 20 may then be utilised either at the user device or at an appropriate entity at the network side when calculating the total charge.

A possible way to provide the communication interfaces of Figure 4 is to use an HTTP/XML (Hypertext Transport Protocol/ eXtensible Markup Language)-based Web Services interface towards the operator network and a similar interface towards the content provider. It is also possible to simply use HTTP-headers for the communication.

In the embodiment of Figure 5 the user device 20 is provided with information regarding the access charges at step 200 and information regarding the content charges at 202, where after the user device itself may calculate at 204 the total charge. This scenario enables operation wherein no action is required from the content provider, or another entity at the network side.

In accordance wit ha specific example, the user device may use appropriate data, for example metadata such as information contained in JAD-files of Java 2 Platform Micro Edition (JME2) to calculate the price of the transmission. JME2 is a Java application environment providing a framework for the deployment and use of Java technology. A JAD file is a Java Application Descriptor file that contains information about a Java Archive Repository (JAR) file. A JAD file contains the name, file size, and version of the actual JAR content file. This information may then be displayed or otherwise reported to the user at 206, preferably before the user accepts the download. The user device may be configured to wait until it receives an indication of acceptance of the total cost of the service, for example an activation of a predefined key or menu option. The request for the service may then be transmitted in response to said indication.

In an another embodiment shown in Figure 6 a user device is provided with access charge information at step 300. The user device may then report the access charge information at 302 to the content provider or another appropriate entity at the network. The information from the user device may then be used at the network side at 304 in calculating the total charge. The full, complete purchase price may then be reported at 306 to the user device based on at least partially information originating from the user device at step 302. The total cost may then be presented to the user at 308.

In a further embodiment the content provider may be able to dynamically adjust the price of the content based on the subscriber's traffic charges. For example, to be able to offer uniform pricing for all users, those with flat-rate data subscriptions may be charged relatively more compared to those with high data traffic costs. The perceived end-user price would stay the same. Communications to the operator may be enabled for example for the purposes of traffic compensation negotiations or other arrangements.

On the operator-side, an interface may be provided for queries from user devices regarding the prices for packet data traffic. The interface may be positioned at a charging server or similar charging element of the network. On the content provider side, the server 24 may be adapted to interpret pricing information provided in various formats. The information can be provided, for example, in the form of an XML-request or can be supplied in the content request HTTP-headers and so on.

The overall high-level message flow of Figure 4 may be as follows. The user device 20 may send at 15 a request to the operator querying the current data charging rate. The charging rate can be given, for example, per Megabyte. An appropriate network node 22, for example a charging server, then responds at 16 with the current data-charging rate. The user device may then request at 17 for a service or content from a content provider 24. The user device includes information regarding the current data charging rate in the request. The content provider may then calculate the total content price, and reply at 18 with the total charge for the content.

Steps 15 and 16 may be performed periodically, for example as once a day or a week. The results can be cached in the memory of the user device. The operator core network may also push the charging rate information to the user device periodically, and/or advice the user device to update the rate information when the rates change.

According to a further embodiment the content provider and the access network operator may interact and automatically agree on various features, for example on possible discounts to the packet data traffic rates. The content provider may, for example, sponsor the traffic charges for some user segments.

Embodiments may be made independent of the actual payment mechanism that is used to pay for the content. Some of the embodiments may allow a non-affiliated content provider to offer a service with a known total price without relationships with the network operator.

The required data processing functions may be provided by means of one or more data processors. Appropriately adapted computer program code product may be used for implementing the embodiments, when loaded to a computer, for example a processor of the communication device and/or any of the other nodes associated with the operation. The program code means may, for example, perform the generation of messages and/or information elements, interpretation and so forth. The program code product for providing the operation may be stored on and provided by means of a carrier medium such as a carrier disc, card or tape. A possibility is to download the program code product via a data network. The required data processing functionalities of the user device 20 may be embedded in, for example, a browser or an appropriate content discovery client 21 of the user device. A mechanism for providing an advice of the charges for the end user may be provided at the user device and/or at the content provider.

The herein described embodiments enable an end user to have a single price for a service inclusing access charges and content charges. This information can be provided for a user before he/she decides to use the service. The total costs or the rate of a service can be also presented during service provision session, for example after a rate of a video streaming service changes, or a certain predefined cost has been exceeded.

It is noted that whilst embodiments of the present invention have been described in relation to communication devices such as mobile stations, embodiments of the present invention are applicable to any other suitable type of devices suitable for communication via a communications network.

It is also noted that although the above example relates a request-response model, the services may be pushed to user devices. For example, a service provider server may detect based on a database or its settings that a communication device is present in an access network, and that it may wish to use a service. In this model a specific request by the end-user may not be necessary.

It is noted that even though the exemplifying embodiments shown and described in this disclosure use the terminology of the 3rd generation (3G) WCDMA (Wideband Code Division Multiple Access) networks, such as UMTS (Universal Mobile Telecommunications System), CDMA2000 systems and wireless local area networks, embodiments of the proposed solution can be used in any communication system wherein advantage may be obtained by means of the embodiments of the invention, fort example for providing an access system for an IPsec tunnel.

It is also noted herein that while the above describes exemplifying embodiments of the invention, there are several variations and modifications which may be made to the disclosed solution without departing from the scope of the present invention as defined in the appended claims.

Claims

1. A method for providing a user device with information relating to a service, wherein content associated with a service provided by a service provider is communicated to the user device via an access system provided by a communications network, said method comprising:

generating information regarding access charges of the access system; and

communicating said information regarding access charges of the access system together with content charges of the service provider to the user device.

2. A method as claimed in claim 1, wherein the step of communicating comprises sending an indication of total cost of the service including content charges and the access charges to the user device.

3. A method as claimed in claim 1, comprising the step of sending said information regarding access charges from a charging entity associated with the access system to a service provider entity, wherein the step of communicating comprises sending an indication of total cost of the service including content charges and the access charges from the service provider entity to the user device.

4. A method as claimed in claim 1, wherein the step of communicating comprises sending an indication of total cost of the service including content charges and the access charges from a charging entity associated with the access system to the user device.

5. A method as claimed in any preceding claim, wherein the step of communicating occurs before the service is taken into use at the user device.

6. A method as claimed in any of claims 1 to 4, wherein the step of communicating occurs during use of the service.

7. A method as claimed in any preceding claim, further comprising sending from the service provider entity to the charging entity information identifying the service and the user device.

8. A method as claimed in any preceding claim, further comprising sending from the service provider entity to the charging entity a message containing information regarding at least any one of the user device, the service, volume of content to be communicated, and a data bearer between the user device and the access network.

9. A method as claimed in any preceding claim, further comprising the steps of

sending a request for the service from the user device to a service provider entity;

discovering an appropriate charging entity in response to receiving the request for the service at the service provider entity; and

sending from the service provider entity to the discovered charging entity information identifying the service and the user device.

10. A method as claimed in any preceding claim, further comprising resolving access charges associated with use of resources of the access system at a charging entity based on information associated with the service and the user device as received from a service provider entity and information from a database.

11. A method as claimed in any preceding claim, wherein the step of sending information regarding access charges from the charging entity comprises sending further information regarding other charges.

12. A method as claimed in claim 11, wherein said step of sending further information comprises sending information regarding total charges for the service.

13. A method as claimed in any preceding claim, further comprising sending an acceptance of the total cost from the user device.

14. A method as claimed in any preceding claim, comprising sending information regarding the access charges from the user device.

15. A method as claimed in claim 14, comprising receiving information regarding access charges at the user device prior the step of sending the information regarding the access charges from the user device.

16. A method as claimed in claim 15, comprising pushing rate information from the communications network to the user device.

17. A method as claimed in claim 15, comprising sending periodically rate information from the communications network to the user device.

18. A method as claimed in claim 15, comprising sending rate information from the communications network to the user device after a rate change.

19. A method as claimed in claim 15, comprising sending a request for rate information from the user device to the communications network.

20. A method as claimed in claim 1, wherein the step of generating comprises generating said information regarding the access charges at the user device.

21. A method as claimed in claim 1, wherein the step of generating comprises generating said information regarding the access charges at the user device based on metadata.

22. A method as claimed in claim 1, comprising processing information received from the user device to obtain a total cost for of the service.

23. A method as claimed in claim 22, wherein the step of processing information comprises processing, at an entity connected to the communications network, information regarding the access charges received from the user device and information regarding content charges to obtain the total cost for of the service.

24. A method as claimed in claim 22, wherein the step of processing information comprises dynamically adjusting the content charges based on information received from the user device.

25. A method as claimed in any preceding claim, comprising including by the user device the information regarding access charges into a request for the service.

26. A method as claimed in any preceding claim, wherein the user device comprises a mobile device, and the access system comprises an access network of a mobile communication network.

27. A method as claimed in any preceding claim, comprising communication of data between the charging entity and the service provider via a separate data network.

28. A method as claimed in claim 27, wherein the separate data network comprises an Internet Protocol network.

29. A computer program comprising program code means configured to perform the steps of any of claims 1 to 27 when the program is run on a computer.

30. A charging server for a communications network, said charging comprising:

means for generating information regarding access charges of an access system of the communications network when content that is associated with a service provided by a service provider is communicated to a user device via the access system; and

an interface for sending said information regarding access charges of the access system for communication together with content charges of the service provider to the user device.

31. A charging server as claimed in claim 30, wherein the interface is configured for communication of said information regarding access charges of the access system to a service provider entity.

32. A charging server as claimed in claim 30 or 31, wherein the means for generating information is configured to process information identifying the service and the user device.

33. A charging server as claimed in any of claims 30 to 32, wherein the means for generating information are configured to resolve access charges associated with use of resources of the access system at a charging entity based on information associated with the service and the user device and information from a database.

34. A charging server as claimed in any of claims 30 to 33, wherein the means for generating information are configured to generate information regarding other charges.

35. A charging server as claimed in claim 34, wherein the means for generating information are configured to generate said information regarding total charges for the service.

36. A charging server as claimed in claim 35, wherein the interface is for communication of said information regarding the total charges for the service to the user device.

37. A charging server as claimed in any of claims 30 to 36, wherein the interface is configured for communication of data via a data network.

38. A charging server as claimed in claim 37, wherein the data network comprises an Internet Protocol network.

39. A charging server as claimed in claim 30, wherein the means for generating are configured to generate the information regarding the access chares based on information received from the user device.

40. A service provider entity, comprising:
an interface for receiving information regarding access charges of the access system for communication of content that is associated with a service provided by the service provider entity to a user device via an access system of a communications network; and
means for sending information regarding access charges of the access system for communication together with content charges of the service provider to the user device.

41. A service provider entity as claimed in claim 40 being configured to receive said information regarding access charges from a charging entity associated with the access system of the communications network.

42. A service provider entity as claimed in claim 41, configured to discover an appropriate charging entity in response to receiving a request for the service.

43. A service provider entity as claimed in claim 42, configured to provide the discovered charging entity with information identifying the service and the user device.

44. A service provider entity as claimed in claim 40 being configured to receive said information regarding access charges from the user device.

45. A communication system comprising at least one of a charging server in accordance with any of claims 30 to 39 and a service provider entity in accordance with any of claims 40 to 44,

46. A method for providing charging information relating to a service provided by a service provider, wherein content associated with the service is communicated to the user device via an access system provided by a communications network, said method comprising:

providing the user device with information regarding access charges of the access system;

providing the user device with information regarding content charges; and

processing said information regarding the access charges of the access system and said information regarding the content charges in the user device to provide a total charge.

47. A method as claimed in claim 46, further comprising receiving by the user device an indication of acceptance of the total cost of the service; and sending a request for the service in response to said indication.

48. A method as claimed in claim 46, comprising receiving information regarding access charges at the user device.

49. A method as claimed in claim 46, comprising pushing rate information from the communications network to the user device.

50. A method as claimed in claim 46, comprising sending periodically rate information from the communications network to the user device.

51. A method as claimed in claim 46, comprising sending rate information from the communications network to the user device after a rate change.

52. A method as claimed in claim 46, comprising sending a request for rate information from the user device to the communications network.

53. A method as claimed in claim 46, wherein the step of generating comprises generating said information regarding the access charges at the user device.

54. A method as claimed in claim 46, wherein the step of generating comprises generating said information regarding the access charges at the user device based on metadata.

55. A user device comprising:
a receiver for receiving content associated with a service via an access system of a communications network;
a controller configured to process information regarding access charges of the access system and information regarding content charges to provide a total charge; and
a user interface for presenting the total charge.

56. A user device as claimed in claim 55 being configured to receive an indication of acceptance of the total cost of the service, and to send a request for the service in response to said indication.

57. A user device as claimed in claim 55, wherein the controller is configured to process information regarding access charges received from the communications network.

58. A user device as claimed in claim 55, wherein the controller is configured to generate said information regarding the access charges.

59. A user device as claimed in claim 55, wherein the controller is configured to generate said information regarding the access charges based on metadata.

60. A user device as claimed in claim 55, comprising a memory for storing access charge information.

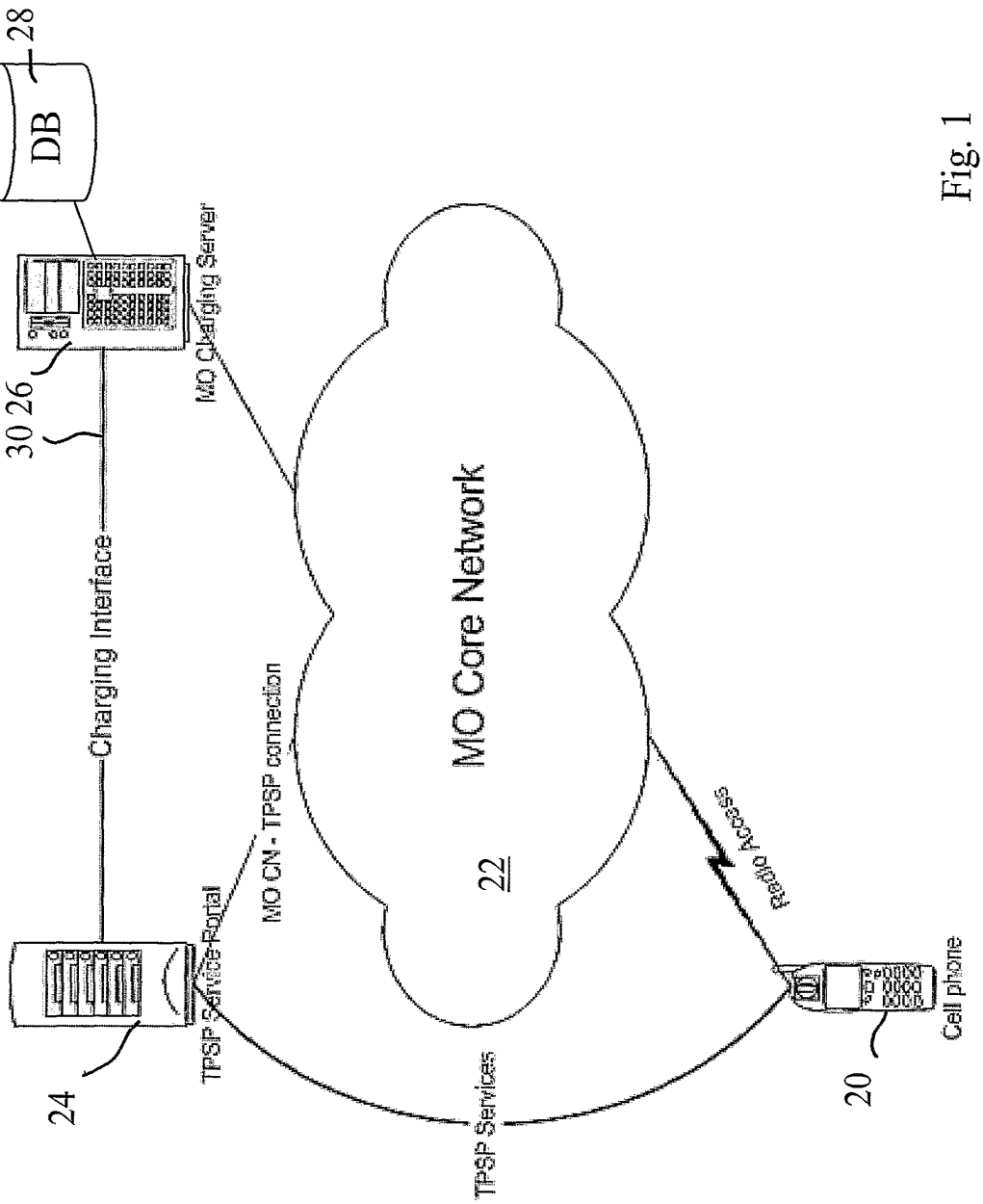

28
DB
MO Charging Server
30 26
Charging Interface
MO Core Network
22
MO CN - TPSP connection
TPSP Service Portal
24
TPSP Services
Radio Access
Cell phone
20

Fig. 1

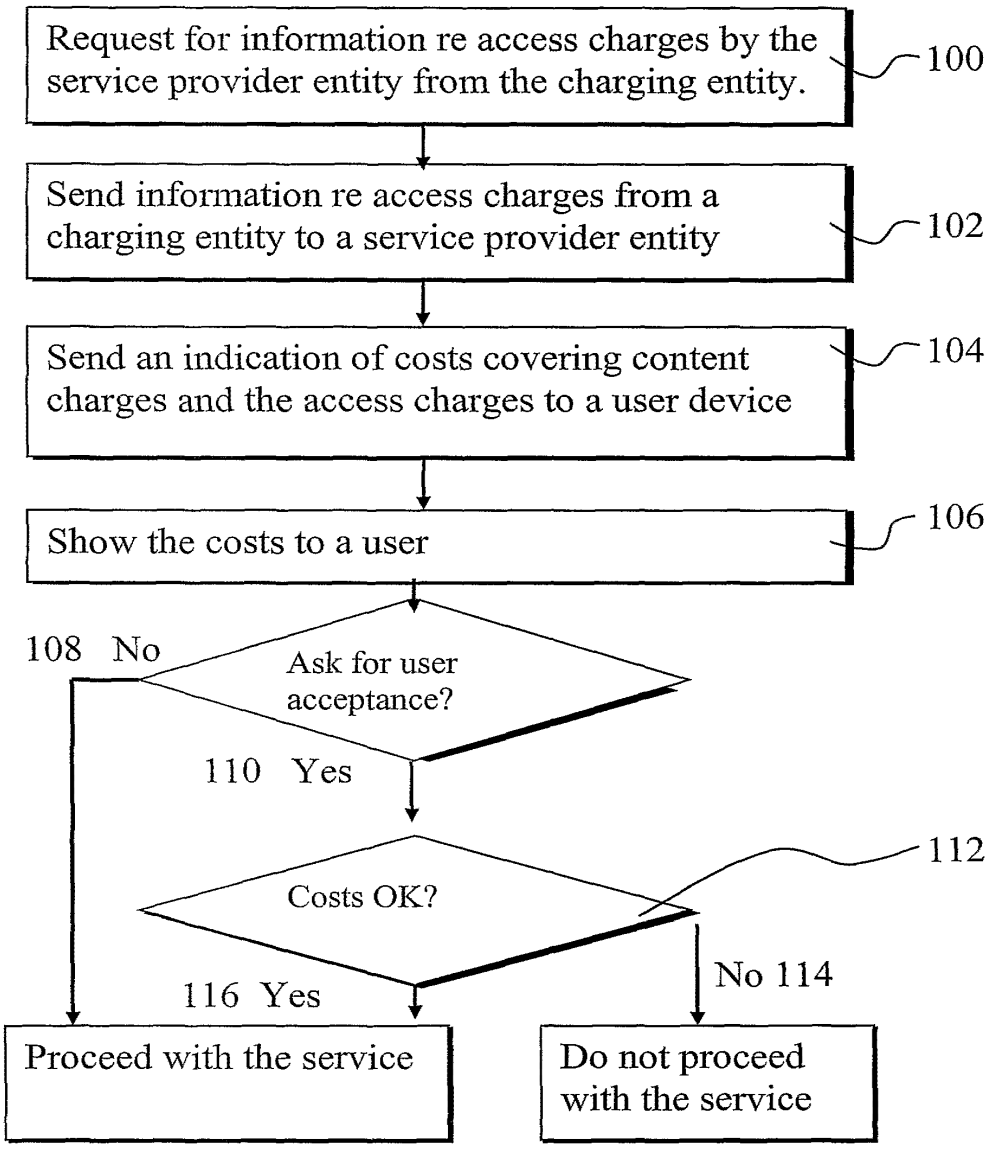

Request for information re access charges by the service provider entity from the charging entity.
100
Send information re access charges from a charging entity to a service provider entity
102
Send an indication of costs covering content charges and the access charges to a user device
104
Show the costs to a user
106
108 No
Ask for user acceptance?
110 Yes
Costs OK?
112
No 114
116 Yes
Proceed with the service
Do not proceed with the service

Fig. 2

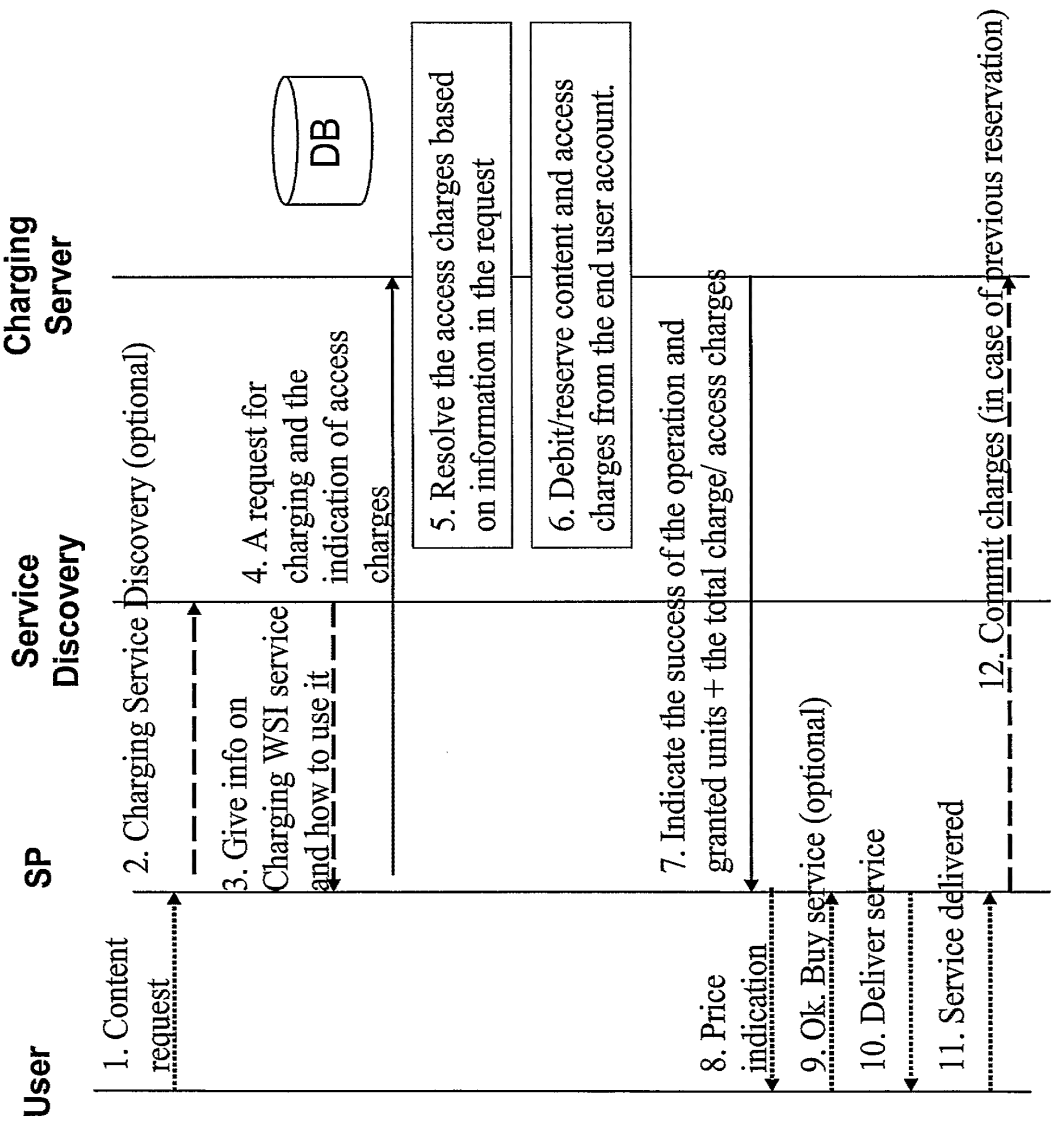


Fig. 3

IPR2025-01571
Apple EX1002 Page 492

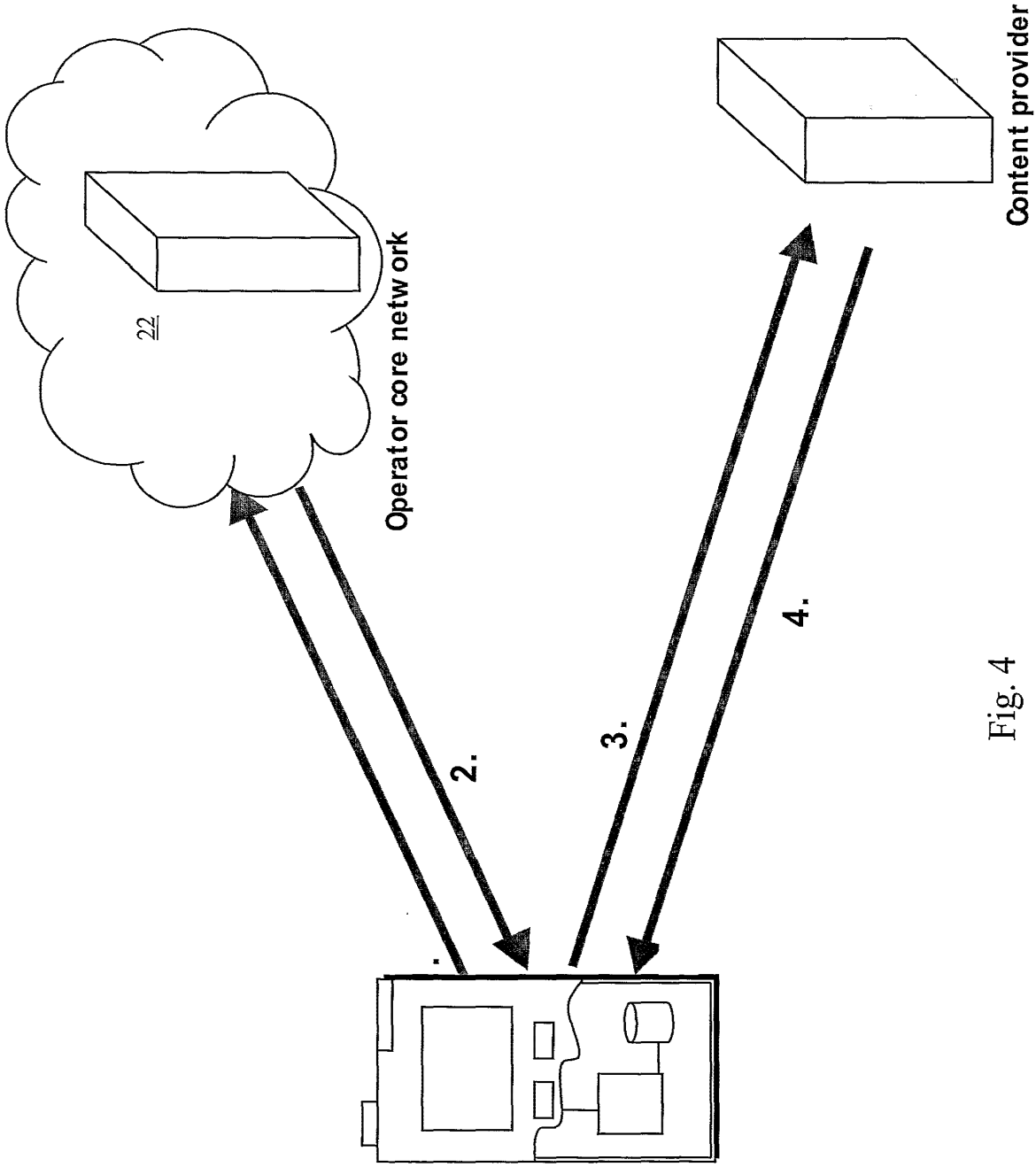


Fig. 4

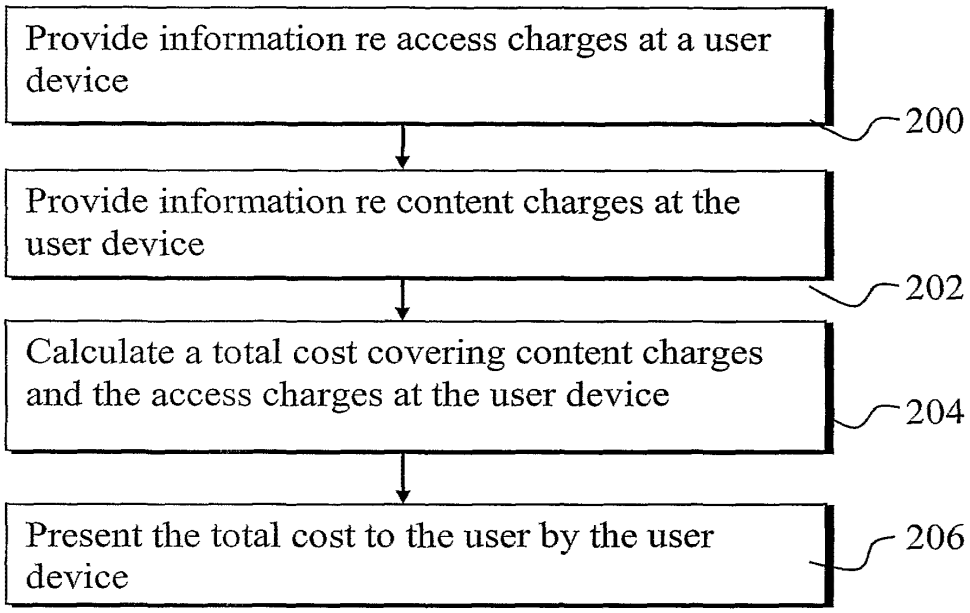

Provide information re access charges at a user device
200
Provide information re content charges at the user device
202
Calculate a total cost covering content charges and the access charges at the user device
204
Present the total cost to the user by the user device
206

Fig. 5

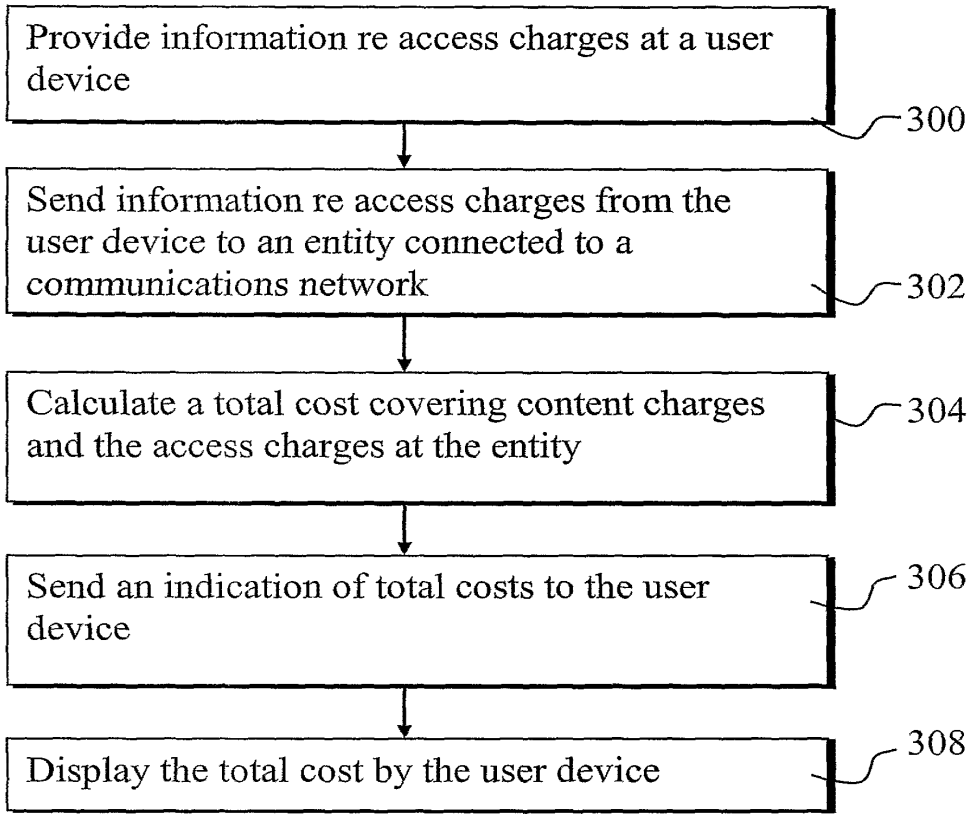

Provide information re access charges at a user device
300
Send information re access charges from the user device to an entity connected to a communications network
302
Calculate a total cost covering content charges and the access charges at the entity
304
Send an indication of total costs to the user device
306
Display the total cost by the user device
308

Fig. 6

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2006/001254

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06Q20/00 H04M15/00

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)
H04M H04L G06Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, PAJ, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2004/039656 A1 (GERBER HEIKO ET AL) 26 February 2004 (2004-02-26) paragraph [0003] - paragraph [0005] paragraph [0008] - paragraph [0012] paragraph [0016] - paragraph [0025]	1-60
X	US 2003/083990 A1 (BERG ANDREAS ET AL) 1 May 2003 (2003-05-01) paragraph [0008] - paragraph [0013] paragraph [0019] - paragraph [0037] paragraph [0043] - paragraph [0055] claims 1-3,6	1-60
X	US 6 240 091 B1 (GINZBOORG PHILIP ET AL) 29 May 2001 (2001-05-29) column 2, line 60 - column 3, line 23 column 5, line 16 - column 12	1-60

-/--

[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 document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
9 August 2006	17/08/2006

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Patlaka, E.

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2006/001254

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6 865 262 B1 (MITTS H{DOT OVER (AKAN ET AL) 8 March 2005 (2005-03-08) column 2, line 1 - line 33 column 3, line 18 - column 9, line 11	1-60
A	US 2002/194143 A1 (BANERJEE DWIP N ET AL) 19 December 2002 (2002-12-19) paragraph [0009] - paragraph [0029]	1-60
A	US 5 737 414 A (WALKER ET AL) 7 April 1998 (1998-04-07) the whole document	1-60

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/IB2006/001254

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2004039656 A1	26-02-2004	DE 10227395 A1	24-12-2003
		EP 1372101 A2	17-12-2003
US 2003083990 A1	01-05-2003	DE 10148540 A1	24-04-2003
		EP 1298599 A1	02-04-2003
US 6240091 B1	29-05-2001	FI 972980 A	15-01-1999
US 6865262 B1	08-03-2005	AU 2443000 A	18-08-2000
		EP 1153505 A2	14-11-2001
		FI 990170 A	30-07-2000
		WO 0045609 A2	03-08-2000
US 2002194143 A1	19-12-2002	NONE	
US 5737414 A	07-04-1998	AT 324629 T	15-05-2006
		AU 5922996 A	11-12-1996
		BR 9606368 A	23-12-1997
		CA 2195968 A1	28-11-1996
		EP 0782728 A1	09-07-1997
		JP 10507053 T	07-07-1998
		WO 9637848 A1	28-11-1996
		US 5949875 A	07-09-1999

IPR2025-01571
Apple EX1002 Page 498

Electronic Acknowledgement Receipt	
EFS ID:	15837774
Application Number:	13705055
International Application Number:	
Confirmation Number:	3375
Title of Invention:	AUTOMATED DEVICE PROVISIONING AND ACTIVATION
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	Krista Susan Jacobsen/Ann Taylor
Filer Authorized By:	Krista Susan Jacobsen
Attorney Docket Number:	RALEP007C03
Receipt Date:	22-MAY-2013
Filing Date:	04-DEC-2012
Time Stamp:	02:05:17
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	P007C03IDS.pdf	989360 b102b4706bdd1d71727cef63a74e399f1a748a02	no	5
Warnings:					
Information:					

This is not an USPTO supplied IDS fillable form					
2	Foreign Reference	WO2006120558A1Nokia.pdf	829615 8b7d3998166eaadb50492ebf5e693219d9e238ca	no	34
Warnings:					
Information:					
			Total Files Size (in bytes):	1818975	

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.
13/705,055	12/04/2012	Gregory G. Raleigh	RALEP007C03	3375

106963 7590 07/01/2013

Headwater Partners I LLC
350 Marine Parkway, Suite 300
Redwood Shores, CA 94065

EXAMINER	
RUDY, ANDREW J	
ART UNIT	PAPER NUMBER
3687	

NOTIFICATION DATE	DELIVERY MODE
07/01/2013	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

Office Action Summary for Applications Under Accelerated Examination	**Application No.** 13/705,055	**Applicant(s)** RALEIGH ET AL.	
	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 --

***Since this application has been granted special status under the accelerated examination program, NO extensions of time under 37 CFR 1.136(a) will be permitted and a SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE:* ONE MONTH OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION – if this is a non-final action or a *Quayle* action.**

(Examiner: For **FINAL** actions, please use PTOL-326.)

The objective of the accelerated examination program is to complete the examination of an application within twelve months from the filing date of the application. Any reply must be filed electronically via EFS-Web so that the papers will be expeditiously processed and considered. If the reply is not filed electronically via EFS-Web, the final disposition of the application may occur later than twelve months from the filing of the application.

Status

1)☒ Responsive to communication(s) filed on *11 December 2012*.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

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

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) _____ is/are rejected.

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

8)☒ Claim(s) *1-30* are subject to restriction and/or election requirement.

* If any claims have been determined allowable, 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.

Application Papers

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

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

11)☐ 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)).

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

Interim copies:

a)☐ All b)☐ Some c)☐ None of the: Interim copies of the priority documents have been received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
4) ☐ Other: _____.

IPR2025-01571
Apple EX1002 Page 502

DETAILED ACTION

Election/Restrictions

1. Restriction to one of the following inventions is required under 35 U.S.C. 121:

   I. Claims 1-27 drawn to a method/system, classified in class 705, subclass 30.

   II. Claims 28-30, drawn to a medium, classified in class 713, subclass 168.

2. The inventions are distinct, each from the other because of the following reasons:

Inventions Group II and Group I are related as process and apparatus for its practice. The inventions are distinct if it can be shown that either: (1) the process as claimed can be practiced by another and materially different apparatus or by hand, or (2) the apparatus as claimed can be used to practice another and materially different process. (MPEP § 806.05(e)). In this case the process may be practice by a different apparatus.

3. Restriction for examination purposes as indicated is proper because all these inventions listed in this action are independent or distinct for the reasons given above and there would be a serious search and/or examination burden if restriction were not required because at least the following reason(s) apply:

The claim language of each group diverge in scope.

Applicant is advised that the reply to this requirement to be complete must include (i) an election of a invention to be examined even though the requirement may be traversed (37 CFR 1.143) **and (ii) identification of the claims encompassing the elected invention**.

The election of an invention may be made with or without traverse. To reserve a right to petition, the election must be made with traverse. If the reply does not distinctly and specifically point out supposed errors in the restriction requirement, the election shall be treated as an election without traverse. Traversal must be presented at the time of election in order to be considered timely. Failure to timely traverse the requirement will result in the loss of right to petition under 37 CFR 1.144. If claims are added after the election, applicant must indicate which of these claims are readable upon the elected invention.

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

4. A telephone call was made to Krista Jacobsen (Reg. No. 59,374) on June 13, 2013 to request an oral election to the above restriction requirement, but did not result in an election being made.

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

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Matthew S. Gart can be reached on 571-272-3955. 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

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	13705055
Filing Date	2012-12-04
First Named Inventor	Raleigh, Gregory G.
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP007C03

U.S.PATENTS

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	6035281		2000-03-07	Crosskey, James P. et al.	
	2	6996393		2006-02-07	Pyhalammi, Seppo et al.	
	3	7760711		2010-07-20	Kung, Fen-Chung et al.	
	4	8000318		2011-08-16	Wiley, William L. et al.	
	5	8098579		2012-01-17	Ray, Amar N. et al.	
	6	8155670		2012-04-10	Fullam, Scott et al.	
	7	8374090		2013-02-12	Morrill, Robert J. et al.	
	8	7457265		2008-11-25	Julka, Vibhor et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C03

	9	7729326		2010-06-01	Sekhar, Ramesh	
	10	7929973		2011-04-19	Zavalkovsky, Arthur et al.	
	11	7945945		2011-05-17	Graham, Richard et al.	
	12	8059530		2011-11-15	Cole, Terry L.	
	13	8266681		2012-09-11	Deshpande, Sumit B. et al.	
	14	8280354		2012-10-02	Smith, Christopher et al.	
	15	8331293		2012-12-11	Sood, Kapil	
	16	8019820		2011-09-13	Son, Giyeong et al.	
	17	8155155		2012-04-10	Chow, Albert T. et al.	
	18	8191116		2012-05-29	Gazzard, Daryl	
	19	6292828		2001-09-18	Williams, David L.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C03

	20	7043226		2006-05-09	Yamauchi, Toshiaki	
	21	7472189		2008-12-30	Mallya, Arvind R. et al.	
	22	7944948		2011-05-17	Chow, Albert T. et al.	
	23	8005009		2011-08-23	McKee, Neil et al.	
	24	7760861		2010-07-20	Croak, Marian et al.	
	25	8060463		2011-11-15	Spiegel, Joel R.	
	26	8224773		2012-07-17	Spiegel, Joel R.	
	27	8352980		2013-01-08	Howcroft, Jerald Robert	
	28	8386386		2013-02-26	Zhu, Kevin	
	29	8340718		2012-12-25	Colonna, Massimo et al.	
	30	8385896		2013-02-26	Proctor, Jr., James A. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C03

	31	8320949		2012-11-27	Matta, Sudheer Poorna Chandra	
	32	8279864		2012-10-02	Wood, Daniel M.	
	33	8271045		2012-09-18	Parolkar, Satish et al.	
	34	8233883		2012-07-31	De Froment, Eric	
	35	8224382		2012-07-17	Bultman, Michael J.	
	36	8184590		2012-05-22	Rosenblatt, Ariel	
	37	8174970		2012-05-08	Adamczyk, Maria et al.	
	38	8165576		2012-04-24	Raju, Vishwanath et al.	
	39	8073721		2011-12-06	Lewis, Lundy	
	40	8032899		2011-10-04	Archer, Charles J. et al.	
	41	7974624		2011-07-05	Gallagher, Michael D. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C03

	42	7907970		2011-03-15	Park, Vincent D. et al.	
	43	7778176		2010-08-17	Morford, Michael Robert|	
	44	7725570		2010-05-25	Lewis, Lundy	
	45	7634388		2009-12-15	Archer, Charles J. et al.	
	46	7633438		2009-12-15	Tysowski, Piotr Konrad	
	47	7593417		2009-09-22	Wang, James et al.	
	48	7551922		2009-06-23	Roskowski, Steve et al.	
	49	7545782		2009-06-09	Rayment, Stephen G. et al.	
	50	7802724		2010-09-28	Nohr, Steven Paul	
	51	7039037		2006-05-02	Wang, Jiwei R. et al.	
	52	6928280		2005-08-09	Xanthos, James et al.	

IPR2025-01571
Apple EX1002 Page 510

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C03

	53	6765925		2004-07-20	Sawyer, Wilson et al.	
	54	5889477		1999-03-30	Fastenrath, Ulrich	
	55	8447980		2013-05-21	Godfrey, James A. et al.	
	56	8429403		2013-04-23	Moret, Eric et al.	
	57	8411587		2013-04-02	Curtis, William et al.	
	58	8396929		2013-03-12	Helfman, Nadav et al.	
	59	8363658		2013-01-29	Delker, Jason R. et al.	
	60	8265004		2012-09-11	Toutonghi, Michael J.	
	61	8233895		2012-07-31	Tysowski, Piotr Konrad	
	62	7685254		2010-03-23	Pandya, Ashish A.	
	63	7181017		2007-02-20	Nagel, Robert H. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C03

	64	6965872		2005-11-15	Grdina, Jerome M.	
	65	8402540		2013-03-19	Kapoor, Harsh et al.	
	66	8135657		2012-03-13	Kapoor, Harsh et al.	
	67	8271992		2012-09-18	Chatley, Scott P. et al.	
	68	8315999		2012-11-20	Chatley, Scott P. et al.	
	69	8332375		2012-12-11	Chatley, Scott P. et al.	
	70	8468337		2013-06-18	Gaur, Santosh P. et al.	
	71	8477778		2013-07-02	Lehmann, Jr., L. Curtis et al.	
	72	6640097		2003-10-28	Corrigan, Louis et al.	

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

U.S.PATENT APPLICATION PUBLICATIONS

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C03

	1	20080120668		2008-05-22	Yau, Frank Chuen-Foo	
	2	20030171112		2003-09-11	Lupper, Alfred et al.	
	3	20070300252		2007-12-27	Acharya, Swarup et al.	
	4	20050007993		2005-01-13	Chambers, Mahdi et al.	
	5	20020164983		2002-11-07	Raviv, Li-On et al.	
	6	20070280453		2007-12-06	Kelley, Sean S. et al.	

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

FOREIGN PATENT DOCUMENTS

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	1889777A	CN		2006-07-19	Huawei Tech. Co. Ltd.		☐
	2	101155343A	CN		2006-09-29	Huawei Tech. Co. Ltd.		☐
	3	101035308A	CN		2006-03-09	Huawei Tech. Co. Ltd.		☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C03

	4	2007124279	WO		2007-11-01	Cisco Technology, Inc.		☐
	5	2005008995	WO		2005-01-27	Starhub Ltd.		☐

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

NON-PATENT LITERATURE DOCUMENTS

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	2013-05-09 Non-Final Rejection in U.S. Application No. 13/712,184, filed December 12, 2012 and entitled "Automated Device Provisioning and Activation"	☐
	2	2012-10-03 Non-Final Rejection in U.S. Application No. 13/461,141, filed May 1, 2012 and entitled "Automated Device Provisioning and Activation"	☐
	3	2012-10-15 Amendment-Req. Reconsideration-After Non-Final Rejection in U.S. Application No. 13/461,141, filed May 1, 2012 and entitled "Automated Device Provisioning and Activation"	☐

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

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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C03

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		Date (YYYY-MM-DD)	2013-07-15
Name/Print	Krista S. Jacobsen	Registration Number	59374

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.**

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 January 2005 (27.01.2005)

PCT

(10) International Publication Number
WO 2005/008995 A1

(51) International Patent Classification[7]: H04L 29/06, 12/28

(74) Agent: DREW & NAPIER LLC; 20 Raffles Place, #17-00 Ocean Towers, Singapore 048620 (SG).

(21) International Application Number:
PCT/SG2004/000213

(22) International Filing Date: 16 July 2004 (16.07.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
200303828-8 21 July 2003 (21.07.2003) SG

(71) Applicant *(for all designated States except US)*: **STARHUB LTD** [SG/SG]; 51 Cuppage Road, #07-00 Starhub Centre, Singapore 229469 (SG).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **COOK, Peter John** [GB/SG]; 269 Bukit Timah Road, #04-08 Casa Rosita, Singapore 259707 (SG). **LEE, Walter, Kheng Kim** [SG/SG]; 18 Yew Siang Road, #02-02 Flynn Park, Singapore 117755 (SG). **LEE, Jin Hian** [MY/SG]; 114E Grange Road, Singapore 249598 (SG). **TAN, Samantha, Lay Har** [SG/SG]; Blk 34 Upper Cross St #13-132, Singapore 050034 (SG). **ANG, Kok Wah** [SG/SG]; Blk 62 Toa Payoh Lorong 4#26-101, Singapore 310062 (SG). **TAN, Cheow Ping** [MY/SG]; Blk 612 Clementi West Street 1#08-310, Singapore 120612 (SG).

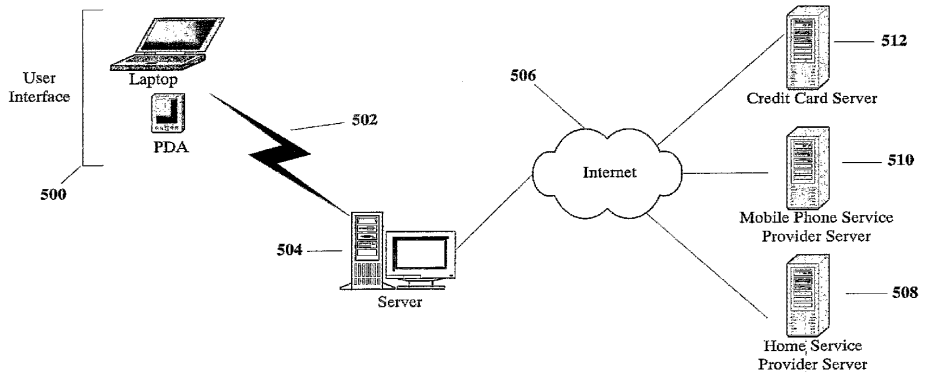
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *with amended claims*

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:** METHOD AND SYSTEM FOR USER-FRIENDLY LOGIN TO SELECTED INTERNET SERVICE PROVIDERS



(57) **Abstract:** A method and system is disclosed for roaming users to access a host service provider's network utilising a variety of authentication methods in an intuitive and user-friendly manner. The interface and workflow greatly enhances ease-of-use by minimising the amount of technical knowledge required by users and providing the ability for support pages to be delivered in user's native languages. This reduces user confusion and customer support costs.

WO 2005/008995 A1

METHOD AND SYSTEM FOR USER-FRIENDLY LOGIN
TO SELECTED INTERNET SERVICE PROVIDERS

FIELD OF INVENTION

The present invention relates to a method and system for allowing users to access a service provider's wireless LAN services in an intuitive and user-friendly manner while supporting a wide range of authentication & billing options.

BACKGROUND

The Internet consists of a large number of computers, devices and networks all interconnected via communications links. Users gain access to the Internet via communications service providers, which can be, among others, Internet service providers, wireless Internet service providers, mobile telephone service providers or fixed line service providers.

Such communications service providers typically have a limited footprint, that is, they can only provide local access to the Internet in certain areas. For example, a mobile telephone service provider may only provide access to the Internet when the mobile telephone user is within the defined coverage area of the said service provider's mobile network. Another example would be an internet service provider that maintains a national telephone number to deliver Internet access nationwide, but is unable to provide a local access number for a subscriber who travels out of the country of service.

In order to provide local Internet services, communications service providers enter into bilateral or multilateral roaming agreements with each other where they provide local ("host") services to subscribers of the other operators ("guests"). Authentication and billing services are provided by the subscribers' "home" operator, which will then settle with an aggregator or the "host" operator directly.

There are a number of access mechanisms for providing roaming local internet access. The most common is via dial-up access, where at least one local access telephone

IPR2025-01571
Apple EX1002 Page 517

(PSTN) number is provided to travellers to each region. Generally, dial-up roaming access is managed by client software that runs on the guest's computer. This software maintains a searchable database of access numbers for every region and will automatically dial an appropriate local access number based on the guest's indicated current location.

A new and emerging method for providing roaming internet access is the IEEE 802.11 series of Wireless LAN technologies, known as WLAN or WiFi "hot-spots." Because WLAN hotspots do not require the use of a telephone (PSTN) number, access is typically currently managed by having a "walled garden" that allows any user to connect to the hotspot, but not go beyond the boundaries of the hotspot. All traffic out of the hotspot is blocked, and all World-Wide Web (HTTP) requests are redirected to a "landing page" which allows guest identification via a username or password pair.

There are a couple of problems with the existing method. First, a guest's native language may be different from that of the landing page, or a client may not be available in the guest's native language. This could potentially confuse the guest, thus leading to lost revenue and higher customer support costs.

Another shortcoming of existing methods is that they generally require guests to follow a slightly different log-in procedure while they are roaming. Instead of merely entering their username and password as they do while they are at home, guests must now enter their username followed by a "domain" in the form username@domain. This additional information is required to allow the host service provider to identify the home provider communications company, but adds an additional burden to the user, and is non-intuitive.

SUMMARY OF THE INVENTION

It is therefore a first object of the present invention to provide a method or system for wireless network or internet access which goes some way to overcoming the above mentioned disadvantages in the prior art or which will at least provide the public with a

IPR2025-01571
Apple EX1002 Page 518

useful choice.

It is a second object of the invention to provide a method and a system that allows a roaming user to utilise the services of a service provider in an intuitive manner, whether or not the user has any pre-existing relationship with the service provider. The user operates a client system that is provided an identifier that identifies a login session. The client system provides the provided identifier to an authentication server system, together with information about the user's identity & billing relationship and a request to gain access to the Internet. The authenticating server verifies the billing relationship, referring some or all of the provided information to other servers as necessary, then grants or denies services to the requesting client system.

Accordingly in a first aspect the present invention consists in a system for providing wireless network or internet access comprising:

an interface configured to input a selection from predetermined service providers

a display configured to enable authentication to said selected service provider in a language and layout depending on said selection

a server allowing network or internet access depending on the success of said authentication.

Preferably said system further comprising a billing module configured to associate a cost with any authenticated network or internet access according to predetermined criteria and communicate said cost to said selected service provider to allow billing.

Preferably said display configured to provide an authentication web page substantially the same layout and language as would be experienced with direct network or internet access through said selected service provider.

Preferably said display configured to provide information at least depending on said cost or said predetermined criteria.

In a second aspect the present invention consists in a system for providing wireless network or internet access configured to:

store predetermined service providers

input a selection from said predetermined service providers

attempt to authenticate to the selected service provider in a format dependant on said selection, and

IPR2025-01571
Apple EX1002 Page 519

allow network or internet access dependant on whether said authentication is successful.

Preferably said system further configured to input any further information dependant on said selection and optionally using said further information in said attempted authentication.

Preferably said system further comprising a RADIUS proxy allowing authentication with a RADIUS proxy server associated with said selected service provider.

Preferably said system configured to communicate with a remote user terminal, wherein a user is able to select a service provider and can authenticate to the selected service provider using the service providers own web page on a remote user terminal.

Preferably said web page is substantially the same layout and language as would be experienced with direct network or internet access through said selected service provider.

Preferably said system configured to supply billing information to said selected service provider dependant on network or internet access provided.

Preferably said system configured to allow further attempts if said authentication is unsuccessful.

In a third aspect the present invention consists in a method of allowing access to the Internet for a user comprising the steps of:

storing predetermined service providers

inputting a selection from said predetermined service providers

attempting to authenticate to the selected service provider in a format dependant on said selection, and

allowing network or internet access dependant on whether said authentication is successful.

Preferably said method further comprising the step of inputting any further information dependant on said selection and optionally using said further information in said attempted authentication.

Preferably said method further comprising the step of authenticating between a local RADIUS proxy and a RADIUS proxy associated with said selected service

IPR2025-01571
Apple EX1002 Page 520

provider.

Preferably said method configured to communicate with a remote user terminal, wherein a user is able to select a service provider and can authenticate to the selected service provider using the service providers own web page on a remote user terminal.

Preferably said web page is substantially the same layout and language as would be experienced with direct network or internet access through said selected service provider.

Preferably said method configured to supply billing information to said selected service provider dependant on network or internet access provided.

Preferably said method configured to allow further attempts if said authentication is unsuccessful.

To those skilled in the art to which the invention relates, many changes in construction and widely differing embodiments and applications of the invention will suggest themselves without departing from the scope of the invention as defined in the appended claims. The disclosures and the descriptions herein are purely illustrative and are not intended to be in any sense limiting.

The invention consists in the foregoing and also envisages constructions of which the following gives examples.

BRIEF DESCRIPTION OF THE DRAWINGS

The preferred forms of the present invention will now be described with reference to the accompanying drawings in which:

Figure 1 A flow diagram of the entire log-in process for a guest at a host operator using the access control panel to authenticate via a roaming agreement with a home operator

Figure 2 Illustrates the "landing page" (displayed by the client) that greets a guest upon an attempt to access the host service provider network.

Figure 3 Illustrates the guest's home operator page (displayed by the client) that is used to provide native language support information, authenticate and bill for the network session via a roaming agreement with the home operator

IPR2025-01571
Apple EX1002 Page 521

Figure 4 A block diagram illustrating an embodiment of the present invention that allows a user to gain access to the network via multiple authentication and billing options.

Figure 5 is a block diagram indicative of the hardware involved in the communication paths there between.

PREFERRED MODE OF IMPLEMENTING THE INVENTION

In a first preferred embodiment of the present invention a method and system for roaming users to access a host service provider's network is provided which utilises a variety of authentication methods in an intuitive and user-friendly manner. In this embodiment an interface and workflow is provided which greatly enhances ease-of-use by minimising the amount of technical knowledge required by users and providing the ability for support pages to be delivered in users' native languages. This reduces user confusion and customer support costs while facilitating the growth of the roaming Internet user market.

In one embodiment, the service gateway controlling network access assigns a unique identifier to the client (such as a Web browser or custom software) upon an access attempt. The identifier allows the service gateway to identify the unique login session. The client then allows the user to select a supported billing relationship, including, but not limited to, the user's home operator or clearinghouse which is affiliated with the host service provider, a mobile telephone service provider or a credit card account. The client provides the selected identifier together with the chosen billing relationship to the service gateway, which then determines the appropriate content that the client should display in order to collect any necessary information as shown in Figure 2.

Access option # 1 (100) could for example represent a selection of affiliated or supported home operators from which the user can one click select (102). Access option # 2 (104) could for example be a drop down box of supported or affiliated mobile telephone service providers from which the user could similarly one click select the provider which they already have a billing relationship with. It is necessary that each of

IPR2025-01571
Apple EX1002 Page 522

the options the user is able to select are predetermined so that the service gateway is able to determine the appropriate remote servers to communicate with as well as further content required. If the users home operator is not affiliated then the credit card option e.g. access option # 3 (106) may still allow access.

Home Service Provider Selection

In particular, if the user's chosen billing relationship allows identification of the user's home service provider, country of origin or preferred language, the service gateway can provide the client with general support information and specific login procedures (e.g. via a Web page) in the user's native language and in a format & layout that would be most familiar to the user as seen in Figure 3.

For example the user ID (200) would be entered along with the password (202) in a single frame where the user might click on login (206). An advantage to this embodiment of the present invention is that the home operator's login page is familiar to the user both in language and environment such that the user is easily able to gain access.

Once the appropriate content has been identified, the service gateway sends it to the client, along with the previously-assigned identifier, a second identifier that indicates the chosen billing relationship and instructions to the client to collect any further required information from the user. One skilled in the art would appreciate that the service gateway need not be a monolithic element – for example, the logic that determined the appropriate information to deliver to the client could reside on a separate system that communicated with the service gateway in a manner transparent to the client.

Authentication

Referring to Figure 1 once the guest has selected the home operator (300) and the user has entered the password and ID (302), the client logic appends the appropriate realm suffix (304) to the user ID according to the specific home operator selected. The service gateway then sends the credentials to the home operator radius proxy via the

IPR2025-01571
Apple EX1002 Page 523

host's radius proxy (306). If the authentication is successful the customer is granted access (308) and can use the Internet in a normal fashion. If authentication is not successful the user is prompted for the ID and password again (310), optionally after a set number of attempts the user will be currently blocked.

The client processes the server's instructions, displays the content to the user and collects any other required information from the user before returning all relevant information to the server for processing, including the identifiers provided by the server.

Upon receipt of all necessary information required to successfully authenticate and bill the user via the selected billing mechanism, the service gateway will query various specialised upstream servers (which could include RADIUS or merchant servers), providing them with the necessary information to enable them to verify the user's credentials and return an appropriate result. Based on the outcome of this verification process, the service gateway will grant or deny the user's system access to the network.

Internet Access

Referring to Figure 4 the network server (400) includes the server engine (402) the host radius proxy (404) the host user database (406) which in turn communicate through the service control point (408) to the user's browser (410). Other communication includes links to the home radius proxy (412) the home user database (414) and other authentication servers (416). Once authentication takes place the server engine (402) allows access in that web page request etc form the user's browser (410) are passed through to the internet and the resulting data stream is passed back to the user's browser (410).

Referring to Figure 5 the hardware layout is illustrated. Interface (500) may for example represent the users own computer, a WAP phone or other WiFi capable data device. It is also possible that the hotspot could provide its own terminals with the facility through the present invention of billing for their use through the users home service provider. Wireless communication (502) between Interface (500) and server

IPR2025-01571
Apple EX1002 Page 524

(504) occurs according to any of the proceeding embodiments of the present invention. Server (504) may communicate through the internet (506), network or other communication paths to a plurality of home service provider servers' (508), mobile phone service provider servers' (510), credit card service provider servers' (512) and any other affiliated service provider servers' or clearinghouse authentication servers'.

IPR2025-01571
Apple EX1002 Page 525

CLAIMS:

1. A system for providing wireless network or internet access comprising:

an interface configured to input a selection from predetermined service providers

a display configured to enable authentication to said selected service provider in a language and layout depending on said selection

a server allowing network or internet access depending on the success of said authentication.

2. A system as claimed in claim 1 further comprising a billing module configured to associate a cost with any authenticated network or internet access according to predetermined criteria and communicate said cost to said selected service provider to allow billing.

3. A system as claimed in claim 2 wherein said display configured to provide an authentication web page substantially the same layout and language as would be experienced with direct network or internet access through said selected service provider.

4. A system as claimed in claim 3 wherein said display configured to provide information at least depending on said cost or said predetermined criteria.

5. A system for providing wireless network or internet access configured to:

store predetermined service providers

input a selection from said predetermined service providers

attempt to authenticate to the selected service provider in a format dependant on said selection, and

allow network or internet access dependant on whether said authentication is successful.

6. A system as claimed in claim 5 further configured to input any further information dependant on said selection and optionally using said further information in said attempted authentication.

IPR2025-01571
Apple EX1002 Page 526

7. A system as claimed in claim 5 further comprising a RADIUS proxy allowing authentication with a RADIUS proxy server associated with said selected service provider.

8. A system as claimed in claim 7 configured to communicate with a remote user terminal, wherein a user is able to select a service provider and can authenticate to the selected service provider using the service providers own web page on a remote user terminal.

9. A system as claimed in claim 8 wherein said web page is substantially the same layout and language as would be experienced with direct network or internet access through said selected service provider.

10. A system as claimed in claim 7 configured to supply billing information to said selected service provider dependant on network or internet access provided.

11. A system as claimed in claim 8 configured to allow further attempts if said authentication is unsuccessful.

12. A method of allowing access to the Internet for a user comprising the steps of:

storing predetermined service providers

inputting a selection from said predetermined service providers

attempting to authenticate to the selected service provider in a format dependant on said selection, and

allowing network or internet access dependant on whether said authentication is successful.

13. A method as claimed in claim 12 further comprising the step of inputting any further information dependant on said selection and optionally using said further information in said attempted authentication.

14. A method as claimed in claim 12 further comprising the step of authenticating

IPR2025-01571
Apple EX1002 Page 527

between a local RADIUS proxy and a RADIUS proxy associated with said selected service provider.

15. A method as claimed in claim 14 configured to communicate with a remote user terminal, wherein a user is able to select a service provider and can authenticate to the selected service provider using the service providers own web page on a remote user terminal.

16. A method as claimed in claim 15 wherein said web page is substantially the same layout and language as would be experienced with direct network or internet access through said selected service provider.

17. A method as claimed in claim 15 configured to supply billing information to said selected service provider dependant on network or internet access provided.

18. A method as claimed in claim 16 configured to allow further attempts if said authentication is unsuccessful.

IPR2025-01571
Apple EX1002 Page 528

AMENDED CLAIMS

[received by the International Bureau on 04 January 2005 (04.01.2005);
original claims, 1, 5, 12, amended, remaining claims unchanged (03 pages)]

1. A system for providing a billing arrangement for wireless network or internet access for an unknown user comprising:

an interface configured to input a selection from predetermined service providers;

a display configured to request authentication information for said selected service provider in a language and layout depending on said selection;

a communication link to said selected service provider, configured to send said authentication information to said selected provider and receive back either a verification or denial of an existing billing arrangement with said unknown user;

a server allowing network or internet access depending on the verification of said authentication information.

2. A system as claimed in claim 1 further comprising a billing module configured to associate a cost with any authenticated network or internet access according to predetermined criteria and communicate said cost to said selected service provider to allow billing.

3. A system as claimed in claim 2 wherein said display configured to provide an authentication web page substantially the same layout and language as would be experienced with direct network or internet access through said selected service provider.

4. A system as claimed in claim 3 wherein said display configured to provide information at least depending on said cost or said predetermined criteria.

5. A system for providing wireless network or internet access including control means having a stored program which when executed on said control means is characterised by:

storing predetermined service providers

receiving a user selection from said predetermined service providers

requesting authentication information via a predetermined format dependant on said selection,

attempting to authenticate to the selected service provider using received

IPR2025-01571
Apple EX1002 Page 529

authentication information, and

allowing network or internet access dependant on whether said authentication is successful.

6. A system as claimed in claim 5 further configured to input any further information dependant on said selection and optionally using said further information in said attempted authentication.

7. A system as claimed in claim 5 further comprising a RADIUS proxy allowing authentication with a RADIUS proxy server associated with said selected service provider.

8. A system as claimed in claim 7 configured to communicate with a remote user terminal, wherein a user is able to select a service provider and can authenticate to the selected service provider using the service providers own web page on a remote user terminal.

9. A system as claimed in claim 8 wherein said web page is substantially the same layout and language as would be experienced with direct network or internet access through said selected service provider.

10. A system as claimed in claim 7 configured to supply billing information to said selected service provider dependant on network or internet access provided.

11. A system as claimed in claim 8 configured to allow further attempts if said authentication is unsuccessful.

12. A method of allowing access to the Internet for a user comprising the steps of:

storing predetermined service providers,

receiving a user selection from said predetermined service providers,

requesting authentication information via a predetermined format dependant on said selection,

IPR2025-01571
Apple EX1002 Page 530

attempting to authenticate to the selected service provider using received authentication information, and

allowing network or internet access dependant on whether said authentication is successful.

13. A method as claimed in claim 12 further comprising the step of inputting any further information dependant on said selection and optionally using said further information in said attempted authentication.

14. A method as claimed in claim 12 further comprising the step of authenticating between a local RADIUS proxy and a RADIUS proxy associated with said selected service provider.

15. A method as claimed in claim 14 configured to communicate with a remote user terminal, wherein a user is able to select a service provider and can authenticate to the selected service provider using the service providers own web page on a remote user terminal.

16. A method as claimed in claim 15 wherein said web page is substantially the same layout and language as would be experienced with direct network or internet access through said selected service provider.

17. A method as claimed in claim 15 configured to supply billing information to said selected service provider dependant on network or internet access provided.

18. A method as claimed in claim 16 configured to allow further attempts if said authentication is unsuccessful.

IPR2025-01571
Apple EX1002 Page 531

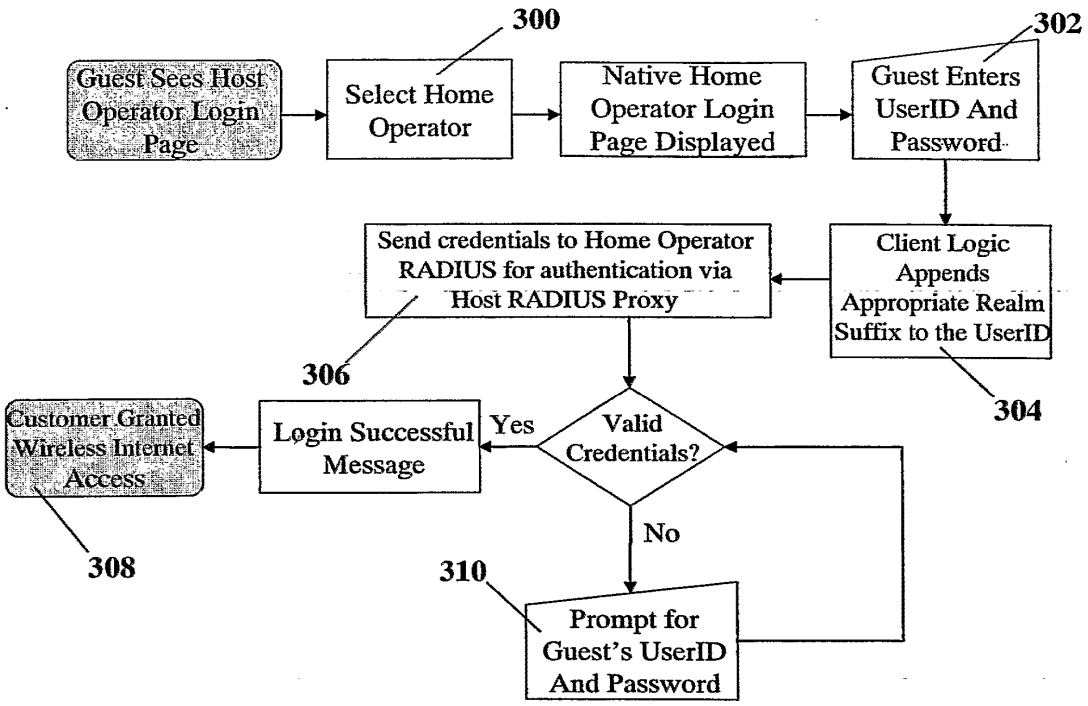


FIGURE 1

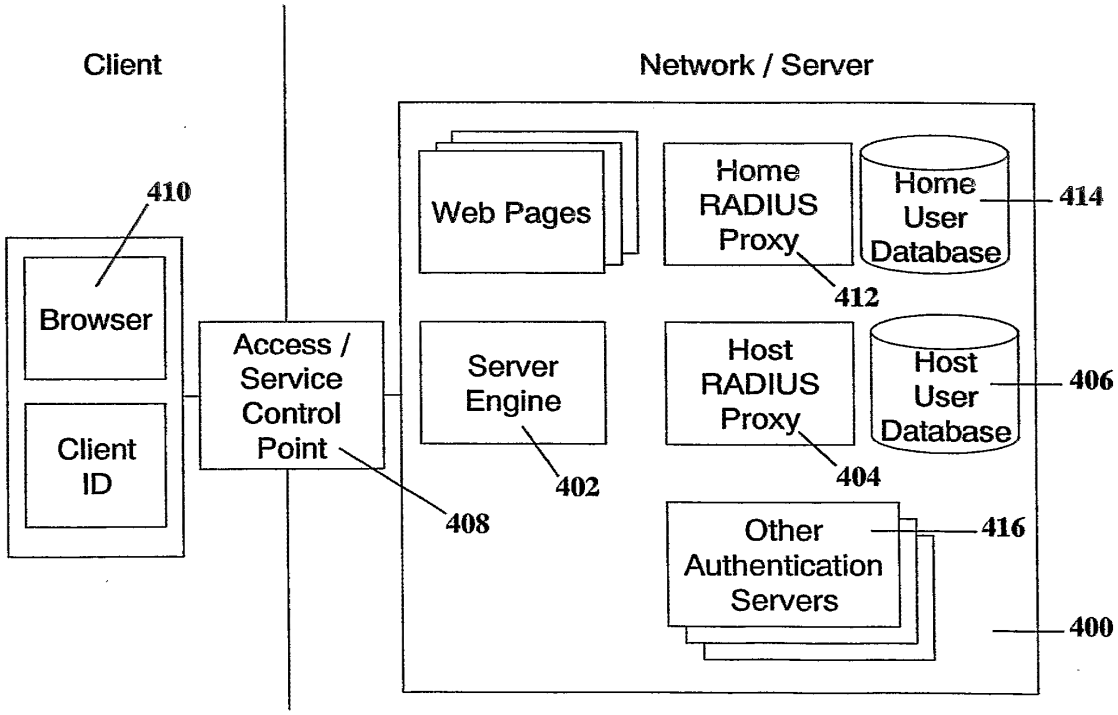


FIGURE 4

IPR2025-01571
Apple EX1002 Page 532

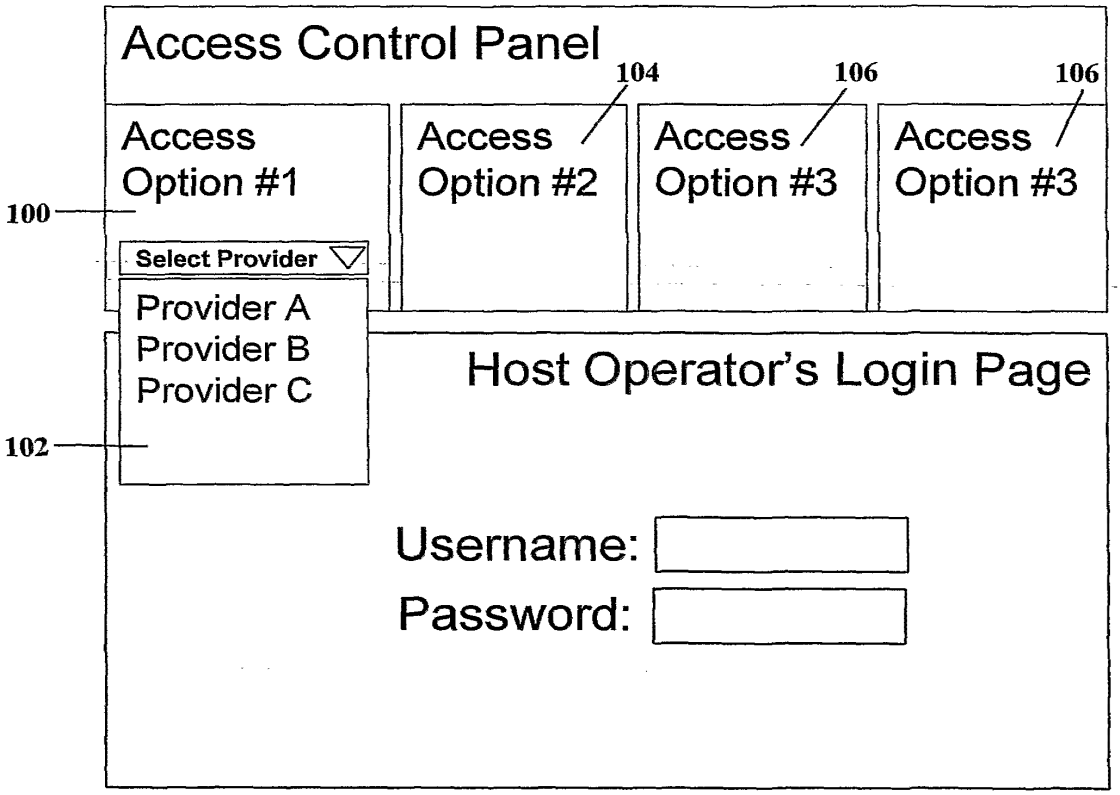


FIGURE 2

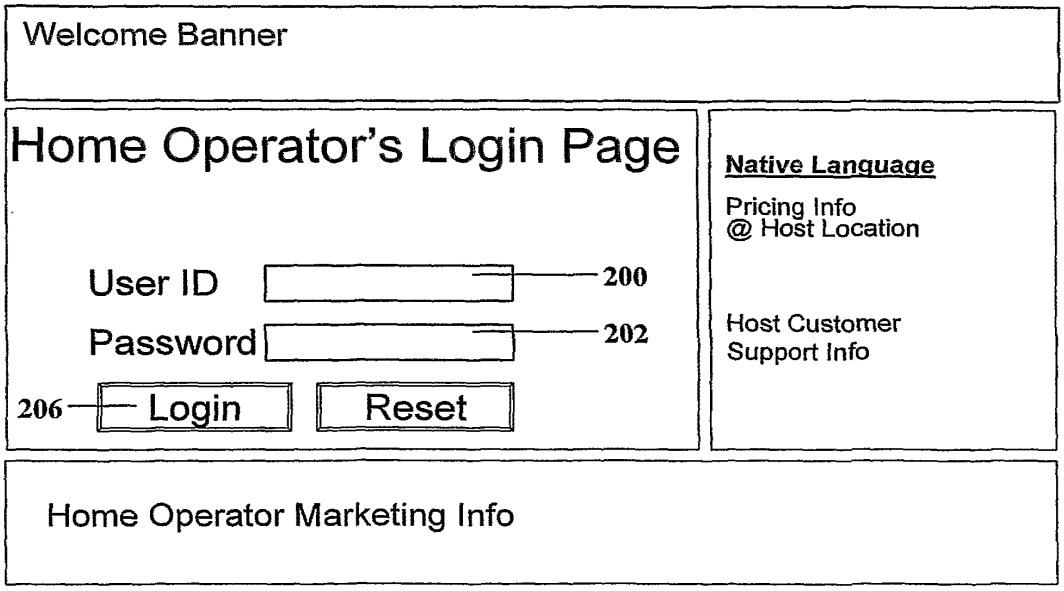


FIGURE 3

IPR2025-01571
Apple EX1002 Page 533

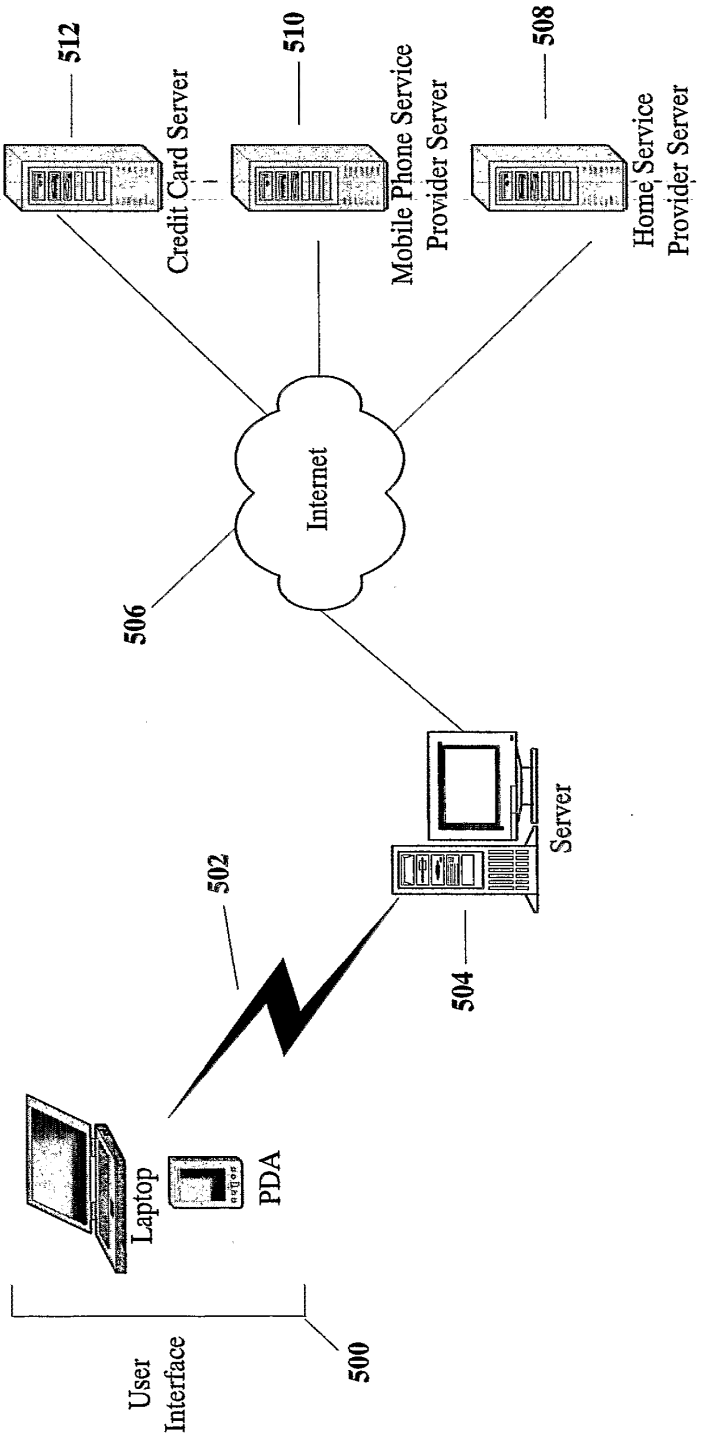


FIGURE 5

IPR2025-01571
Apple EX1002 Page 534

INTERNATIONAL SEARCH REPORT

International Application No
PCT/SG2004/000213

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 H04L12/28

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC, COMPENDEX, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 241 902 A (STAR HOME GMBH) 18 September 2002 (2002-09-18) paragraphs '0227! - '0242! paragraphs '0253! - '0262! figures 2-6	1-18
Y	US 5 881 234 A (SCHWOB PIERRE R) 9 March 1999 (1999-03-09) column 3, line 4 - column 5, line 21; figure 1	1-18

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 October 2004	04/11/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Bengi-Akyuerek, K

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/SG2004/000213

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	DATABASE WPI Section EI, Week 200257 Derwent Publications Ltd., London, GB; Class T01, AN 2002-534781 XP002302414 YOON H S: "Multinational electronic commerce method using internet" & KR 2002 011 604 A ((YOON-I) YOON H S) 9 February 2002 (2002-02-09) abstract	1-18
A	US 5 898 780 A (LU JUAN ET AL) 27 April 1999 (1999-04-27) column 1, line 9 - column 2, line 4 figures 1-8	1-18

Form PCT/ISA/210 (continuation of second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/SG2004/000213

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1241902 A	18-09-2002	EP 1241902 A2	18-09-2002
		EP 1347661 A1	24-09-2003
		US 2002164983 A1	07-11-2002
US 5881234 A	09-03-1999	AU 2992897 A	19-11-1997
		WO 9741586 A1	06-11-1997
KR 2002011604 A	09-02-2002	NONE	
US 5898780 A	27-04-1999	NONE	

Form PCT/ISA/210 (patent family annex) (January 2004)

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 November 2007 (01.11.2007)

PCT

(10) International Publication Number
WO 2007/124279 A2

(51) International Patent Classification:
H04M 1/66 (2006.01)

(21) International Application Number:
PCT/US2007/066514

(22) International Filing Date: 12 April 2007 (12.04.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/408,764 21 April 2006 (21.04.2006) US

(71) Applicant *(for all designated States except US)*: **CISCO TECHNOLOGY, INC., ET AL.** [US/US]; 170 West Tasman Drive, Sjc/10/2/1, San Jose, California 95134-1706 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **LEE, Shze Chew** [MY/US]; 881 Las Palmas, Irvine, California 92602 (US). **GUTMAN, Andrew M.** [US/US]; 26 Saucito, Foothill Ranch, California 92610 (US). **WILLIS, Edward Dean** [US/US]; 3100 Independence Parkway #311-164, Plano, Texas 75075 (US).

(74) Agents: **LAFFERTY, Wm. Brook** et al.; Scientific-Atlanta, Inc., Intellectual Property Dept., 5030 Sugarloaf Parkway, Lawrenceville, Georgia 30044 (US).

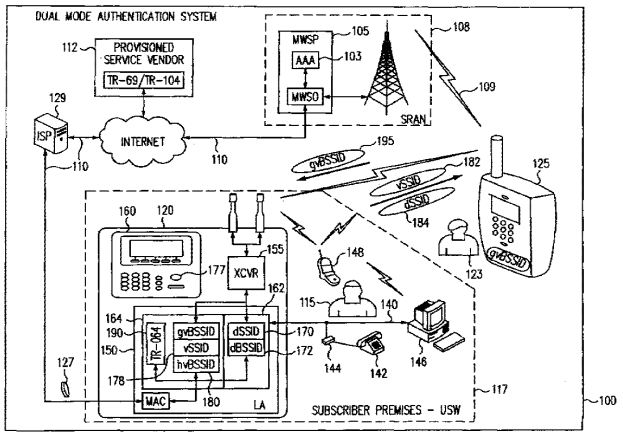
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, 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, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

[Continued on next page]

(54) Title: SIMPLIFIED DUAL MODE WIRELESS DEVICE AUTHENTICATION APPARATUS AND METHOD



(57) Abstract: Provisioned wireless service (PWS) authentication apparatus and method simplifies determination of PWS authentication state by dual mode access point (DMAP) receiving an identifying credential from supplicant dual mode mobile station (DMMS) within predefined authentication period and comparing with authentication credential. DMMS is provisioned PWS upon authentication. DMAP having multiple BSSID remotely configurable to differentiate between provisioned services (e.g., voice, VoIP) and standard wireline/fixed wireless services. DMAP and DMMS are each identifiable by respective unique provisioned service BSSID. Identifying credential can be pass code supplied to DMMS user by DMAP operator to facilitate authenticated association and to deter wireless channel interlopers.

WO 2007/124279 A2

IPR2025-01571
Apple EX1002 Page 538

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.

SIMPLIFIED DUAL MODE WIRELESS DEVICE AUTHENTICATION APPARATUS AND METHOD

by

SHZE CHEW LEE
ANDREW GUTMAN
EDWARD DEAN WILLIS

TECHNICAL FIELD

The present invention relates to security apparatus and methods and, in particular, to apparatus and methods for authentication of a dual-mode wireless device.

BACKGROUND

With the confluence of electronic communications, data, and computing services, (collectively, services) there arises a need to bridge the disparate network infrastructures supporting these services and to address resulting new opportunities and challenges. A wireline network (WLN) employs a structured transmission medium, including copper wire, fiber optic cable, and other defined waveguides. By comparison, a wireless network can be any network with a physical layer that permits constituent devices to communicate using an unstructured transmission medium, such as the atmosphere, or space. Wireless networks have developed within two formerly distinct

IPR2025-01571
Apple EX1002 Page 540

spheres: wireless wide area networks (WWAN), which were cast in the formal likeness of wireline telephony networks; and wireless local area networks (WLAN), which are often informally structured, if at all, having coverage zones of at least three of magnitude less than a WWAN. Currently popular WWAN networks can provide mobile wireless services, as specified by the AMPS, D-AMPS, PCS, GSM, and UMTS wireless mobile service standards. A growing diversity of WLAN standards describe the physical-to-network architectures of fixed wireless services, with devices operable with WLAN frequently being capable of being operable with more than one type of fixed wireless service. Dual-mode devices were developed to meet the diverse needs of those using both WWAN and WLAN systems.

Dual-mode services are becoming attractive to mobile operators and their subscribers because of three trends: a growing population of mobile subscribers, the prevalence of home broadband connections, and the availability of low-cost, home wireless access points that support local wireless networking. To satisfy this evolving need, technology manufacturers are developing and introducing into the marketplace, dual-mode devices, that is, devices capable of communicating over mobile radio networks, such as mobile phone networks, and wireless local area networks,

IPR2025-01571
Apple EX1002 Page 541

such as those found in the increasingly popular "hotspots," or access zones for wireless networking, frequently providing the myriad of services available over the Internet.

A dual mode device can offer advantages over a single mode device. First, although mobile wireless systems may provide mobile wireless services to the high-mobility receiving stations of subscribers within a broad geographic area, they bear the disadvantages of poor indoor reception and uneven signal availability, particularly in dense urban environments hilly terrain. Second, fixed wireless systems can deliver a vast range of broadband services to stationary or low-mobility receivers located indoors, within a broadcast zone (e.g., hot spots or hot zones), but are disadvantaged by sharply-limited signal range, security and billing concerns, and the uncertainties arising from proprietary ownership and non-uniform product availability. Thus, a dual-mode device can enable a mobile service subscriber to switch from mobile wireless services to fixed wireless services, for example, in an area of poor mobile wireless service coverage. In addition, with a dual-mode device, using dual-mode services, mobile wireless service subscribers may make voice calls when outdoors in the ordinary manner, using the facilities of the subscribed

IPR2025-01571
Apple EX1002 Page 542

mobile wireless service at the standard tariff rate. While indoors or in a remote geographic location where a signal compatible with the subscribed mobile wireless network is unavailable, a dual-mode device may permit customers to make and receive voice calls using a fixed wireless network. To reflect the offloading of the subscriber's call bandwidth from the mobile wireless service provider's to a less-expensive fixed wireless network and the Internet, the mobile wireless provider may offer the mobile wireless subscriber lower tariff rates when using a fixed-wireless link. Also, a dual-mode device makes possible voice call handoff and transfer of communication links as a subscriber roams between mobile wireless and fixed wireless systems. Furthermore, dual-mode devices and services create an opportunity for subscribers or vendors who wish to assist a third party with obtaining provider-authorized allocations of mobile wireless voice or dual-mode services. Nevertheless, there is a substantial need to provide apparatus and methods rendering the desired degree of security to protect a mobile wireless provider infrastructure from Internet-based threats, as well as to safeguard provider network operator for their subscribers from interlopers and miscreants.

IPR2025-01571
Apple EX1002 Page 543

BRIEF DESCRIPTION OF THE DRAWINGS

These and other features, aspects and advantages of the present invention will be more fully understood when considered with respect to the following detailed description, appended claims and accompanying drawings, wherein:

FIG. 1 is a graphical depiction of a dual-mode authentication system, as an embodiment of the invention herein;

FIG. 2 is a generalized flow diagram of a subscriber-provisioner dual-mode authentication operation, according to an embodiment of the present invention; and

FIG. 3 is a generalized flow diagram of a subscriber-passthrough dual-mode authentication operation, according to another embodiment of the present invention.

DETAILED DESCRIPTION

The inventive embodiments of the invention described herein include apparatus and methods for provisioning provisioned wireless services (PWS) to an authorized device by a provisioned service provider (PSP) in which a supplicant device may become an authorized device after successful authentication. A PWS can be any wireless service including, without limitation voice service, short

IPR2025-01571
Apple EX1002 Page 544

message service (SMS), multimedia message service (MMS), video broadcasts, instant messaging, news and financial information, games and interactive gaming, Web-based services, and premium data services, to name a few.

A PSP can be a mobile wireless service provider, which also may operate a WWAN, also known as a radio area network, or RAN. A mobile telephone network is an exemplary RAN. Typically, WWAN provide service signals over a broad geographic region, using high-powered (more than 10W per channel) transmitters that are licensed to broadcast within defined frequency bands, which typically are allocated and regulated by a public authority. WWAN signals may be encoded or use sophisticated signaling techniques to provide privacy between communicating parties from potential eavesdroppers. Current WLAN transmit signals that are low-powered (under 0.1W per channel), limited-range (under about 300 m), and generated within prescribed frequency bands (e.g., 2.4 GHz, 5 GHz, 11 GHz, and 60 GHz). In general, such fixed wireless networks may be designated "unlicensed spectrum" wireless networks (USW), because by international consent, no operating license is required for wireless systems designed to operate within these constraints. USW can include networks employing the wireless protocols defined by the IEEE Std.

IPR2025-01571
Apple EX1002 Page 545

802.11 family of standards (including IEEE WLAN Stds. 802.11a, 802.11b, 802.11g, 802.11n, and 802.11j); IEEE Std. 802.15 (including wireless personal area networks - WPAN); IEEE Std. 802.16 (including wireless metropolitan area networks - WMAN); and by the ETSI Broadband Radio Access Network and Radio LAN Standards (e.g., HiperLAN2, HiperMAN, and HiperRAN), as well as, the TTR Korea WiBRO mobile network standard.

In large part, a wireline network (WLN) can be based on one of the family of standards, IEEE Std. 802.3 CSMA/CD Access Method, including 10 Mbps "Ethernet" (Stds. 802.3a, 802.3i, and 802.3j), 100 Mbps "Fast Ethernet" (Std. 802.3u), 1000 Mbps Gigabit Ethernet [GbE] (Stds. 802.3z, 802.3ab), and 10,000 Mbps GbE (Std. 802.3ae) Because IEEE Stds. 802.3 specify the lowermost networking layers (e.g., OSI Layers 1-3), the inventive embodiments herein are foreseeably operable with access technologies having bandwidth greater than 10 Gigabit Ethernet WLN. Each of the foregoing standards and specifications are incorporated herein, in their entirety. Also as used herein, the term generic access network (GAN) refers to both USW and WLN, when convenient to distinguish both from RAN-based networks. Furthermore, a WLN may include the Internet,

IPR2025-01571
Apple EX1002 Page 546

where a person having ordinary skill in the art would recognize that inclusion is appropriate.

As used herein, the like terms "provision" and "provisioned" in verb form, and "provisioning" in gerund form, refer to a process including one or more of, without limitation: creating for an authorized user a service account for a subscribed service, the appropriate access to that account, the rights associated with that account, and the resources for managing the accounts; configuring one or both of authorized user hardware and software to activate the subscribed service; creating or modifying a record in an authorized user database and associating it with the service(s) and service level for which the authorized user has subscribed; providing the authorized user with subscribed provisioned wireless service resources, in accordance with the subscription agreement; and issuing preselected allocation units of PWS to the authorized user, upon request. Performing AAA services in conjunction with PWS requests and usage can be a provisioning activity as well. In general, AAA services include authentication, authorization and accounting, whereby prior to service, a PWS requester is authenticated and authorized to use the service offered by a MWSP or PSV in response to the PWS request; and while the PWS is delivered, PWS usage is

IPR2025-01571
Apple EX1002 Page 547

metered and usage data is collected and can be associated with billing and collection.

PWS offered over a subscribed RAN (SRAN) typically are within the context of well-established and highly regulated access control, security, integrity, cost recovery, billing, enforcement, and Quality of Service mechanisms. GAN may lack one, more, or all of these features, simplifying the quest of unscrupulous users to purloin, misuse, or compromise valuable wireless services. To address the disparities in the regulatory and business structures between SRAN and GAN, and to encourage providers to offer valuable data and services regardless of the transmission medium used, a number of entities have put forth standards, provisional recommendations, and proposals for interoperative infrastructure management and policy enforcement. Pragmatic implementations tend to control access to services at a point close to service use, namely the customer premises, by remote management of customer premises equipment (CPE) through which such data and services are requested.

It is desirable to implement embodiments of the present invention in cooperation with remotely managed customer premises equipment (CPE) in accordance with a managed access architecture, premises network, and

IPR2025-01571
Apple EX1002 Page 548

management, control, and interoperability principles and standards, articulated by the following exemplary DSL Forum Technical Reports, as amended: TR-044, Auto-Configuration for Basic Internet (IP-based) Services, December 2001; TR-046 Auto-Configuration Architecture & Framework, February 2002; TR-064, LAN-Side DSL CPE Configuration, May 2004; TR-069, CPE WAN Management Protocol, May 2004; TR-092, Broadband Remote Access Server (BRAS) Requirements Document, August 2004; TR-094, Multi-Service Delivery Framework for Home Networks, August 2004; TR-104, DSLHome™ Provisioning Parameters for VoIP CPE, September 2005; TR-110, DSLHome™ Reference Models for VoIP Configurations in the DSL Home, September 2005; and TR-111, Applying TR-069 to Remote Management of Home Networking Devices, December 2005. It is to be understood that other CPE-management models also may apply, including without limitation, those described in European Telecommunications Standards Institute document: Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); NGN management; OSS Architecture Release 1 (ETSI TS 188 001 V0.2.9 (2005-07)); and by IEEE Std. 802.21. The foregoing standards of the IEEE, ETSI, Korea TTR, and DSL Forum are incorporated herein by reference, in their entirety.

IPR2025-01571
Apple EX1002 Page 549

In general, the three fundamental security processes include access control, authentication, and audit. Of these constituent security processes, access control is a policy-based process that determines whether a supplicant is permitted to access a requested resource or service (i.e., "Are you permitted to access this resource?"). Authentication is a credential-based process by which a supplicant verifies its identity to the authenticator (i.e., "Are you who you say you are?"). Authentication also may include identification, and non-repudiation functions. Audit is an administrative process by which the appropriateness of policy-defined access to resources is monitored, and by which security enforcement mechanisms may be invoked upon identification of a policy violation. Audit also may include analysis of integrity (e.g., of link, data, or identity), intrusion detection, and containment. Finally, authorization can be an executive process that comprehends at least two of the constituent security processes, usually incorporating requirements of security policy, regulatory framework, and the like. For example, in an authorization process where a security policy implements authentication, a supplicant is required to prove its identity before access credentials are issued to the supplicant. In practice, security processes may

IPR2025-01571
Apple EX1002 Page 550

vary in scope vertically and horizontally, and be almost as diverse in implementation as the applications needing security. A security process of vertical scope may operate at increasingly complex and abstract layers, e.g., authentication may be described within the context of a device level, a user level, an organization level, and an enterprise level. Similarly, horizontal security processes can include compartments that span communication occurring at one or more points along a communication path. For example, authentication may be compartmentalized with respect to a simple device-to-device exchange, to remote network links, or to a complete end-to-end secure communication exchange. End-to-end security also may result from cooperation of a sequence of cooperating authentication compartments which, in the whole, span the communication path. Frequently, contiguous subprocesses interact or overlap, although there may be no requirement for a given security process to be continuously operable over any portion of the communication path or over more than one physical or logical layer. Cryptographic processes may also be a constituent of authorization, and may include key creation, management, and distribution and encrypted communications. Thus, even if a supplicant is properly authenticated to the desired horizontal and

IPR2025-01571
Apple EX1002 Page 551

vertical layers of security, the supplicant may not be able to participate in particular communications because the authorization process denied a requisite encryption key to the supplicant. The aforementioned security principles, as used herein are provided in National Institute of Standards and Technology (NIST) Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook; and NIST Special Publication 800-48, Wireless Network Security: 802.11, Bluetooth and Handheld Devices, which documents are hereby incorporated herein in their entirety. Desirably, security processes exemplified in the present embodiments can implement or facilitate AAA processes of a provisioned service provider, and may further be enhanced by remote configuring of a local authenticator in an USW access point, in accordance with a foregoing remote configuration as a CPE.

Within the above context, FIG. 1 illustrates an embodiment of dual-mode authentication system 100 according to the present invention that includes a USW access point. Mobile wireless service provider (MWSP) 105, coupled to a RAN-based subscribed radio area network (SRAN) 108 and a wireline network (WLN) 110, can provision PWS, when requested, directly, or through an intermediary, which may be a Provisioned Services Vendor (PSV) 112. PSV 112, also

IPR2025-01571
Apple EX1002 Page 552

coupled to the WLN 110, can provision PWS to an authorized device, and may provision PWS in cooperation with another provisioned service provider (PSP), which may include MWSP 105. The authorized device may be dual-mode access point (DMAP) 120 of unlicensed spectrum wireless network (USW) 117 operated by MWSP provisioned service subscriber (PSS) 115. DMAP 120 can be a USW access point adapted to couple USW 117 to wireline network (WLN) 110, and to be remotely configurable by a PSP. An authorized user also can be PSS Guest 123. Guest 123 can communicate using dual mode mobile station (DMMS) 125. DMMS 125 can be configurable to communicate, in a first mode, with DMAP 120 over USW 117 and, in a second mode, with MWSP 105 over SRAN 108. DMSS 125 need not be configured to communicate in both modes simultaneously. DMMS 125 may be a supplicant wireless device, e.g., as it seeks to associate with DMAP 120, or may be an associated device, e.g., after association is completed. It is desirable to adapt DMAP 110 to be configurable as a remotely managed CPE using a remote CPE management technique, such as the aforementioned techniques for remotely managed CPE. Using DMMS 125 in communication with the DMAP 120, Guest 123 can request, and may be authorized to receive, a predefined PWS allocation unit, hereafter, a PWS token 127, requested from one of MWSP 105,

IPR2025-01571
Apple EX1002 Page 553

PSV 112, and PSS 115. DMAP 120 can be configured to employ a first predefined authentication technique, in which DMAP 120 authenticates the identity of DMMS 125 and, upon DMMS 125 authentication by the predefined authentication technique, to provision PWS token 127 to DMMS 125. Alternatively, DMAP 120 can be configured to facilitate PWS provisioning by employing a second predefined authentication technique, in which DMAP 125 passes authentication credentials obtained from DMMS 125 through to a provisioned service provider (PSP), including one of MWSP 105 and PSV 112. Upon authentication of DMMS 125, the PWS provisioner can transmit PWS token 127 to DMAP 120, which can pass PWS token 127 to DMMS 125.

In general, DMAP 120 can implement link-layer and device-level authentication, as described by IEEE Std. 802.11 (1999) and by IEEE Std. 802.1X, including WEP, WPA, WPA2, MAC filtering, and the like. See, for example, the white paper entitled: "A Comprehensive Review of 802.11 Wireless LAN Security and the Cisco Wireless Security Suite" (October 2003) at URL: http://www.cisco.com/warp/public/cc/pd/witc/ao1200ap/prodlit/wswpf_wp.pdf (verified March 21, 2006), hereinafter referred to as "A Comprehensive Review." However, provisioned service providers may demand user-level

IPR2025-01571
Apple EX1002 Page 554

authentication of supplicant guest 123 attempting to access provisioned services, so that the identity of guest 123 is verified. To this end, it may be convenient to implement selected embodiments of the present invention to provide user-level authentication. User-level authentication implementations are well-known in the converged arts art of computer and network security, as may be typified in "A Comprehensive Review", as well as in the Broadcom Corporation White Paper entitled "Securing Home Wi-Fi® Networks: A Simple Solution Can Save Your Identity," Wireless-WP200-x, (May 18, 2005) at URL http://www.54g.org/pdf/Wireless-WP200-RDS.pdf(verified March 21, 2006); and in the Cisco Systems, Inc. Application Note, entitled: "802.1x and EAP-Based Authentication Across Congested WAN Links," March 2002, at URL http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/authp_an.pdf (verified March 16, 2006). The foregoing references are hereby incorporated by reference herein in their entirety, but are exemplary, are not to be considered inclusive or limiting examples.

Also, effective security implementations in a wireless/USW environment can include successive layers of constituent security processes, sequences of constituent security processes, and combinations thereof. In a fixed

IPR2025-01571
Apple EX1002 Page 555

wireless environment/USW, one device-level authentication implementation, e.g., OSA, effects connectivity between devices in the physical link layer, but is susceptible to breach when viewed from the perspective of a logical, end-to-end implementation. Other device-level authentication methods, such as MAC filtering, can provide an appropriately greater degree of security than OSA, but are not intended to verify the identity of the entity using the device. In this instance, entity authentication techniques may be used to verify the identity of the entity by comparing identification information provided by the entity to the content of a known and trusted information repository. User-level authentication is a form of entity authentication capable of being adapted to the fixed wireless/USW environment, in which the user of a USW supplicant device can provide a credential verifiably asserting the user's identity.

Embodiments of the present invention can be adapted to implement horizontal and vertical constituent and executive security processes which cooperate to identify one of the authentication state, indicating whether guest 123 has proven its identity through DMMS 125, and the eligibility state, indicating whether DMMS 125 is a supplicant device eligible to receive provisioned wireless services. In

IPR2025-01571
Apple EX1002 Page 556

selected exemplary embodiments, it is desirable to configure an authenticator, such as local authenticator 150 to implement link-layer, and device-to-device, authentication and identification. Relative to link layer and device-to-device authentication, local authenticator can determine whether supplicant device DMMS 125 is as mobile device, which may be allowed to associate with DMAP 110, and which potentially may be eligible to request provisioned services. The inventive embodiments herein desirably provide remote CPE configuration of local authenticator 150 by provisioned service providers MWSP 105 and PSV 112, by which local authenticator 150 can be configured to implement user-level authentication. In exemplary embodiments, guest 123 may be authenticated at a user level to receive provisioned wireless services using DMMS 125. Local authenticator 150 can challenge a supplicant, such as DMMS 125, to prove its identity, with the result of the challenge being represented by an authentication state. DMMS 125 can communicate to DMAP 110 a pass code entered by guest 123. Local authenticator 150 can evaluate the pass code to determine an authentication state with respect to guest 123. If the authentication state of DMMS 125 indicates that the identity of guest 123 using DMMS 125 is authenticated, then local authenticator

IPR2025-01571
Apple EX1002 Page 557

150 may use the identification information to further qualify supplicant device DMMS 125 for eligibility to received selected provisioned services. The term eligibility can comprehend product capabilities as well as service or QoS features that may be available to guest 123 under term of a provisioned service subscription agreement, which agreement may be made between PSS 115 and PSV 112 or MWSP 105.

Embodiments of the present invention can effect one or both of authentication and provisioning, at least in part, by securely transmitted authentication, authorization, and provisioning information from upstream provisioned service providers including, without limitation, MWSP 105 and PSV 112. In contrast, authentication and other security mechanisms and methods that operate autonomously within the local communication range of an access point, typically have at least one non-secure broadcast, through which an interloper or miscreant may be able to gain access to the network broadcasting its availability. Furthermore, in some local authentication schemes, an access point is adapted to allow the device-level authentication, linking and association of other supplicant mobile stations that may present acceptable device-level authentication or identifying credentials to the soliciting access point,

IPR2025-01571
Apple EX1002 Page 558

within an activation or accession period. These schemes may permit interloping or miscreant mobile stations may be among the plural supplicant devices. Advantageously, embodiments of the present invention can limit accession by supplicant devices by terminating access point activation upon successful authentication of a supplicant device, even if the authentication period of predetermined length has not elapsed.

Thus, PWS authentication according to embodiments of the present invention, can provide a secure authentication process by which the identity of Guest 123 using DMMS 125 is verified. Although embodiments of the present invention are conveniently illustrated in the context of access points, such as DMAP 120, which are capable of providing one or both of multiple SSID and BSSID, it must be understood that PWS authentication can be implemented with DMAP 120 providing a single SSID, a single BSSID, or both. In such an instance, differentiation between provisioned and non-provisioned services (e.g., VoIP and ISP data, respectively) can be implemented in a component or function cooperating with DMAP 120, such as a router (not shown) capable of managing data packets tagged or identified by content or requisite QoS. DMAP 120 may operate with PWS authenticated mobiles stations such as DMMS 125 and may

IPR2025-01571
Apple EX1002 Page 559

reject traffic from non-PWS-authenticated mobile stations. In such a case, DMAP 120 may accept all traffic from the PWS-authenticated client, with the router (not shown) coupled thereto, managing service differentiation. Router service differentiation, for example, may be accomplished by using internal queueing policies, by priority handling techniques generally guided by IEEE Stds. 802.1p or 802.1q, or by combinations thereof. The router (not shown) may be configured to differentially manage provisioned traffic from a PWS-authenticated mobile station, such as DMMS 125, and also may offer virtual LAN (VLAN) functions. The aforementioned IEEE Stds. 802.1p and 802.1q are hereby incorporated herein in their entirety. DMAP 120 may be configured to accept provisioned service traffic from one or more PWS-authenticated mobile stations, such as DMMS 125, and to reject non-provisioned service traffic. DMAP 120 also may be a constituent of a multifunction dual-mode wireless service apparatus in which the aforementioned router (not shown) also is a constituent device cooperating with DMAP 120.

Also disposed on the premises of PSS 115 can be subscriber home network (SHN) 140, which may subsume, and may be at least partially co-located with USW 117. SHN 140 home can include subscriber home telephone 142. If

IPR2025-01571
Apple EX1002 Page 560

telephone 142 is an analog device, an adaptor such as foreign exchange system gateway (FXS) 144, may be coupled between SHN 140 and telephone 142. An FXS gateway can be adapted to connect a standard analog telephone or fax machine to a digital, IP-based data networks, and can be exemplified by Linksys® SPA1001 Phone Adapter, produced by Cisco/Linksys®, Irvine, CA. FXS 144 enables a user to communicate with other digital communication devices to which FXS 144 is coupled, such as DMAP 120. Advantageously, using an adaptor such as FXS 144, PSS 115 can use telephone 142 to remotely control, configure, and operate DMAP 120, at least in part, including supplying activation and security codes to DMAP 120. Conveniently, telephone 142 may be located in a room or office, on the premises of PSS 115, remote to DMAP 120 but coupled to SHN 140. SHN 140 also may include computer 146, irrespective of type or configuration (e.g., desktop, laptop, personal digital assistant), or mode of connection (e.g., wired or wireless). DMAP 120 may Computer 146 may be dispositioned with the appropriate hardware and software, which may be useful in communicating with, and at least partially configuring, DMAP 120. Also, PSS 115 may have, as part of SHN 140, wireless handset 148, which may possess dual mode mobile station functionality, or may operate as a

IPR2025-01571
Apple EX1002 Page 561

communicating device on USW 117. Handset 148 may be adapted to allow PSS 115 to modify a configuration of DMAP 120. DMAP 120 further may be a constituent of a multifunction dual mode wireless service apparatus, which includes one or more functions of an analog telephone adaptor (ATA), having FXS and outgoing foreign-service office (FXO) features, but which may be adapted to receive signals from analog telephony devices coupled thereto, which signals can be used to modify or configure the operation or function of DMAP 120, including activating DMAP 120 for an authentication period.

DMAP 120 can include subscriber interface 160, transceiver 155, and local authenticator (LA) 150. Desirably, subscriber interface 160 includes features such as manual entry keys, and a display, which may be a screen display or other display providing DMAP-related information and feedback to PSS in a visually perceivable format. Advantageously, all or part of subscriber interface 160 may be provided in hardware, software, or an operable combination thereof. In addition, subscriber interface 160 may be a distributed interface, in that a portion of interface 160 can be implemented on computer 146, for example, in a web browser interface. This convenient functionality can allow PSS 115 to remotely control,

IPR2025-01571
Apple EX1002 Page 562

configure, and operate DMAP 120, at least in part, including supplying activation and security codes to DMAP 120. Conveniently, computer 146 may be located in a room or office, on the premises of PSS 115, remote to DMAP 120 but coupled to SHN 140. Typically, DMAP 120 includes transceiver 155, configured to bidirectionally wirelessly communicate with associated and supplicant wireless devices, including DMMS 125. DMAP 120 also may wirelessly communicate with computer 146 and PSS wireless handset 148 if the respective devices are configured and disposed to do so. Local authenticator (LA) 150 is a processing unit of DMAP 120, adapted to perform one or more of effecting association of supplicant wireless devices with DMAP 120 in the context of USW 117; facilitating recognition, verification, and differentiation of signals from associated devices; and to preserve and manage connectivity among associated devices coupled to DMAP 120. Moreover, LA 150 can be adapted to authenticate, in a first authentication mode, or to facilitate authentication, in a second authentication mode, of supplicant devices including DMMS 125. Also, upon authentication of DMMS 125, LA 150 can be configured to provision PWS token 127 to DMMS 125, or to pass PWS token 127 to DMMS 125, after DMMS 125 is authenticated by a PSP, such as MWSP 105 or PSV 112.

IPR2025-01571
Apple EX1002 Page 563

It may be desirable to differentiate between PWS and non-provisioned services, with the latter being provided, for example, by ISP 129. It also may be desirable to further differentiate between different types or classes of PWS provided by the same PSP (e.g., MWSP 105, PSV 112) or between the same type or class of PWS provided by a first PSP, e.g., MWSP 105, and a second PSP, e.g., PSV 112. To facilitate explanation of differentiated service management, PWS hereafter are referred to a "voice services," and non-provisioned services hereafter are referred to a "data services." Currently, wireless devices such as DMAP 120, typically employ a unique, typically alphanumeric, identifier, called a service set identifier (SSID) that wireless networking devices use to establish and to maintain wireless connectivity. Multiple access points on a network or sub-network, including DMAP 120, can use the same SSID to identify the particular wireless network which it forms or with which it is associated. An access point, including DMAP 120, also can employ a unique identifier, namely a basic service set identifier (BSSID) to distinguish itself from other wireless network access points. DMAP 120 can be configured with a basic service set, relative to wireless networking devices, such as DMMS 125, which may seek to associate with DMAP 120. By

IPR2025-01571
Apple EX1002 Page 564

extension, the basic service set of DMAP 120 may be uniquely identified with a basic service set identifier (BSSID) that may be used in a manner similar to a medium access controller (MAC) address relative to other base stations. Embodiments of the present invention can be implemented where DMAP 120 is capable of producing a single SSID, which implementation may provide one undifferentiated service channel adapted to convey both provisioned data and non-provisioned data. Desirably, DMAP 120 can be capable of producing multiple SSIDs and BSSIDs. Exemplary access points capable of producing multiple, configurable SSIDs include the CISCO AIRONET 1100 Series Access Point, the LINKSYS WRTP54G Wireless Router with VoIP, and the LINKSYS WAP54GP Wireless-G Access Point, both available from Cisco Systems, Inc., San Jose, California.

In that regard, DMAP 120 may be configured to have a data-service BSSID (dBSSID 170) to identify a basic service set established for non-provisioned signal (e.g., data) communication; and a host voice-service BSSID (hvBSSID 180) to identify a basic service set established for signal communications related to provisioned wireless services, e.g., voice services. Separation of data and voice services can be advantageous when it is desirable, as here, to separately manage non-provisioned and provisioned

IPR2025-01571
Apple EX1002 Page 565

traffic. Thus configured with plural BSSIDs, DMAP 120 can perform content filtering. In addition, it may be desirable to assign multiple hvBSSIDs 180 to DMAP 120, permitting further differentiation of provisioned services, for example, based upon predefined content characteristics. LA 150 also can include data service interface 162 and provisioned service interface 164. Data service interface 162 generally recognizes and processes data and non-provisioned service content, such that PSS 115 may have control over, and associated privacy of, the content of signals directed to dBSSID 170. Data service interface also can process traffic from SHN 140, and can direct voice service signals therefrom to provisioned service interface 164. Provisioned service interface 164 generally recognizes and processes provisioned service content, such as voice services, such that the respective PSP (e.g., MWSP 105 or PSV 112) has control over the content of signals directed to hvBSSID 180.

Desirably, vBSSID numbers may be assigned in a manner similar to MAC addresses, i.e., a range of vBSSID values for dual-mode access points, such as DMAP 120, can be allocated to defined entities, such as a PSV 112 or mobile wireless service provider (MWSP) 105. Thus, each dual mode access point, such as DMAP 110, may be provided with at

IPR2025-01571
Apple EX1002 Page 566

least one respective unique vBSSID, such as hvBSSID 180. Typically, BSSIDs are programmable into an access point and, thus, DMAP 120 may have hvBSSID 180 pre-assigned thereto, for example, before it is placed in USW 117 for use by PSS 115. Alternately, a PSP, such as MWSP 105, or PSV 112, may remotely configure DMAP 120 by assigning a unique hvBSSID 180 as part of a registration process, and thereby establish provisioned service filtering, e.g., voice-service filtering, in DMAP 120. The registration process may be part of aforementioned CPE configuration and management process, in accordance with a remote management protocol, such as TR-069 CPE WAN Management Protocol. In this example, it is desirable to include in DMAP 120 managed CPE device interface 190 that can initiate and maintain filtering to implement differentiated content management, in accordance with CPE-side configuration management and maintenance functions, similar to those described in DSL Forum Technical Report TR-064. In a particular example, through the facility of interface 190, a PSP, such as MWSP 105 and PSV 112, may remotely provision services and functions of DMAP 120 in accordance with provisioning parameters for VoIP CPE services (e.g., DSL Forum Technical Report TR-104), with VoIP signals being processed differentially from others, and managed according

IPR2025-01571
Apple EX1002 Page 567

to a VoIP provisioning agreement between the selected PSP and PSS 115. With voice-service filtering, signals received over USW 117 and directed to hvBSSID 180 can be managed, metered, and transmitted over WLN 110 to the respective PSP, e.g., PSV 112 or MWSP 105. Suitable voice signals for such voice-service filtering, can include voice-over-Internet-Protocol (VoIP) signals, as well as related voice traffic, such as voice-over-WLAN (VoWLAN) signals. Advantageously, signals not directed to hvBSSID 180 may not be controlled, altered, or affected by voice-service filtering. Accordingly, the radio set of DMAP 120, as represented of transceiver 155, may establish and manage a voice channel for provisioned voice signals (e.g., VoIP signals) separately from a data channel for non-provisioned signals (e.g., bulk data packet signals). Interface 190 may conveniently be disposed and operable within LA 150.

DMAP 120 may broadcast to indicate availability to provide wireless service. While broadcasting, DMAP 120 can transmit over voice channel 182, for example, a voice beacon bearing vSSID 178 to supplicant devices, associated devices, or both, thereby identifying voice channel 182. Similarly, DMAP 120 can transmit over data channel 184, for example, a data beacon bearing dSSID 172 to supplicant devices, associated devices, or both, thereby identifying

IPR2025-01571
Apple EX1002 Page 568

data channel 184. Accordingly, an exemplary supplicant wireless device, which may be DMMS 125, can identify an appropriate channel 182, 184 over which to communicate with DMAP 120. Exemplary DMAP 120 can provide, through voice service interface 135, a voice-service channel typically identified by vSSID 150 and, through data service interface 137, a data-service channel typically identified by dSSID 155.

It can be expedient to allocate and assign a range, or block, of vBSSID values to an identified DMMS entity including, for example, a DMMS manufacturer, DMMS distributor, DMMS vendor, DMMS service provider, PSV 112, and MWSP 105. By associating a vBSSID in this way, gvBSSID 195 may be indicative of the provider of DMMS 125, its corresponding service capabilities, and its corresponding appliance feature sets (e.g., VoIP, MMS, video, GPS). Beneficially, DMMS 125 can be assigned unique vBSSID, for example, gvBSSID 195, as a virtual MAC address corresponding to and identifying DMMS 125. gvBSSID 195 may indicate that DMMS 125 corresponds to a series of VoIP-capable appliances of a particular manufacture; is capable of SIP-based VoIP messaging; and was supplied to guest 163 within the context of an agreement with PSV 112. Embodiments of the present invention can be implemented to

IPR2025-01571
Apple EX1002 Page 569

configure DMAP 120 to provision, to accept, or to reject specific services to selected gvBSSID identifiers. Selection or rejection of a particular gvBSSID may be accomplished using well-known MAC filtering techniques or functional equivalents thereof. For example, DMAP 120 can be configured by PSV 112, to reject voice-service requests from those DMMS bearing gvBSSID identifiers which denote dual-mode appliances not within the scope of a voice-service agreement with PSV 112. MWSP 105 and other PSP may be able to similarly interact with DMAP 120, or the remotely managed functions of DMAP 120 may be exclusively under the control of PSV 112.

For numerous reasons, Guest 123 may wish to receive authorization to use PWS on DMMS 125. One exemplary reason may arise from DMMS 125 being located out of range of signals from SRAN 108. For example, Guest 123 may be indoors or may be in a foreign geographic region where RAN signals compatible with DMMS 125 may be unavailable. USW 117 may be disposed in a public venue such as an airport or large shopping plaza, for example, and PSS 115 may operate USW 117 in that venue. USW 117 also may be disposed outdoors, owing to the deployment of fixed wireless "neighborhood area" or "metropolitan area" networks currently undergoing widespread deployment, as well as more

IPR2025-01571
Apple EX1002 Page 570

robust WiFi™ equipment. Conveniently, Guest 123 may be able to communicate with DMAP 120 over USW 117 using DMMS 125, and thus may seek to be provisioned with PWS, including, for example, an allocation of VoIP services, in order to make and receive calls while in range of USW 117 or a compatibly interoperating USW. Similarly, Guest 123 may wish to receive non-voice PWS (e.g., priority stock market feeds available from PSV 112), which may not otherwise be available to Guest 123 through services offered by PSS 115 through ISP 129. Alternatively, Guest 123 may be a guest in the private home of PSS 115, and PSS 115 may wish to transfer PWS token 127 to DMMS 125 of Guest 123. PWS token may be representative of a portion of preallocated PWS or credit for PWS, for which accounting may be maintained in DMAP 120 for PSS 115, or in a PWS account of PSS 115 managed by a PSP, such as MWSP 105 or PSV 112.

Beneficially, DMMS 125 can be configured to facilitate DMAP 120 with provisioning voice service (as an exemplary PWS) to DMMS 125 by adapting to communicate voice signals through provisioned service interface 164 by way of DMAP voice channel 182, which may be identified by vSSID 178. Similarly, DMMS 125 may seek to associate with DMAP 120 and to communicate data signals through data service

IPR2025-01571
Apple EX1002 Page 571

interface 162, using data channel 184 that can be identified by dSSID 155 and be configured separately and distinctly from voice channel 182. As indicated above, some form of authentication can be desirable for wireless communication services, particularly for provisioned services, such as voice services (e.g., VoIP services), which may use a potentially vulnerable wireless link. DMMS 125 may facilitate DMAP 120 provisioning of voice services by supplying to DMAP 120 identifying credentials during association supplication or upon request of DMAP 120. Identifying credentials may include a predetermined pass code, a predefined unique supplicant device identifier, and a combination thereof. DMAP 120 may store therein one or more pass codes and one or more predefined unique supplicant device identifiers corresponding to wireless devices that may be authenticated to DMAP 120. Authentication of DMMS 125 to DMAP 120 can be designated "PWS authentication." By providing identifying credentials, PWS authentication of the identity of supplicant device DMMS 125 can be simplified, potentially expediting authorization of DMMS 125 to be provisioned with PWS. It also may be beneficial to perform a "pre-access authorization," which may include, for example, authenticating the identity of Guest 123 using well-known

IPR2025-01571
Apple EX1002 Page 572

authentication methods, with a successful pre-access authentication being followed by PSS 115 providing Guest 123 a PWS authentication pass code.

In a particular example of advantageous inventive embodiments herein, Guest 163 may desire to use DMMS 125 through DMAP 120 to receive provisioned voice services (e.g., VoIP) across USW 117. Although DMMS 125 may be able to couple to mobile wireless link 109 to receive voice services from MWSP 105, Guest 123 may wish to place a VoIP call through DMAP 120 and across WLN 110, perhaps because of a lower tariff charged by MWSP 105 for IP-based traffic. PSV 112 may be capable of provisioning PWS, such as VoIP voice service, to DMMS 125, for example, as a discount vendor of MWSP 105 services. PSV 112 may coordinate such third party provisioning with the MWSP AAA entity 103, so that DMMS 125 can be authorized to make and receive VoIP calls using the facilities of MWSP 105. Typically, communications between PSV 112 and MWSP AAA 103 are made using secure communication techniques, with safeguards against Internet interlopers and miscreants. Both PSV 112 and MWSP AAA 103 may decline to provision PWS requested by an outside party, such as Guest 123, unless sufficient safeguards are undertaken, including authenticating the identity of a requester, of the supplicant device for which

IPR2025-01571
Apple EX1002 Page 573

the provisioned service is requested, or both. Therefore, to satisfy a desire of MWSP 105 and PSV 112 for secure access to provisioned services, it may be expedient to provide authentication of supplicant device DMMS 125 as it requests to be provisioned, PWS through DMAP 120, including voice service over IP-based WLN 110. PSS 115 also may desire safeguards operable with DMAP 120 to reduce the likelihood of intrusion into USW 117 by a miscreant seeking to misappropriate or misuse assets associated with DMAP 120, including for example, PWS token 127 or sensitive data and access information of PSS 115, relating to service provisioning through DMAP 120 with a PSP. At the same time, from the perspective of Guest 123 and also of PSS 115, it can be desirable to simplify the mechanics of these safeguards, particularly in scenarios where PSS 115 and Guest 123 can cooperatively operate DMAP 120 and DMMS 125, respectively, to facilitate PWS authentication of DMMS 125 for PWS provisioning, including supplying PWS token 127. In one exemplary scenario, which may be useful in circumstances where PSS 115 is a business owner offering a hotspot to customers or other transient persons, PSS 115 can verify the identity of Guest 123, that is perform pre-access authentication of Guest 123, using an identification credential such as a vehicle operator's permit (i.e.,

IPR2025-01571
Apple EX1002 Page 574

driver's license), a passport, or other form of identification suitable for the level of security desired. Biometric and other physical personal authentication techniques may be used in addition or in substitution. PSS 115 may not require Guest 123 to produce an identification credential for pre-access authentication, for example, where Guest 123 is a long-time customer, or where USW 117 is disposed in the home of PSS 115 and Guest 123 is person known to PSS 115. Upon a satisfactory pre-access authentication, or if PSS 115 is willing to proceed based on trust of Guest 123, then PSS 115 may offer Guest 123 an identification credential to be used with DMMS 125 during PWS authentication, that is, when Guest 123 operates DMMS 125 to request PWS from a PSP. Pre-access authentication may be a constituent process component of a simple but exemplary PWS authentication method embodiment according to the present invention. However, it is to be understood that PWS authentication of Guest 123 using DMMS 125 by DMAP 120 according to embodiments of the present invention is desirably a user-level authentication that does not require pre-authentication.

An exemplary PWS authentication method embodiment according to the present invention may proceed when PSS 115 activates DMAP 120 by depressing single key 177.

IPR2025-01571
Apple EX1002 Page 575

Conveniently, activation key 177 may be dedicated to facilitating association of DMMS 125 with DMAP 120. In response to activation by key 177, DMAP 120 may broadcast, for a predefined authentication period, a voice beacon bearing vSSID 178 on voice channel 182. It can be beneficial to limit the predefined authentication period, for example, to about three minutes, to provide sufficient time for DMMS 125 to perform USW-authentication and to become associated with DMAP 120, yet to minimize the ability of a miscreant or interloper having a USW-capable device from associating with DMAP 120. The actual length of the predefined authentication period may be adjustable to meet the operating environment in which DMAP 120 is deployed. During the predefined authentication period, DMMS 125 can similarly be activated, for example, by Guest 123, causing DMMS 125 to become a supplicant device to the wireless network (USW 117) represented by DMAP 120, identifiable by broadcasting a supplicant device probe request frame on every available USW radio channel, including DMAP 120 voice channel 182. In response, DMAP 120 can transmit a voice beacon over voice channel 182 bearing vSSID 178, as a probe response frame. DMMS 125 then may select DMAP 120 for voice-service access and may send an open authentication request, a form of USW-

IPR2025-01571
Apple EX1002 Page 576

authentication, to DMAP 120. Typically, open authentication is directed to facilitating connectivity and, once in communication with DMMS 125, LA 150 in DMAP 120 can provide a favorable authentication reply to DMMS 125. Upon successful USW-authentication, DMMS 125 may send an association request frame to DMAP 120, transmitting gvBSSID 195, which also may indicate a request to be provisioned voice-service, for example, in the form of PWS token 127 by DMAP 120, where DMAP 120 is configured to provision PWS token 127, or through DMAP 120 over data network link 120, where a PSP such as MWSP 105 or PSV 112 may be designated to engage DMMS 125 in AAA functions to establish authorization to be provisioned the requested wireless service (e.g., voice service). DMAP 120 may have stored therein gvBSSID 195, corresponding to DMMS 125, and it may be sufficient for selected embodiments of PWS authentication methods that gvBSSID 195 identifies DMMS 125 as a dual-mode device, which can be permitted to request, and to be provisioned PWS token 127 and that receipt by DMAP 120 of an identification credential from DMMS 125, in the form of gvBSSID 195, can authenticate supplicant device DMMS 125 to DMAP 120. If the request of DMMS 125 is unsuccessful (e.g., signal loss or authentication failure) during the predefined authentication period, DMAP 120 may

IPR2025-01571
Apple EX1002 Page 577

permit to DMMS 125 having gvBSSID 195, to continue authentication and association attempts, until the predefined authentication period expires, while denying access to other supplicant devices seeking access but without gvBSSID 195.

Alternatively, PSS 115 may enter a host pass code into DMAP 120 by way of interface 160, which is stored by LA 150 during a predefined authentication period. PSS 115 can issue to Guest 123 a guest pass code that is the same as, or corresponds to, the host pass code entered by PSS 115 into DMAP 120. As Guest 123 activates DMMS 125 to become a supplicant device, Guest 123 enter the guest pass code into DMMS 125. When DMMS requests to associate with DMAP 120 during the authentication period, DMMS 125 can undertake a USW-authentication with DMAP 120, in accordance with the network authentication and encryption protocols employed in USW 117. In addition, DMMS 125 can implement an embodiment of the inventive PWS authentication methods by transmitting the guest pass code to DMAP 120. LA 150 can process the guest pass code received from DMMS 125 and compare it with the host pass code supplied by PSS 115. Upon a favorable comparison, DMMS 125 can be considered to be an authenticated device. DMMS 125 may transmit gvSSID 195 along with the guest pass code as a component of the PWS

IPR2025-01571
Apple EX1002 Page 578

authentication identification credentials, or may transmit gvBSSID 195 subsequently, after LA 150 indicates a favorable comparison of guest pass code to stored host pass code. If pre-access authentication is employed to authenticate the identity of Guest 123, then pass code-type PWS authentication of DMMS 125 can be sufficient to infer verification of the identity of Guest 123, if such security is indicated. Otherwise, pass code-type authentication can be sufficient to verify the identity of DMMS 125. Foreseeable variations of the foregoing authentication techniques may be employed, including using biometric authentication devices coupled to DMMS 125 or DMAP 120, for example, as an adjunct to or in substitution for, codes provided by PSS 115. Even if USW-authentication and PWS authentication processes are successfully completed between DMAP 120 and DMMS 125, a successful exchange of encryption keys, such as through a WEP security encryption protocol, may be additionally implemented to permit DMMS 125 to successfully exchange voice services through DMAP 120 over wired network 120. As used herein, the term USW-authentication can include network authentication and encryption protocols such as, without limitation, WEP, WPA, WPA2, IEEE Std. 802.11i, IEEE Std. 802.1x, RADIUS, and EAP security protocols.

IPR2025-01571
Apple EX1002 Page 579

Although the identity of DMMS 125 may be verified, it may not be authorized (or capable) of receiving the requested PWS. Thus, LA 150 may examine gvBSSID 195 to determine whether the identity of DMMS 125 corresponds to a type of DMMS permitted to receive PWS token 127. Alternatively, DMAP 120 may direct gvBSSID 195 as an identifying credential to the PSP identified as being designated to provision PWS for requests coming from DMAP 120. e.g., PSV 112. Also, DMAP 120 may be configured by PSV 112, to examine gvBSSID 195 and to determine whether to provision DMMS 125 with requested PWS (e.g., voice services) over WLN 110, once DMMS 125 has been PWS-authenticated. In addition, embodiments of the present invention may receive or request from DMMS 125 other information which may be pertinent to determining whether to provision PSW to authenticated device DMMS 125, for example, whether authenticated device DMMS 125 is associated with an active subscription between Guest 123 and the provisioning PSP, the class of service requested, QoS requirement, the number of tokens to be allocated, etc. In certain exemplary embodiments of PSW authentication, DMAP 120 may use gvBSSID 195 to perform a type of MAC address authentication, in which the gvBSSID 195 of DMMS 125 is verified against a locally configured list of

IPR2025-01571
Apple EX1002 Page 580

allowed guest vBSSIDs, or against AAA information maintained on an external authentication server, for example, of PSV 112, MWSP 105, or of MWSP AAA 103 (for convenience, simply "PSV 112"). Alternatively, as another embodiment of PSW authentication, DMAP 120 may communicate gvBSSID 195 to PSV 112, where approval or rejection of DMMS 125 may be made, based on a variety of criteria. Moreover, DMAP 120 may be configured to permit enrollment of selected DMMS 125, that is, to enter gvBSSID 195 on the locally configured list of DMAP 120, or to facilitate enrollment of DMMS 125 by forwarding gvBSSID 195 to PSV 112. Enrollment may permit DMAP 120 or PSV 112 to grant or transfer PWS access credits, including representations thereof (e.g., PWS token 127), to DMMS 125, which may permit DMMS 125 to receive voice services (e.g., make and receive VoIP calls) through DMAP 120, or to otherwise be provisioned by PSV 112 to use voice services over suitable USW other than USW 117. If DMAP 120 confirms, or is notified by PSV 112, that DMMS 125 is permitted to associate with DMAP 120, then USW-authentication may be employed. In alternative embodiments of the present invention, USW-authentication may be performed prior to PSW authentication.

FIG. 2 illustrates an embodiment of an authentication method 200 according to the present invention, namely,

IPR2025-01571
Apple EX1002 Page 581

subscriber-provisioner DMAP PWS authentication method 200, which also may feature PWS provisioning. FIG. 2 is described with respect to FIG. 1 and the reference numerals of FIG. 2 refer to like entities in FIG. 1. Method 200 may be beneficial, for example, when a voice-services subscriber seeks to facilitate and manage the allocation of provisioned voice and selected IP services to a guest, while selectively controlling provisioning functions at the subscriber location. Method 200 may also be desirable, for example, to a small business owner, for example, PSS 115, hosting a wireless networking hotspot, for example, USW 117, through which allocation units of VoIP and other provisioned services may be purchased by customers of the small business. As used with respect to FIG. 1, a voice-service allocation unit can be designated as a "token," such as PWS token 127. Pursuant to a request or agreement by PSS 115, DMAP 120 may be authorized and configured (Step 205) by a PSP, such as PSV 112 or MWSP 105, to seek voice-service requests from supplicant devices, such as DMMS 125, and to offer to authenticated supplicant devices PWS token 127, which can be a voice-service token.

Once configured, the PSP may supply DMAP 120 with PWS tokens or functional equivalents (Step 210), which may be requested by Guest DMMS. It may be beneficial for PSS 115

IPR2025-01571
Apple EX1002 Page 582

to purchase selected quantities of PWS token 127, perhaps at a discount, for example, through a volume-purchaser discount agreement with a preselected PSP, e.g., MWSP 105. In addition, PSS 115 may have a defined block of provisioned service credits (e.g., PWS tokens 127) associated with an account with MWSP 105, which may be managed by MWSP AAA unit 103 and which may be supplied to properly authenticated supplicants, for example, who request PWS. Therefore, MWSP 105 can authorize DMAP 120 (step 205) to offer a defined quantity of PWS tokens to properly authorized and authenticated guest devices, such as DMMS 125. MWSP 105 also may associate with DMAP 120 a predetermined number of PWS token 127 for provisioning to DMMS 125, in addition to performing other configurations to DMAP 120, for example, in accordance with CPE management protocols, e.g., TR-064, TR-069, and TR-104.

In embodiments of PWS authentication method 200, subscriber PSS 115 can activate DMAP 120 (Step 215), for example, by entering a pass code. When activated, DMAP 120 can be enabled to broadcast availability for association requests and to accept requests for association from supplicant devices for a predefined authentication period (step 220). During the predefined authentication period, DMAP 120 can broadcast vSSID 178 (step 225) to indicate its

IPR2025-01571
Apple EX1002 Page 583

availability for voice-service calls 182. A supplicant device, such as DMMS 125 may reply to DMAP 120 by supplying identifying credentials which may include, or be supplemented by, one or both of a pass code or gvBSSID 195 (step 230). Desirably, PSS 115 can provide the pass code to Guest 123, who enters the pass code into DMMS 125. DMAP 120 can receive the request to associate, along with the pass code, transmitted by DMMS 125, within the predefined authentication period. DMAP 120 can employ LA 150 to evaluate the identifying credentials received from DMMS 125, for example, to perform PWS authentication (step 235). Step 235 also may include USW-authentication. If the pass code supplied by DMMS 125 satisfactorily compares with an authentication credential stored in a first memory in DMAP 120 during the authentication period, then DMMS 125 can be considered to be authenticated. If, on the other hand, the comparison is unsatisfactory, DMMS 125 may reattempt to be authenticated within the predefined authentication period. The authentication period may be terminated once the authentication of DMMS 125 is successful, for example, to deter interlopers. The (first) authentication credential can include the pass code provided to Guest 123 by PSS 115; an authentication certificate, identifier, or symbol supplied securely by MWSP 105 or PSV 112; or a combination

IPR2025-01571
Apple EX1002 Page 584

thereof. DMMS 125 also may supply DMAP 110 with an additional identifying credential concurrently with the pass code, or in response to a communication separate in time from DMMS 125 supplying the pass code. Exemplary additional identifying credentials include, without limitation, gvBSSID 195, a PWS subscriber identifier (not shown), and a unique personal identifier, such as a vehicle operator's license). LA 150 can include a second memory in which to store a second authentication credential, used to evaluate an additional identifying credential. In selected embodiments of the present invention, successful PWS authentication may be completed after LA 150 verifies the pass code, the additional identifying credential, or both.

Upon successful authentication of the identifying credentials of DMMS 125, it is desirable to determine whether supplicant device DMMS 125 is a supplicant device suitable to be granted access to PWS resources (step 240), including receiving relevant information from DMMS 125, including, for example, gvBSSID 195 and the terms of the PWS request (class of service, QoS, number of tokens, etc.). LA 150 can process the information gathered from DMMS 125 at Step 245, to determine whether DMMS 125 should receive PWS token 127 (step 250), as well as how many PWS token 127 and other terms of PWS provisioning. In

IPR2025-01571
Apple EX1002 Page 585

embodiments of the present invention, LA 150 may store a list or template of gvBSSID values indicative of wireless devices which may be authorized by MWSP 105 to receive PWS token 127 from DMAP 120. LA 150 also may evaluate gvBSSID 195 to determine whether DMMS 125 is capable of using the requested PWS resources or is limited by capability or by agreement in gaining access to PWS resources. Such a list or template can be dynamically updated via WLN 110 by WMSP 105, or MWSP AAA 103.

Where LA 150 determines that the PWS request of DMMS 125 can be fulfilled (step 255), then DMAP 125 can provide voice service PWS token 127 to DMMS 125 (step 260), permitting DMMS 125 to use PWS in an allocation corresponding to granted PWS token 127. On the other hand, where LA 150 determines at Step 255 that the PWS request of DMMS 125 cannot be fulfilled, it may be desirable to permit DMMS 125 to re-attempt a request to receive an allocation of PWS before the predefined authentication period elapses (step 220). Once DMMS 125 is provisioned PWS token 127, it may be desirable to terminate the predefined authentication period, for example, to deter miscreant operators of a USW wireless device from seeking to interlope on USW 117 or impermissibly gain access to PWS.

IPR2025-01571
Apple EX1002 Page 586

FIG. 3 illustrates another embodiment of an authentication method 300 according to the present invention, namely subscriber-passthrough DMAP PWS authentication method 300, which also may feature PWS provisioning. Similar to FIG.2, FIG. 3 is described with respect to FIG. 1 and the reference numerals of FIG. 3 refer to like entities in FIG. 1. Method 300 may be beneficial, for example, when a voice-services subscriber seeks to facilitate and manage the allocation of provisioned voice and selected IP services to a guest, while passing through authentication and provisioning functions to a designated PSP, such as MWSP 105 or PSV 112.

As used with respect to FIG. 1, a voice-service allocation unit can be designated as a "token," such as PWS token 127. Method 300 may also be desirable, for example, to a small business owner PSS 115, hosting a wireless networking hotspot, such as USW 117, but where PSS 115 does not desire to resell PWS tokens. Method 300 also may desirable where PSS 115 operates a home network and wishes to facilitate a request of Guest 123 to receive PWS tokens 127 for DMMS 125, but not to be a host-provisioner. To commence an embodiment of the present inventive methods, namely an embodiment of a subscriber-passthrough DMAP PWS authentication method, subscriber PSS 115 can activate DMAP

IPR2025-01571
Apple EX1002 Page 587

120 (Step 310), for example, by entering a pass code. Activation of DMAP 120 can continue for a predefined authentication period (step 320). When activated, DMAP 120 can broadcast vSSID 178 to indicate availability (Step 325) for association requests and to accept requests for association from supplicant devices, including DMMS 125, for example, to make and receive voice-service calls over voice channel 182. A supplicant device, such as DMMS 125, may reply to DMAP 120 by supplying identifying credentials within the predefined authentication period. DMMS 125 identifying credentials may include, or be supplemented by, one or both of a pass code or gvBSSID 195 (step 330).

Desirably, where a pass code is employed, PSS 115 can provide the pass code to Guest 123, who enters the pass code into DMMS 125. PSS 115 may supply the pass code to Guest 123 subsequent to a successful pre-access authentication. DMAP 120 can receive the request to associate, along with the pass code, transmitted by supplicant device DMMS 125, and can employ LA 150 to evaluate the identifying credentials received from DMMS 125, for example, to perform PWS authentication (step 335). Step 335 also may include USW-authentication, as described with respect to Step 235 in FIG. 2. If the pass code supplied by DMMS 125 satisfactorily compares with the pass

IPR2025-01571
Apple EX1002 Page 588

code stored in DMAP 120 during the authentication period, then DMMS 125 can be considered to be authenticated. If, on the other hand, the comparison is unsatisfactory, DMMS 125 may reattempt to be authenticated within the predefined authentication period. The authentication period may be terminated once the authentication of DMMS 125 is successful, for example, to deter interlopers. Also, it may be desirable to terminate the authentication period upon a failed authentication attempt.

Upon successful authentication of the identifying credentials of DMMS 125, it is desirable to determine whether supplicant device DMMS 125 is a supplicant device suitable to be granted access to PWS resources (step 340), which can be indicated by gvBSSID 195. Upon a favorable evaluation of DMMS 125 suitability to access PWS resources, LA 150 may receive DMMS 125 request (Step 345) for a PWS token 127, e.g., a voice service token. The request may include, without limitation, gvBSSID 195 and the terms of the PWS request (class of service, QoS, number of tokens, etc.). LA 150 can pass through (Step 350) gvBSSID 195, and other information, including that collected at Step 345, to a designated PSP, such as MWSP AAA 103 and PSV 112. PSW authentication, as well as provisioning of PSW tokens 127, can be performed and managed (Step 355) by the designated

IPR2025-01571
Apple EX1002 Page 589

one of MWSP AAA 103 or PSV 112. Such PSP authentication and provisioning may be desirable to Guest 123, for example, where Guest 123 is a subscriber to PWS services of MWSP 105 or PSV 112, and may be using USW 117 and DMAP 120 to access PWS tokens 127, which may be associated with an existing PWS provisioning account of Guest 123 for DMMS 125.

Upon a favorable authentication and provisioning of PWS tokens 127 on behalf of DMMS 125 at Step 355, the designated PSP may then communicate PWS tokens 127 through to DMAP 120 which, in turn, transmit the requested PWS tokens 127 to DMMS 125 (Step 360). Once DMMS 125 is provisioned PWS token 127 at Step 360, it may be desirable to terminate the predefined authentication period, for example, to deter miscreant operators of a USW wireless device from seeking to interlope on USW 117 or impermissibly gain access to PWS. It also may be desirable to permit DMMS 125 to re-attempt authorization during the predefined authentication period, as well as to terminate the authentication period upon an unsuccessful authentication attempt.

A variety of hardware and software functions have been described herein. Depending upon the implementation, many of the hardware functions may be emulated using software.

IPR2025-01571
Apple EX1002 Page 590

Likewise, software functions may be performed using hardware components having hardwired circuitry; and some of the hardware or software functions may be configured using alternative technologies known to skilled artisans, including without limitation, firmware and application specific integrated circuits. The elements in the Figures are to be taken as logical and thus, can be implemented in a consolidated or distributed manner to achieve a desired result.

Moreover, many alterations and modifications may be made by those having ordinary skill in the art, without departing from the spirit and scope of the invention. Therefore, it must be understood that the illustrated embodiments have been set forth only for the purposes of example, and that it should not be taken as limiting the invention as defined by the following claims. The following claims are, therefore, to be read to include not only the combination of elements which are literally set forth, but all equivalent elements for performing substantially the same function in substantially the same way to obtain substantially the same result. The claims are thus to be understood to include what is specifically illustrated and described above, what is conceptually

IPR2025-01571
Apple EX1002 Page 591

equivalent, and also what incorporates the ideas of the invention.

IPR2025-01571
Apple EX1002 Page 592

CLAIMS

What is claimed is:

1. A fixed wireless (USW) access point, comprising:

a local authenticator:

wherein the local authenticator is configured to be activated by a subscriber;

wherein the local authenticator is configured to receive an identifying credential from a dual mode mobile station;

wherein the local authenticator is configured to analyze the identifying credential, thereby determining an authentication state resulting therefrom; and

wherein the local authenticator is configured to one of grant access and deny access by the dual mode mobile station to the USW access point responsive to the authentication state.

2. The USW access point of Claim 1, wherein the local authenticator is configured to differentially process a signal communicated with the dual mode mobile station in response to the authentication state.

IPR2025-01571
Apple EX1002 Page 593

3. The USW access point of Claim 2, further comprising:

a provisioned service interface coupled to the local authenticator, wherein the provisioned service interface is configured to differentially process the provisioned service signal in response to the authentication state.

4. The USW access point of Claim 3:

wherein the provisioned service interface is configured to provide a provisioned service channel identifiable by a provisioned service set identifier (vSSID),

wherein the provisioned service interface is configured to correspond to a provisioned service basic service set identifiable by a provisioned service basic service set identifier (hvBSSID),

wherein the hvBSSID corresponds to the vSSID and is configurably unique to the provisioned service interface, and

wherein the signal communicated with the dual mode mobile station is a provisioned service signal communicated over the provisioned service channel to the USW access point corresponding to hvBSSID.

IPR2025-01571
Apple EX1002 Page 594

5. The USW access point of Claim 4, wherein the provisioned service interface is configured to accept the identifying credential within a predefined authentication period and configured to determine an authentication state corresponding to an identifying credential, if accepted within the predefined authentication period.

6. The USW access point of Claim 3, wherein the local authenticator further comprises a managed CPE interface coupled to a provisioned service provider and coupled to the provisioned service interface, the managed CPE interface being remotely configurable by the provisioned service provider, the managed CPE interface modifying differential processing of the provisioned service signal in response to the authentication state.

7. The USW access point of Claim 4, wherein the identifying credential comprises a provisioned service basic service set identifier (gvBSSID) configurably unique to the dual mode mobile station, and wherein the managed CPE interface is configured to modify differential processing of the provisioned service signal in response to the gvBSSID.

IPR2025-01571
Apple EX1002 Page 595

8. The USW access point of Claim 5 configured such that a single keystroke on a key coupled to the provisioned service interface commences the predefined authentication period and activates the provisioned service interface to determine the authentication state corresponding to the identifying credential, if accepted within the predefined authentication period.

9. A method for authenticating to a USW access point, a dual mode mobile station seeking provisioning of a provisioned wireless service, the method comprising:

receiving an identifying credential from the dual mode mobile station by the USW access point;

evaluating the identifying credential from the dual mode mobile station by the USW access point relative to an authentication credential stored in the USW access point; and

determining a PWS authentication state of the dual mode mobile station corresponding to the identifying credential.

IPR2025-01571
Apple EX1002 Page 596

10. The method of Claim 7, further comprising:

if the PWS authentication state is authenticated, then receiving a request for a provisioned service token from the dual mode mobile station;

evaluating an eligibility state of the dual mode mobile station for being provisioned a provisioned service token; and

if the eligibility state is eligible, then provisioning the provisioned service token to the dual mode mobile station by the USW access point.

11. The method of Claim 7, wherein evaluating the identifying credential further comprises:

evaluating the identifying credential from the dual mode mobile station by the USW access point relative to a provisioning management configuration received from a managed CPE interface disposed in the USW access point.

12. The method of Claim 9, wherein receiving the identifying credential from the dual mode mobile station comprises is receiving the identifying credential from the dual mode mobile station within a predefined authentication period.

IPR2025-01571
Apple EX1002 Page 597

13. The method of Claim 10, wherein the identifying credential comprises a pass code, a provisioned service basic service set identifier (gvBSSID) configurably unique to the dual mode mobile station, or both.

14. A method for authenticating to a USW access point a dual mode mobile station seeking provisioning of a provisioned wireless service, the method comprising:

receiving a pass code from the dual mode mobile station by the USW access point;

receiving a provisioned service basic service set identifier (gvBSSID) configurably unique to the dual mode mobile station; and

transmitting the pass code and the gvBSSID received by the USW access point to a provisioned services provider, wherein the provisioned services provider determines a PWS authentication state of the dual mode mobile station responsive to the pass code and the gvBSSID, and wherein upon authentication the provisioned services provider provisions a PWS token to dual mode mobile station.

IPR2025-01571
Apple EX1002 Page 598

15. The method of Claim 14, wherein receiving a pass code further comprises receiving the pass code within a predefined authentication period from the dual mode mobile station.

16. The method of Claim 15, wherein subsequent to transmitting to the provisioned services provider, the method further comprises:

receiving the PWS token from the provisioned services provider by the USW access point; and

supplying the PWS token to the dual mode mobile station by the USW access point.

17. An authentication apparatus, comprising:

means for receiving an identifying credential from a wireless supplicant device;

means for storing an authentication credential; and

means for evaluating the identifying credential, wherein the identifying credential is compared with the authentication credential, and an authentication state is determined in response thereto.

IPR2025-01571
Apple EX1002 Page 599

18. The authentication apparatus of Claim 17, further comprising:

means for activating the means for receiving during a predefined authentication period;

means for receiving a provisioned service basic service set identifier (gvBSSID) configurably unique to the wireless supplicant device during the predefined authentication period; and

means for provisioning a PWS token to the wireless supplicant device if the authentication state is authenticated,

wherein the means for evaluating the identifying credential further comprises means for evaluating the gvBSSID and the identifying credential relative to the authentication credential in response to which an authentication state is determined.

19. The authentication apparatus of Claim 17, further comprising:

means for remote CPE management of the authentication device coupled to the means for evaluating the identifying credential and modifying the authentication state responsive to a remote CPE configuration.

IPR2025-01571
Apple EX1002 Page 600

20. The authentication apparatus of Claim 18, further comprising:

means for remote CPE management of the authentication device coupled to the means for evaluating the identifying credential and means for evaluating the gvBSSID; and

modifying the authentication state responsive to a remote CPE configuration.

21. The authentication apparatus of Claim 17, further comprising:

means for activating the means for receiving during a predefined authentication period;

means for receiving a provisioned service basic service set identifier (gvBSSID) configurably unique to the wireless supplicant device during the predefined authentication period; and

means for provisioning a PWS token to the wireless supplicant device if the authentication state is authenticated,

wherein the means for evaluating the identifying credential further comprises means for evaluating the gvBSSID and the identifying credential relative to

IPR2025-01571
Apple EX1002 Page 601

the authentication credential in response to which an authentication state is determined.

22. An authentication apparatus, comprising:

means for activating the authentication apparatus for receiving during a predefined authentication period;

means for receiving an identifying credential from a wireless supplicant device during the predefined authentication period, wherein the identifying credential is a pass code;

first means for storing a first authentication credential corresponding to the identifying credential;

first means for evaluating the identifying credential relative to the first authentication credential, wherein the first means for evaluating is coupled to the first means for storing and;

means for receiving a provisioned service basic service set identifier (gvBSSID) configurably unique to the wireless supplicant device during the predefined authentication period;

second means for storing a second authentication credential corresponding to the gvBSSID;

IPR2025-01571
Apple EX1002 Page 602

second means for evaluating the gvBSSID relative to the second authentication credential, wherein the second means for evaluating is coupled to the second means for storing;

means for remote CPE management of the authentication device coupled to the first means for evaluating the identifying credential and the second means for evaluating the gvBSSID, and for receiving a remote CPE configuration from a provisioned service provider;

means for determining a PWS authentication state responsive to evaluating the identifying credential relative to the first authentication credential and for evaluating the gvBSSID relative to the second authentication credential, wherein the PWS authentication state is modified responsive to a remote CPE configuration; and

means for provisioning a PWS token to the wireless supplicant device if the PWS authentication state is authenticated.

IPR2025-01571
Apple EX1002 Page 603

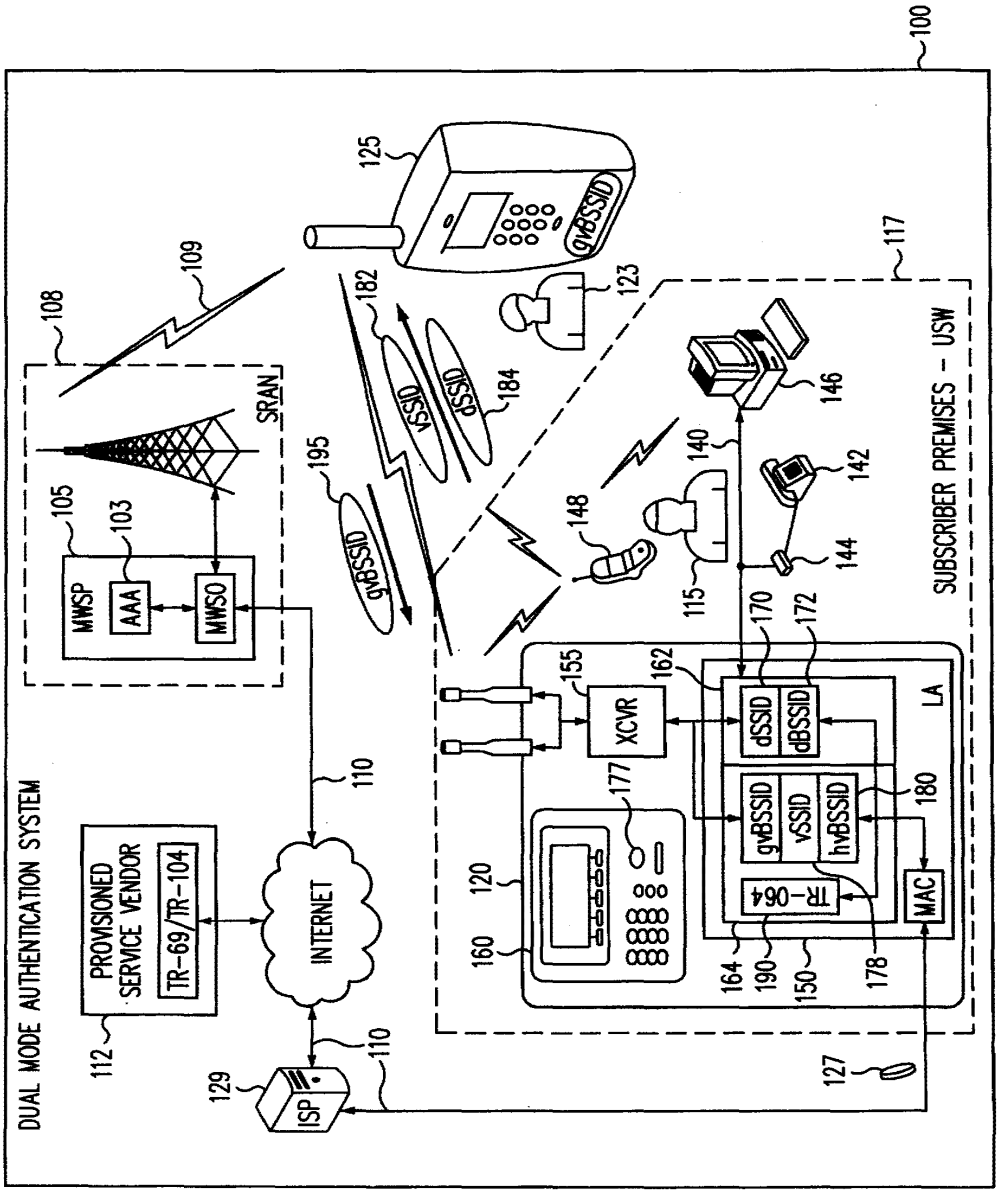

100
DUAL MODE AUTHENTICATION SYSTEM
PROVISIONED SERVICE VENDOR
TR-69/TR-104
112
INTERNET
110
ISP
129
MWSP
AAA
MWSO
105
103
SRAN
108
109
125
gvBSSID
182
vSSID
dSSID
184
195
123
117
SUBSCRIBER PREMISES - USW
146
140
142
148
144
115
170
172
155
XCVR
162
dSSID
dBSSID
LA
177
120
160
gvBSSID
vSSID
hvBSSID
180
FT-064
MAC
164
190
150
178
127

FIG. 1

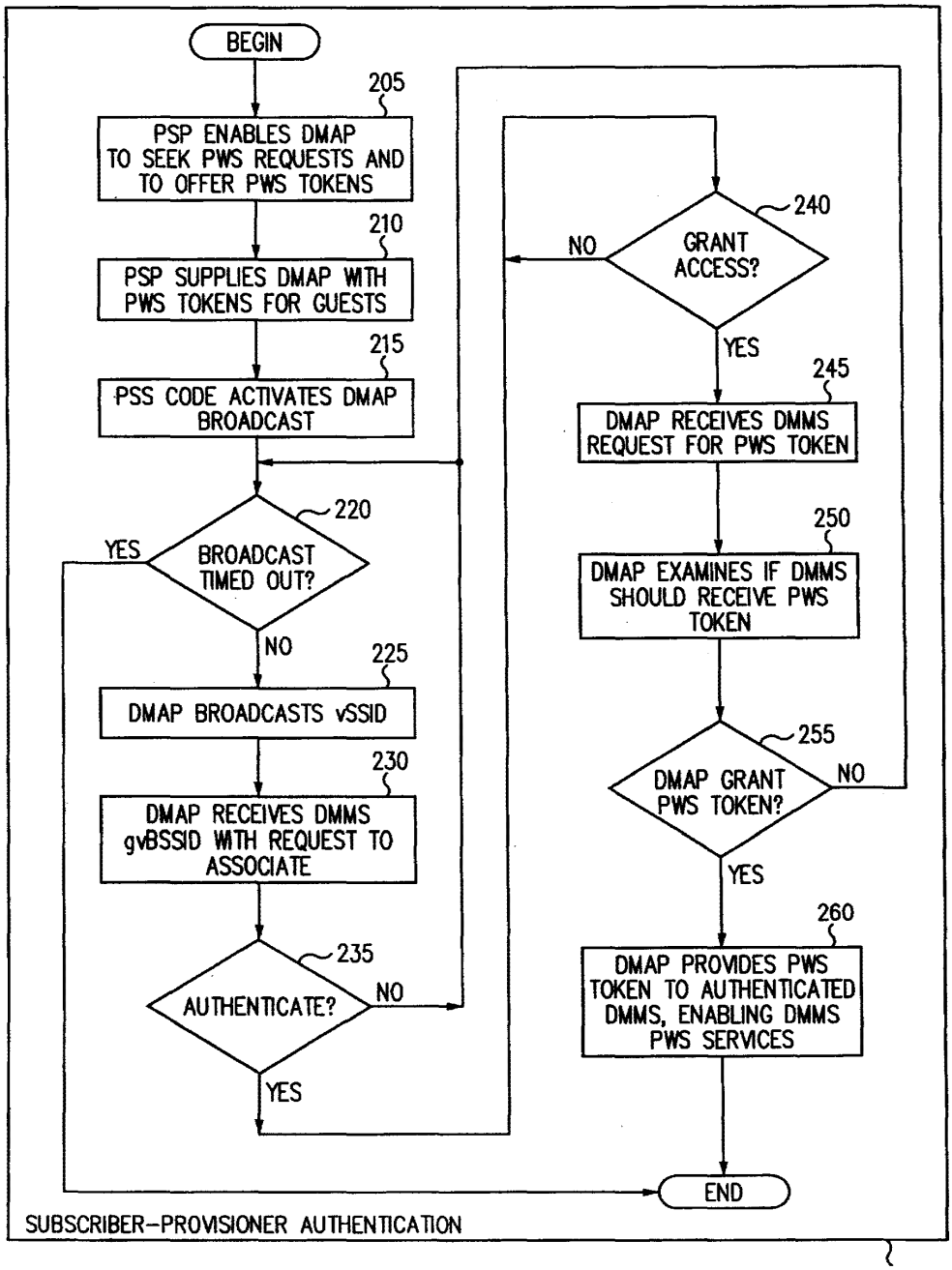

BEGIN
205
PSP ENABLES DMAP TO SEEK PWS REQUESTS AND TO OFFER PWS TOKENS
210
PSP SUPPLIES DMAP WITH PWS TOKENS FOR GUESTS
215
PSS CODE ACTIVATES DMAP BROADCAST
220
YES
BROADCAST TIMED OUT?
NO
225
DMAP BROADCASTS vSSID
230
DMAP RECEIVES DMMS gvBSSID WITH REQUEST TO ASSOCIATE
235
AUTHENTICATE?
NO
YES
240
NO
GRANT ACCESS?
YES
245
DMAP RECEIVES DMMS REQUEST FOR PWS TOKEN
250
DMAP EXAMINES IF DMMS SHOULD RECEIVE PWS TOKEN
255
DMAP GRANT PWS TOKEN?
NO
YES
260
DMAP PROVIDES PWS TOKEN TO AUTHENTICATED DMMS, ENABLING DMMS PWS SERVICES
END
SUBSCRIBER–PROVISIONER AUTHENTICATION
200

FIG. 2

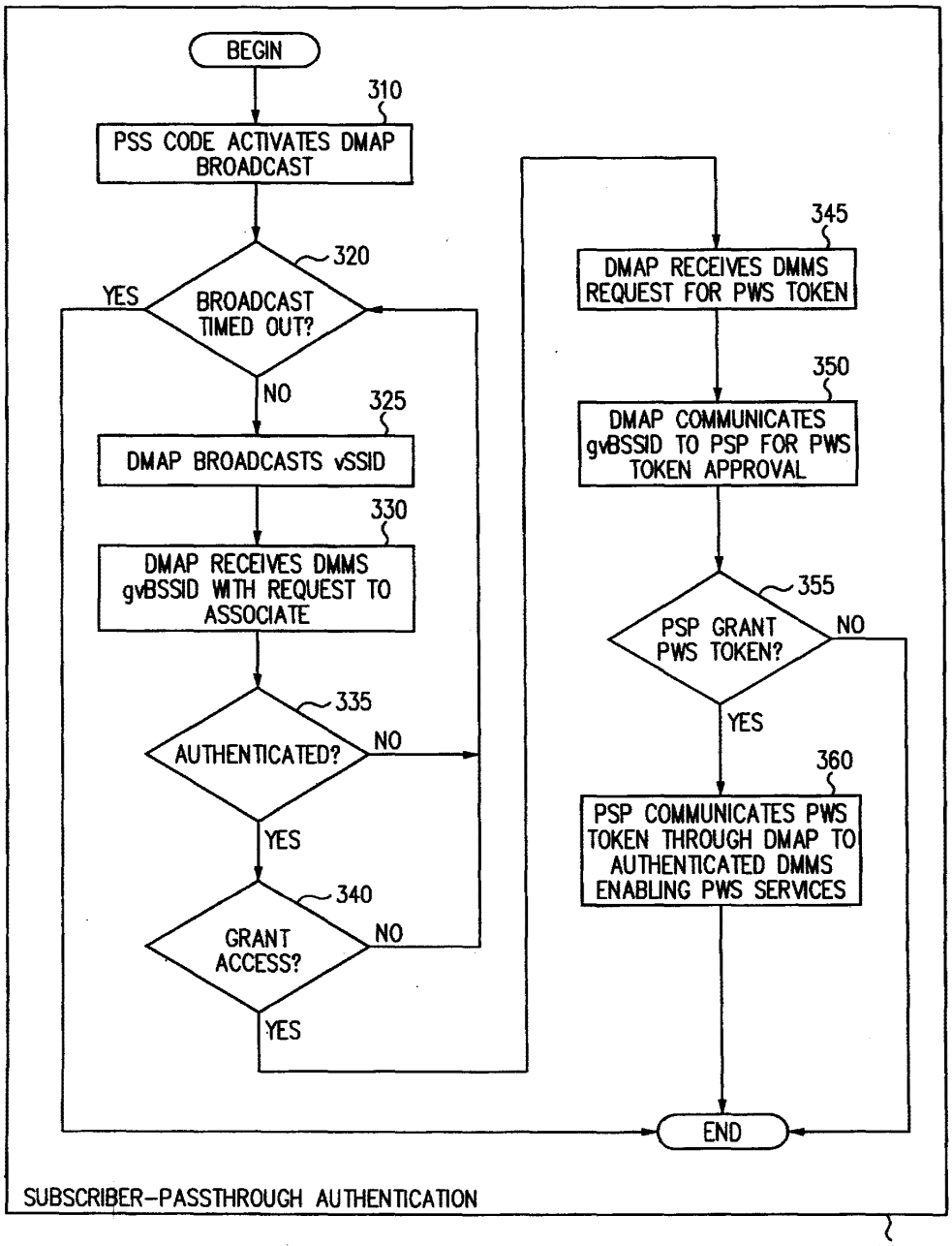

BEGIN
310
PSS CODE ACTIVATES DMAP BROADCAST
320
YES
BROADCAST TIMED OUT?
NO
325
DMAP BROADCASTS vSSID
330
DMAP RECEIVES DMMS gvBSSID WITH REQUEST TO ASSOCIATE
335
AUTHENTICATED?
NO
YES
340
GRANT ACCESS?
NO
YES
345
DMAP RECEIVES DMMS REQUEST FOR PWS TOKEN
350
DMAP COMMUNICATES gvBSSID TO PSP FOR PWS TOKEN APPROVAL
355
PSP GRANT PWS TOKEN?
NO
YES
360
PSP COMMUNICATES PWS TOKEN THROUGH DMAP TO AUTHENTICATED DMMS ENABLING PWS SERVICES
END
SUBSCRIBER-PASSTHROUGH AUTHENTICATION
300

FIG. 3

(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101155343 B
(45)授权公告日 2012.09.05

(21)申请号 200610159722.7

(22)申请日 2006.09.29

(73)专利权人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼

(72)发明人 顾亮 吴建军 李木森 谢安宁 何贤会

(74)专利代理机构 上海明成云知识产权代理有限公司 31232
代理人 成春荣 竺云

(51)Int.Cl.
H04L 12/18(2006.01)
H04L 12/58(2006.01)
H04W 48/12(2009.01)

(56)对比文件
WO 2006/011763 A2,2006.02.02,
CN 1450751 A,2003.10.22,
LAN/MAN Standards Committee.IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment 2:Physical and MAC Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1.《IEEE Std 802.16e&#8482-2005 and IEEE Std 802.16&#8482-2004/Cor 1-2005》.2006,
Yeongmoon Son et al.MBS Refinement.《IEEE C802.16e-05/242》.2005,

审查员 王小千

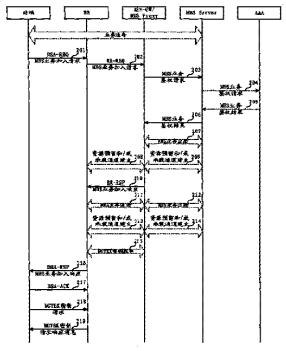
权利要求书 4 页 说明书 18 页 附图 5 页

(54)发明名称

无线网络中终端加入多播广播业务的方法及其系统

(57)摘要

本发明涉及无线通信领域，公开了一种无线网络中终端加入多播广播业务的方法及其系统，使得终端能够成功加入MBS业务，接收MBS业务内容。本发明中，终端从网络侧获取多播广播业务MBS业务参数，其中包含指示空口连接的第一标识和指示业务内容的第二标识，使得终端在收到该MBS业务参数后，能够从第一标识指示的空口连接中接收第二标识指示的MBS业务内容，成功加入该MBS业务。终端可以通过发送加入MBS业务的请求消息发起MBS业务加入过程，获取MBS业务参数，加入所需的MBS业务；网络侧也可以主动发起的MBS业务加入过程，向终端发送MBS业务参数，邀请终端加入MBS业务。



CN 101155343 B

IPR2025-01571
Apple EX1002 Page 607

1. 一种无线网络中终端加入多播广播业务的方法，其特征在于，终端从网络侧获取多播广播业务 MBS 业务参数，该 MBS 业务参数中包含用于指示空口连接的第一标识和用于指示业务内容的第二标识；

所述终端根据所述 MBS 业务参数，从所述第一标识指示的空口连接中接收所述第二标识指示的 MBS 业务内容；

其中，如果接入服务网或 MBS 域内当前无终端接收该 MBS 业务，则还包含以下步骤：

MBS 服务器直接更新其保存的所述 MBS 业务的下行播放列表；或者，

由接入服务网网关或 MBS 代理向所述 MBS 服务器请求注册该 MBS 业务，触发该 MBS 服务器更新其保存的所述 MBS 业务的下行播放列表。

2. 根据权利要求 1 所述的无线网络中终端加入多播广播业务的方法，其特征在于，所述终端通过发送加入 MBS 业务的请求消息，或通过网络侧发起的 MBS 业务加入过程从所述网络侧获取所述 MBS 业务参数。

3. 根据权利要求 2 所述的无线网络中终端加入多播广播业务的方法，其特征在于，所述终端通过动态业务流添加过程发送所述加入 MBS 业务的请求消息，所述请求消息中包含 MBS 内容标识和 / 或 MBS 域标识。

4. 根据权利要求 2 所述的无线网络中终端加入多播广播业务的方法，其特征在于，通过 3 层多播技术辅助所述 MBS 业务的加入过程，终端发送的所述加入 MBS 业务的请求消息中包含所述 MBS 业务的 IP 多播地址列表和 / 或 MBS 内容标识。

5. 根据权利要求 2 所述的无线网络中终端加入多播广播业务的方法，其特征在于，所述网络侧在终端入网时或要求动态建立 MBS 业务时，向所述终端发送加入 MBS 业务的请求，发起所述 MBS 业务加入过程；

所述向终端发送的加入 MBS 业务的请求中包含所述 MBS 业务的空口连接标识、至少一个 MBS 内容标识、和 / 或多播安全联盟标识。

6. 根据权利要求 2 所述的无线网络中终端加入多播广播业务的方法，其特征在于，

在所述网络侧向所述终端发起 MBS 业务加入过程或所述终端发送所述加入 MBS 业务的请求消息之前，所述终端订阅所述 MBS 业务并获取所述 MBS 业务的授权密钥。

7. 根据权利要求 2 所述的无线网络中终端加入多播广播业务的方法，其特征在于，

在所述网络侧向所述终端发起 MBS 业务加入过程或向所述终端下发所述 MBS 业务参数之前，所述网络侧根据所述终端的 MBS 业务签约信息和 / 或该终端的 MBS 业务认证结果对所述终端进行 MBS 业务鉴权，确定所述终端有权接收所述 MBS 业务。

8. 根据权利要求 7 所述的无线网络中终端加入多播广播业务的方法，其特征在于，网络侧发起所述 MBS 业务加入过程的网元是以下之一：锚接入服务网网关或该网关中的功能实体、MBS 服务器、MBS 代理；

网络侧对所述终端进行 MBS 业务鉴权的网元是以下之一：锚接入服务网网关或该网关中的功能实体，MBS 服务器，MBS 代理，认证、授权、计费服务器。

9. 根据权利要求 8 所述的无线网络中终端加入多播广播业务的方法，其特征在于，所述锚接入服务网网关或该网关中的功能实体、MBS 服务器、MBS 代理、认证、授权、计费服务器中任一网元完成终端的 MBS 业务鉴权后，将鉴权结果和 / 或所述 MBS 业务签约信息下发到上述其他网元之一或其任意组合。

IPR2025-01571
Apple EX1002 Page 608

10. 根据权利要求 3 或 4 所述的无线网络中终端加入多播广播业务的方 法，其特征在于，所述终端发送的加入 MBS 业务的请求消息中还包含 MBS 业务鉴权信息，所述网络侧根据所述终端的 MBS 业务签约信息、MBS 业务鉴权信息和 / 或该终端的 MBS 业务认证结果对所述终端进行 MBS 业务鉴权，确定所述终端是否有权接收所述 MBS 业务。

11. 根据权利要求 3 或 4 所述的无线网络中终端加入多播广播业务的方法，其特征在于，所述加入 MBS 业务的请求中还包含指示所述终端最大 MBS 业务能力的信息，所述方法还包含 ：

网络侧根据所述终端的最大 MBS 业务能力和 / 或网络侧保存的该 MBS 的业务资源预留信息，鉴定所述终端是否能够接收所述 MBS 业务。

12. 根据权利要求 1 至 9 中任一项所述的无线网络中终端加入多播广播业务的方法，其特征在于，所述 MBS 业务参数还包含 MBS 业务服务质量参数，所述终端收到所述 MBS 业务参数后，根据本终端最大 MBS 业务能力和所述 MBS 业务服务质量参数，确定所述终端是否能够接收所述 MBS 业务。

13. 根据权利要求 1 至 9 中任一项所述的无线网络中终端加入多播广播业务的方法，其特征在于，如果所述 MBS 业务的播送范围是动态建立的，且基站内当前无终端接收该 MBS 业务，则还包含以下步骤 ：

接入服务网网关直接更新其保存的所述 MBS 业务的下行播放列表 ；或者，

由所述基站向所述接入服务网网关请求注册该 MBS 业务，触发该接入服务网网关更新其保存的所述 MBS 业务的下行播放列表。

14. 根据权利要求 1 至 9 中任一项所述的无线网络中终端加入多播广播业务的方法，其特征在于，在所述终端加入 MBS 业务后，还包含以下步骤 ：

MBS 服务器、接入服务网网关 /MBS 代理、基站分别更新所述 MBS 业务的用户统计数。

15. 根据权利要求 1 至 9 中任一项所述的无线网络中终端加入多播广播业务的方法，其特征在于，如果基站与接入服务网网关之间用于承载所述 MBS 业务的资源和 / 或承载通道不是预先配置的，则还包含以下步骤 ：

如果在终端请求加入所述 MBS 业务时，还未进行基站与接入服务网网关之间的资源预留和 / 或建立相应承载通道，且所述基站持有所述 MBS 业务要求的资源预留信息和 / 或承载通道信息，则所述基站根据 MBS 业务要求的资源预留信息和 / 或承载通道信息请求接入服务网网关或 MBS 代理进行资源预留和 / 或建立承载通道 ；

所述接入服务网网关或 MBS 代理根据网络资源状况和服务策略，确定是否接受所述资源预留请求和 / 或承载通道建立请求。

16. 根据权利要求 1 至 9 中任一项所述的无线网络中终端加入多播广播业务的方法，其特征在于，还包含以下步骤 ：

如果在所述终端通过 MBS 业务鉴权后还未进行相应的资源预留和 / 或建立相应的承载通道，

则接入服务网网关或 MBS 代理通过向基站发送资源预留请求和 / 或承载通道建立请求，为所述 MBS 业务在基站和接入服务网之间的传输进行资源预留和 / 或建立承载通道 ；或者，由 MBS 服务器下发所述 MBS 业务要求的资源预留信息和 / 或承载通道信息，所述基站根据该资源预留信息和 / 或承载通道信息请求服务网网关或 MBS 代理进行资源预留和 / 或建

IPR2025-01571
Apple EX1002 Page 609

立承载通道；

所述基站或接入服务网网关或 MBS 代理根据网络资源状况和服务策略确定是否接受对应的资源预留请求和 / 或承载通道建立请求。

17. 根据权利要求 1 至 9 中任一项所述的无线网络中终端加入多播广播业务的方法，其特征在于，如果接入服务网网关与 MBS 服务器之间的用于承载所述 MBS 业务的资源不是预先配置的，则还包含以下步骤：

如果在所述终端请求加入所述 MBS 业务时，还未进行相应的资源预留 和 / 或建立相应的承载通道，且所述接入服务网网关 /MBS 代理持有所述 MBS 业务要求的资源预留信息和 / 或承载通道信息，则所述接入服务网网关或 MBS 代理根据 MBS 业务要求的资源预留信息和 / 或承载通道信息，请求 MBS 服务器进行资源预留和 / 或建立承载通道；

所述 MBS 服务器根据网络资源状况和服务策略，确定是否接受所述资源预留请求和 / 或承载通道建立请求。

18. 根据权利要求 1 至 9 中任一项所述的无线网络中终端加入多播广播业务的方法，其特征在于，还包含以下步骤：

如果在所述终端通过 MBS 业务鉴权后，还未进行相应的资源预留和 / 或建立相应的承载通道，

则 MBS 服务器通过向接入服务网网关或 MBS 代理发送资源预留请求和 / 或承载通道建立请求，为所述 MBS 业务在接入服务网和 MBS 服务器之间的传输进行相应的资源预留和 / 或建立相应的承载通道；

或，由所述 MBS 服务器下发所述 MBS 业务要求的资源预留信息和 / 或承载通道信息，所述接入服务网网关或 MBS 代理根据该资源预留信息和 / 或承载通道信息请求 MBS 服务器进行相应的资源预留和 / 或建立相应的承载通道；

所述接入服务网网关或 MBS 代理或 MBS 服务器根据网络资源状况和服务策略确定是否接受对应的资源预留请求和 / 或承载通道建立请求。

19. 根据权利要求 1 至 9 中任一项所述的无线网络中终端加入多播广播业务的方法，其特征在于，所述第一标识是空口单播连接标识、或空口多播连接标识、或空口广播标识；

所述第二标识是 MBS 内容标识或所述多播组的 IP 多播地址；

所述 MBS 业务参数还包含以下之一或其任意组合：

所述 MBS 业务对应的 MBS 域标识、MBS 内容标识、多播安全联盟标识、单播安全联盟标识、MBS 业务服务质量参数、MBS 服务流标识。

20. 根据权利要求 19 所述的无线网络中终端加入多播广播业务的方法，其特征在于，所述终端获取所述多播安全联盟标识后，从基站获取所述 MBS 的业务密钥，利用所述 MBS 业务密钥和网络侧下发给所述终端的 MBS 授权密钥生成 MBS 业务加密密钥，通过所述 MBS 业务加密密钥接收所述 MBS 业务内容。

21. 根据权利要求 20 所述的无线网络中终端加入多播广播业务的方法，其特征在于，所述 MBS 业务密钥由所述基站生成，或由所述基站从所述接入服务网网关或所述 MBS 代理获取。

22. 根据权利要求 1 至 9 中任一项所述的无线网络中终端加入多播广播业务的方法，其特征在于，如果所述 MBS 业务在 IP 层使用 IP 多播技术，则还包含以下步骤：所述接入服务

IPR2025-01571
Apple EX1002 Page 610

网网关或所述 MBS 代理通知多播路由器将所述终端加入相应的多播组。

23. 一种无线网络中终端加入多播广播业务的系统，包含终端和网络侧，其特征在于，所述网络侧包含用于为所述终端提供 MBS 业务参数的单元，所述业务参数包含指示空口连接的第一标识和指示业务内容的第二标识；

所述终端包含用于从所述网络侧获取所述 MBS 业务参数的单元，和根据所获取的 MBS 业务参数，从所述第一标识指示的空口连接中接收所述第二标识指示的 MBS 业务内容的单元；

其中，在接入服务网或 MBS 域内当前无终端接收该 MBS 业务时，MBS 服务器用于直接更新其保存的所述 MBS 业务的下行播放列表；或者，接入服务网网关或 MBS 代理用于向所述 MBS 服务器请求注册该 MBS 业务，触发该 MBS 服务器更新其保存的所述 MBS 业务的下行播放列表。

24. 根据权利要求 23 所述的无线网络中终端加入多播广播业务的系统，其特征在于，所述终端还包含用于向网络侧发送加入 MBS 业务的请求消息，通过所述请求消息发起 MBS 业务加入过程，获取所述 MBS 业务参数的单元。

25. 根据权利要求 23 所述的无线网络中终端加入多播广播业务的系统，其特征在于，所述网络侧还包含用于在终端入网时或要求动态建立 MBS 业务时，向所述终端发起 MBS 业务加入过程，为所述终端提供所述 MBS 业务参数的单元。

26. 根据权利要求 23 所述的无线网络中终端加入多播广播业务的系统，其特征在于，所述网络侧还包含以下单元之一或其任意组合：

用于对所述终端是否有能力接收所述 MBS 业务进行评判的单元；

用于对所述终端进行 MBS 业务鉴权的单元；

用于对所述 MBS 业务进行资源预留的单元；

用于为所述 MBS 业务建立承载通道的单元；

用于对所述 MBS 业务进行注册和 / 或下行播放列表更新的单元；

用于为所述 MBS 业务生成密钥的单元；

用于为所述 MBS 业务进行用户数统计的单元。

27. 根据权利要求 23 至 26 中任一项所述的无线网络中终端加入多播广播业务的系统，其特征在于，所述单元是以下之一或其任意组合：

基站，接入服务网网关和 / 或 MBS 代理，MBS 服务器，认证、授权、计费服务器。

IPR2025-01571
Apple EX1002 Page 611

无线网络中终端加入多播广播业务的方法及其系统

技术领域

[0001] 本发明涉及无线通信领域，特别涉及多播广播技术。

背景技术

[0002] IEEE802.16是电子和电气工程师协会(Institute ofElectrical andElectronics Engineers，简称“IEEE”)于2001年12月颁布的，用于在城域网中提供最后一公里无线宽带接入的标准。IEEE802.16标准主要包含802.16a、802.16RevD与802.16e三个标准。

[0003] 微波接入全球互通(Worldwide Interoperability for Microwave Access，简称“WiMAX”)是目前业界对基于IEEE802.16系列标准的无线城域网接入技术，其基本目标是提供一种在城域网一点对多点的多厂商环境下，可有效互操作的宽带无线接入手段。

[0004] 具体地说，802.16系列标准规定了WiMAX系统的空中接口部分协议层，主要包括物理层(PHY)，以及媒体接入控制(Medium Access Control，简称“MAC”)层。其中，PHY层在物理上完成对信号的调制解调以及编解码等操作，而MAC层主要完成WiMAX系统的媒体接入控制功能。

[0005] 图1示出WiMAX端到端参考模型。其中R1接口为无线空中接口，主要由IEEE802.16d/e定义。其余接口均为有线接口。

[0006] 如图可见，WiMAX主要包含移动台(Mobile Station，简称“MS”)/用户站(Subscribe Station，简称“SS”)、接入服务网络(Access ServiceNetwork，简称“ASN”)与连接服务网络(Connectivity Service Network，简称“CSN”)。

[0007] 其中，ASN定义为为WiMAX用户终端提供无线接入服务的网络功能集合，ASN包含了BS和ASN网关(ASN GateWay简称“ASN-GW”)网元，一个ASN可能被多个CSN共享。

[0008] CSN定义为为WiMAX用户终端提供IP连接服务。

[0009] MS/SS为(移动)终端，用户使用该终端接入WiMAX网络。

[0010] 人们通常所说的通信是在一个节点和另外一个节点之间的通信，但是随着用户需求的增加，以及多种媒体的引入，用户需要进行一对多或多对多的通信，从而产生了点到多点(Point to Multipoint，简称“PTM”)的传输模式。为了在移动网上支持这些模式，实现一对多的多播广播业务，同时为了有效地利用移动网络资源，现有技术在WiMAX的基础上定义了MBS业务。MBS业务是在移动网络中提供一个数据源向多个用户发送数据的点到多点业务，实现网络资源共享，提高网络资源的利用率，尤其是空口接口资源。WiMAX定义的MBS不仅能实现纯文本低速率的消息类多播和广播，而且还能实现高速多媒体业务的多播和广播，这无疑顺应了未来移动数据发展的趋势。

[0011] 基于WiMAX网络的MBS业务支持两种接入模式：单基站接入和多基站接入。在多基站接入模式下，定义了MBS域(即MBS Zone，用MBS_zoneID来标识)的概念，所谓一个MBS域就是一个基站的集合，一个MBS域内的所有基站用相同的Multicast CID和MBS组安全联盟(MBS Group SecurityAssociation，简称“MBS GSA”)，发送同一MBS业务流的内

IPR2025-01571
Apple EX1002 Page 612

容，注册了 MBS 服务的终端可以在该 MBS 域内通过多个基站接收 MBS 业务数据，并且处于空闲态的终端在 MBS 域内跨基站移动时，不需重建连接，可以不受影响的接收 MBS 业务，实现 MBS 业务的无缝切换。单基站接入 MBS 是多基站接入 MBS 的一种特例，MBS 域范围限定为一个基站覆盖范围内，一个 MBS 域内接收该 MBS 的所有用户使用同一个多播连接标识。现有技术对单 基站模式没有详细的描述；但是对多基站模式下，基站如何发送 MBS 数据，终端如何接收 MBS 数据，以及基站如何通知终端感兴趣的 MBS 数据的发送，都有相应的描述。

[0012] 现有协议对 MBS 系统中空口有相应的描述，但没有关于终端如何加入 MBS 业务的相关技术。

发明内容

[0013] 本发明的主要目的在于提供一种无线网络中终端加入多播广播业务的方法及其系统，使得终端能够成功加入 MBS 业务，接收 MBS 业务内容。

[0014] 为实现上述目的，本发明提供了一种无线网络中终端加入多播广播业务的方法，终端从网络侧获取多播广播业务 MBS 业务参数，该 MBS 业务参数中包含用于指示空口连接的第一标识和用于指示业务内容的第二标识；

[0015] 所述终端根据所述 MBS 业务参数，从所述第一标识指示的空口连接中接收所述第二标识指示的 MBS 业务内容；

[0016] 其中，如果接入服务网或 MBS 域内当前无终端接收该 MBS 业务，则还包含以下步骤：

[0017] MBS 服务器直接更新其保存的所述 MBS 业务的下行播放列表；或者，

[0018] 由接入服务网网关或 MBS 代理向所述 MBS 服务器请求注册该 MBS 业务，触发该 MBS 服务器更新其保存的所述 MBS 业务的下行播放列表。

[0019] 其中，所述终端通过发送加入 MBS 业务的请求消息，或通过网络侧发起的 MBS 业务加入过程从所述网络侧获取所述 MBS 业务参数。

[0020] 此外在所述方法中，所述终端通过动态业务流添加过程发送所述加入 MBS 业务的请求消息，所述请求消息中包含 MBS 内容标识和 / 或 MBS 域标识。

[0021] 此外在所述方法中，通过 3 层多播技术辅助所述 MBS 业务的加入过程，终端发送的所述加入 MBS 业务的请求消息中包含所述 MBS 业务的 IP 多播地址列表和 / 或 MBS 内容标识。

[0022] 此外在所述方法中，所述网络侧在终端入网时或要求动态建立 MBS 业务时，向所述终端发送加入 MBS 业务的请求，发起所述 MBS 业务加入过程；

[0023] 所述向终端发送的加入 MBS 业务的请求中包含所述 MBS 业务的空口连接标识、一个或多个 MBS 内容标识、和 / 或多播安全联盟标识。

[0024] 此外在所述方法中，在所述网络侧向所述终端发起 MBS 业务加入过程或所述终端发送所述加入 MBS 业务的请求消息之前，所述终端先订阅所述 MBS 业务并获取所述 MBS 业务的授权密钥。

[0025] 此外在所述方法中，在所述网络侧向所述终端发起 MBS 业务加入过程或向所述终端下发所述 MBS 业务参数之前，所述网络侧根据所述终端的 MBS 业务签约信息和 / 或该终端的 MBS 业务认证结果对所述终端进行 MBS 业务鉴权，确定所述终端有权接收所述 MBS 业

IPR2025-01571
Apple EX1002 Page 613

务。

[0026] 此外在所述方法中，网络侧发起所述 MBS 业务加入过程的网元是以下之一：锚接入服务网网关或该网关中的功能实体、MBS 服务器、MBS 代理；

[0027] 网络侧对所述终端进行 MBS 业务鉴权的网元是以下之一：锚接入服务网网关或该网关中的功能实体，MBS 服务器，MBS 代理，认证、授权、计费服务器。

[0028] 此外在所述方法中，所述锚接入服务网网关或该网关中的功能实体、MBS 服务器、MBS 代理、认证、授权、计费服务器中任一网元完成终端的 MBS 业务鉴权后，将鉴权结果和 / 或所述 MBS 业务签约信息下发到上述其他网元之一或其任意组合。

[0029] 此外在所述方法中，所述终端发送的加入 MBS 业务的请求消息中还包 含 MBS 业务鉴权信息，所述网络侧根据所述终端的 MBS 业务签约信息、MBS 业务鉴权信息和 / 或该终端的 MBS 业务认证结果对所述终端进行 MBS 业务鉴权，确定所述终端是否有权接收所述 MBS 业务。

[0030] 此外在所述方法中，所述加入 MBS 业务的请求中还包含指示所述终端最大 MBS 业务能力的信息，网络侧根据所述终端的最大 MBS 业务能力和 / 或网络侧保存的该 MBS 的业务资源预留信息，鉴定所述终端是否能够接收所述 MBS 业务。

[0031] 此外在所述方法中，所述 MBS 业务参数还包含 MBS 业务服务质量参数，所述终端收到所述 MBS 业务参数后，根据本终端最大 MBS 业务能力和所述 MBS 服务质量参数，确定所述终端是否能够接收所述 MBS 业务。

[0032] 此外在所述方法中，如果所述 MBS 业务的播送范围是动态建立的，且基站内当前无终端接收该 MBS 业务，则还包含以下步骤：

[0033] 接入服务网网关直接更新其保存的所述 MBS 业务的下行播放列表；

[0034] 或，由所述基站向所述接入服务网网关请求注册该 MBS 业务，触发该接入服务网网关更新其保存的所述 MBS 业务的下行播放列表。

[0035] 此外在所述方法中，在所述终端加入 MBS 业务后，还包含以下步骤：

[0036] MBS 服务器、接入服务网网关 /MBS 代理、基站分别更新所述 MBS 业务的用户统计数。

[0037] 此外在所述方法中，如果基站与接入服务网网关之间用于承载所述 MBS 业务的资源和 / 或承载通道不是预先配置的，则还包含以下步骤：

[0038] 如果在终端请求加入所述 MBS 业务时，还未进行基站与接入服务网网关之间的资源预留和 / 或建立相应承载通道，且所述基站持有所述 MBS 业务要求的资源预留信息和 / 或承载通道信息，则所述基站根据 MBS 业务要求的资源预留信息和 / 或承载通道信息请求接入服务网网关或 MBS 代理进行资源 预留和 / 或建立承载通道；

[0039] 所述接入服务网网关或 MBS 代理根据网络资源状况和服务策略，确定是否接受所述资源预留请求和 / 或承载通道建立请求。

[0040] 此外在所述方法中，还包含以下步骤：

[0041] 如果在所述终端通过 MBS 业务鉴权后还未进行相应的资源预留和 / 或建立相应的承载通道，

[0042] 则接入服务网网关或 MBS 代理通过向基站发送资源预留请求和 / 或承载通道建立请求，为所述 MBS 业务在基站和接入服务网之间的传输进行资源预留和 / 或建立承载通道；

IPR2025-01571
Apple EX1002 Page 614

或者由 MBS 服务器下发所述 MBS 业务要求的资源预留信息和 / 或承载通道信息，所述基站根据该资源预留信息和 / 或承载通道信息请求服务网网关或 MBS 代理进行资源预留和 / 或建立承载通道 ；

[0043] 所述基站或接入服务网网关或 MBS 代理根据网络资源状况和服务策略确定是否接受对应的资源预留请求和 / 或承载通道建立请求。

[0044] 此外在所述方法中，如果接入服务网网关与 MBS 服务器之间的用于承载所述 MBS 业务的资源不是预先配置的，则还包含以下步骤 ：

[0045] 如果在所述终端请求加入所述 MBS 业务时，还未进行相应的资源预留和 / 或建立相应的承载通道，且所述接入服务网网关 /MBS 代理持有所述 MBS 业务要求的资源预留信息和 / 或承载通道信息，则所述接入服务网网关或 MBS 代理根据 MBS 业务要求的资源预留信息和 / 或承载通道信息，请求 MBS 服务器进行资源预留和 / 或建立承载通道 ；

[0046] 所述 MBS 服务器根据网络资源状况和服务策略，确定是否接受所述资源预留请求和 / 或承载通道建立请求。

[0047] 此外在所述方法中，还包含以下步骤 ：

[0048] 如果在所述终端通过 MBS 业务鉴权后，还未进行相应的资源预留和 / 或 建立相应的承载通道，

[0049] 则 MBS 服务器通过向接入服务网网关或 MBS 代理发送资源预留请求和 / 或承载通道建立请求，为所述 MBS 业务在接入服务网和 MBS 服务器之间的传输进行资源预留和 / 或建立承载通道 ；

[0050] 或，由所述 MBS 服务器下发所述 MBS 业务要求的资源预留信息和 / 或承载通道信息，所述接入服务网网关或 MBS 代理根据该资源预留信息和 / 或承载通道信息请求 MBS 服务器进行资源预留和 / 或建立承载通道 ；

[0051] 所述接入服务网网关或 MBS 代理或 MBS 服务器根据网络资源状况和服务策略确定是否接受对应的资源预留请求和 / 或承载通道建立请求。

[0052] 此外在所述方法中，所述第一标识是空口单播连接标识、或空口多播连接标识、或空口广播标识 ；

[0053] 所述第二标识是 MBS 内容标识或所述多播组的 IP 多播地址 ；

[0054] 所述 MBS 业务参数还包含以下之一或其任意组合 ：

[0055] 所述 MBS 业务对应的 MBS 域标识、至少一个 MBS 内容标识、多播安全联盟标识、单播安全联盟标识、MBS 业务服务质量参数、MBS 服务流标识。

[0056] 此外在所述方法中，所述终端获取所述多播安全联盟标识后，从基站获取所述 MBS 的业务密钥，利用所述 MBS 业务密钥和网络侧下发给所述终端的 MBS 授权密钥生成的 MBS 业务加密密钥，通过所述 MBS 业务加密密钥接收所述 MBS 业务内容。

[0057] 此外在所述方法中，所述 MBS 业务密钥由所述基站生成，或由所述基站从所述接入服务网网关或所述 MBS 代理获取。

[0058] 此外在所述方法中，如果所述 MBS 业务在 IP 层使用 IP 多播技术，则还包含以下步骤 ：所述接入服务网网关或所述 MBS 代理通知多播路由器将所 述终端加入相应的多播组。

[0059] 本发明还提供了一种无线网络中终端加入多播广播业务的系统，包含终端和网络侧，所述网络侧包含用于为所述终端提供 MBS 业务参数的单元，所述业务参数包含指示空

IPR2025-01571
Apple EX1002 Page 615

口连接的第一标识和指示业务内容的第二标识；

[0060] 所述终端包含用于从所述网络侧获取所述 MBS 业务参数的单元，和根据所获取的 MBS 业务参数，从所述第一标识指示的空口连接中接收所述第二标识指示的 MBS 业务内容的单元；

[0061] 其中，在接入服务网或 MBS 域内当前无终端接收该 MBS 业务时，MBS 服务器用于直接更新其保存的所述 MBS 业务的下行播放列表；或者，接入服务网网关或 MBS 代理用于向所述 MBS 服务器请求注册该 MBS 业务，触发该 MBS 服务器更新其保存的所述 MBS 业务的下行播放列表。

[0062] 其中，所述终端还包含用于向网络侧发送加入 MBS 业务的请求消息，通过所述请求消息发起 MBS 业务加入过程，获取所述 MBS 业务参数的单元。

[0063] 此外在所述系统中，所述网络侧还包含用于在终端入网时或要求动态建立 MBS 业务时，向所述终端发起 MBS 业务加入过程，为所述终端提供所述 MBS 业务参数的单元。

[0064] 此外在所述系统中，所述网络侧还包含以下单元之一或其任意组合：

[0065] 用于对所述终端是否有能力接收所述 MBS 业务进行评判的单元；

[0066] 用于对所述终端进行 MBS 业务鉴权的单元；

[0067] 用于对所述 MBS 业务进行网络侧资源预留的单元；

[0068] 用于为所述 MBS 业务建立承载通道的单元；

[0069] 用于对所述 MBS 业务进行注册和 / 或下行播放列表更新的单元；

[0070] 用于为所述 MBS 业务生成密钥的单元。

[0071] 用于为所述 MBS 业务进行用户数统计的单元。

[0072] 此外在所述系统中，所述设备是以下之一或其任意组合：

[0073] 基站，接入服务网网关和 / 或 MBS 代理，MBS 服务器，认证、授权、计费服务器。

[0074] 通过比较可以发现，本发明的技术方案与现有技术的主要区别在于，终端从网络侧获取多播广播业务 MBS 业务参数，其中包含指示空口连接的第一标识和指示业务内容的第二标识，使得终端在收到该 MBS 业务参数后，能够从第一标识指示的空口连接中接收第二标识指示的 MBS 业务内容，成功加入该 MBS 业务。

[0075] 终端可以通过发送加入 MBS 业务的请求消息发起 MBS 业务加入过程，获取 MBS 业务参数，加入所需的 MBS 业务；网络侧也可以主动发起的 MBS 业务加入过程，向终端发送 MBS 业务参数，邀请终端加入 MBS 业务。从而使网络侧和终端侧均能根据实际需求主动操作。

[0076] 终端可以通过 DSA 过程发送 MBS 业务请求消息，在该消息中携带 MBS 域标识，告知网络侧该终端所需要加入的 MBS 业务。由于 MBS 域中可能同时包含多个 MBS 业务，为了明确标识，在该消息中还可以携带 MBS 内容标识，以便唯一指示所要加入的 MBS 业务，使得终端无需同时加入同一 MBS 域中其他 MBS 业务。另外，在 MBS 内容标识是全局唯一的情况下，也可以只携带 MBS 内容标识。

[0077] 或者，终端可以通过因特网组管理协议（Internet Group Management Protocol，简称“IGMP”）协议消息发送 MBS 业务请求，在消息中携带 IP 多播地址，同样能够明确指示网络侧该终端所需要加入的 MBS 业务。

[0078] 在网络侧，MBS 服务器可以通过与 AAA 服务器交互对该终端进行 MBS 业务鉴权，

IPR2025-01571
Apple EX1002 Page 616

或由 ASN 网关 /MBS 代理根据预先获取的鉴权结果对该终端进行 MBS 业务鉴权，通过业务鉴权，确保加入该 MBS 业务的终端均已经订阅了该 MBS 业务并获得了该业务的授权，防止非法用户获取相关服务，妨害合法用户的权益。

[0079] 网络侧或终端本身对终端的最大能力和该 MBS 业务所需的最低要求进行比较，确定终端是否有能力承载该 MBS 业务，防止终端在能力范围以外接收业务，造成网络资源的浪费和终端的额外损耗。

[0080] 在终端加入该业务时，基站或 ASN 网关或 MBS 代理或 MBS 服务器需要对其下使用该 MBS 业务的用户数目进行重新统计，从而能够采用合理的模式承载该 MBS 业务；在之前没有终端使用该 MBS 业务时，ASN 网关或 MBS 代理或 MBS 服务器需要进行相关的业务播放列表的更新，确保播放列表的内容与实际相符合。

[0081] 如果基站与 ASN 网关或 ASN 网关与 MBS 服务器之间用于承载该 MBS 业务的资源或承载通道不是预先配置的，且还未进行相应的资源预留和承载通道的建立，则基站或 ASN 网关或 MBS 服务器可以根据 MBS 业务实际要求的资源预留信息和承载通道信息，在向终端下发 MBS 业务参数之前的任意时间，进行相应的资源预留和承载通道的建立。

[0082] 附图说明

[0083] 图 1 是现有技术中 WiMAX 的网络结构示意图；

[0084] 图 2 是根据本发明第一实施方式的无线网络中终端加入 MBS 业务的方法流程图；

[0085] 图 3 是根据本发明第四实施方式的无线网络中终端加入 MBS 业务的方法流程图；

[0086] 图 4 是根据本发明第五实施方式的无线网络中终端加入 MBS 业务的方法流程图；

[0087] 图5是根据本发明第六实施方式的无线网络中终端加入MBS业务的方 法流程图。

具体实施方式

[0088] 为使本发明的目的、技术方案和优点更加清楚，下面将结合附图对本发明作进一步地详细描述。

[0089] 在本发明中，终端从网络侧获取多播广播业务 MBS 业务参数，其中包含指示空口连接的第一标识和指示业务内容的第二标识，使得终端在收到该 MBS 业务参数后，能够从第一标识指示的空口连接中接收第二标识指示的 MBS 业务内容，成功加入该 MBS 业务。

[0090] 下面对本发明第一实施方式进行说明。本发明第一实施方式涉及无线网络中终端加入MBS业务的方法，在本实施方式中，由终端主动发起MBS业务加入过程，终端在加入MBS业务之前已经明确其感兴趣的 MBS 业务在哪些 MBS 域 (MBS Zone) 内播送，实际操作中，终端可在业务通告阶段 (ServiceAnnounce) 获得相关信息；终端还可在当前 BS 广播的 DCD 消息中获知当前 BS 属于哪些 MBS Zone，如果广播的这些 MBS Zone 中有终端感兴趣的 MBS 业务所在的 MBS Zone，终端即可发起 MBS 业务加入过程。具体如图 2 所示。

[0091] 在步骤 201 中，终端发送 MBS 业务加入请求消息 DSA-REQ 至 BS，该消息中携带欲加入的 MBS 业务所在的 MBS Zone 标识 (MBS Zone ID) 和 / 或 MBS 业务鉴权信息。

[0092] 可选的，该消息还可携带终端当前支持的最大 MBS 业务能力信息，用于告知网络侧并由网络侧根据 MBS 业务的实际服务质量 (Quality of Service，简称“QoS”) 要求决策此终端是否能够正常接收业务。

[0093] 在步骤 202 中，BS 收到终端的 MBS 业务加入请求后，首先验证请求消息的消息认

IPR2025-01571
Apple EX1002 Page 617

证码 HMAC/CMAC 以验证终端是否是网络的合法用户，验证成 功后 BS 向接入服务网络网关 (Access Service Network GateWay，简称“ASN-GW”) 发送 MBS 业务加入请求消息，如 RR-REQ，该消息中携带终端标志 MSID、MBS Zone ID 和 / 或 MBS 业务鉴权信息等。在本步骤中还存在以下几种情况 ：

[0094] a) 如果 BS 与 ASN-GW 间的用于承载该 MBS 业务的资源不是预先配置的，且还未进行相应的资源预留，且 BS 当前持有该 MBS 业务要求的资源预留信息，则 BS 向 ASN-GW 发送的 MBS 业务加入请求消息还包含资源预留申请，请求为该 MBS 业务在 BS 和 ASN-GW 上进行相应的资源预留 ；

[0095] b) 如果 BS 与 ASN-GW 间的用于传输该 MBS 业务的承载通道不是预先配置的，且还未创建相应的承载通道，如果 BS 持有 MBS 业务要求的承载通道信息则上述 BS 向 ASN-GW 发送的 MBS 业务加入请求消息还包含承载通道建立请求，为传输该 MBS 业务在 BS 和 ASN-GW 上申请建立承载通道。BS 和 ASN-GW 间的承载通道的实现可以通过通用路由封装 (Generic RouteEncapsulation，简称“GRE”)、虚拟局域网 (Virtual Local Area Network，简称“VLAN”)、多协议标记交换 (Multi Protocol Label Switching，简称“MPLS”) 等隧道技术，可参见现有技术。

[0096] c) 对于请求消息中包含终端的最大 MBS 业务能力信息的情况，如果 BS 持有 MBS 业务的实际能力要求，即 MBS 业务要求的资源预留信息，则 BS 直接判断该终端是否能够正常接收此 MBS ；如果 BS 上没有该 MBS 业务的资源预留信息，则 BS 向 ASN-GW 发送的 MBS 业务加入请求消息还包含终端的最大 MBS 业务能力信息，请求 ASN-GW 进一步对其进行判决。

[0097] 在步骤 203 中，ASN-GW 收到来自 BS 的 MBS 业务加入请求后，向 MBS 服务器 (MBS Server) 发送 MBS 业务鉴权请求，请求 MBS 服务器验证该终端是否具有接收该 MBS 业务的权利。该请求中还可携带 MBS Zone ID、终端的网络接入标识 (Network Access ID，简称“NAI”) 和 / 或 MBS 业务鉴 权信息等。在本步骤中还存在以下几种情况 ：

[0098] a) 如果 ASN-GW 或 ASN-GW 上的功能实体，如业务流授权者 (ServiceFlow Authorization，简称“SFA”) 或 MBS Proxy，已经保存有 MBS 业务的授权信息 (业务认证结果)，则 ASN-GW 无需再向 MBS Server 发送 MBS 业务鉴权请求，自行根据维护的 MBS 授权信息处理相应终端的 MBS 业务加入请求即可。

[0099] b) 如果 ASN-GW 与 MBS Server 间的用于承载该 MBS 业务的资源不是预先配置的，且还未进行相应的资源预留，并且 ASN-GW 持有 MBS 业务要求的资源预留信息，则在本步骤中 ASN-GW 向 MBS Server 发送的 MBS 业务鉴权请求消息中还包含资源预留申请，为承载该 MBS 业务在 ASN-GW 和 MBS Server 上申请相应的资源预留。

[0100] c) 如果 ASN-GW 与 MBS Server 间的用于传输该 MBS 业务的承载通道不是预先配置的，且还未创建相应的承载通道，并且 ASN-GW 持有 MBS 业务要求的承载通道信息则在本步骤中 ASN-GW 向 MBS Server 发送的 MBS 业务鉴权请求消息还包含承载通道建立请求，为传输该 MBS 业务在 ASN-GW 和 MBS Server 上申请建立承载通道。ASN-GW 和 MBS Server 间的承载通道的实现可以是 GRE、第二层隧道协议 (Layer2 Tunneling Protocol，简称“L2TP”)、VLAN、MPLS、IP 安全 (IP Security，简称“IPSec”) 等隧道技术也可是 IP 多播技术，如 IGMP、多播监听发现 (Multicast ListenerDiscovery，简称“MLD”) 等。

[0101] d)ASN-GW 收到终端的最大 MBS 业务能力信息后，如果 ASN-GW 持有 MBS 业务的实际

IPR2025-01571
Apple EX1002 Page 618

能力要求，即资源预留信息，则 ASN-GW 根据收到的终端最大能力信息和该 MBS 业务所要求的资源预留信息，判断该终端是否能够正常接收该 MBS 业务；反之，如果 ASN-GW 当前没有该 MBS 业务的资源预留信息，则临时保存接收到的该终端的最大能力信息，以便后续进一步判决。

[0102] 在步骤 204 中，MBS Server 收到来自 ASN-GW 的 MBS 业务鉴权请求后，如果自身维护了该终端的 MBS 业务授权信息，则检索 MBS 业务授权信息，查找并确认该终端是否具有享受该 MBS 业务的权利，如终端是否在该 MBS 业务的订阅组中，以及该终端是否已经被授权，获取该 MBS 业务的授权密钥 (MAK) 等；如果 MBS Server 没有维护相应的信息，无法独立判断终端是否具有享受该 MBS 业务的能力，则 MBS Server 还需向终端开户所在的 AAA 服务器请求进行 MBS 业务鉴权。

[0103] 如果 AAA 服务器收到来自 MBS 服务器的鉴权请求，则进入步骤 205，根据用户签约信息和服务策略判断该终端是否具有享受该 MBS 业务的能力，并将业务鉴权结果返回 MBS Server。同时，可选的，AAA 服务器还可以将该终端的 MBS 业务签约信息下发给 MBS Server，以便 MBS Server 在之后的过程中能够直接处理接收到的该终端的 MBS 业务鉴权请求。

[0104] 在步骤 206 中，MBS Server 将 MBS 业务鉴权结果返回 ASN-GW。同时，可选的，MBS Server 可以将该终端的 MBS 业务鉴权信息下发给 ASN-GW 或 ASN-GW 中的某个功能实体，如 SFA 或 MBS Proxy，以便 ASN-GW 在今后的过程中能够直接处理接收到的该终端的 MBS 业务加入请求。在本步骤中还存在以下任意情况：

[0105] a) 可选的，如果 MBS 业务的播送范围是动态建立的，且该 ASN 或 MBSZone 内还没有任何终端接收该 MBS 业务，则 MBS 业务鉴权成功后 MBSServer 可直接更新该 MBS 业务的下行播放列表，即在该 MBS 业务的下行播放列表中添加 ASN-GW 或 MBS Proxy 的标识或 IP 地址。

[0106] b) 可选的，MBS 业务鉴权成功后，MBS Server 更新该 MBS 业务的用户统计数，以便 MBS Server 确定当前使用该 MBS 业务的实际用户数。

[0107] c) 可选的，如果 ASN 网络实体，如 BS、ASN-GW，之前没有获知 MBS 业务要求的资源预留信息和 / 或承载通道信息，则本步骤中 MBS Server 可同时下发该 MBS 业务要求的资源预留信息和 / 或承载通道信息。

[0108] d) 对应步骤 203 的可选项 b)，如果 MBS Server 收到来自 ASN-GW 的资源预留申请，则根据自身的资源状况和服务策略判断是否接受该资源预留申请，并在本步骤中向 ASN-GW 返回资源预留的结果。

[0109] e) 对应步骤 203 的可选项 c)，如果 MBS Server 收到来自 ASN-GW 的承载通道建立请求，则 MBS Server 根据自身的资源状况和服务策略判断是否接受该请求，并在本步骤中向 ASN-GW 返回承载通道建立的结果。

[0110] 可选的，在步骤 207 中，如果 MBS 业务的播送范围是动态建立的，且该 ASN 或 MBS Zone 内还没有任何终端接收该 MBS 业务，且在步骤 206 中，MBS Server 没有更新下行播放列表，则 MBS 业务鉴权成功后 ASN-GW 或 MBS Proxy 向 MBS Server 注册该 MBS 业务，触发 MBS Sever 更新其保存的该 MBS 业务的下行播放列表，即在该 MBS 业务的下行播放列表中添加 ASN-GW 或 MBS Proxy 的标识或 IP 地址；另外，如果之前没有建立 ASN-GW 与 MBS Server 间的承载通道，或当前还未下发该 MBS 业务的承载通道信息和 / 或资源预留信息 (即 ASN-GW/

IPR2025-01571
Apple EX1002 Page 619

MBS Proxy 没有该 MBS 业务的承载通道信息和 / 或资源预留信息，无法请求 MBS Sever 建立相应的承载通道和 / 或预留相应的资源），则 MBS Server 在回应注册请求的同时，将 MBS 业务的承载通道信息和 / 或资源预留信息下发至 ASN-GW/MBS Proxy。

[0111] 可选的，在步骤 208 中，如果 BS 与 ASN-GW 间的用于传输该 MBS 业务的承载通道和 / 或资源预留不是预先配置的，且还未进行相应的资源预留和 / 或创建相应的承载通道（即在步骤 202 中，BS 未发送承载通道建立请求和 / 或资源预留请求），则 ASN-GW 向 BS 发送资源预留请求和 / 或承载通道建立请求，为传输该 MBS 业务在 BS 和 ASN-GW 间传输进行资源预留和 / 或建立相应的承载通道。

[0112] 可选的，在步骤 209 中，如果 ASN-GW 与 MBS Server 间的用于传输该 MBS 业务的承载通道和 / 或资源预留不是预先配置的，且还未进行相应的资源预留和 / 或创建相应的承载通道（即在步骤 203 中，ASN-GW 未发送承载通道建立请求和 / 或资源预留请求），则在本步骤中，ASN-GW 向 MBS Server 发送资源预留请求和 / 或承载通道建立请求，为传输该 MBS 业务在 ASN-GW 和 MBS Server 间传输进行资源预留和 / 或建立相应的承载通道。

[0113] 步骤 208 和步骤 209 可以以任意先后顺序进行，或并行展开。

[0114] 接着进入步骤 210，ASN-GW 收到来自 MBS Sever 的 MBS 业务鉴权结果后，根据该鉴权结果向 BS 返回 MBS 业务加入请求的结果。在此步骤中还存在以下任意情况：

[0115] a) 对应步骤 202 中情况 a)，如果 ASN-GW 收到 BS 的资源预留申请，则根据网络资源状况和服务策略判断是否接受该资源预留申请。如果接受，则进行相应的资源预留。在本步骤中向 BS 返回资源预留的结果。

[0116] b) 对应步骤 202 中情况 b)，如果 ASN-GW 收到 BS 的承载通道创建请求，则 ASN-GW 根据网络资源状况和服务策略判断是否接受该请求。如果接受，则进行相应的承载通道建立。在本步骤中向 BS 返回承载通道建立的结果。

[0117] c) 可选的，如果在步骤 203d) 中，ASN-GW 没有该 MBS 所需的资源预留信息，无法进行终端能力的判断，但在之后的步骤中，如步骤 206 中，收到了 MBS Server 下发的 MBS 业务资源预留信息，则 ASN-GW 根据 MBSServer 下发的 MBS 业务资源预留信息和步骤 203d) 中保存的终端最大 MBS 业务能力信息判断该终端是否能够正常接收该 MBS 业务。并在本步骤中通知 BS 判决结果。

[0118] d) 可选的，如果 MBS 业务的播送范围是动态建立的，且该 BS 内还没有任何终端接收该 MBS 业务，则 MBS 业务鉴权成功后 ASN-GW 还需更新 该 MBS 业务的下行播放列表，即在该 MBS 业务的下行播放列表中添加基站标识 BSID；

[0119] e) 可选的，ASN-GW 在收到 MBS 业务鉴权成功的消息后，可以直接更新该 MBS 业务的用户统计数，以便 ASN-GW 或 MBS Proxy 正确统计该 BS 范围内当前使用该 MBS 业务的用户数，进而也可获知该 ASN 或 MBS Zone 内使用该 MBS 业务的用户数；

[0120] f) 对应步骤 206 中的 c)，可选的，ASN-GW 在获得 MBS 业务的资源预留信息和承载通道信息后，在本步骤中将该信息一并下发给 BS。

[0121] 可选的，在步骤 211 中，BS 收到加入 MBS 业务请求的应答后，如果 MBS 业务的播送范围是动态建立的，且该 BS 内还没有任何终端接收该 MBS 业务，ASN-GW 也没有更新下行播放列表，则 MBS 业务鉴权成功后，BS 向 ASN-GW 注册该 MBS 业务，触发 ASN-GW 更新其保存的该 MBS 业务的下行播放列表，即在该 MBS 业务的下行播放列表中添加基站标识 (BSID)；ASN-GW

IPR2025-01571
Apple EX1002 Page 620

更新下行播放列表后，如果当前还没有建立ASN-GW与MBS Server间的承载通道，且ASN-GW未向MBS Server发起该MBS业务的注册，则ASN-GW可以进一步向MBS Server注册，以更新MBS Server上该MBS业务下行播放列表，即触发MBS Server在该MBS业务的下行播放列表中添加ASN-GW或MBS Proxy的标识或IP地址。

[0122] 可选的，在步骤212中，ASN-GW收到BS的注册请求后，如果当前ASN-GW与MBS Server间的用于传输该MBS业务的承载通道和/或资源预留没有建立，且在之前的步骤中，ASN-GW未向MBS Sever发起注册，则ASN-GW可在本步骤中向MBS Sever注册该MBS业务，由MBS Sever在响应注册请求时，下发相应的资源预留信息和/或承载通道信息，ASN-GW收到的后，在响应BS的注册请求时，进一步将该MBS业务的资源预留信息和/或承载通道信息下发至BS。

[0123] 可选的，在步骤213中，BS收到资源预留信息和/或承载通道信息后，如果BS与ASN-GW间的用于传输该MBS业务的承载通道和/或资源预留不是预先配置的，且在之前的步骤中，BS未曾发送相应的资源预留请求和/或承载通道的创建请求，且ASN-GW未曾主动下发资源预留请求和/或承载通道的创建请求，则在本步骤中，BS向ASN-GW发送资源预留请求和/或承载通道建立请求，为传输该MBS业务在BS和ASN-GW间传输进行资源预留和/或建立相应的承载通道。

[0124] 可选的，在步骤214中，ASN-GW为该MBS业务进行相应的资源预留和/或建立相应承载通道后，如果ASN-GW与MBS Server间的用于传输该MBS业务的承载通道和/或资源预留不是预先配置的，且在之前的步骤中，还未进行相应的资源预留和/或创建相应的承载通道，则在本步骤中，ASN-GW向MBS Server发送资源预留请求和/或承载通道建立请求，为传输该MBS业务在ASN-GW和MBS Server间传输进行资源预留和/或建立相应的承载通道。

[0125] 可选的，在步骤215中，如果BS使用链路层多播方式传送该MBS业务且该MBS业务不是广播业务，则BS还需获取MBS组业务加密密钥(MBSGroup Traffic Encryption Key，简称“MGTEK”)，该密钥用于生成MBS业务在空口传输时的业务加密密钥(MTK)。

[0126] BS可以通过向ASN-GW发送MGTEK密钥的请求消息，请求ASN-GW将其生成的MGTEK下发给BS，如果ASN-GW当前还未为该MBS业务产生MGTEK，则先为该MBS业务生成MGTEK，再将生成的MGTEK下发给BS。

[0127] 如果BS已有MGTEK或该MGTEK可由BS生成，则省略本步骤或在本步骤中触发BS生成MGTEK。

[0128] 接着进入步骤216，BS向终端发送MBS业务加入响应消息DSA-RSP，该消息中携带终端请求加入的MBS业务对应的MBS Zone ID、空口连接标识CID或空口多播连接标识MCID、该CID或MCID上承载的所有MBS内容标识、多播安全联盟标识GSA ID。

[0129] 接着进入步骤217，终端收到MBS业务加入响应消息后向BS发送MBS业务加入确认消息DSA-ACk，用来确认该过程已完成。

[0130] 可选的，在终端加入该MBS业务时，BS可以更新其覆盖范围内该MBS业务的用户统计数。

[0131] 接着进入步骤218，终端获得多播安全联盟标识后，向BS发起密钥请求消息Key Request，用于请求该MBS业务的多播业务密钥MGTEK，该请求消息中携带该MBS业务的GSA

IPR2025-01571
Apple EX1002 Page 621

ID。

[0132] 接着进入步骤 219，BS 收到请求后，将之前产生或获得的 MGTEK 发送给终端，由终端根据预先获得的 MAK 和 MGTEK 共同生成 MBS 业务加密密钥 MTK，并根据从网络侧获取的多播广播业务参数接收相应的 MBS 业务。在本实施方式中，资源预留信息是指分类器参数和规则、QoS 参数和 / 或头压缩参数和规则等承载该 MBS 业务所需的资源的描述信息。承载通道信息是指承载通道类型、承载通道标识和 / 或承载通道协议类型等承载该 MBS 业务的承载通道所需的资源描述消息。终端的最大 MBS 业务能力信息是指终端当前持有的能接收 MBS 业务的最大资源描述信息，如带宽、丢包率等。通常是指终端的设备能力或当前未被占用的资源总和。MBS 业务是指 IEEE802.16d/e 定义的一个服务流 (SF)。

[0133] 值得一提的是，在本实施方式中，如果终端请求加入的是 MBS 多播业务，则终端在加入 MBS 业务之前需要先订阅该 MBS 业务并获取该 MBS 业务的授权密钥 (MAK)。如果终端请求加入的是 MBS 广播业务，则在上述流程中不需要鉴权过程，步骤 201 至 203 的请求消息中可不携带 MBS 的鉴权信息，或该鉴权信息仅用于通知网络侧各节点该终端加入该 MBS 业务。此时步骤 204 的业务鉴权可以省略，并且之后的步骤中也无需再下发任何业务鉴权结果或业务授权信息。

[0134] 本发明第二实施方式涉及无线网络中终端加入 MBS 业务的方法，本实施方式与第一实施方式大致相同，其区别在于，在第一实施方式中，终端在加入 MBS 业务的请求消息中携带 MBS Zone ID，来标识需要加入的 MBS 业务，然而由于一个 MBS Zone 中可能存在多个 MBS 业务，在本实施方式中，终端在请求消息中除了携带 MBS Zone ID 外，还需携带该 MBS 业务的 MBS 内容标识 MBS Content ID。因此，在本实施方式中，需要修改空口标准 IEEE802.16e，使得在 DSA-REQ 消息中可携带 MBS Content ID。

[0135] 本发明第三实施方式涉及无线网络中终端加入 MBS 业务的方法，本实施方式与第二实施方式大致相同，其区别在于，在第二实施方式中，终端在加入 MBS 业务的请求消息中需携带请求加入的 MBS 业务的 MBS Zone ID 和具体的 MBS Content ID，而本实施方式在第二实施方式的基础上进行了改进，在本实施方式中，MBS 业务的 MBS Content ID 是全局唯一的，在业务加入请求消息中，只需携带指定的 MBS Content ID 即可，无需关心业务在哪个 MBS Zone 上播送。在本实施方式中，同样需要修改空口标准 IEEE802.16e，要求在 DSA-REQ 中可携带 MBS Content ID。

[0136] 本发明第四实施方式涉及无线网络中终端加入 MBS 业务的方法，在本实施方式中，使用 3 层多播技术辅助完成终端加入 MBS 业务的过程，使得在不更改现有空口协议 (IEEE802.16d/e) 的基础上，完成终端加入指定的某个 MBS 业务的过程。

[0137] 在本实施方式中，终端在加入 MBS 业务之前就已经获得了其感兴趣的 MBS 业务相关的 IP 多播地址列表、MBS 业务承载的 MBS Content ID 列表、IP 多播地址和 MBS Content ID 的对应关系和 / 或该 MBS 业务在哪些 MBSZone 内播送，具体应用中，终端如可在业务通告阶段或通过其它途径获得上述信息。终端在发起 MBS 业务加入过程前，如果获知该业务在哪些 MBS Zone 内播送，则还可通过检测当前 BS 广播的 DCD 消息获知当前 BS 属于哪些 MBS Zone，以便确定当前终端是否处于其感兴趣的 MBS 业务所在的 MBSZone，如果不是则不用发起加入过程。具体如图 3 所示。

[0138] 在步骤 301 中，终端发送 MBS 业务加入请求 IGMP Join 至锚 ASN-GW(Anchor

IPR2025-01571
Apple EX1002 Page 622

ASN-GW)，该消息中携带欲加入的 IP 多播地址和 / 或业务鉴权信息。该消息可承载在终端的初始业务流 (Initial Service Flow，简称“ISF”) 通道上。

[0139] 在步骤 302 中，锚 ASN-GW 收到终端的 MBS 业务加入请求后，向 MBSProxy 发送 MBS 业务加入请求，该请求中携带终端标识 MSID 和终端欲加入的 IP 多播组地址和 / 或业务鉴权信息。

[0140] 在步骤 303 中，MBS Proxy 收到 MBS 业务加入请求后向 MBS Server 发送 MBS 业务鉴权请求，用于请求验证该终端是否具有接收该 MBS 业务的权利。该请求中还可携带终端的网络接入标识 NAI、IP 多播组地址和 / 或 MBSContent ID 等。在此步骤中还存在以下几种情况：

[0141] a) 如果 MBS Proxy 或 MBS Proxy 所在的 ASN-GW 上的某个功能实体，如 SFA，已经保存有 MBS 业务的授权信息，即 MBS Proxy 已经能够进行 MBS 业务鉴权处理，则 MBS Proxy 无需再向 MBS Server 发送 MBS 业务鉴权请求，自行根据维护的 MBS 授权信息处理相应终端的 MBS 业务加入请求即可。

[0142] b) 如果 ASN-GW 与 MBS Server 间的用于传输该 MBS 业务的承载通道不是预先配置的，且还未创建相应的承载通道，则 MBS Proxy 向 MBS Server 发送的 MBS 业务鉴权请求消息还包含承载通道建立请求，为传输该 MBS 业务在 ASN-GW 和 MBS Server 上申请建立承载通道。ASN-GW 和 MBS Server 间的承载通道的实现可以是 GRE、L2TP、VLAN、MPLS、IPSec 等隧道技术也可是 IP 多播技术，如 IGMP、MLD 等。

[0143] 在步骤 304 中，MBS Server 收到 MBS 业务鉴权请求后，如果自身维护了终端的 MBS 业务授权信息，则检索 MBS 业务授权信息查找并确认该终端是否具有享受该 MBS 业务的能力；如果 MBS Server 没有维护相应的授权信息，不能判断终端是否具有享受该 MBS 业务的能力，则 MBS Server 还需向终端开户所在的 AAA 服务器请求进行 MBS 业务鉴权。

[0144] 在步骤 305 中，AAA 根据用户签约信息和服务策略判断该终端是否具有享受该 MBS 业务的能力，并将业务鉴权结果告知 MBS Server。此时，可选的，AAA 可同时将该终端的 MBS 业务授权信息下发给 MBS Server，以便 MBS Server 在之后的过程中能够直接处理接收到的该终端的 MBS 业务鉴权请求。

[0145] 在步骤 306 中，MBS Server 将 MBS 业务鉴权结果返回 MBS Proxy。同时，可选的，MBS Server 可以将该终端的 MBS 业务授权信息下发给 MBSProxy 或 MBS Proxy 所在 ASN-GW 中的某个功能实体，如 SFA，以便 MBSProxy 在之后的过程中能够直接处理接收到的该终端的 MBS 业务加入请求。另外，在本步骤中还可能存在以下几种情况：

[0146] a) 可选的，如果 MBS 业务的播送范围是动态建立的，且该 ASN 或 MBS Zone 内还没有任何终端接收该 MBS 业务，则 MBS 业务鉴权成功后 MBSServer 可以直接更新该 MBS 业务的下行播放列表，即在该 MBS 业务的下行播放列表中添加 ASN-GW 或 MBS Proxy 的标识或 IP 地址。

[0147] b) 可选的，MBS 业务鉴权成功后，MBS Server 更新该 MBS 业务的用户统计数，以便 MBS Server 统计出使用该 MBS 业务的实际用户数。

[0148] c) 可选的，如果 ASN-GW 和 / 或 MBS Porxy 之前没有获知 MBS 业务要求的资源预留信息和 / 或承载通道信息，则本步骤中 MBS Server 可同时下发该 MBS 业务要求的资源预留信息和 / 或承载通道信息。

IPR2025-01571
Apple EX1002 Page 623

[0149] d) 对应步骤 303b)，MBS Server 根据自身的资源状况和服务策略判断是否接受承载通道的创建请求，并在本步骤中向 MBS Proxy 返回承载通道建 立的结果。

[0150] MBS Proxy 收到来自 MBS 服务器的 MBS 业务鉴权结果后，接着进入步骤 307 或步骤 308，步骤 307 和步骤 308 不存在先后关系。

[0151] 在步骤 307 中，MBS Proxy 根据该鉴权结果向 Anchor ASN-GW 返回该 MBS 业务加入请求的结果。

[0152] 在步骤 308 中，MBS Proxy 根据该鉴权结果向 BS 发送 MBS 业务加入请求，如 RR-REQ。在本步骤中还可能存在以下几种情况：

[0153] a) 如果 BS 与 ASN-GW 间的用于承载该 MBS 业务的资源不是预先配置的，且还未进行相应的资源预留（即在之前的步骤中 BS 未曾发送资源预留申请），则 MBS Proxy 向 BS 发送的终端加入 MBS 业务的响应消息中还包含资源预留申请，为承载该 MBS 业务在 BS 和 ASN-GW 上申请相应的承载资源。

[0154] b) 如果 BS 与 ASN-GW 间的用于传输该 MBS 业务的承载通道不是预先配置的，且还未创建相应的承载通道（即在之前的步骤中 BS 未曾发送承载通道创建请求），则 MBS Proxy 向 BS 发送的终端加入 MBS 业务的响应消息中还包含承载通道建立请求，为传输该 MBS 业务在 BS 和 ASN-GW 上申请建立承载通道。BS 和 ASN-GW 间的承载通道的实现可以是 GRE、VLAN、MPLS 等隧道技术。

[0155] c) 可选的，如果 MBS 业务的播送范围是动态建立的，且该 BS 内还没有任何终端接收该 MBS 业务，则 MBS 业务鉴权成功后 MBS Proxy 可以直接更新该 MBS 业务的下行播放列表，即在该 MBS 业务的下行播放列表中添加基站标识 BSID。

[0156] d) 可选的，MBS 业务鉴权成功后，MBS Proxy 更新该 MBS 业务的用户统计数，以便 ASN-GW 或 MBS Proxy 统计出该 BS 下使用该 MBS 业务的用户数，进而也可获知 ASN 或 MBS Zone 内使用该 MBS 业务的用户数。

[0157] 在步骤 309 中，BS 收到该 MBS 业务加入请求响应后，如果该响应是成功响应，则 BS 向终端发送 MBS 业务加入请求消息 DSA-REQ，该消息中携带欲加入的 MBS 业务对应的 MBS Zone ID、空口连接标识 CID 或空口多播连接标识 MCID、该 CID 或 MCID 上承载的所有 MBS 内容标识 MBS ContentID、多播安全联盟标识 GSA ID 或单播安全联盟、MBS 业务的 QoS 参数中一个或多个。

[0158] 可选的，在步骤 310 中，如果 BS 决定使用链路层多播方式传送该 MBS 业务且该 MBS 业务不是广播业务，则 BS 还需获取 MBS 组业务加密密钥 MGTEK，该密钥用于生成 MBS 业务在空口传输时的业务加密密钥 MTK。

[0159] BS 可以通过向 ASN-GW 发送 MGTEK 密钥的请求消息，请求 ASN-GW 将其生成的 MGTEK 下发给 BS，如果 ASN-GW 当前还未为该 MBS 业务产生 MGTEK，则先为该 MBS 业务生成 MGTEK，再将生成的 MGTEK 下发给 BS。

[0160] 如果 BS 已有 MGTEK 或该 MGTEK 可由 BS 生成，则省略本步骤或在本步骤中触发 BS 生成 MGTEK。

[0161] 本步骤与步骤 309 并无固定的先后顺序。

[0162] 接着进入步骤 311，终端收到来自 BS 的 DSA-REQ 消息后，根据 MBS 业务的 QoS 参数要求和终端本身所能承受的最大 MBS 业务能力判断是否能正常接收该 MBS 业务，如果能则

IPR2025-01571
Apple EX1002 Page 624

保存相应的 MBS 业务上下文。终端回应 MBS 业务加入响应消息 DSA-RSP 至 BS，消息中携带加入 MBS 业务的结果。

[0163] 可选的，步骤 312，如果 MBS 业务的播送范围是动态建立的，且之前该 BS 内还没有任何终端接收该 MBS 业务，即 BS 未曾向 MBS Proxy 注册该 MBS 业务，则 BS 向 MBS Proxy 发起业务注册，以更新 ASN-GW 中该 MBS 业务的下行播放列表，即在该 MBS 业务的下行播放列表中添加基站标识 BSID。

[0164] 同样可选的，在步骤 313 中，MBS Proxy 更新 ASN-GW 中该 MBS 业务 的下行播放列表后，如果之前 ASN 或 MBS Zone 内没有任何终端接收该 MBS 业务，即 MBS Proxy 没有向 MBS Server 注册过该 MBS 业务，则在本步骤中 MBS Proxy 向 MBS Server 注册以更新 MBS Server 中该 MBS 业务下行播放列表，即在 MBS Server 中该 MBS 业务的下行播放列表中添加 ASN-GW 或 MBSProxy 的标识或 IP 地址。

[0165] 可选的，在本步骤中，如果 ASN-GW/MBS Proxy 与 MBS Server 间的用于传输该 MBS 业务的承载通道和 / 或资源预留没有建立，且之前未曾下发相应的资源预留信息和 / 或承载通道信息。则 MBS Server 在响应 ASN-GW 的注册请求的同时下发资源预留信息和 / 或承载通道建立信息。ASN-GW 收到后进一步在响应 BS 的注册请求时将该 MBS 业务的资源预留信息和 / 或承载通道信息下发至 BS。

[0166] 可选的，在步骤 314 中，如果 BS 与 ASN-GW 间的用于传输该 MBS 业务的承载通道和 / 或资源预留不是预先配置的，且在之前的步骤中，BS 未进行相应的资源预留请求和 / 或创建相应的承载通道请求，ASN-GW 或 MBSProxy 也未主动发起资源预留请求和 / 或创建相应的承载通道请求，则在本步骤中，BS 向 ASN-GW 发送资源预留请求和 / 或承载通道建立请求，为传输该 MBS 业务在 BS 和 ASN-GW 间传输进行资源预留和 / 或建立相应的承载通道。

[0167] 可选的，在步骤 315 中，ASN-GW 或 MBS Proxy 收到来自 BS 的资源预留请求和 / 或承载通道建立请求后，可根据网络资源情况确定是否同意进行相应的资源预留和 / 或建立相应的承载通道。另外，如果该 ASN-GW 与 MBSServer 间的用于传输该 MBS 业务的承载通道和 / 或资源预留不是预先配置的，且在之前的步骤中，未向 MBS Sever 发送相应的资源预留请求和 / 或创建相应承载通道的请求，则 MBS Proxy 向 MBS Server 发送资源预留请求和 / 或承载通道建立请求，为传输该 MBS 业务在 ASN-GW 和 MBS Server 间传输进行资源预留和 / 或建立相应的承载通道。

[0168] 在步骤 316 中，BS 将终端的 MBS 业务加入请求响应结果发送给 MBSProxy 或 Serving ASN-GW。在本步骤中还可能存在以下几种情况：

[0169] a) 如果在步骤 308a) 中，MBS Proxy 向 BS 发送的终端加入 MBS 业务的响应消息中还包含资源预留申请，则在本步骤中 BS 根据空口资源状况和准入控制策略判断是否接受资源预留申请。如果接受，则进行相应的资源预留。在本步骤中向 MBS Proxy 返回资源预留的结果。

[0170] b) 如果在步骤 308b) 中，MBS Proxy 向 BS 发送的终端加入 MBS 业务的响应消息中还包含承载通道创建请求，则在本步骤中，BS 根据空口资源状况和准入控制策略判断是否接受该承载通道建立申请。如果接受，则进行相应的承载通道建立。在本步骤中向 MBS Proxy 返回承载通道建立的结果。

[0171] 在步骤 317 中，BS 收到 MBS 业务加入响应 DSA-RSP 消息后向终端发送 MBS 业务加

IPR2025-01571
Apple EX1002 Page 625

入确认消息 DSA-ACK，用来确认该过程已完成。

[0172] 在步骤 318 中，终端获得多播安全联盟标识后，向 BS 发起密钥请求消息 Key Request，用于请求该 MBS 业务的多播业务密钥 MGTEK，该请求消息中携带该 MBS 业务的 GSA ID。

[0173] 在步骤 319 中，BS 收到请求后，将之前产生或获得的 MGTEK 发送给终端，由终端根据预先获得的 MAK 和 MGTEK 共同生成 MBS 业务加密密钥 MTK，并根据从网络侧获取的多播广播业务参数接收相应的 MBS 业务。

[0174] 值得一提的是，在本实施方式中，如果终端请求加入的是 MBS 多播业务，则终端在加入 MBS 业务之前需要先订阅该 MBS 业务并获取该 MBS 业务的授权密钥 (MAK)。如果终端请求加入的是 MBS 广播业务，则在上述流程中不需要鉴权过程，步骤 301 至 303 的请求消息中可不携带 MBS 的鉴权信息，或该鉴权信息仅用于通知网络侧各节点该终端加入该 MBS 业务。并且步骤 304 的业务鉴权可以省略，之后的步骤中也无需再下发任何业务鉴权结果或业务授权信息。

[0175] 本发明第五实施方式涉及无线网络中终端加入 MBS 业务的方法，本实施方式与第四实施方式大致相同，其区别在于，在第四实施方式中，终端在发起 MBS 业务加入过程之前，已经获取 IP 多播地址和 MBS Content ID 的对应关系，而在本实施方式中，终端在加入 MBS 业务之前没有获取 IP 多播地址和 MBS Content ID 的对应关系，由网络侧在终端加入 MBS 业务过程中将其通知终端。

[0176] 具体如图 4 所示，步骤 401 至步骤 417 与步骤 301 至步骤 317 相类似，在此不再赘述。

[0177] 在步骤 418 中，MBS Proxy/Serving ASN-GW 收到 BS 发送的 MBS 业务加入结果后，向终端发送其加入的 IP 多播地址对应的 MBS Content ID 列表，该消息还可携带欲加入的 MBS 业务对应的 MBS Zone ID、空口连接标识 CID 或空口多播连接标识 MCID、该 CID 或 MCID 上承载的所有 MBS 内容标识 MBS Content ID、多播安全联盟标识 GSA ID 或单播安全联盟中的一个或多个。

[0178] 本步骤与步骤 417 不存在固定的先后关系。

[0179] 步骤 419 和步骤 420 与步骤 318 和步骤 319 相类似。

[0180] 本发明第六实施方式无线网络中终端加入 MBS 业务的方法，在本实施方式中，由网络侧主动发起的 MBS 业务加入过程，该过程可发生在终端入网后预置流的建立过程中，也可发生在网络侧实体要求动态建立 MBS 业务时。对于多播业务，在网络侧请求终端加入 MBS 业务之前，该终端需要先订阅该 MBS 业务并获取该 MBS 业务的授权密钥 MAK，其中订阅消息可包含在用户的签约消息中。具体如图 5 所示。

[0181] 在本实施方式中，网络侧实体发送 MBS 业务创建请求存在以下几种可能性：

[0182] 如果在终端初始入网阶段，用户的签约消息已经下发到接入网实体 Anchor ASN-GW 中，则在步骤 501 中，可由 Anchor ASN-GW 或 AnchorASN-GW 中的功能实体，如 SFA，向 MBS Proxy 发起 MBS 业务创建请求，该请求中还需携带终端标识 MSID。

[0183] 或者在步骤 501′ 中，由 MBS Server 向 MBS Proxy 发送 MBS 业务创建请求，该消息中携带 NAI 或 MSID。在该步骤中还可以包含以下可选项：

[0184] a) 可选的，如果 MBS 业务的播送范围是动态建立的，且该 ASN 或 MBSZone 内还没有

IPR2025-01571
Apple EX1002 Page 626

任何终端接收该MBS业务，则MBS Server可以直接更新该MBS业务的下行播放列表，即在该MBS业务的下行播放列表中添加ASN-GW或MBS Proxy的标识或IP地址。

[0185] b)可选的，MBS Server可以更新该MBS业务的用户统计数，以便MBSServer统计出当前使用该MBS业务的实际用户数。

[0186] 在步骤502中，如果MBS Proxy在终端入网鉴权认证阶段就已经获得用户签约消息，则MBS Proxy可直接触发MBS业务创建请求，或者，MBS Proxy在收到来自MBS Sever或Anchor ASN-GW的MBS业务创建请求后，进一步向BS发起该MBS业务创建请求。如果MBS业务传输在IP层时使用IP多播技术，则MBS Proxy还负责通知相应的多播路由器(Multicast Route，简称“MR”)，将该终端加入相应的多播组。

[0187] 此外，在本步骤中还可以包含以下可选项：

[0188] a)可选的，如果MBS业务的播送范围是动态建立的，且之前该BS内还没有任何终端接收此MBS业务，则MBS Proxy可以直接更新该MBS业务的下行播放列表，即在该MBS业务的下行播放列表中添加基站标识BSID。

[0189] b)可选的，MBS Proxy更新该MBS业务的用户统计数，以便ASN-GW或MBS Proxy统计出该BS下使用该MBS业务的用户数，进而也可获知ASN网络或MBS Zone内使用该MBS业务的用户数。

[0190] c)如果ASN-GW与BS间的用于承载该MBS业务的资源不是预先配置的，且还未进行相应的资源预留，则MBS Proxy向BS发送的MBS业务创建请求消息还可以包含资源预留申请，为承载该MBS业务在BS和ASN-GW上申请相应的承载资源。

[0191] d)如果BS与ASN-GW间的用于传输该MBS业务的承载通道不是预先配置的，且还未创建相应的承载通道，则MBS Proxy向BS发送的终端加入MBS业务的请求消息还包含承载通道建立请求，为传输该MBS业务在BS和ASN-GW上申请建立承载通道。BS和ASN-GW间的承载通道的实现可以是GRE、VLAN、MPLS等隧道技术。

[0192] 可选的，步骤503，如果BS使用链路层多播方式传送该MBS业务且该MBS业务不是广播业务，则BS向MBS Proxy请求MBS业务密钥MGTEK，该密钥用于生成MBS业务在空口传输时的业务加密密钥MTK。

[0193] BS可以通过向ASN-GW发送MGTEK密钥的请求消息，请求ASN-GW将其生成的MGTEK下发给BS，如果ASN-GW当前还未为该MBS业务产生MGTEK，则先为该MBS业务生成MGTEK，再将生成的MGTEK下发给BS。

[0194] 如果BS已有MGTEK或该MGTEK可由BS生成，则省略本步骤或在本步骤中触发BS生成MGTEK。

[0195] 在步骤504中，BS向终端发送MBS业务加入请求消息DSA-REQ，该消息中携带欲加入的MBS业务对应的MBS Zone ID、空口连接标识CID或空口多播连接标识MCID、该CID或MCID上承载的所有MBS内容标识MBSContent ID、多播安全联盟标识GSA ID或单播安全联盟、MBS业务的QoS参数中一个或多个。

[0196] 在步骤505中，终端收到DSA-REQ消息后，根据MBS业务的QoS参数要求和终端本身所能承受的最大MBS业务能力判断是否能正常接收该MBS业务，如果能则保存相应的MBS业务上下文。终端向BS返回MBS业 务加入响应消息DSA-RSP，消息中携带加入MBS业务的结果。

IPR2025-01571
Apple EX1002 Page 627

[0197] 可选的，在步骤 506 中，如果 MBS 业务的播送范围是动态建立的，且之前该 BS 内还没有任何终端接收此 MBS 业务，即 BS 没有向 MBS Proxy 注册过该 MBS 业务，则 BS 向 ASN-GW 发起注册以更新该 MBS 业务的下行播放列表，即在 ASN-GW 中该 MBS 业务的下行播放列表中添加基站标识 BSID。

[0198] 同样可选的，在步骤 507 中，MBS Proxy 更新 ASN-GW 中该 MBS 业务的下行播放列表后，如果之前 ASN 或 MBS Zone 内没有任何终端接收该 MBS 业务，即 MBS Proxy 没有向 MBS Server 注册过该 MBS 业务，则在本步骤中 MBS Proxy 向 MBS Server 注册以更新 MBS Server 中该 MBS 业务下行播放列表，即在 MBS Server 中该 MBS 业务的下行播放列表中添加 ASN-GW 或 MBSProxy 的标识或 IP 地址。

[0199] 可选的，在本步骤中，如果 ASN-GW/MBS Proxy 与 MBS Server 间的用于传输该 MBS 业务的承载通道和 / 或资源预留没有建立，且之前未曾下发相应的资源预留信息和 / 或承载通道信息。则 MBS Server 在响应 ASN-GW 的注册请求的同时下发资源预留信息和 / 或承载通道建立信息。ASN-GW 收到后进一步在响应 BS 的注册请求时将该 MBS 业务的资源预留信息和 / 或承载通道信息下发至 BS。

[0200] 可选的，在步骤 508 中，如果 BS 与 ASN-GW 间的用于传输该 MBS 业务的承载通道和 / 或资源预留不是预先配置的，且还未进行相应的资源预留和 / 或创建相应的承载通道，且在步骤 502 中，MBS Proxy 向 BS 发送的 MBS 业务创建请求消息未包含资源预留申请和 / 或承载通道建立请求，则在本步骤中，BS 向 ASN-GW 或 MBS Proxy 发送资源预留请求和 / 或承载通道建立请求，为传输该 MBS 业务在 BS 和 ASN-GW 间传输进行资源预留和 / 或建立相应的承载通道。

[0201] 可选的，在步骤 509 中，ASN-GW 或 MBS Proxy 收到来自 BS 的资源预 留请求和 / 或承载通道建立请求后，可根据空口资源情况确定是否同意进行相应的资源预留和 / 或建立相应的承载通道。并且，如果 ASN-GW 与 MBS Server 间的用于传输该 MBS 业务的承载通道和 / 或资源预留不是预先配置的，且还未进行相应的资源预留和 / 或创建相应的承载通道，则 ASN-GW 或 MBS Proxy 向 MBS Server 发送资源预留请求和 / 或承载通道建立请求，为传输该 MBS 业务在 ASN-GW 和 MBS Server 间传输进行资源预留和 / 或建立相应的承载通道。

[0202] 在步骤 510 中，BS 收到 DSA-RSP 消息后，将 MBS 业务加入请求结果返回 MBS Proxy，具体可通过响应消息 RR-RSP。另外，在本步骤中还可能存在以下几种情况：

[0203] a) 对应步骤 502a)，如果 MBS Proxy 向 BS 发送的 MBS 业务创建请求消息未包含资源预留申请，则在本步骤中，BS 根据空口资源状况和准入控制策略判断是否接受该资源预留申请。如果接受，则进行相应的资源预留。并在本步骤中一并告知 ASN-GW 资源预留的结果。

[0204] b) 对应步骤 502b)，如果 MBS Proxy 向 BS 发送的 MBS 业务创建请求消息未包含承载通道建立请求，则在本步骤中，BS 根据空口资源状况和准入控制策略判断是否接受申请的承载通道建立。如果接受，则进行相应的承载通道建立。并在本步骤中一并告知 ASN-GW 承载通道建立的结果。

[0205] MBS Proxy 获知 MBS 业务创建结果后，通知 MBS 业务创建请求的发起者。如果 MBS 业务创建请求的发起方是 Anchor ASN-GW，即对应步骤 501 和步骤 501′，则进入步骤 511，MBS Proxy 将业务创建结果返回 AnchorASN-GW；如果 MBS 业务创建请求的发起方是

IPR2025-01571
Apple EX1002 Page 628

MBS Server，即对应步骤 501′，则进入步骤 511′，MBS Proxy 将业务创建结果返回 MBS Server；如果 MBS 业务创建请求的发起方是 MBS Proxy，则可省略本步骤。

[0206] 在步骤 512 中，BS 收到 MBS 业务加入响应消息 DSA-RSP 后向终端发送 MBS 业务加入确认消息 DSA-ACK，用来确认该业务加入过程已完成。

[0207] 在步骤 513 中，终端获得多播安全联盟标识后，向 BS 发起密钥请求消息 Key Request，用于请求该 MBS 业务的多播业务密钥 MGTEK，该请求消息中携带该 MBS 业务的 GSA ID。

[0208] 在步骤 514 中，BS 收到请求后，将之前产生或获得的 MGTEK 发送给终端，由终端根据预先获得的 MAK 和 MGTEK 共同生成 MBS 业务加密密钥 MTK，并根据从网络侧获取的多播广播业务参数接收相应的 MBS 业务。

[0209] 值得一提的是，以上各实施方式中，各实体可以独立存在或存在于一个功能实体内，上述实体在同一个物理实体内时，它们之间的交互使用的是内部原语。如 ASN-GW 和 BS 可以为同一物理实体，Anchor ASN-GW 和 ServingASN-GW 可以为同一物理实体，MBS Proxy 和 ASN-GW 可以为同一物理实体等等。

[0210] 其中，MBS Proxy 实体是 ASN 网络或 MBS Zone 内为终端处理 MBS 业务信令和 / 或业务的功能实体。在上述各实施方式中，该功能实体可位于 Anchor ASN-GW 中也可位于 Serving ASN-GW 中，也可独立存在于 MBS Zone 内。当 MBS Proxy 位于 Anchor ASN-GW 中时，其与 Anchor ASN-GW 间的消息交互就通过内部原语实现。

[0211] 本发明第七实施方式涉及无线网络中终端加入多播广播业务的系统，包含终端和网络侧，其中，网络侧包含用于在终端入网时或要求动态建立 MBS 业务时，向终端发起 MBS 业务加入过程，为终端提供 MBS 业务参数的单元。该业务参数包含指示空口连接的第一标识和指示业务内容的第二标识；终端还包含用于从网络侧获取 MBS 业务参数的单元；根据所获取的 MBS 业务参数，从第一标识指示的空口连接中接收第二标识指示的 MBS 业务内容的单元；和 / 或用于向网络侧发送加入 MBS 业务的请求消息，通过请求消息发起 MBS 业务加入过程，获取 MBS 业务参数的单元。

[0212] 另外，网络侧还可以包含以下单元之一或其任意组合：

[0213] 用于对终端是否有能力接收 MBS 业务进行评判的单元；

[0214] 用于对终端进行 MBS 业务鉴权的单元；

[0215] 用于对 MBS 业务进行网络侧资源预留的单元；

[0216] 用于为 MBS 业务建立承载通道的单元；

[0217] 用于对 MBS 业务进行注册和 / 或下行播放列表更新的单元；

[0218] 用于为 MBS 业务生成密钥的单元。

[0219] 上述单元可以是以下之一或其任意组合：基站，ASN-GW 和 / 或 MBS 代理，MBS 服务器，AAA 服务器。

[0220] 虽然通过参照本发明的某些优选实施方式，已经对本发明进行了图示和描述，但本领域的普通技术人员应该明白，可以在形式上和细节上对其作各种改变，而不偏离本发明的精神和范围。

IPR2025-01571
Apple EX1002 Page 629

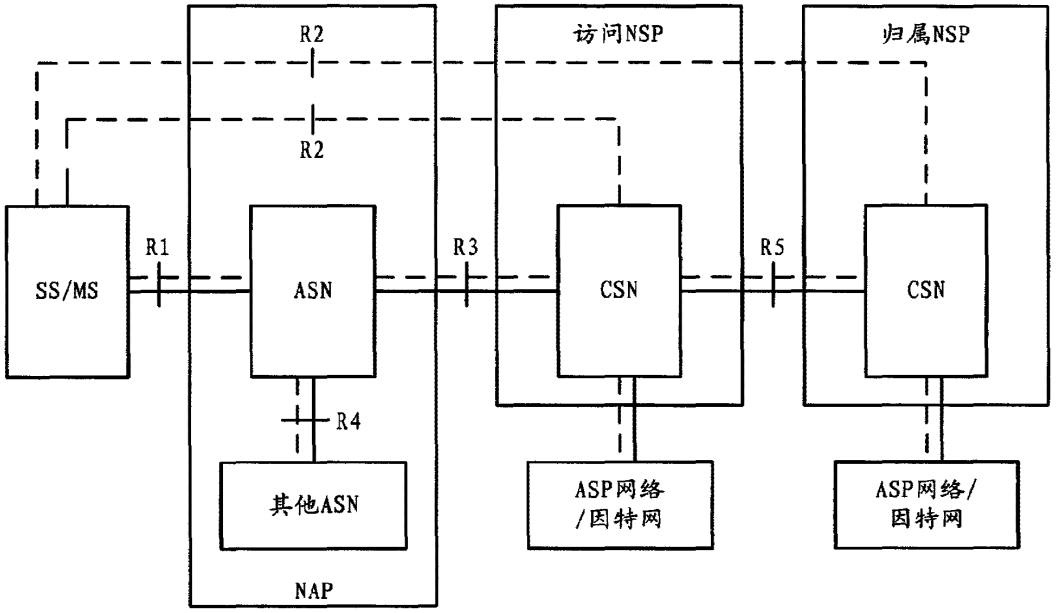


图 1

IPR2025-01571
Apple EX1002 Page 630

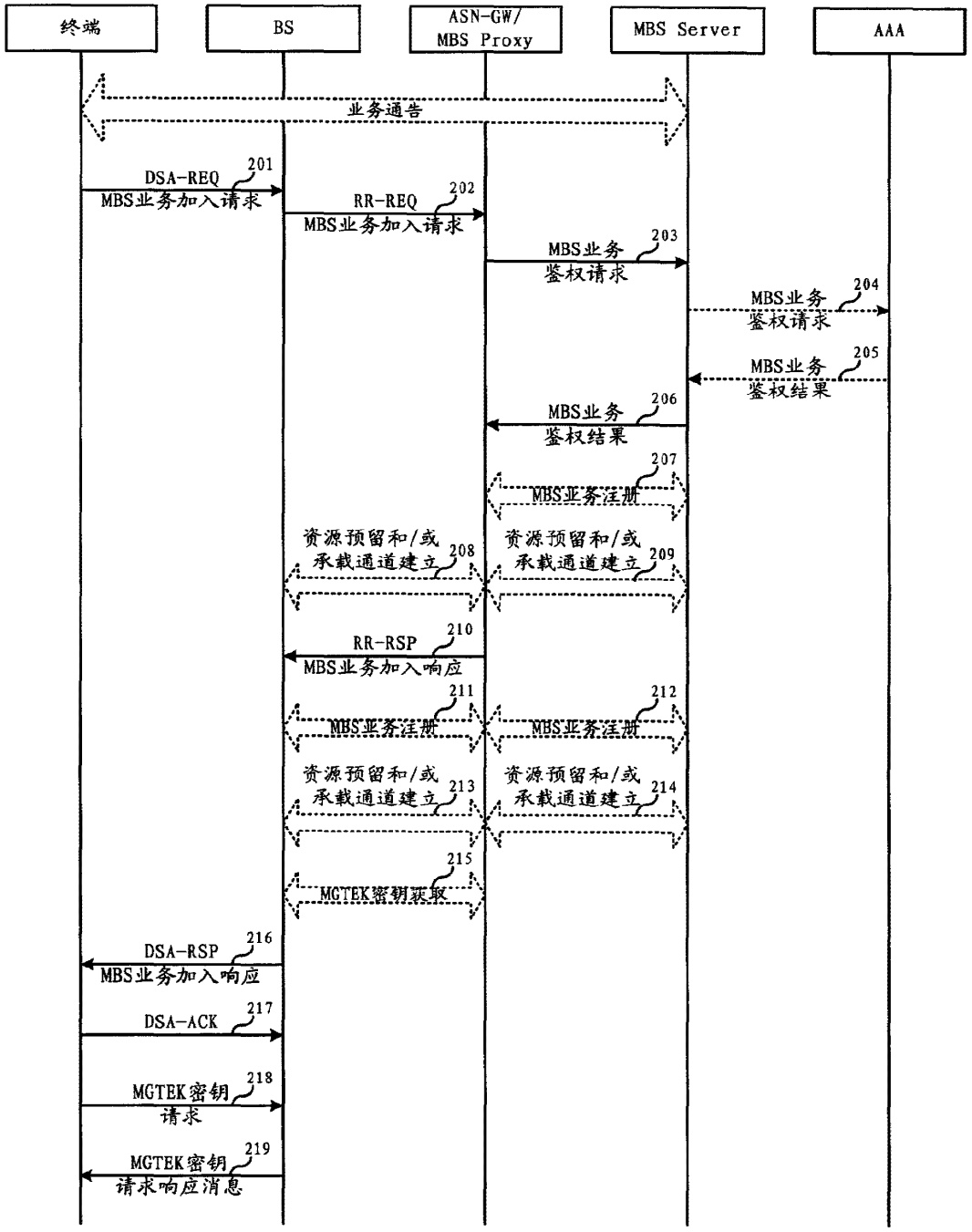


图 2

IPR2025-01571
Apple EX1002 Page 631

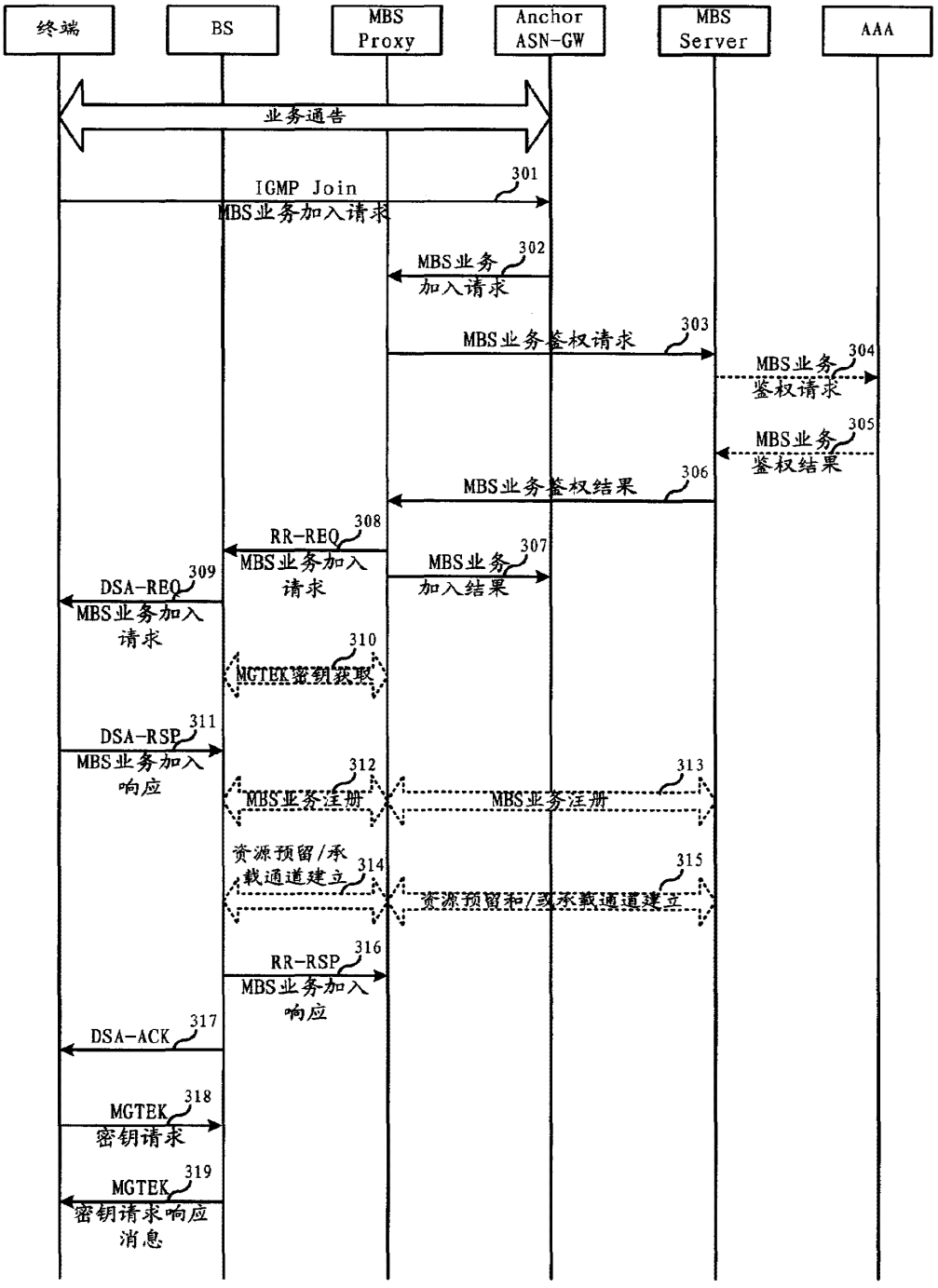


图 3

IPR2025-01571
Apple EX1002 Page 632

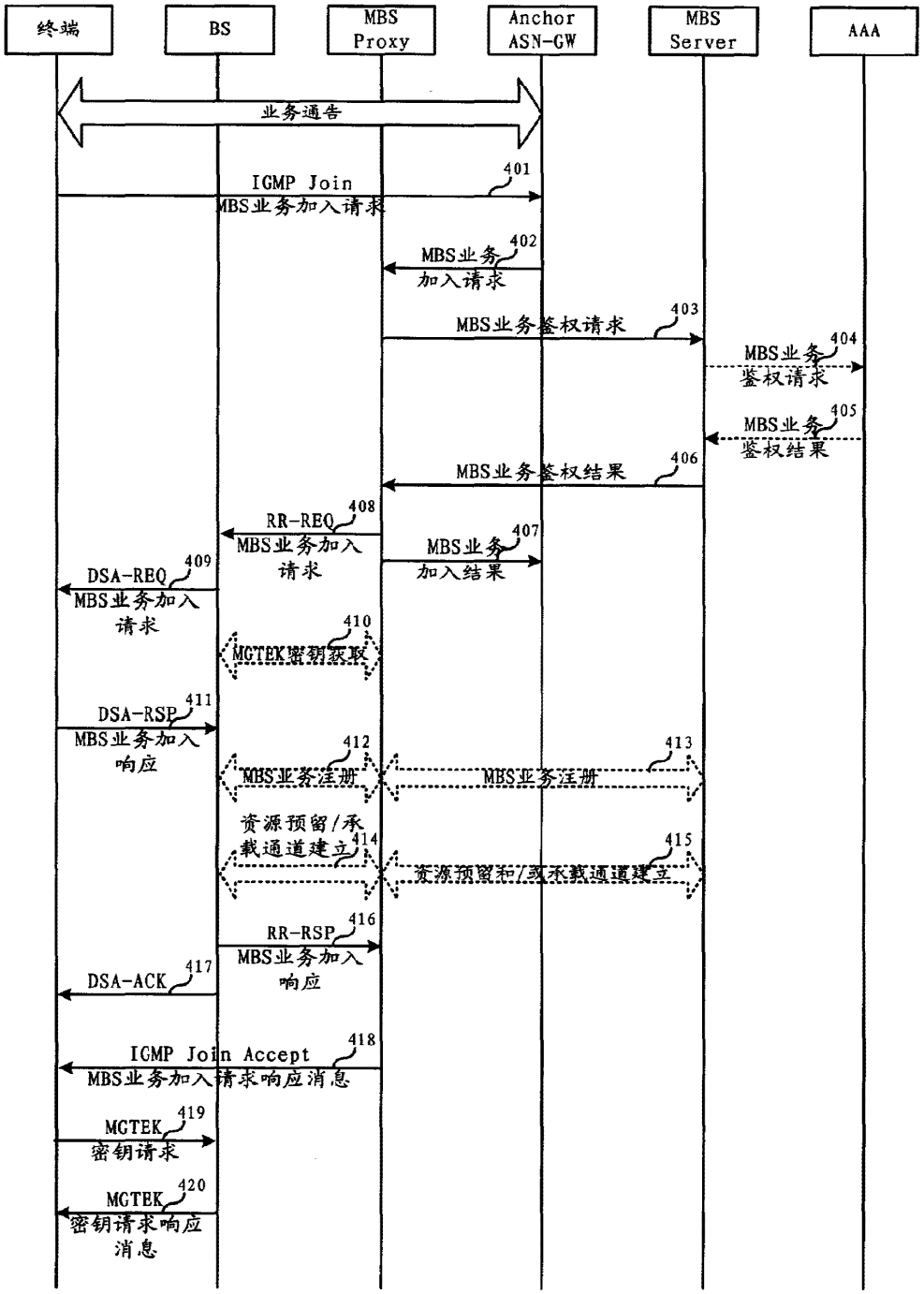


图 4

IPR2025-01571
Apple EX1002 Page 633

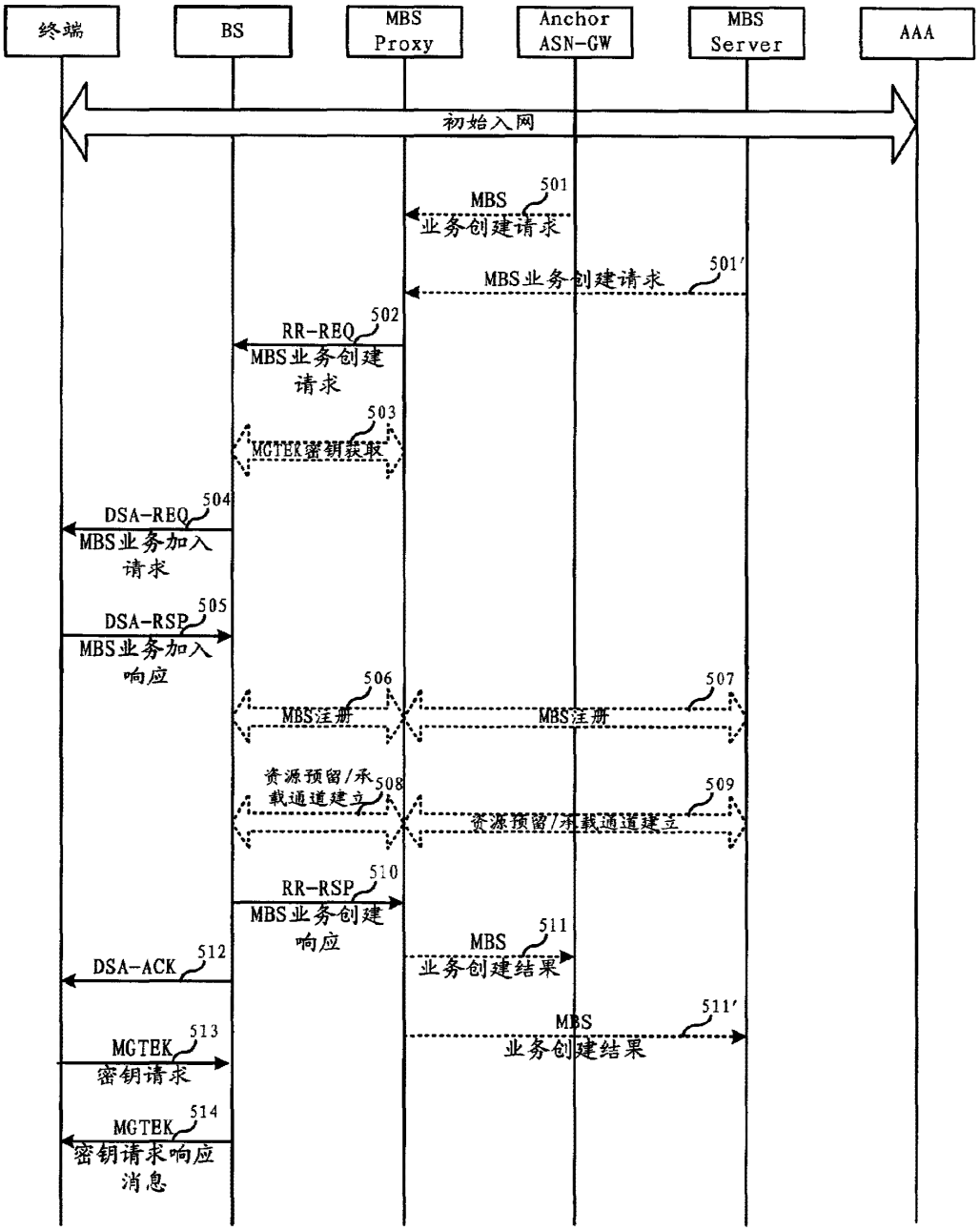


图 5

IPR2025-01571
Apple EX1002 Page 634

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04Q 7/20 (2006.01)
H04Q 7/38 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200610059298.9

[43] 公开日 2007 年 9 月 12 日

[11] 公开号 CN 101035308A

[22] 申请日 2006.3.9
[21] 申请号 200610059298.9
[71] 申请人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼
[72] 发明人 邓永锋 胡伟华 郭均祥

[74] 专利代理机构 北京康信知识产权代理有限责任公司
代理人 余 刚 尚志峰

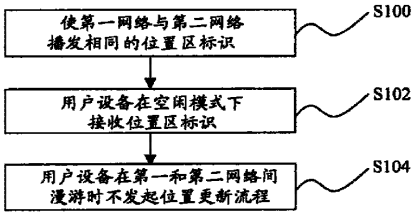
权利要求书 5 页 说明书 16 页 附图 6 页

[54] 发明名称

无线通信系统和移动性管理方法

[57] 摘要

本发明公开了一种无线通信系统和移动性管理方法。无线通信系统包括第一无线网络和第二无线网络。第一无线网络和第二无线网络播发的位置区标识相同，位置区标识由移动终端接收，从而使处于空闲模式下的移动终端在第一无线网络与第二无线网络之间漫游时，不发起位置更新流程。在第一无线网络的核心网中的支持节点和第二无线网络的核心网中的支持节点中的至少一个支持节点的配置信息中设置用于表示优选网络的信息。



IPR2025-01571
Apple EX1002 Page 635

1. 一种无线通信系统，包括第一无线网络和第二无线网络，其特征在于，所述第一无线网络和第二无线网络播发的位置区标识相同。

2. 根据权利要求 1 所述的无线通信系统，其特征在于，所述第二无线网络是所述第一无线网络的演进网络。

3. 根据权利要求 1 所述的无线通信系统，其特征在于，所述第一无线网络与所述第二无线网络的覆盖范围至少部分重叠。

4. 根据权利要求 3 所述的无线通信系统，其特征在于，所述位置区标识为路由区标识或跟踪区标识。

5. 根据权利要求 1 至 4 中任一项所述的无线通信系统，其特征在于，在所述第一无线网络的核心网中的支持节点和所述第二无线网络的核心网中的支持节点中的至少一个支持节点的配置信息中包括用于表示优选网络的信息。

6. 根据权利要求 5 所述的无线通信系统，其特征在于，所述用于表示优选网络的信息选自包括以下内容的组：不优选网络、优选第一无线网络、以及优选第二无线网络。

IPR2025-01571
Apple EX1002 Page 636

7. 根据权利要求 6 所述的无线通信系统，其特征在于，所述系统还包括至少一个移动终端，当所述用于表示优选网络的信息为优选第一无线网络时，所述移动终端的上下文保留在所述第一无线网络的核心网中，当所述用于表示优选网络的信息为优选第二无线网络时，所述移动终端的上下文保留在所述第二无线网络的核心网中。

8. 一种用于多网络间的移动性管理方法，其特征在于，包括以下步骤：

为多网络覆盖区域设置相同的位置区标识；

当移动终端在所述多网络间漫游时，所述移动终端获取所述位置区标识，而不发起位置更新流程。

9. 根据权利要求 8 所述的移动性管理方法，其特征在于，所述多网络包括第一无线网络和第二无线网络，所述第二无线网络为所述第一无线网络的演进网络。

10. 根据权利要求 9 所述的移动性管理方法，其特征在于，所述第一无线网络与所述第二无线网络的覆盖区域至少部分重叠。

11. 根据权利要求 10 所述的移动性管理方法，其特征在于，所述第一无线网络的位置区标识为该网络覆盖区域的路由区标识，所述第二无线网络的位置区标识被直接设置为所述第一无线网络的路由区标识。

12. 根据权利要求 9 至 11 中任一项所述的移动性管理方法，其特征在于，所述方法还包括在所述多网络的核心网的支持节点中的至少一个支持节点的配置信息中设置用于表示优选网络的信息。

IPR2025-01571
Apple EX1002 Page 637

13. 根据权利要求 12 所述的移动性管理方法，其特征在于，所述方法还包括，根据所述用于表示优选网络的信息，将移动终端的上下文保留在第一无线网络或第二无线网络中。

14. 一种用于多网络间的移动性管理方法，其特征在于，在第一无线网络的核心网中的支持节点和第二无线网络的核心网中的支持节点中的至少一个支持节点的配置信息中设置用于表示优选网络的信息。

15. 根据权利要求 14 所述的移动性管理方法，其特征在于，所述用于表示优选网络的信息选自包括以下内容的组：不优选网络；优选第一无线网络，所述移动终端的上下文保留在第一无线网络的核心网中；以及优选第二无线网络，所述移动终端的上下文保留在第二无线网络的核心网中。

16. 根据权利要求 15 所述的移动性管理方法，其特征在于，所述设置用于表示优选网络的信息的步骤是通过在所述支持节点中的配置信息中增加一个字段，该字段为 3 比特，其值对应于移动终端的上下文的优选保存的网络位置。

17. 根据权利要求 15 所述的移动性管理方法，其特征在于，如果所述第二无线网络为优选网络，则当移动终端从第三无线网络漫游至所述第一无线网络时，通过比较由广播信道下发的位置区标识与其保存的位置区标识，判决发起位置区更新流程，包括以下信令流程：

1）所述移动终端发送包括原注册信息的注册请求到所述第一无线网络的核心网中的第一支持节点；

IPR2025-01571
Apple EX1002 Page 638

2）所述第一支持节点将接收到的所述原注册信息发送给所述第三无线网络的核心网中的原支持节点，以获取用户信息；

3）所述原支持节点发送用户信息给所述第一支持节点；

4）所述移动终端通过第一支持节点进行鉴权；

5）所述第一支持节点检查其内配置的所述优选网络信息以及所述移动终端的接入能力，判决所述移动终端应驻留在所述第二无线网络侧，所述第一支持节点选择所述第二无线网络的核心网中的一个新支持节点，并向其发送用户上下文配置请求消息，请求该新支持节点为所述移动终端生成移动性管理上下文；

6）所述新支持节点将自身注册成所述移动终端的服务节点；

7）在所述原支持节点中所述移动终端上下文将被删除，或者所述移动终端被标志为不在其服务区；

8）归属用户服务器确认所述新支持节点注册成功，用户签约信息转移给所述新支持节点，计费策略信息也随之转移到所述新支持节点；

9）所述新支持节点接受所述移动终端的网络附着，并且分配一个临时身份给所述移动终端，并向所述第一支持节点确认用户上下文配置完成；以及

10）所述第一支持节点收到用户上下文配置响应消息后，向所述移动终端确认注册完成。

IPR2025-01571
Apple EX1002 Page 639

18 根据权利要求 17 所述的移动性管理方法，其特征在于，所述信令流程 5）中所述的所述第一支持节点选择所述第二无线网络的核心网中的一个新支持节点的步骤，是在支持所述移动终端所在的路由区的支持节点中进行选择。

19. 根据权利要求 14 至 17 中任一项所述的移动性管理方法，其特征在于，所述第二无线网络为所述第一无线网络的演进网络。

20. 根据权利要求 19 所述的移动性管理方法，其特征在于，所述第一无线网络与所述第二无线网络的覆盖范围至少部分重叠。

21. 根据权利要求 19 所述的移动性管理方法，其特征在于，所述第三无线网络的类型与所述第一无线网络和所述第二无线网络中的一种的类型相同。

IPR2025-01571
Apple EX1002 Page 640

无线通信系统和移动性管理方法

技术领域

本发明涉及无线移动通信领域，尤其涉及无线通信系统和移动性管理方法。

背景技术

通用移动通信系统（Universal Mobile Telecommunications System，UMTS）是采用宽带码分多址接入（Wideband Code Division Multiple Access，WCDMA）空中接口技术的第三代移动通信系统（3G），通常也把 UMTS 称为 WCDMA 通信系统。如图 1 所示，UMTS 采用了与第二代移动通信系统（2G）类似的结构，包括无线接入网络（Radio Access Network，RAN）**20** 和核心网络（Core Network，CN）**30**。其中无线接入网络 **20** 用于处理所有与无线有关的功能，而核心网络 **30** 处理 UMTS 内所有的话音呼叫和数据连接，并实现与外部网络 **40** 的交换和路由功能。核心网络从逻辑上分为电路交换域（Circuit Switched Domain，CS）**32** 和分组交换域（Packet Switched Domain，PS）**34**。UMTS 陆地无线接入网（UMTS Territorial Radio Access Network，UTRAN）**20**、核心网络 **30**、与用户设备（User Equipment，UE）**10** 一起构成了整个 UMTS。

如图 2 所示，UTRAN 包含一个或几个无线网络子系统（Radio Network Subsystem，RNS）**22**。一个无线网络子系统 **22** 由一个无线网络控制器（Radio Network Controller，RNC）**24** 和一个或多个基站（NodeB）**26** 组成。无线网络控制器 **24** 与核心网络 **30** 之间的

IPR2025-01571
Apple EX1002 Page 641

接口是 Iu 接口，NodeB **26** 与无线网络控制器 **24** 通过 Iub 接口连接。在 UTRAN 内部，无线网络控制器 **24** 之间通过 Iur 接口互联，Iur 接口可以通过无线网络控制器 **24** 之间的直接物理连接或通过传输网连接。无线网络控制器 **24** 用来分配和控制与之相连或相关的 NodeB **26** 的无线资源（Radio Resource）。NodeB **26** 则完成 Iub 接口与 Uu 接口之间的数据流的转换，同时也参与一部分无线资源管理。

NodeB **26** 是 WCDMA 系统的基站，包括无线收发信机和基带处理部件。通过标准的 Iub 接口与无线网络控制器 **24** 互连，主要完成 Uu 接口物理层协议的处理。它的主要功能是扩频、调制、信道编码以及解扩、解调、信道解码，还包括基带信号和射频信号的相互转换等功能。

无线网络控制器 **24** 用于控制 UTRAN 的无线资源，主要完成连接建立和断开、切换、宏分集合并、无线资源管理控制等功能。

以上的网络架构是基于 3GPP Rel6 以前版本的架构，目前 3GPP（3rd Generation Partnership Project）正在研究一种全新的演进网络架构，以满足未来十年甚至更长时间内移动网络的应用需求。由于是一种全新的网络架构，因此现有架构的所有节点、功能、和流程都将发生实质性的变化。

3GPP 考虑到未来网络的竞争能力，目前正在积极研究一种演进的 3GPP 网络系统，目前有很多种演进方案在 3GPP 展开了讨论，网络演进的目的是希望提供一种低时延、高数据速率、高系统容量和覆盖、低成本、完全基于 IP 的网络。

其中，网络演进的目标之一就是实现演进的 UMTS 陆地无线接入网（Evolved UMTS Territorial Radio Access Network，E-UTRAN）和 UTRAN、GSM/EDGE 无线接入网（GSM/EDGE Radio Access

IPR2025-01571
Apple EX1002 Page 642

Network，GERAN）之间的移动性管理，目前提出了一种解决所述3GPP 接入系统间移动性管理的方案，该方案基于如图 3 所示的网络架构。

现有的不同无线接入类型（Radio Access Type，RAT）间的移动性管理方案对于位置区的规划采用的是基于不同的接入技术的方案。如图 3 所示，长期演进（Long Term Evolution，LTE）路由区（Routing Area，RA）**52** 为演进的 E-UTRAN 小区，2G/3G 路由区 **50** 为传统网络中的 UMTS 或 GPRS 小区。当作为移动终端的用户设备 **10** 在演进的系统架构演进（System Architecture Evolution，SAE）网络和传统的 2G/3G 网络间漫游时，用户设备 **10** 为了接收网络提供的业务，需要向网络侧发起路由区更新过程。在这种网络架构下，用户设备发起的路由区更新流程如下：

1）当用户设备 **10** 从 2G/3G 网络覆盖下进入演进的 SAE 网络覆盖下，用户设备 **10** 通过监听广播信道获得其所在的演进网络路由区标识（identify）信息。发现与原有的 2G/3G 网络路由区标识不匹配，则用户设备 **10** 向网络侧发起路由区更新流程。

2）用户设备 **10** 发送一个路由区更新请求到 MME/UPE（Mobility Management Entity，移动性管理实体；User Plane Entity，用户平面实体）**82**，消息包括原来的注册信息（如临时身份等，如果没有临时身份就用永久身份）。路由区更新请求还可以包括缺省 IP 接入承载（Access Bearer）信息（如用户优选的 IP 地址和 APN）。

3）MME/UPE **82** 将接收到的原注册信息发送给原来的 MME/UPE **25** 以获取用户的信息。

4）原来的 MME/UPE **25** 发送用户信息（如永久用户身份）给新 MME/UPE **82**。

IPR2025-01571
Apple EX1002 Page 643

5）用户设备通过新的 MME/UPE **82** 进行鉴权。

6）新 MME/UPE **82** 将自身注册成用户设备 **10** 的服务节点。

7）在原 MME/UPE **25** 中用户设备 **10** 的信息将被删除，或者用户设备 **10** 被标志为不在本服务区。

8）归属用户服务器（Home Subscriber Server，HSS）**60** 确认 MME/UPE **82** 注册成功，授权使用缺省 IP 接入承载的用户签约信息转移给 MME/UPE **82**，计费策略信息也随之转移到 MME/UPE **82**。

9）选择 Inter AS Anchor **70**。

10）Inter AS Anchor **70** 配置 IP 层。用户平面在 UPE-Inter AS Anchor 之间建立起来，并且使用缺省的计费和策略。

11）MME/UPE **82** 将缺省 IP 接入承载的服务质量（Quality of Service，QOS）配置信息提供给演化的无线接入网络。MME/UPE **82** 接受用户设备 **10** 的位置更新请求，并为用户设备 **10** 分配一个临时标识。

12）MME/UPE **82** 确认用户设备路由区更新成功。

从上面的流程可以看出，现有的不同无线接入类型间的空闲模式（LTE_IDLE）下的移动性管理方案存在如下的缺点：在空闲模式下，用户设备从 2G/3G 移动到 SAE/LTE 接入系统时，将发生位置更新的一系列过程，包括 MME/UPE 之间用户设备上下文（UE Context）的转移，MME 向 HSS 注册，UPE 向 Inter AS Anchor 做路由更新等，因此将导致一系列的空闲模式下的位置管理信令流量。而由于演进网络建网初期 E-UTRAN 小区覆盖范围较小，随着用户设备的漫游，其在 E-UTRAN 和 UTRAN、GERAN 之间频繁移动，

IPR2025-01571
Apple EX1002 Page 644

从而导致系统频繁进行位置更新的流程，极大地增加了空闲模式下的信令流量负荷。

发明内容

本发明的主要目的在于提供一种移动性管理方法及无线通信系统，用于克服由于现有技术的局限和缺陷而造成的在不同无线接入类型的接入网络之间频繁移动导致的系统频繁进行位置更新的问题。

为了实现上述目的，根据本发明的第一方面，本发明提供了一种无线通信系统。该无线通信系统包括第一无线网络和第二无线网络。当处于空闲模式下的移动终端所接收到的位置区标识发生变化时，其发起位置更新流程。第一无线网络和第二无线网络播发的位置区标识相同，使得处于空闲模式下的移动终端在第一无线网络与第二无线网络之间漫游时，不发起位置更新流程。

在该无线通信系统中，第一无线网络与第二无线网络的覆盖范围可以部分重叠。第一无线网络和第二无线网络中的一种可以是另一种的演进网络。第一无线网络和第二无线网络中的一种可以包括2G、2.5G、和3G网络中的至少一种。位置区标识可以为路由区标识或跟踪区标识。

为了实现上述目的，根据本发明的第二方面，本发明提供了一种移动性管理方法。为多网络覆盖区域设置相同的位置区标识。位置区标识由移动终端接收，从而使处于空闲模式下的移动终端在多网络间漫游时，不发起位置更新流程。

多网络可以包括第一无线网络和第二无线网络。第一无线网络与第二无线网络的覆盖范围可以部分重叠。第一无线网络和第二无

IPR2025-01571
Apple EX1002 Page 645

线网络中的一种可以是另一种的演进网络。第一无线网络和第二无线网络中的一种可以包括 2G、2.5G、和 3G 网络中的至少一种。

位置区标识可以为路由区标识或跟踪区标识。第一无线网络的位置区标识可以为该网络覆盖区域的路由区标识，第二无线网络的位置区标识被直接设置为第一无线网络的路由区标识。

为了实现上述目的，根据本发明的第三方面，本发明提供了一种移动性管理方法。在第一无线网络的核心网中的支持节点和第二无线网络的核心网中的支持节点中的至少一个支持节点的配置信息中设置用于表示优选网络的信息。

第一无线网络与第二无线网络的覆盖范围可以部分重叠。第一无线网络和第二无线网络中的一种可以是另一种的演进网络。

用于表示优选网络的信息可以选自包括以下内容的组：不优选网络；优选第一无线网络，移动终端的上下文保留在第一无线网络的核心网中；以及优选第二无线网络，移动终端的上下文保留在第二无线网络的核心网中。

设置用于表示优选网络的信息的步骤可以是通过在支持节点中的配置信息中增加一个字段，字段可以为 3 比特，其值对应于移动终端的上下文的优选保存网络位置。

如果第二无线网络为优选网络，则当移动终端从第三无线网络漫游至第一无线网络时，通过比较由广播信道下发的位置区标识与其保存的位置区标识，判决发起位置区更新流程，包括以下信令流程：

1）移动终端发送包括原注册信息的注册请求到第一无线网络的核心网中的第一支持节点；

IPR2025-01571
Apple EX1002 Page 646

2）第一支持节点将接收到的原注册信息发送给第三无线网络的核心网中的原支持节点，以获取用户信息；

3）原支持节点发送用户信息给第一支持节点；

4）移动终端通过第一支持节点进行鉴权；

5）第一支持节点检查其内配置的优选网络信息以及移动终端的接入能力，判决移动终端应驻留在第二无线网络侧，第一支持节点选择第二无线网络的核心网中的一个新支持节点，并向其发送用户上下文配置请求消息，请求该新支持节点为移动终端生成移动性管理上下文；

6）新支持节点将自身注册成移动终端的服务节点；

7）在原支持节点中移动终端上下文将被删除，或者移动终端被标志为不在其服务区；

8）归属用户服务器确认新支持节点注册成功，用户签约信息转移给新支持节点，计费策略信息也随之转移到新支持节点；

9）新支持节点接受移动终端的网络附着，并且分配一个临时身份给移动终端，并向第一支持节点确认用户上下文配置完成；以及

10）第一支持节点收到用户上下文配置响应消息后，向移动终端确认注册完成。

第三无线网络的类型可与第一无线网络和第二无线网络中的一种的类型相同。

IPR2025-01571
Apple EX1002 Page 647

通过上述技术方案，本发明实现了如下技术效果。由于不同无线接入类型的网络采用相同的位置区标识，使得移动终端在不同无线接入类型的网络的覆盖区域间漫游时，不会发起位置更新的流程，避免了由于系统频繁进行位置更新流程而导致的空闲模式下的信令流量负荷的大量增加。此外，保持移动终端的实际驻留网络和保留移动终端上下文的网络的一致性，有效的减小了移动终端上下文的迁移。

附图说明

此处所说明的附图用来提供对本发明的进一步理解，构成本申请的一部分，本发明的示意性实施例及其说明用于解释本发明，并不构成对本发明的不当限定。在附图中：

图 1 是 UMTS 系统结构图；

图 2 是 UTRAN 网络结构图；

图 3 示出 3GPP SAE/LTE 与 2G/3G 接入系统间的移动；

图 4 是根据本发明的移动性管理方法的流程图；

图 5 是根据本发明的无线通信系统的框图；

图 6 是根据本发明的移动性管理方法的流程图；

图 7 是根据本发明实施例的演进路由区规划示意图；

图 8 是根据本发明实施例的演进路由区的结构示意图；以及

图 9 示出根据本发明实施例的用户设备附着流程。

IPR2025-01571
Apple EX1002 Page 648

具体实施方式

下面将参考附图详细说明本发明。

本发明基于现有的演进网络架构，提出了一种新的不同无线接入类型间位置区的规划方案，并提出了基于此位置区规划方案的移动性管理方案，有效的解决了用户设备在 E-UTRAN 和 UTRAN、GERAN 之间频繁移动导致的系统频繁进行位置更新的问题。

如图 4 所示，本发明所提供的无线通信系统包括：第一无线网络 **1**；第二无线网络 **2**。当处于空闲模式下的用户设备 **10** 所接收到的路由区或跟踪区标识发生变化时，其发起位置更新流程。第一无线网络 **1** 和第二无线网络 **2** 播发的路由区或跟踪区标识相同，使得处于空闲模式下的用户设备 **10** 在第一无线网络 **1** 与第二无线网络 **2** 之间漫游时，不发起位置更新流程。

在该无线通信系统中，第一无线网络 **1** 与第二无线网络 **2** 的覆盖范围可以部分重叠。第一无线网络 **1** 和第二无线网络 **2** 中的一种可以是另一种的演进网络。第一无线网络 **1** 和第二无线网络 **2** 中的一种可以是 2G、2.5G、或 3G 网络。

如图 5 所示，本发明所提供的移动性管理方法包括为多网络覆盖区域设置相同的位置区标识，当移动终端在多网络间漫游时，移动终端获取位置区标识，而不发起位置更新流程。多网络包括第一无线网络和第二无线网络。具体步骤如下：S100，使第一无线网络与第二无线网络播发相同的位置区标识；S102，当用户设备在处于空闲模式时，其接收无线网络所播发的位置区标识；以及 S104，当用户设备在第一无线网络与第二无线网络之间漫游时，不发起位置更新流程。

IPR2025-01571
Apple EX1002 Page 649

第一无线网络与第二无线网络的覆盖范围可以部分重叠。第一无线网络和第二无线网络中的一种可以是另一种的演进网络。第一无线网络和第二无线网络中的一种可以是 2G、2.5G 或 3G 网络。位置区标识可以为路由区标识或跟踪区标识。

如图 6 所示，本发明所提供的另一种移动性管理方法包括以下步骤：S200，在第一无线网络的核心网和/或第二无线网络的核心网中的支持节点的配置信息中增加一个字段，该字段可以为 3 比特，其值对应于用户设备的上下文的优选保存网络位置；S202，使字段表示优选网络信息，例如，不优选；优选第一无线网络，用户设备的上下文保留在第一无线网络的核心网中；以及优选第二无线网络，用户设备的上下文保留在第二无线网络的核心网中。

如果配置为优选第一无线网络时（S204），则当用户设备从第三无线网络漫游至第二无线网络时，发起位置更新流程（S206）。如果配置为优选第二无线网络时（S208），则当用户设备从第三无线网络漫游至第一无线网络时，发起位置更新流程（S210）。

第一无线网络与第二无线网络的覆盖范围可以部分重叠。第一无线网络和第二无线网络中的一种是另一种的演进网络。第三无线网络的类型与第一无线网络和第二无线网络中的一种的类型相同。

第一无线网络和第二无线网络播发的位置区标识可以相同。无论第一无线网络和第二无线网络播发的位置区标识是否相同，在第一无线网络的核心网和/或第二无线网络的核心网中的支持节点的配置信息中都可以包括用于表示优选网络的信息，该用于表示优选网络的信息可以是增加的字段。

如果第二无线网络被配置为优选网络，则当用户设备从第三无线网络漫游至第一无线网络时，通过比较由广播信道下发的位置区

IPR2025-01571
Apple EX1002 Page 650

标识与其保存的位置区标识，判决发起位置区更新流程，包括以下信令流程：

1）用户设备发送包括原注册信息的注册请求到第一无线网络的核心网中的第一支持节点；

2）第一支持节点将接收到的原注册信息发送给第三无线网络的核心网中的原支持节点，以获取用户信息；

3）原支持节点发送用户信息给第一支持节点；

4）用户设备通过第一支持节点进行鉴权；

5）第一支持节点检查其内配置的优选网络信息以及用户设备的接入能力，判决用户设备应驻留在第二无线网络侧，第一支持节点选择第二无线网络的核心网中的一个新支持节点，并向其发送用户上下文配置请求消息，请求该新支持节点为用户设备生成移动性管理上下文；

6）新支持节点将自身注册成用户设备的服务节点；

7）在原支持节点中用户设备上下文将被删除，或者用户设备被标志为不在其服务区；

8）归属用户服务器确认新支持节点注册成功，用户签约信息转移给新支持节点，计费策略信息也随之转移到新支持节点；

9）新支持节点接受用户设备的网络附着，并且分配一个临时身份给用户设备，并向第一支持节点确认用户上下文配置完成；

IPR2025-01571
Apple EX1002 Page 651

10）第一支持节点收到用户上下文配置响应消息后，向用户设备确认注册完成。

[实施例一]

在新的演进路由区（Evolved Routing Area，ERA）规划方案中，原有的2G/3G网络覆盖的区域仍保持原有的路由区规划，而演进网络覆盖的区域则采用和同地区的传统2G/3G网络联合规划的方式，形成演进路由区（演进路由区还可以自定义称为：统一（unified）路由区、联合（united）路由区、接合（joint）路由区、关联（associated）路由区、或组合（combined）路由区）。在本实施例中，可以将原有的2G/3G网络视为第一无线网络，演进网络视为第二无线网络。

图7所示的是演进路由区规划示意图。图中共有三种类型的网络覆盖：由无线网络控制器**24**管理的3G网络的UTRAN小区；由边界无线站（Edge Radio Station，ERS）**84**管理的演进网络的E-UTRAN网络小区；由基站控制器（Base Station Controller，BSC）**28**管理的2G网络的GERAN小区。其中由于BSC **28**控制的GERAN小区为独立的传统2G/3G网络覆盖，则BSC **28**下的小区按照现有的路由区规划方案，分解成多个路由区 **56**。而无线网络控制器 **24**控制的UTRAN小区和ERS **84**控制的E-UTRAN小区覆盖同一地区，因此将UTRAN小区和E-UTRAN小区进行统一规划，形成统一的演进路由区 **54**。

如图8所示，演进路由区由两部分组成：传统的3G网络覆盖下的UTRAN小区组成的路由区RA **56**；演进网络覆盖的E-UTRAN小区组成的跟踪区TA1 **58**和TA2 **59**。在演进路由区规划方案中，针对每一个演进路由区都定义一个路由区标识。考虑到演进网络从现有的2G/3G网络中平滑演进的需求，可以采用将演进网络覆盖的E-UTRAN 小区并入到传统网络的路由区的方式规划演进路由区。

IPR2025-01571
Apple EX1002 Page 652

即新增的 E-UTRAN 小区组成的跟踪区 TA **58**、**59** 的标识直接采用原有的 UTRAN 小区组成的路由区 RA **56** 的标识。

当用户设备 **10** 在演进路由区中漫游时，无论是从传统的 3G 网络覆盖下的 UTRAN 小区漫游到演进网络覆盖的 E-UTRAN 小区，还是从演进网络覆盖的 E-UTRAN 小区漫游到传统的 3G 网络覆盖下的 UTRAN 小区，由于两种网络覆盖的位置区标识相同，用户设备 **10** 不会发起位置更新的流程，避免了由于演进网络建网初期 E-UTRAN 小区覆盖范围较小而导致的系统频繁进行位置更新流程和由此极大增加的空闲模式下的信令流量负荷。

[实施例二]

本发明在演进路由区规划方案的基础上，提出了一种根据策略优选无线接入类型驻留的路由区更新方案。优选技术的实现方法如下：将控制同一演进路由区 ERA 的服务 GPRS 支持节点（Serving GPRS Support Node，SGSN）和演进系统 SAE MME/UPE 规划为一个资源池。在 SGSN 或 MME 的配置信息中增加一个 3bit 的字段，用于保留运营商配置的优选网络信息，字段设置方式为：000 表示不优选网络；001 表示优选 E-UTRAN 网络，当用户设备驻扎在此演进路由区 ERA 时，其上下文由池内的 SAE MME 保留；010 表示优选 2G/3G 网络，当用户设备驻扎在此演进路由区 ERA 时，其上下文由池内 SGSN 保留。同时，可以对本方案进行灵活扩展，只需要对该字段增加新的定义即可。

应用此种路由更新的方法，当优选 E-UTRAN 网络时，由于用户设备的上下文始终保存在演进网络侧，当用户设备处于 E-UTRAN 网络覆盖下时，可以便捷的获得演进网络的优质服务；而建网的初期则可以优选 GSM 网络，此时用户设备的上下文始终保存在 SGSN 中。由于建网初期，E-UTRAN 网络的建网范围有限，

IPR2025-01571
Apple EX1002 Page 653

用户设备在绝大多数的情况下将处于现有的 2G/3G 覆盖下，保持用户设备的实际驻留网络和保留用户设备上下文的网络的一致性，有效的减小了用户设备上下文的迁移。

类似实施例一，可以将原有的 2G/3G 网络视为第一无线网络，演进网络（E-UTRAN 网络）视为第二无线网络。那么第一无线网络的核心网中的支持节点为 SGSN，第二无线网络的核心网中的支持节点为 MME/UPE。

值得注意的是，本实施例的实现可以基于实施例一的实现，但是也可以在第一无线网络和第二无线网络播发的位置区标识不相同的情况下得以实现。

图 9 示出 E-UTRAN 为优选网络的情况下用户设备路由区更新的完整消息流程。这是假设 E-UTRAN 网络被配置为优选网络，并且用户设备从另一 E-UTRAN 路由区漫游至该演进路由区的情况。根据实际情况，也可能是 2G/3G 网络被配置为优选网络。另外，用户设备漫游前所处的第三无线网络也可能是 2G/3G 网络。该用户设备附着的流程描述如下：

1）用户设备 **10** 漫游至演进路由区的 UTRAN 网络覆盖部分，通过比较广播信道下发的路由区标识与其保存的路由区标识，判决发起路由区更新流程。用户设备 **10** 发送一个注册请求到 SGSN **28**，消息包括原来的注册信息（如临时身份等，如果没有临时身份就用永久身份）。

2）SGSN **28** 将接收到的原注册信息发送给原来的 MME/UPE **82a**，以获取用户的信息。

IPR2025-01571
Apple EX1002 Page 654

3）原来的 MME/UPE **82a** 发送用户信息（如永久用户身份）给 SGSN **28**。

4）用户设备 **10** 通过 SGSN **28** 进行鉴权。

5）SGSN **28** 检查其内配置的优选网络信息以及用户设备 **10** 的接入能力（是否能够接入演进网络），判决用户设备 **10** 应驻留在演进网络侧。由于 MME/UPE 与演进的基站（Evolved NodeB，ENB）间是多对多的连接关系，因此 SGSN **28** 应根据负荷分担原则选择一 MME/UPE **82b**，并向其发送用户上下文配置请求消息，请求该 MME/UPE **82b** 为用户设备 **10** 生成 MM 上下文。该消息包括，用户永久标识，用户的位置信息，安全信息等。

6）新 MME/UPE **82b** 将自身注册成用户设备 **10** 的服务节点。

7）在原 MME/UPE **82a** 中用户设备 **10** 的信息将被删除，或者用户设备 **10** 被标志为不在本服务区。

8）HSS **60** 确认 MME/UPE **82b** 注册成功，用户签约信息转移给 MME/UPE **82b**，计费策略信息也随之转移到 MME/UPE **82b**。

9）新的 MME/UPE **82b** 接受用户设备 **10** 的网络附着，并且分配一个临时身份给用户设备 **10**，并向 SGSN **28** 确认用户上下文配置完成。

10）SGSN **28** 收到用户上下文配置响应消息后，向用户设备 **10** 确认注册完成。

11）Inter AS Anchor **76** 配置 IP 层。用户平面在 UPE-Inter AS Anchor 之间建立起来，并且使用缺省的计费和策略。

IPR2025-01571
Apple EX1002 Page 655

通过本发明的上述实施例，克服了现有的不同无线接入类型间的空闲模式下的移动性管理方案的如下缺点：在空闲模式下，用户设备从 2G/3G 移动到 SAE/LTE 接入系统时，将发生位置更新的一系列过程，包括 MME/UPE 之间用户设备上下文的转移，MME 向 HSS 注册，UPE 向 Inter AS Anchor 做路由更新等，因此将导致一系列的空闲模式下的位置管理信令流量。而由于演进网络建网初期 E-UTRAN 小区覆盖范围较小，随着用户设备的漫游，其在 E-UTRAN 和 UTRAN、GERAN 之间频繁移动，从而导致系统频繁进行位置更新的流程，极大地增加了空闲模式下的信令流量负荷。本发明提出的新的不同无线接入类型间位置区的规划方案，有效的解决了用户设备在 E-UTRAN 和 UTRAN、GERAN 之间频繁移动导致的系统频繁进行位置更新的问题。此外，保持用户设备的实际驻留网络和保留用户设备上下文的网络的一致性，有效的减小了用户设备上下文的迁移。

以上所述仅为本发明的优选实施例而已，并不用于限制本发明，对于本领域的技术人员来说，本发明可以有各种更改和变化。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

IPR2025-01571
Apple EX1002 Page 656

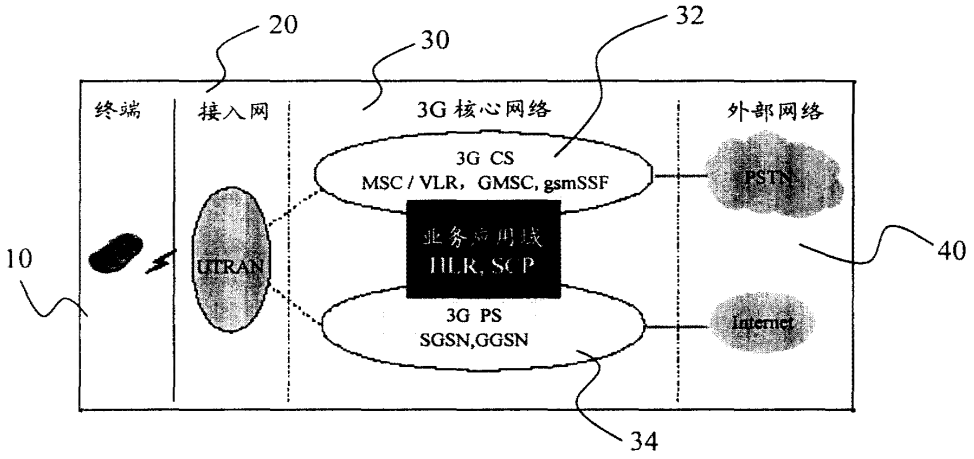


图 1

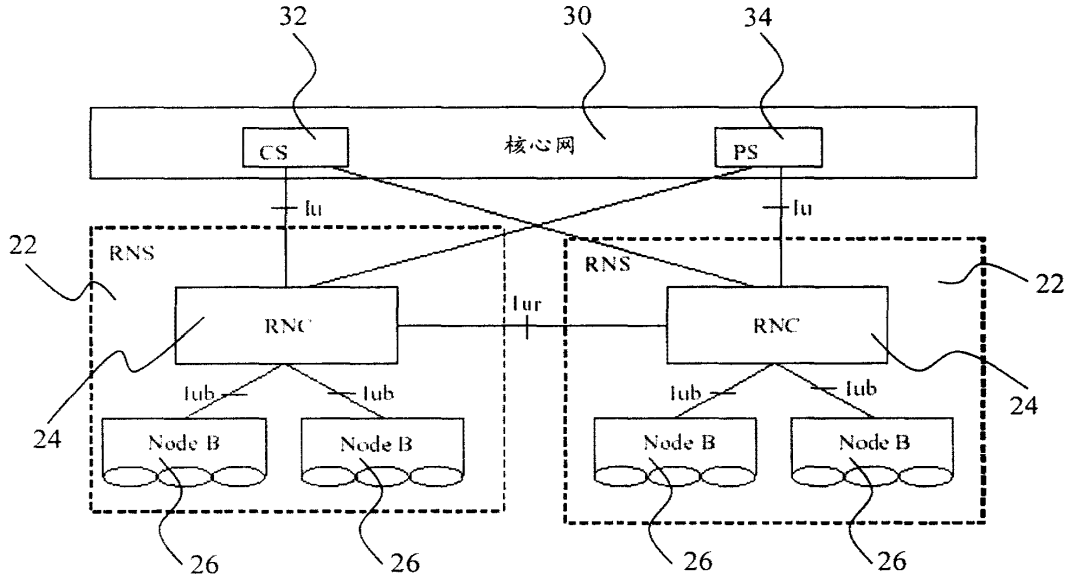


图 2

IPR2025-01571
Apple EX1002 Page 657

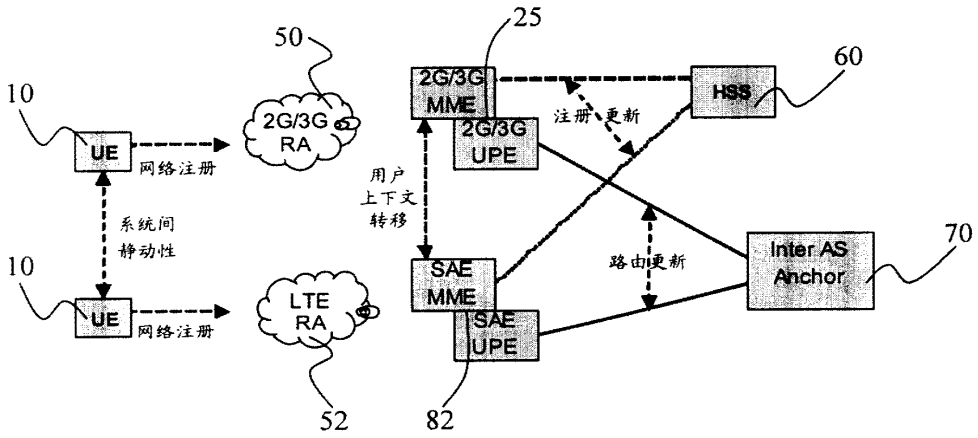


图 3

IPR2025-01571
Apple EX1002 Page 658

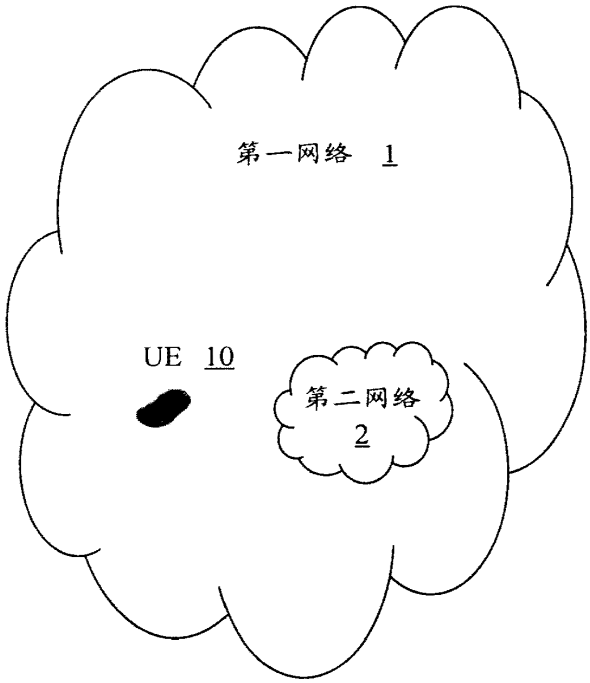


图 4

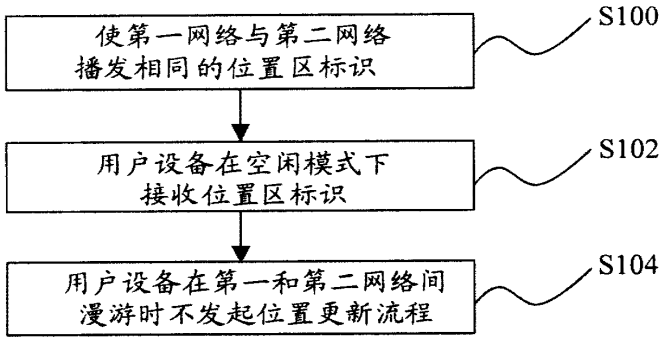


图 5

IPR2025-01571
Apple EX1002 Page 659

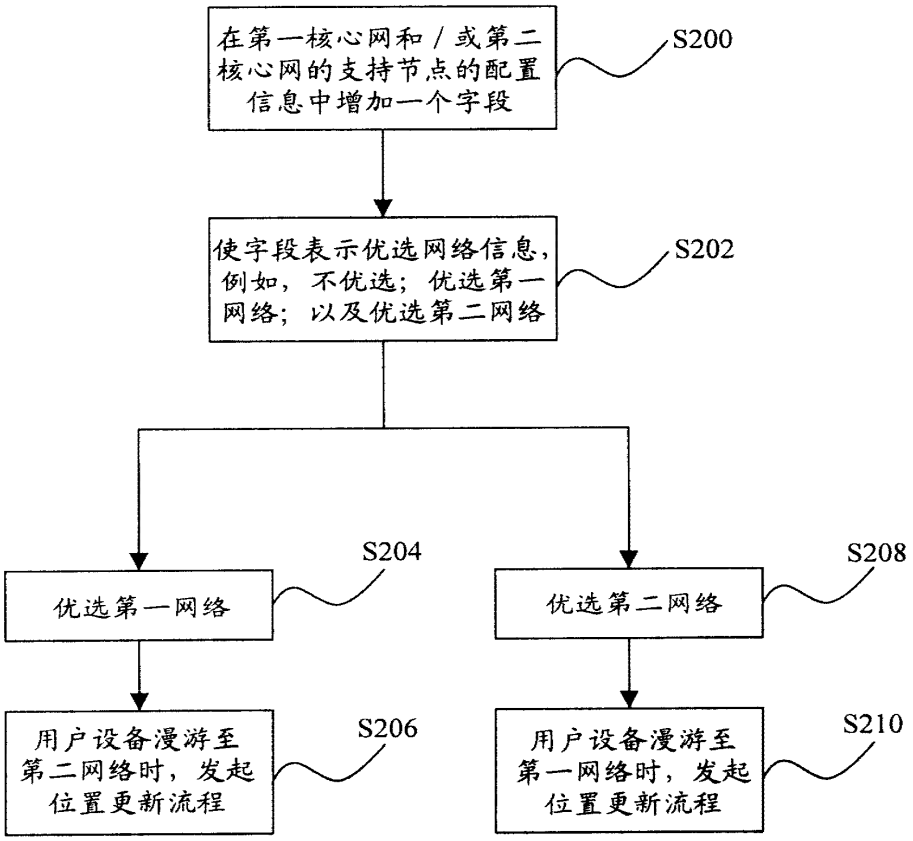


图 6

IPR2025-01571
Apple EX1002 Page 660

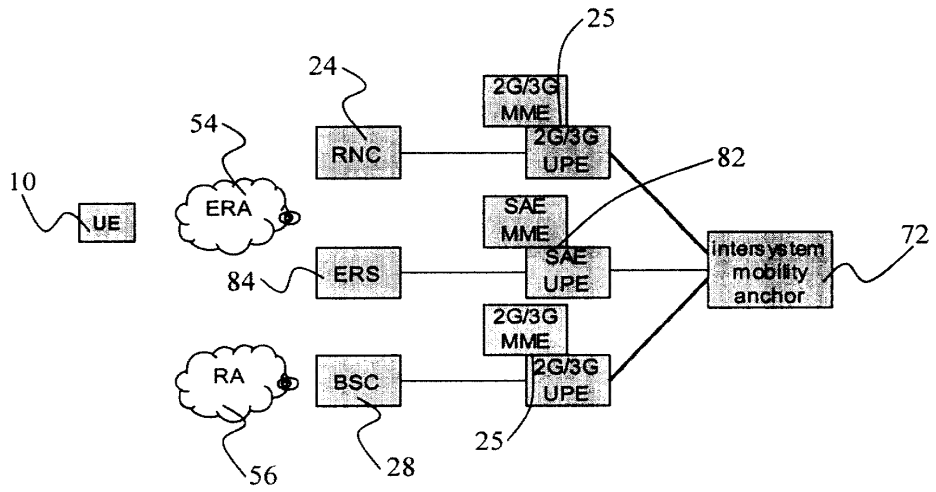


图 7

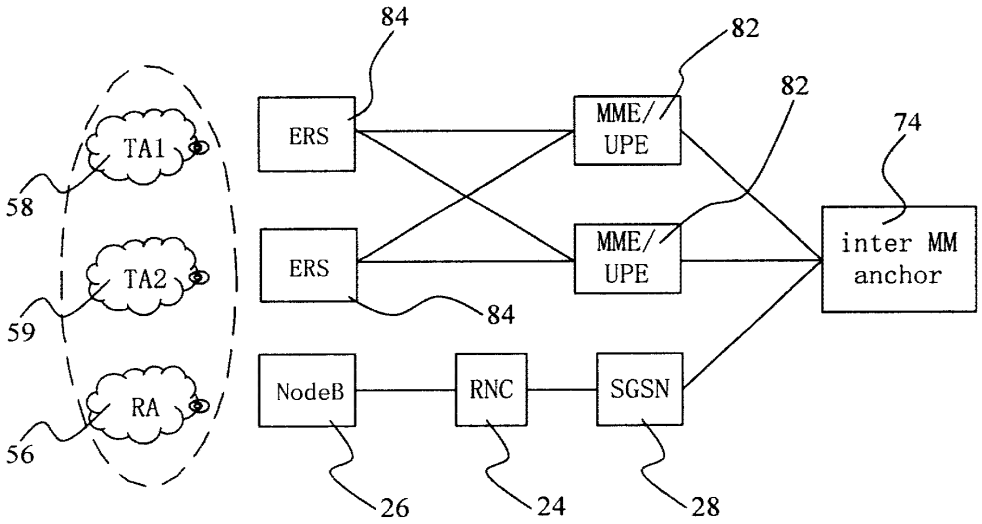


图 8

IPR2025-01571
Apple EX1002 Page 661

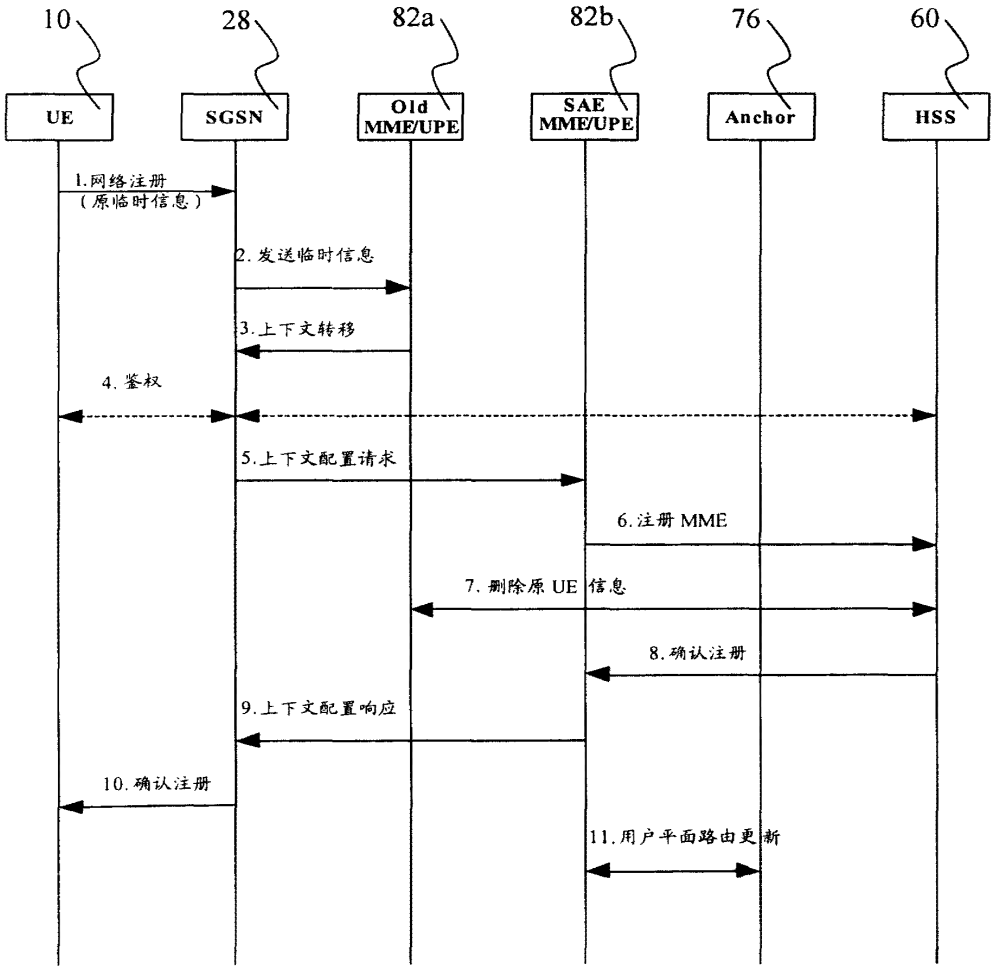


图 9

IPR2025-01571
Apple EX1002 Page 662

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04Q 7/38 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200610098897.1

[43] 公开日 2007 年 1 月 3 日

[11] 公开号 CN 1889777A

[22] 申请日 2006.7.19
[21] 申请号 200610098897.1
[71] 申请人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼
[72] 发明人 吴晓明 丁 岩 张晓鹏

[74] 专利代理机构 北京德琦知识产权代理有限公司
代理人 项 京 宋志强

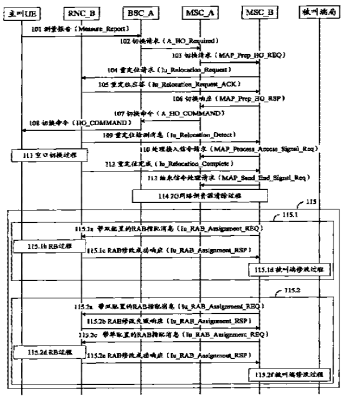
权利要求书 3 页 说明书 13 页 附图 2 页

[54] 发明名称

从第二代切换回第三代移动通信系统的业务更改方法

[57] 摘要

本发明公开了一种 SCUDIF 呼叫 3G 网络切换到 2G 网络，再由 2G 网络切换回 3G 网络时的业务更改方法，该方法包括以下步骤：A、3G 网络中的核心网确定切换回的业务在 2G 网络中被降质后，通知接入网将所述业务修改为 SCUDIF 呼叫业务；B、所述接入网根据所述通知将所述业务修改为 SCUDIF 呼叫业务。 应用本发明能够在用户从 2G 网络切换回 3G 网络时，将在 2G 网络中被降质的 SCUDIF 呼叫恢复为 SCUDIF 呼叫业务。



IPR2025-01571
Apple EX1002 Page 663

1、一种无限制/限制数字信息业务更改及回落 SCUDIF 呼叫从第三代移动通信 3G 网络切换到第二代移动通信 2G 网络，再由 2G 网络切换回 3G 网络时的业务更改方法，其特征在于，该方法包括以下步骤：

A、3G 网络中的核心网确定切换回的业务在 2G 网络中被降质后，通知接入网将所述业务修改为 SCUDIF 呼叫业务；

B、所述接入网根据所述通知将所述业务修改为 SCUDIF 呼叫业务。

2、根据权利要求 1 所述的方法，其特征在于，步骤 A 所述 3G 网络中的核心网确定切换回的业务在 2G 网络中被降质的方法为：

3G 网络中的核心网根据呼叫建立阶段记录的用户业务能力值，与所述切换回的业务进行比较，在该用户业务能力值与所述切换回的业务不相同时，确定所述切换回的业务在 2G 网络中被降质。

3、根据权利要求 2 所述的方法，其特征在于，所述 3G 网络中的核心网记录用户业务能力值的方法为：

在用户终端呼叫建立阶段，由该用户终端所接入的 3G 网络的移动交换中心 MSC 记录用户业务能力值。

4、根据权利要求 1 所述的方法，其特征在于，步骤 A 所述核心网通知接入网将所述业务修改为 SCUDIF 呼叫业务的方法为：

核心网向接入网发送携带多媒体、语音业务双配置的无线接入承载 RAB 指配消息，或者携带多媒体、语音业务双配置的重定位请求消息；

所述 RAB 指配消息在按照语音业务切换过程，将业务切换回 3G 网络之后发送；

所述重定位请求消息在业务从 2G 网络切换回 3G 网络的重定位过程中发送；所述重定位请求消息的 RAB 参数中，携带多媒体、语音业务双配置；

所述步骤 B 中，接入网根据 RAB 指配消息或者重定位请求消息中携带的配置信息，将业务修改为 SCUDIF 呼叫业务。

IPR2025-01571
Apple EX1002 Page 664

5、根据权利要求 4 所述的方法，其特征在于，

当接入网支持用户能力双配置时，继续执行步骤 B，并在步骤 B 之后进一步向核心网返回相应的成功响应；

否则，向核心网返回相应的失败响应。

6、根据权利要求 5 所述的方法，其特征在于，所述接入网向核心网返回的失败响应中包含失败原因值；

当所述核心网向接入网发送的消息为 RAB 指配消息，且失败原因为配置不支持时，核心网向接入网发送仅携带多媒体单配置的 RAB 指配消息；

所述步骤 B 中，接入网根据所述 RAB 指配消息将业务修改为多媒体业务；

在步骤 B 之后进一步向核心网返回 RAB 指配成功响应。

7、根据权利要求 4 所述的方法，其特征在于，所述多媒体、语音业务双配置的类型，由预先在核心网中设置的策略指定；

所述双配置类型包括：多媒体为首选业务、语音为可选业务的双配置，或者语音为首选业务、多媒体为可选业务的双配置。

8、根据权利要求 7 所述的方法，其特征在于，所述多媒体、语音业务双配置为：多媒体为首选业务、语音为可选业务的双配置；

所述携带多媒体、语音业务双配置的方法为：将 RAB 指配消息、或者重定位请求消息中的 RAB 参数的首选业务配置为多媒体业务，并在可选 RAB 配置信元值中配置语音业务；

所述步骤 B 中，接入网根据所述双配置将业务修改为多媒体首选、语音可选的 SCUDIF 呼叫业务。

9、根据权利要求 7 所述的方法，其特征在于，所述多媒体、语音业务双配置为：语音为首选业务、多媒体为可选业务的双配置；

所述携带多媒体、语音业务双配置的方法为：将 RAB 指配消息、或者重定位请求消息中的 RAB 参数的首选业务配置为语音业务，并在可选 RAB 配置信元值中配置多媒体业务；

所述步骤 B 中，接入网根据所述双配置将业务修改为语音首选、多媒体可

IPR2025-01571
Apple EX1002 Page 665

选的 SCUDIF 呼叫业务。

10、根据权利要求 9 所述的方法，其特征在于，步骤 B 之后进一步包括：

当无线资源满足时，接入网请求所述核心网将语音业务修改为多媒体业务。

11、根据权利要求 1 所述的方法，其特征在于，步骤 A 所述核心网通知接入网将所述业务修改为 SCUDIF 呼叫业务的方法为：

核心网向接入网发送携带多媒体单配置的无线接入承载 RAB 指配消息，或者携带多媒体单配置的重定位请求消息；

所述 RAB 指配消息在按照语音业务切换过程，将业务切换回 3G 网络之后发送；

所述重定位请求消息在业务从 2G 网络切换回 3G 网络的重定位过程中发送；所述重定位请求消息的 RAB 参数中，携带多媒体单配置；

所述步骤 B 中，接入网根据 RAB 指配消息或者重定位请求消息中携带的配置信息，将业务修改为多媒体业务。

12、根据权利要求 4 或 11 所述的方法，其特征在于，步骤 A 所述核心网通知接入网将所述业务修改为 SCUDIF 呼叫业务的方法为：

核心网的移动交换中心 MSC 向接入网的无线网络控制器 RNC 发送携带业务配置信息的 RAB 指配消息，或者携带业务配置信息的重定位请求消息；

所述步骤 B 中，RNC 根据 RAB 指配消息或者重定位请求消息中携带的业务配置信息，将业务修改为 SCUDIF 呼叫业务。

IPR2025-01571
Apple EX1002 Page 666

从第二代切换回第三代移动通信系统的业务更改方法

技术领域

本发明涉及移动通信系统间切换技术，特别涉及从第二代切换回第三代移动通信系统的业务更改方法。

背景技术

随着第三代移动通信（3G）宽带码分多址接入（WCDMA）技术的日趋成熟，全球许多国家都已部署 WCDMA 网络。在 3G 网络的建设过程中，为了降低建网成本、提供业务连续服务的功能，需要以第二代移动通信（2G）网络为依托，逐步实现连续覆盖的目标。因此，在较长的一段时间内，2G 网络和 3G 网络将共同存在、互相补充。

无限制数字信息/限制数字信息（UDI/RDI）业务更改及回落（SCUDIF）呼叫是 3G 网络提供的一种支持双承载能力信元值（BCIE）的多媒体呼叫，在无线资源不满足或者网络不支持等一些特定情况下，SCUDIF 呼叫将被降质为语音呼叫；而在无线资源满足或者一些特定的条件满足时，SCUDIF 呼叫将能够由语音呼叫提升为多媒体呼叫。

当用户在 2G 网络和 3G 网络共同覆盖的区域内进行多媒体业务通话时，使用双模终端的用户会出现从 3G 网络到 2G 网络、或者从 2G 网络到 3G 网络的系统间切换；

如果用户的呼叫为 SCUDIF 呼叫，那么，在从 3G 网络切换到 2G 网络的过程中，由于 2G 网络不支持多媒体业务，所以用户的多媒体业务将被降质为语音业务；

若终端的网络选择优选为 3G 网络，当无线资源条件满足时，终端会再次切换回 3G 网络，根据第三代合作伙伴计划的技术规范 3GPP TS 23.009 R6 协议

IPR2025-01571
Apple EX1002 Page 667

的描述，从2G网络到3G网络的系统间切换采用重定位过程实现，由于此前用户从3G网络切换到2G网络时，SCUDIF呼叫已经被降质为语音呼叫，所以在从2G网络切换回3G网络后，用户的业务仍然为语音业务。

如此，在3G网络的接入网侧出现了信息缺失，因此，即使在无线资源条件满足的情况下，无线网络控制器（RNC）设备也不会主动请求将业务从语音业务提升为多媒体业务，导致用户在系统间切换之后不能切换回SCUDIF呼叫业务。

发明内容

有鉴于此，本发明的主要目的在于提供一种SCUDIF呼叫3G网络切换到2G网络，再由2G网络切换回3G网络时的业务更改方法，达到将在2G网络中被降质的SCUDIF呼叫恢复为SCUDIF呼叫的目的。

为达到上述目的，本发明的技术方案具体是这样实现的：

一种无限制/限制数字信息业务更改及回落SCUDIF呼叫从第三代移动通信3G网络切换到第二代移动通信2G网络，再由2G网络切换回3G网络时的业务更改方法，该方法包括以下步骤：

A、3G网络中的核心网确定切换回的业务在2G网络中被降质后，通知接入网将所述业务修改为无限制/限制数字信息业务更改及回落SCUDIF呼叫业务；

B、所述接入网根据所述通知将所述业务修改为SCUDIF呼叫业务。

其中，步骤A所述3G网络中的核心网确定切换回的业务在2G网络中被降质的方法可以为：

3G网络中的核心网根据呼叫建立阶段记录的用户业务能力值，与所述切换回的业务进行比较，在该用户业务能力值与所述切换回的业务不相同时，确定所述切换回的业务在2G网络中被降质。

其中，所述3G网络中的核心网记录用户业务能力值的方法可以为：

在用户终端呼叫建立阶段，由该用户终端所接入的3G网络的移动交换中

IPR2025-01571
Apple EX1002 Page 668

心 MSC 记录用户业务能力值。

其中，步骤 A 所述核心网通知接入网将所述业务修改为 SCUDIF 呼叫业务的方法可以为：

核心网向接入网发送携带多媒体、语音业务双配置的无线接入承载 RAB 指配消息，或者携带多媒体、语音业务双配置的重定位请求消息；

所述 RAB 指配消息可以在按照语音业务切换过程，将业务切换回 3G 网络之后发送；

所述重定位请求消息可以在业务从 2G 网络切换回 3G 网络的重定位过程中发送；所述重定位请求消息的 RAB 参数中，可以携带多媒体、语音业务双配置；

所述步骤 B 中，接入网可以根据 RAB 指配消息或者重定位请求消息中携带的配置信息，将业务修改为 SCUDIF 呼叫业务。

其中，当接入网支持用户能力双配置时，继续执行步骤 B，并在步骤 B 之后可以进一步向核心网返回相应的成功响应；

否则，可以向核心网返回相应的失败响应。

其中，所述接入网向核心网返回的失败响应中可以包含失败原因值；

当所述核心网向接入网发送的消息为 RAB 指配消息，且失败原因为配置不支持时，核心网可以向接入网发送仅携带多媒体单配置的 RAB 指配消息；

所述步骤 B 中，接入网可以根据所述 RAB 指配消息将业务修改为多媒体业务；

在步骤 B 之后可以进一步向核心网返回 RAB 指配成功响应。

其中，所述多媒体、语音业务双配置的类型，可以由预先在核心网中设置的策略指定；

所述双配置类型包括：多媒体为首选业务、语音为可选业务的双配置，或者语音为首选业务、多媒体为可选业务的双配置。

其中，所述多媒体、语音业务双配置可以为：多媒体为首选业务、语音为可选业务的双配置；

所述携带多媒体、语音业务双配置的方法可以为：将 RAB 指配消息、或者

IPR2025-01571
Apple EX1002 Page 669

重定位请求消息中的 RAB 参数的首选业务配置为多媒体业务，并在可选 RAB 配置信元值中配置语音业务;

所述步骤 B 中，接入网可以根据所述双配置将业务修改为多媒体首选、语音可选的 SCUDIF 呼叫业务。

其中，所述多媒体、语音业务双配置可以为：语音为首选业务、多媒体为可选业务的双配置;

所述携带多媒体、语音业务双配置的方法可以为：将 RAB 指配消息、或者重定位请求消息中的 RAB 参数的首选业务配置为语音业务，并在可选 RAB 配置信元值中配置多媒体业务;

所述步骤 B 中，接入网可以根据所述双配置将业务修改为语音首选、多媒体可选的 SCUDIF 呼叫业务。

进一步地，在步骤 B 之后可以包括：当无线资源满足时，接入网请求所述核心网将语音业务修改为多媒体业务。

其中，步骤 A 所述核心网通知接入网将所述业务修改为 SCUDIF 呼叫业务的方法可以为:

核心网向接入网发送携带多媒体单配置的无线接入承载 RAB 指配消息，或者携带多媒体单配置的重定位请求消息;

所述 RAB 指配消息可以在按照语音业务切换过程，将业务切换回 3G 网络之后发送;

所述重定位请求消息可以在业务从 2G 网络切换回 3G 网络的重定位过程中发送；所述重定位请求消息的 RAB 参数中，携带多媒体单配置;

所述步骤 B 中，接入网可以根据 RAB 指配消息或者重定位请求消息中携带的配置信息，将业务修改为多媒体业务。

由上述技术方案可见，本发明的这种从第二代移动通信系统切换回第三代移动通信系统的业务更改方法，3G 网络中的核心网确定切换回的业务在 2G 网络中被降质后，通知接入网将所述业务修改为 SCUDIF 呼叫业务；所述接入网根据所述通知将所述业务修改为 SCUDIF 呼叫业务。如此，可以恢复 3G 网络

IPR2025-01571
Apple EX1002 Page 670

下接入网侧的业务信息，从而达到了将在 2G 网络中被降质的 SCUDIF 呼叫恢复为 SCUDIF 呼叫的目的。

附图说明

图 1 为本发明实施例一实现业务更改的方法流程图。

图 2 为本发明实施例二实现业务更改的方法流程图。

具体实施方式

为使本发明的目的、技术方案及优点更加清楚明白，以下参照附图并举实施例，对本发明作进一步详细说明。

本发明的主要思想是：当 SCUDIF 呼叫从 3G 网络切换到 2G 网络，再由 2G 网络切换回 3G 网络时，3G 网络中的核心网确定切换回的业务在 2G 网络中被降质后，通知接入网将所述业务修改为 SCUDIF 呼叫业务；所述接入网根据所述通知将所述业务修改为 SCUDIF 呼叫业务。

本发明提供了两种核心网通知接入网进行业务修改的方式：以 RAB 指配消息通知，和以重定位请求消息通知。前一种方式是在系统间切换完成之后，核心网向接入网发送携带多媒体、语音双配置的 RAB 指配消息，以通知接入网进行业务修改；后一种方式是在系统间切换的重定位过程中，核心网在向接入网发送的重定位请求消息中的 RAB 参数中携带多媒体、语音双配置，以通知接入网进行业务修改。

多媒体、语音双配置可以是多媒体为首选业务、语音为可选业务的双配置，也可以是语音为首选业务、多媒体为可选业务的双配置。本发明可以预先在核心网中设置相应的策略，由该策略指定在 RAB 指配消息、或者重定位请求消息中所携带的双配置类型。

下面通过在核心网中的移动交换中心（MSC），和接入网中的无线网络控制器（RNC）之间实施本发明的两个实施例，对本发明的技术方案进行详细说明。

IPR2025-01571
Apple EX1002 Page 671

实施例一:

本实施例采用 MSC 在 RAB 指配消息中携带多媒体为首选业务、语音为可选业务双配置的方式，通知 RNC 将业务修改为 SCUDIF 呼叫业务。

通常，RAB 指配消息用于业务建立阶段，使用 RAB 指配消息能够建立、修改、或者删除用户的业务。

本实施例中，用户的双模终端处于 2G 网络和 3G 网络双网覆盖区域，正在进行支持双 BCIE 的 SCUDIF 呼叫。由于用户处于移动之中，导致无线资源变化，使用户从 3G 网络切换到 2G 网络，而 SCUDIF 呼叫在用户由 3G 网络切换到 2G 网络时将被降质为语音呼叫;

当用户的移动使得无线资源条件满足时，用户再次从 2G 网络切换回 3G 网络，该切换过程按照语音业务的系统间切换过程进行;

当整个系统间切换完成之后，3G 网络的 MSC 根据呼叫建立阶段记录的用户业务能力值判断用户的业务在 2G 网络中是否被降质，当确定用户的业务被降质后，MSC 主动向 RNC 下发 RAB 指配消息，该消息中携带可选 RAB 配置信元值（Alternative RAB Configuration IE），以及多媒体为首选业务、语音为可选业务的双配置，以通知 RNC 将业务修改为 SCUDIF 呼叫业务。

图 1 为本发明实施例一实现业务更改的方法流程图。参见图 1，图中的 BSC_A 和 MSC_A 分别是 2G 网络中的 BSC、MSC 设备，RNC_B 和 MSC_B 分别是 3G 网络中的 RNC、MSC 设备。该方法包括以下步骤:

步骤 101: 主叫用户设备（UE）向 BSC_A 上报测量报告(Measure_Report)，BSC_A 根据该测量报告，确定需要进行 2G 网络到 3G 网络的系统间切换。

步骤 102: BSC_A 通过 A 接口向 MSC_A 发送切换请求消息(A_HO_Required)。

步骤 103: MSC_A 通过移动应用部分（MAP）信令向 3G 网络的 MSC_B 请求系统间切换(MAP_Prep_HO_REQ)。

步骤 104: MSC_B 向 RNC_B 发送重定位请求(Iu_Relocation_Request)，请求 3G 网络的 RNC_B 分配切换用业务资源。

IPR2025-01571
Apple EX1002 Page 672

步骤 105：RNC_B 分配切换用业务资源，并向 MSC_B 发送重定位准备完成的应答消息(Iu_Relocation_Request_ACK)。

步骤 106：MSC_B 通过 E 接口通知 MSC_A 系统间切换准备完成(MAP_Prep_HO_RSP)。

步骤 107：MSC_A 向 BSC_A 发送切换命令(A_HO_COMMAND)，进行切换过程。

步骤 108：BSC_A 通知 UE 执行切换(HO_COMMAND)。

步骤 109：RNC_B 监测到主叫 UE 在 3G 网络中的活动之后，通知 MSC_B(Iu_Relocation_Detect)。

步骤 110：MSC_B 收到该活动通知之后，通过 MAP 消息通知 MSC_A(MAP_Process_Access_Signal_Req)。

步骤 111：进行空口切换。

本步骤中的空口切换过程为现有技术，因此，对于空口切换的具体实施方法，在此不再赘述。

步骤 112：空口切换完成后，RNC_B 通知 MSC_B 整个重定位过程完成(Iu_Relocation_Complete)，即完成了 2G 网络到 3G 网络的系统间切换。

步骤 113：MSC_B 通过 MAP 消息通知 MSC_A 系统间切换完成(MAP_Send_End_Signal_Req)。

步骤 114：对 2G 网络侧资源进行清除。

本步骤中的 2G 网络侧资源清除过程为现有技术，因此，对于该资源清除过程的具体实施方法，在此不再赘述。

至此，从 2G 网络到 3G 网络的语音业务系统间切换完成，下面将进行本发明的业务更改过程。

步骤 115：MSC_B 确定用户的业务在 2G 网络中被降质后，使用 RAB 指配消息通知 RNC_B 将用户的业务修改为 SCUDIF 呼叫业务。

在呼叫建立阶段，用户所接入的 3G 网络中的 MSC 将记录用户的业务能力值；在通话过程中，虽然用户可能会切换到其他网络，但是用户最初所接入的

IPR2025-01571
Apple EX1002 Page 673

3G 网络中的 MSC 将通过与用户终端的信令交互获知用户的通话状态；在用户通话未结束之前，用户最初所接入的 3G 网络中的 MSC 将一直保留该用户的业务能力值；因此，本步骤中，MSC_B 可以根据呼叫建立阶段记录的用户业务能力值，与用户当前切换回的业务进行比较，在该用户业务能力值与所述切换回的业务不相同时，确定该切换回的业务在 2G 网络中被降质。例如，本实施例中，MSC_B 记录的用户业务能力值为 SCUDIF 呼叫业务，而切换回的业务为语音业务，则 MSC_B 确定用户的业务在 2G 网络中被降质。

本步骤中，MSC_B 经过判断，确定用户的业务在 2G 网络中被降质后，通过在 RAB 指配消息中携带表示多媒体为首选业务、语音为可选业务的双配置以通知 RNC_B 将业务修改为 SCUDIF 呼叫业务。具体实施方法是：将所述 RAB 指配消息的首选业务配置为多媒体业务，并在可选 RAB 配置信元值中配置语音业务。

由于，只有支持 3GPP TS R6 以后的版本的 RNC 设备，才能支持用户能力双配置，因此，根据 RNC_B 支持的协议版本不同，分以下两种情况进行说明：第一种情况：若切换后的 RNC 设备支持 3GPP R6 以后的版本，即 RNC_B 支持用户能力双配置，则执行步骤 115.1a。

步骤 115.1a：MSC_B 向 RNC_B 发送 RAB 指配请求消息(Iu_RAB_Assignment_REQ)，该消息中携带表示：多媒体业务为首选业务、语音业务为可选业务的双配置。

步骤 115.1b：RNC_B 根据该 RAB 指配消息对 RAB 进行修改，将用户的业务修改为多媒体业务，且语音业务为用户的可选业务。

本步骤中，RAB 修改，即无线承载（RB）重配过程为现有技术，因此，对于修改 RAB 的具体实施方法，在此不再赘述。

步骤 115.1c：RAB 修改完成后，RNC_B 向 MSC_B 返回成功响应(Iu_RAB_Assignment_RSP)，至此，主叫端业务更改过程完成，用户的业务被修改为多媒体首选、语音可选的 SCUDIF 呼叫业务。

步骤 115.1d：MSC_B 通知网络及被叫端用户进行业务修改。

IPR2025-01571
Apple EX1002 Page 674

本步骤中，MSC_B 可以在系统间切换完成后的任何时刻，向网络及被叫端用户发起修改业务的通知。被叫端业务修改过程为现有技术，因此，对于被叫端业务修改的具体实施方法，在此不再赘述。

至此，系统间切换完成，并且用户的业务已被修改为 SCUDIF 呼叫业务。

第二种情况: 若切换后的 RNC 设备仅支持 3GPP R6 以前的版本，即 RNC_B 仅支持用户能力单配置方案，则执行步骤 115.2a。

步骤 115.2a：MSC_B 向 RNC_B 发送 RAB 指配请求消息(Iu_RAB_Assignment_REQ)，该消息中携带表示：多媒体业务为首选业务、语音业务为可选业务的双配置。

步骤 115.2b: RNC_B 接收该 RAB 指配消息，由于 RNC_B 不支持双配置，RNC_B 向 MSC_B 返回失败响应(Iu_RAB_Assignment_RSP)。

步骤 115.2c: MSC_B 收到失败响应后，对失败原因进行分析，当失败原因是配置不支持时，MSC_B 重新向 RNC_B 发送 RAB 指配请求(Iu_RAB_Assignment_REQ)，该消息中仅携带多媒体配置方案。

步骤 115.2d: RNC_B 根据该 RAB 指配消息对 RAB 进行修改，将用户的业务修改为多媒体业务。

本步骤中，RAB 修改过程为现有技术，因此，对于修改 RAB 的具体实施方法，在此不再赘述。

步骤 115.2e：RAB 修改完成后，RNC_B 向 MSC_B 返回成功响应(Iu_RAB_Assignment_RSP)，至此，主叫端修改过程完成，用户的业务被修改为多媒体业务。

步骤 115.2f: MSC_B 通知网络及被叫端用户进行业务修改。

本步骤中，MSC_B 可以在系统间切换完成后的任何时刻，向网络及被叫端用户发起修改业务的通知。被叫端业务修改过程为现有技术，因此，对于被叫端业务修改的具体实施方法，在此不再赘述。

若步骤 115.2d 修改失败，即第二次修改请求失败，则不再进行修改尝试。

至此，系统间切换完成，并且用户的业务已被修改为多媒体业务。

IPR2025-01571
Apple EX1002 Page 675

由上述技术方案可见，本实施例中，首先按照语音业务的系统间切换过程对用户进行 2G 网络到 3G 网络的切换;

待整个系统间切换完成之后，3G 网络中的 MSC 根据呼叫建立阶段记录的用户业务能力值，与所述切换回的业务进行比较，判断用户的业务在 2G 网络中是否被降质;

在该用户的业务能力值与所述切换回的业务不相同时，确定用户的业务被降质，MSC 主动向 RNC 下发 RAB 指配消息，并在该消息中携带多媒体为首选业务、语音为可选业务双配置，通知 RNC 将业务修改为 SCUDIF 呼叫业务，从而实现了将被降质的 SCUDIF 呼叫恢复为 SCUDIF 呼叫的目的。

实施例二:

本实施例采用 MSC 在重定位请求消息中的 RAB 参数中携带语音为首选业务、多媒体为可选业务双配置的方式，通知 RNC 将业务修改为 SCUDIF 呼叫业务。

重定位请求消息是在系统间切换的重定位过程中，由 MSC 向 RNC 发送的请求。

本实施例中，用户的双模终端处于 2G 网络和 3G 网络双网覆盖区域，正在进行支持双 BCIE 的 SCUDIF 呼叫。由于用户处于移动之中，导致无线资源变化，使用户从 3G 网络切换到 2G 网络，而 SCUDIF 呼叫在用户由 3G 网络切换到 2G 网络时将被降质为语音呼叫;

当用户的移动使得无线资源条件满足时，用户再次从 2G 网络切换回 3G 网络，在该切换过程中，3G 网络的 MSC 根据呼叫建立阶段记录的用户业务能力值判断用户的业务在 2G 网络中是否被降质，当确定用户的业务被降质后，MSC 利用重定位请求消息中的 RAB 参数携带多媒体为首选业务、语音为可选业务双配置，以通知 RNC 将业务修改为 SCUDIF 呼叫业务。

图 2 为本发明实施例二实现业务更改的方法流程图。参见图 2，图中的 BSC_A 和 MSC_A 分别是 2G 网络中的 BSC、MSC 设备，RNC_B 和 MSC_B 分别是 3G 网络中的 RNC、MSC 设备。该方法包括以下步骤:

IPR2025-01571
Apple EX1002 Page 676

步骤 201：主叫用户设备（UE）向 BSC_A 上报测量报告(Measure_Report)，BSC_A 根据该测量报告，确定需要进行 2G 网络到 3G 网络的系统间切换。

步骤 202：BSC_A 通过 A 接口向 MSC_A 发送切换请求消息(A_HO_Required)。

步骤 203：MSC_A 通过移动应用部分（MAP）信令向 3G 网络的 MSC_B 请求系统间切换(MAP_Prep_HO_REQ)。

步骤 204：MSC_B 向 RNC_B 发送重定位请求(Iu_Relocation_Request)，请求 3G 网络的 RNC_B 分配切换用业务资源；并且，当 MSC_B 确定用户的业务在 2G 网络中被降质后，在该重定位请求消息的 RAB 参数中携带表示多媒体为首选业务、语音为可选业务的双配置，以通知 RNC_B 将业务修改为 SCUDIF 呼叫业务。

本步骤中，MSC_B 判断用户的业务在 2G 网络中是否被降质的方法与实施例一步骤 115 中的方法相同，请参见实施例一步骤 115 的描述。

本步骤中，MSC_B 经过判断，确定用户的业务在 2G 网络中被降质后，按照 3GPP 技术规范中规定的重定位请求的格式，在重定位请求的 RAB 参数中携带双配置，即将所述 RAB 参数的首选业务配置为多媒体业务，并在所述 RAB 参数的可选 RAB 配置信元值中配置语音业务。

步骤 205：RNC_B 接收该重定位请求，并根据其自身是否支持所述业务修改，作出相应的响应。

由于，只有支持 3GPP TS R6 以后的版本的 RNC 设备，才能支持用户能力双配置，因此，根据 RNC_B 支持的协议版本不同，本步骤中分以下两种情况进行说明：

第一种情况：若 RNC 设备支持 3GPP R6 以后的版本，即 RNC_B 支持用户能力双配置，则执行步骤 205.1a。

步骤 205.1a：RNC_B 根据该重定位请求中的 RAB 参数对 RAB 进行修改，将用户的业务修改为多媒体业务，且语音业务为用户的可选业务。

本步骤中，RAB 修改过程为现有技术，因此，对于修改 RAB 的具体实施

IPR2025-01571
Apple EX1002 Page 677

方法，在此不再赘述。

步骤 205.1b：RNC_B 分配切换用业务资源，并向 MSC_B 发送重定位准备完成的应答消息(Iu_Relocation_Request_ACK)，继续执行步骤 206。

本步骤中，通过在重定位请求的 RAB 参数中携带双配置，直接在 3G 网络下建立了支持双 BCIE 的 SCUDIF 通话，实现了将用户的业务修改为 SCUDIF 呼叫业务的目的。

第二种情况：若 RNC 设备仅支持 3GPP R6 以前的版本，即 RNC_B 仅支持用户能力单配置方案，则执行步骤 205.2。

步骤 205.2: RNC_B 接收该重定位请求，由于 RNC_B 不支持双配置，RNC_B 向 MSC_B 返回切换失败应答(Iu_Relocation_Request_ACK)，系统间切换失败，且业务更改失败，结束本流程业务更改。

步骤 206：本实施例的步骤 206 至步骤 214，与实施例一的步骤 106 至步骤 114 的操作完全相同，请参照实施例一中的相应部分，在此不再赘述。

步骤 215：MSC_B 通知网络及被叫端用户进行业务修改。

本步骤中，MSC_B 可以在系统间切换完成后的任何时刻，向网络及被叫端用户发起修改业务的通知。被叫端业务修改过程为现有技术，因此，对于被叫端业务修改的具体实施方法，在此不再赘述。

至此，完成本实施例的系统间切换，且用户的业务被更改为多媒体首选、语音可选的 SCUDIF 呼叫业务。

由上述技术方案可见，本实施例中，在系统间切换的重定位过程中，3G 网络的 MSC 根据呼叫建立阶段记录的用户业务能力值，与所述切换回的业务进行比较，判断用户的业务在 2G 网络中是否被降质;

在该用户的业务能力值与所述切换回的业务不相同时，确定用户的业务被降质，MSC 利用了重定位请求消息中的 RAB 参数携带多媒体为首选业务、语音为可选业务的双配置，通知 RNC 将业务修改为 SCUDIF 呼叫业务;

当 RNC 设备支持 3GPP TS R6 以后的协议版本时，能够直接在 3G 网络下建立支持双 BCIE 的 SCUDIF 通话，从而达到了将在 2G 网络中被降质的 SCUDIF

IPR2025-01571
Apple EX1002 Page 678

呼叫恢复为 SCUDIF 呼叫的目的。

上述两个实施例中，预先在 MSC 中设置的策略所指定的双配置为：多媒体为首选业务、语音为可选业务的双配置。预先在 MSC 设置的策略所指定的双配置也可以为：语音为首选业务、多媒体为可选业务的双配置。在 RAB 指配消息、或者重定位请求消息中携带语音为首选业务、多媒体为可选业务双配置的方法为：将所述 RAB 指配消息、或者重定位消息中的 RAB 参数的首选业务配置为语音业务，并在可选 RAB 配置信元值中配置多媒体业务。

对于在 RAB 指配消息、或者重定位消息中携带表示：语音为首选业务、多媒体为可选业务的双配置的情况，当切换后的 RNC 支持用户能力双配置，且无线资源满足时，RNC 将请求 MSC 将语音业务修改为多媒体业务。

此外，在 MSC 通知 RNC 进行业务修改时，也可以使用携带多媒体单配置的 RAB 指配消息、或者重定位请求消息，这样能够保证在 RNC 不支持用户能力双配置时将业务提升为多媒体业务，但是，由于用户没有可选的业务，当无线资源不满足时，用户不能将多媒体业务降质为语音业务，这将增加掉话的几率。因此，在实施本发明时，推荐采用在 RAB 指配消息、或者重定位消息中携带双配置的方法，将业务恢复为 SCUDIF 呼叫业务。

以上所述仅为本发明的较佳实施例而已，并非用于限定本发明的保护范围。凡在本发明的精神和原则之内所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

IPR2025-01571
Apple EX1002 Page 679

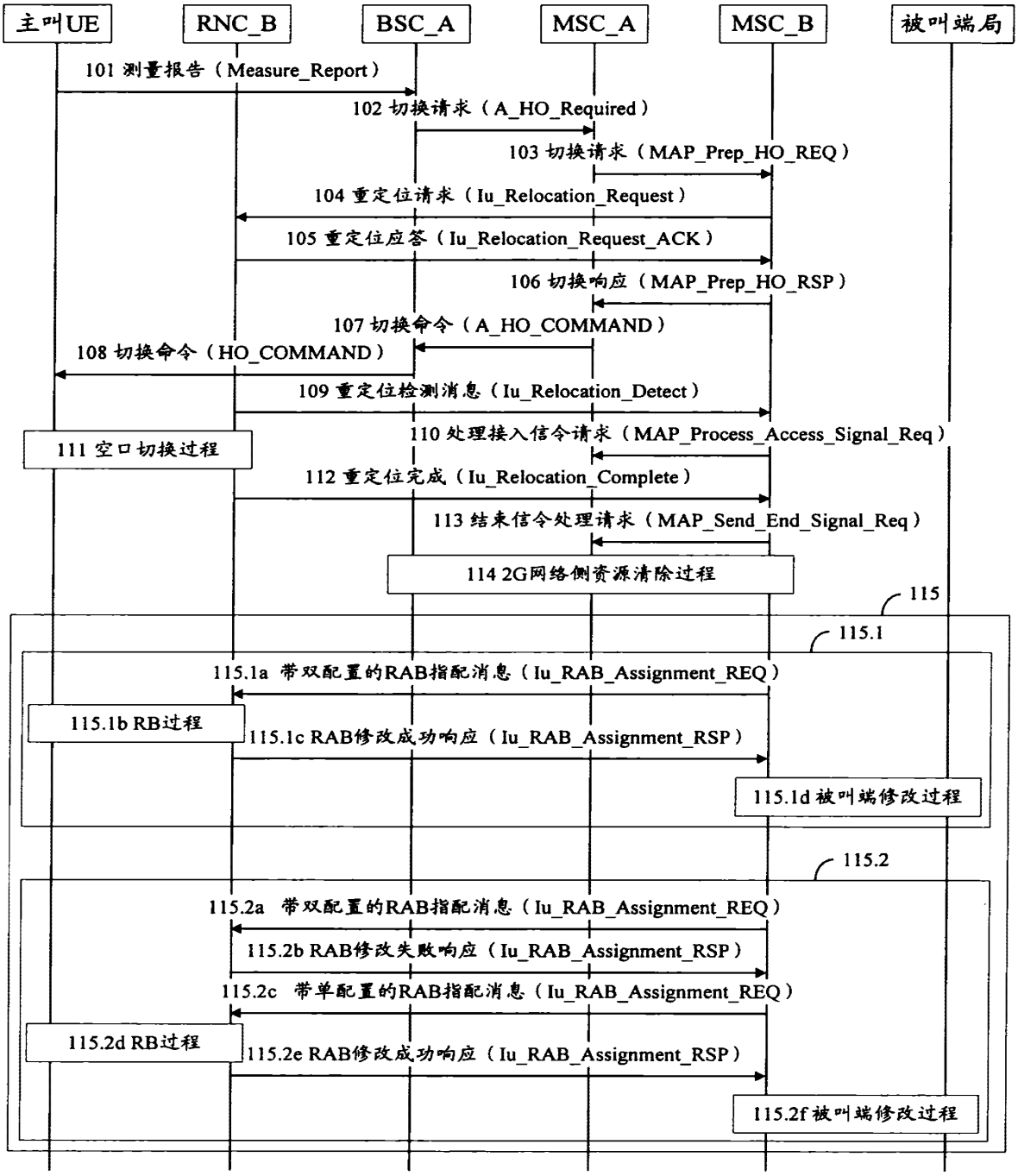


图 1

IPR2025-01571
Apple EX1002 Page 680

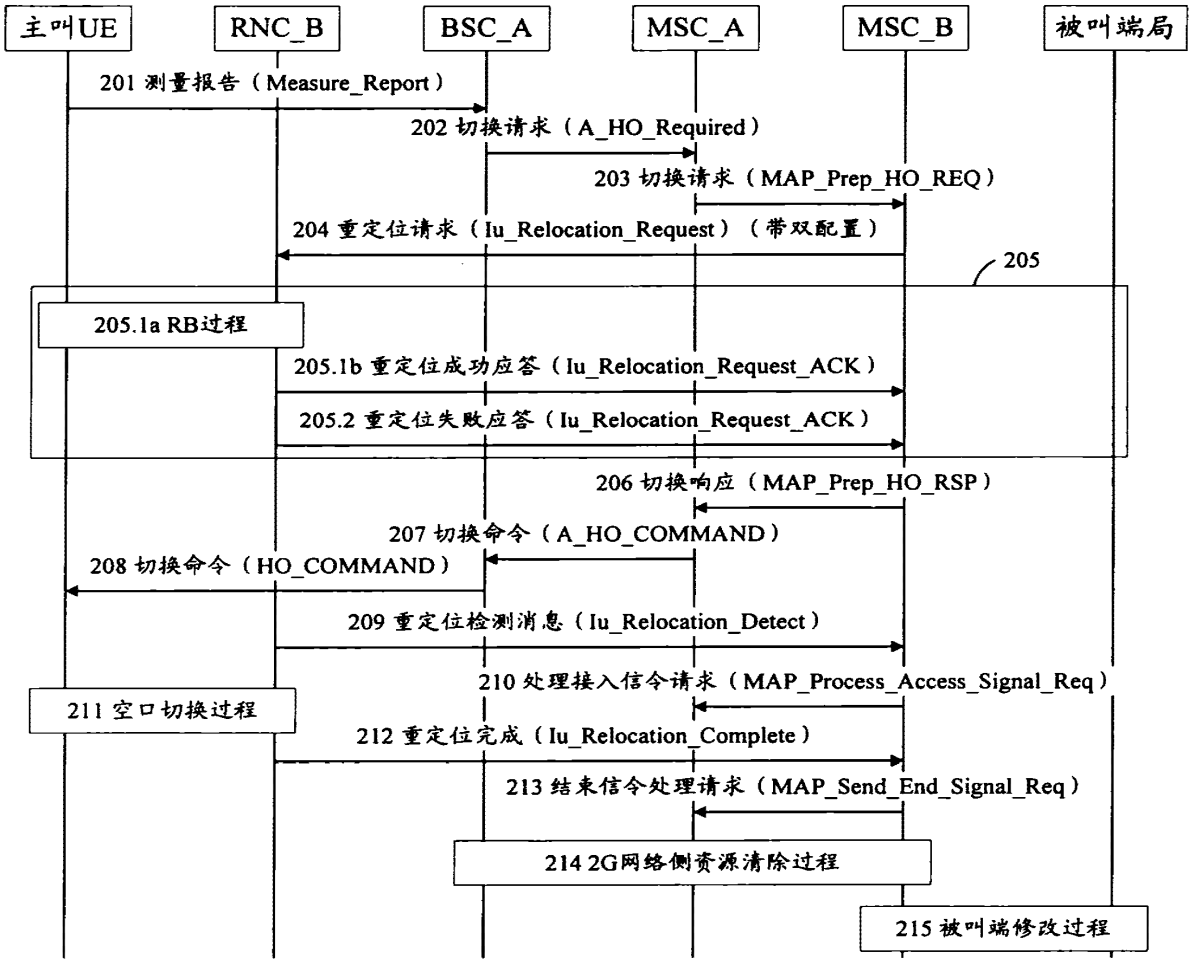


图 2

IPR2025-01571
Apple EX1002 Page 681

Electronic Patent Application Fee Transmittal	
Application Number:	13705055
Filing Date:	04-Dec-2012
Title of Invention:	AUTOMATED DEVICE PROVISIONING AND ACTIVATION
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Filer:	Krista Susan Jacobsen/Ann Taylor
Attorney Docket Number:	RALEP007C03
Filed as Large Entity	

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
		Total in USD ($)		**180**

Electronic Acknowledgement Receipt	
EFS ID:	16323418
Application Number:	13705055
International Application Number:	
Confirmation Number:	3375
Title of Invention:	AUTOMATED DEVICE PROVISIONING AND ACTIVATION
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	Krista Susan Jacobsen/Ann Taylor
Filer Authorized By:	Krista Susan Jacobsen
Attorney Docket Number:	RALEP007C03
Receipt Date:	15-JUL-2013
Filing Date:	04-DEC-2012
Time Stamp:	22:44:42
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$180
RAM confirmation Number	8841
Deposit Account	505876
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees) Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees) Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	P007C03.pdf	1868413 146dc4acf98d838e58d0a4de1fd5dbd951f0c014	no	10
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
2	Foreign Reference	Starhub.pdf	656227 34c62e843998321805c9a9e280b3233bc8a53e75	no	22
Warnings:					
Information:					
3	Foreign Reference	Cisco.pdf	1398028 a85c7e6d6f08a1f6747fb7d21a9fb93427e3c5e3	no	69
Warnings:					
Information:					
4	Foreign Reference	CN101155343B.pdf	2070647 cc7a6c8344a80e179d9f2601a49cb9a37f359e87	no	28
Warnings:					
Information:					
5	Foreign Reference	CN101035308A.pdf	1231903 bb1b6fa1721a042823731a8283b8d37b6b313b35	no	28
Warnings:					
Information:					
6	Foreign Reference	CN1889777A.pdf	928344 9a22716535cc0ec62b3db71f323c7634d266e61a	no	19
Warnings:					
Information:					
7	Non Patent Literature	OAinP007C4.pdf	1066914 9af6ea5041981aad0d884e26f6f2d424c699d4fa	no	30
Warnings:					
Information:					

8	Non Patent Literature	OAinP071.pdf	162196 a155b75e1c7df893b873a0e1822aeb39588eefac	no	5
Warnings:					
Information:					
9	Non Patent Literature	OARinP071.pdf	398122 eac34026d38a68b94a579a21e69bc394ca36840e	no	11
Warnings:					
Information:					
10	Fee Worksheet (SB06)	fee-info.pdf	30272 38d36626f9a03494b9b18dff47fbe326996c0447	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	9811066	

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.

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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C03

U.S.PATENTS

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.

U.S.PATENT APPLICATION PUBLICATIONS

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	20100241544		2010-09-23	Benson, Dan et al.	
	2	20090157792		2009-06-18	Fiatal, Trevor	

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

FOREIGN PATENT DOCUMENTS

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

NON-PATENT LITERATURE DOCUMENTS

IPR2025-01571
Apple EX1002 Page 687

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C03

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

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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C03

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).

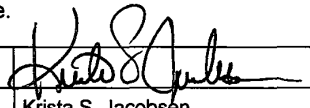
☐ See attached certification statement.

☐ 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		Date (YYYY-MM-DD)	2013-07-17
Name/Print	Krista S. Jacobsen	Registration Number	59374

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.**

Electronic Acknowledgement Receipt	
EFS ID:	16347627
Application Number:	13705055
International Application Number:	
Confirmation Number:	3375
Title of Invention:	AUTOMATED DEVICE PROVISIONING AND ACTIVATION
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	Krista Susan Jacobsen/Ann Taylor
Filer Authorized By:	Krista Susan Jacobsen
Attorney Docket Number:	RALEP007C03
Receipt Date:	17-JUL-2013
Filing Date:	04-DEC-2012
Time Stamp:	22:33:00
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	P007C03.pdf	699322 598dee10e9646df5e0a320246b718c47d85076c3	no	3

Warnings:
Information:

This is not an USPTO supplied IDS fillable form	
Total Files Size (in bytes):	699322

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:	RUDY, Andrew J.
Serial No.:	13/705,055	Art Unit:	3687
Filed:	December 4, 2012	Conf. No.:	3375
Title:	Automated Device Provisioning and Activation		

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

AMENDMENT AND RESPONSE

Madam:

In response to the Restriction Requirement dated July 1, 2013, the deadline for response being August 1, 2013, please amend the above-identified application as follows:

Amendments to the Claims begin on page 2.

Remarks begin on page 9.

IPR2025-01571
Apple EX1002 Page 692

AMENDMENTS TO THE CLAIMS

Without prejudice and without surrender of any subject matter, please amend the claims as follows:

1. (Currently amended) A method performed by a network system, the method comprising:

providing a **first ~~plurality of~~** service control link**[[s]]** to a **first ~~plurality of~~** end-user device**[[s]]** communicatively coupled to the network system **over a first set of one or more wireless networks**, **the first ~~each~~** service control link secured **at least in part** by **at least a first ~~an~~** encryption protocol, **the first ~~a particular~~** service control link **for ~~of the plurality of service control links~~** supporting control-plane communications between the network system and **the first ~~a particular~~** end-user device**, ~~of the plurality of end-user devices over one or more wireless access networks~~ the first end-user device comprising a first set of two or more device agents, the first set of two or more device agents including a particular device agent**;

providing a second service control link to a second end-user device communicatively coupled to the network system over a second set of one or more wireless access networks, the second set of one or more wireless access networks being the same as or different from the first set of one or more wireless access networks, the second service control link secured at least in part by at least a second encryption protocol, the second encryption protocol being the same as or different from the first encryption protocol, the second service control link for supporting control-plane communications between the network system and the second end-user device, the second end-user device comprising a second set of two or more device agents;

receiving a server message from a particular server of a plurality of servers communicatively coupled to the network system, the server message comprising message payload**, at least a portion of the message payload** for delivery to the **first ~~particular~~** end-user device;

generating an encrypted message comprising **the at least a portion of** the message payload and an identifier identifying **the[[a]]** particular device agent **~~of a plurality of device agents on the particular end-user device~~**, the identifier configured to assist in delivering **the** at

IPR2025-01571
Apple EX1002 Page 693

least a portion of the message payload to the particular device agent ~~on the particular end-user device~~; and

sending the encrypted message to the **first** ~~particular~~ end-user device over the **first** ~~particular~~ service control link.

2. (Currently amended) The method of claim 1, wherein the particular server comprises a service usage ~~history~~ server, a policy management server, an access control integrity server, a network traffic analysis server, a beta test server, a service download control server, a billing event server, an activation server, a transaction server, an authentication server, or a content management server.

3. (Currently amended) The method of claim 1, wherein the **at least a portion of the** message payload comprises information associated with a service usage or cost.

4. (Previously presented) The method of claim 3, wherein the information associated with a service usage or cost comprises a service usage value, a projected service usage value, a service usage plan limit, a projected service usage overage warning, a projected service cost overage warning, a service plan period time duration, a service plan time remaining before end of period, or information about a service overage.

5. (Currently amended) The method of claim 1, wherein the **at least a portion of the** message payload is based, at least in part, on a user preference.

6. (Currently amended) The method of claim 1, wherein the **at least a portion of the** message payload comprises **at least an aspect of:** a service offer, an advertisement, or a transaction offer.

7. (Currently amended) The method of claim 1, wherein the **at least a portion of the** message payload comprises a device agent instruction, a setting, an agent configuration, or a software update for the particular device agent.

IPR2025-01571
Apple EX1002 Page 694

8. (Currently amended) The method of claim 1, wherein the **at least a portion of the** message payload comprises information associated with software or a media file.

9. (Currently amended) The method of claim 1, wherein the **at least a portion of the** message payload comprises information associated with a service policy.

10. (Currently amended) The method of claim 1, wherein the **at least a portion of the** message payload comprises an indication of additional data or information available to the particular device agent.

11. (Currently amended) The method of claim 1, wherein the **at least a portion of the** message payload is configured to assist in causing the **first** ~~**particular**~~ end-user device to present, through a user interface, information associated with the **at least a portion of the** message payload.

12. (Currently amended) The method of claim 1, wherein the server message is a first server message, and wherein the message payload is a first message payload, and wherein the identifier identifying the particular device agent ~~**of the plurality of device agents on the particular end-user device**~~ is a first identifier, and further comprising receiving a second server message from the particular server or from another server of the plurality of servers communicatively coupled to the network system, the second server message comprising second message payload, and wherein the encrypted message further comprises **at least a portion of** the second message payload and a second identifier configured to assist in delivering **the** at least a portion of the second message payload to a second device agent **of the first set of two or more device agents**~~**on the particular end-user device**~~, the second device agent being the particular device agent or another device agent of the **first set of two or more device agents**~~**plurality of device agents on the particular end-user device**~~.

13. (Currently amended) The method of claim 1, wherein the server message is a first server message, and wherein the particular server is a first server, and wherein the message payload is first message payload, and wherein the particular device agent is a first device agent, and

IPR2025-01571
Apple EX1002 Page 695

wherein the encrypted message is a first encrypted message, and wherein the identifier is a first identifier, and further comprising:

receiving a second server message from a second server of the plurality of servers **communicatively coupled to the network system**, the second server message comprising second message payload**, at least a portion of the second message payload for delivery to the first end-user device**;

generating a second encrypted message comprising **the at least a portion of** the second message payload and a second identifier configured to assist the **first ~~particular~~** end-user device in delivering **the at least a portion of** the second message payload to a second device agent of the **first set ~~plurality~~** of **two or more** device agents **~~on the particular end-user device~~**; and

sending the second encrypted message to the **first ~~particular~~** end-user device over the **first ~~particular~~** service control link.

14. (Currently amended) The method of claim 1, wherein the **first ~~particular~~** service control link supports asynchronous transmissions by the network system.

15. (Currently amended) The method of claim 1, further comprising sending a credential, a certificate, or a token to the **first ~~particular~~** end-user device or obtaining the credential, the certificate, or the token from the **first ~~particular~~** end-user device during a service authorization sequence.

16. (Previously presented) The method of claim 15, wherein the credential comprises a phone number, an identification number, a security signature, a security credential, a subscriber identity module (SIM) identifier, a mobile equipment identifier (MEID), or a device identifier.

17. (Previously presented) The method of claim 1, wherein the particular device agent comprises software.

18. (Currently amended) The method of claim 1, further comprising:

IPR2025-01571
Apple EX1002 Page 696

triggering a transmission to maintain the **first ~~particular~~** service control link when a time since sending the encrypted message to the **first ~~particular~~** end-user device would otherwise cause the **first ~~particular~~** service control link to terminate**~~, and~~**

~~determining when to send the encrypted message to the particular end-user device~~.

19. (Currently amended) The method of claim 1, wherein the sending the encrypted message to the **first ~~particular~~** end-user device over the **first ~~particular~~** service control link is not based on whether the particular device agent is running on the **first ~~particular~~** end-user device.

20. (Currently amended) The method of claim 1, wherein **the particular ~~at least one of the plurality of~~** server**[[s]]** comprises a content transaction server configured to provide an electronic commerce offering and transaction platform to the **first ~~particular~~** end-user device.

21. (Canceled)

22. (Currently amended) The method of claim 1, wherein a transmission over the **first ~~particular~~** service control link is within an ambient service, the ambient service **being** provided at no cost to a user or a subscriber associated with the **first ~~particular~~** end-user device.

23. (Currently amended) The method of claim 1, wherein the **first ~~plurality of~~** service control link**[[s]]** enables **the[[a]]** particular server **~~of the plurality of servers~~** to push the **at least a portion of the** message payload to **~~a selected one of~~** the **particular ~~plurality of~~** device agent**~~s on any one of the plurality of end-user devices~~**.

24. (Canceled)

25. (Currently amended) The method of claim 1, wherein providing the **first ~~plurality of~~** service control link**[[s]]** to the **first ~~plurality of~~** end-user device**[[s]]** comprises providing the **first ~~plurality of~~** service control link**[[s]]** to a **~~plurality of~~** service control device link agent**[[s]]** **on the first end-user device**, **the ~~each service control device link agent on one of the plurality of end-user devices, a particular~~** service control device link agent **~~on the particular~~**

IPR2025-01571
Apple EX1002 Page 697

~~end-user device~~ for delivering agent messages over an agent communication bus to at least **the particular** ~~one of the plurality of~~ device agent~~s on the particular end-user device~~.

26. (Currently amended) The method of claim 25, wherein the encrypted message is a first encrypted message, and wherein the identifier is configured to assist the ~~particular~~ service control device link agent in generating a second encrypted message for delivery to the particular device agent, the second encrypted message comprising the at least a portion of the message payload.

27. (Currently amended) A network system**,** comprising:

means for providing a **first** ~~plurality of~~ service control link**[[s]]** to a **first** ~~plurality of~~ end-user device**[[s]]** communicatively coupled to the network system **over a first set of one or more wireless networks**, **the first** ~~each~~ service control link secured **at least in part** by **at least a first** ~~an~~ encryption protocol, **the first** ~~a particular~~ service control link **for** ~~of the plurality of service control links~~ supporting control-plane communications between the network system and **the first** ~~a particular~~ end-user device**,** ~~of the plurality of end-user devices over one or more wireless access networks~~ **the first end-user device comprising a first set of two or more device agents, the first set of two or more device agents including a particular device agent**;

means for providing a second service control link to a second end-user device communicatively coupled to the network system over a second set of one or more wireless access networks, the second set of one or more wireless access networks being the same as or different from the first set of one or more wireless access networks, the second service control link secured at least in part by at least a second encryption protocol, the second encryption protocol being the same as or different from the first encryption protocol, the second service control link for supporting control-plane communications between the network system and the second end-user device, the second end-user device comprising a second set of two or more device agents;

means for receiving a server message from a particular server of a plurality of servers communicatively coupled to the network system, the server message comprising message payload**, at least a portion of the message payload for delivery to the first end-user device**;

IPR2025-01571
Apple EX1002 Page 698

means for generating an encrypted message comprising **the at least a portion of** the message payload and an identifier identifying **the[[a]]** particular device agent ~~**of a plurality of device agents on the particular end-user device**~~, the identifier configured to assist in delivering **the** at least a portion of the message payload to the particular device agent ~~**on the particular end-user device**~~; and

means for sending the encrypted message to the **first** ~~**particular**~~ end-user device over the **first** ~~**particular**~~ service control link.

28-30. (Canceled)

31. (New) The method of claim 1, further comprising sending a credential, a certificate, or a token to the particular device agent or obtaining the credential, the certificate, or the token from the particular device agent during a service authorization sequence.

32. (New) The network system recited in claim 27, wherein the message payload comprises an indication of additional data or information available to the particular device agent.

33. (New) The network system recited in claim 27, wherein the message payload is configured to assist in causing the first end-user device to present, through a user interface, information associated with the at least a portion of the message payload.

34. (New) The network system recited in claim 27, further comprising means for sending a credential, a certificate, or a token to the particular end-user device or obtaining the credential, the certificate, or the token from the particular end-user device during a service authorization sequence.

35. (New) The network system recited in claim 27, wherein providing the first service control link to the first end-user device comprises providing the first service control link to a service control device link agent on the first end-user device, the service control device link agent for delivering agent messages over an agent communication bus to at least the particular device agent.

IPR2025-01571
Apple EX1002 Page 699

REMARKS

The Office Action dated July 1, 2013, imposed a restriction requirement on claims 1-30, asserting that claims 1-27 (Group I) are directed to a first invention, and claims 28-30 (Group II) are directed to a second invention.

Applicant elects the claims of Group I, namely, claims 1-27, without traverse, for further prosecution. Claims 28-30 are being canceled.

Claims 1-3, 5-15, 18-20, 22, 23, and 25-27 are being amended herein. Claims 21 and 24 are being canceled. Claims 31-35 are being added. No new matter is being added by these amendments.

Claim 31 is supported at least by paragraphs [00374], [00375], and [00465]. Claim 32 is supported at least by paragraph [00327]. Claim 33 is supported at least by paragraphs [0031] and [00440]. Claim 34 is supported at least by paragraphs [00374], [00375], and [00465]. Claim 35 is supported at least by paragraphs [00168], [00169], [00184], and [00327].

After entry of the amendments herein, claims 1-20, 22, 23, 25-27, and 31-35 are pending.

IPR2025-01571
Apple EX1002 Page 700

CONCLUSION

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 31, 2013 By: _____

Krista S. Jacobsen
Reg. No. 59,374
Head Counsel
Headwater Partners I LLC
350 Marine Parkway, Suite 300
Redwood Shores, CA 94065
(650) 517-2798

CERTIFICATE OF ELECTRONIC TRANSMISSION

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being filed electronically via EFS-Web addressed to the Commissioner for Patents on:

Date: July 31, 2013 By: _____
Ann Taylor

IPR2025-01571
Apple EX1002 Page 701

Electronic Acknowledgement Receipt	
EFS ID:	16467842
Application Number:	13705055
International Application Number:	
Confirmation Number:	3375
Title of Invention:	AUTOMATED DEVICE PROVISIONING AND ACTIVATION
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	Krista Susan Jacobsen/Ann Taylor
Filer Authorized By:	Krista Susan Jacobsen
Attorney Docket Number:	RALEP007C03
Receipt Date:	31-JUL-2013
Filing Date:	04-DEC-2012
Time Stamp:	16:06:40
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		P007C03RRR.pdf	239842 378418b1a5a20478f58fd1f90d6aa2cfb3e587ef	yes	10

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Response to Election / Restriction Filed	1	1
	Claims	2	8
	Applicant Arguments/Remarks Made in an Amendment	9	10
Warnings:			
Information:			
	Total Files Size (in bytes):	239842	

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 13/705,055	Filing Date 12/04/2012	☐ 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 **07/31/2013**

	(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))	* 30	Minus	** 30	= 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
/KIMBERLY PANNELL/

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.

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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Andrew J RUDY
	Attorney Docket Number	RALEP007C03

U.S.PATENTS						
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	5630159	A	1997-05-13	Zancho, William F.	
	2	5633484	A	1997-05-27	Zancho, William F. et al.	
	3	5814798	A	1998-09-29	Zancho, William F.	
	4	5915008	A	1999-06-22	Dulman, Scott	
	5	6654814		2003-11-25	Britton, Kathryn H. et al.	
	6	6934249	B1	2005-08-23	Bertin, Olivier et al.	
	7	6957067		2005-10-18	Iyer, Pradeep J. et al.	
	8	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Andrew J RUDY
	Attorney Docket Number	RALEP007C03

	9	7039713	B1	2006-05-02	Van Gunter, David et al.	
	10	7286848	B2	2007-10-23	Vireday, Richard P. et al.	
	11	7313237	B2	2007-12-25	Bahl, Paramvir et al.	
	12	7444669	B1	2008-10-28	Bahl, Paramvir et al.	
	13	7493659	B1	2009-02-17	Wu, Handong et al.	
	14	7496652		2009-02-24	Pezzutti, David	
	15	7499438		2009-03-03	Hinman, Brian L. et al.	
	16	7535880		2009-05-19	Hinman, Brian L. et al.	
	17	7548976	B2	2009-06-16	Bahl, Paramvir et al.	
	18	7478420		2009-01-13	Wright, Michael et al.	
	19	7593730	B2	2009-09-22	Khandelwal, Deepak et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Andrew J RUDY
	Attorney Docket Number	RALEP007C03

	20	7502672		2009-03-10	Kolls, H. Brock	
	21	7720960	B2	2010-05-18	Pruss, Richard Manfred et al.	
	22	7774456	B1	2010-08-10	Lownsbrough, Derek Leigh et al.	
	23	7801985	B1	2010-09-21	Pitkow, Jim et al.	
	24	7881697	B2	2011-02-01	Baker, Matthew Donald et al.	
	25	7899438	B2	2011-03-01	Baker, Matthew Donald et al.	
	26	7929959	B2	2011-04-19	DeAtley, Dallas et al.	
	27	7945238	B2	2011-05-17	Baker, Matthew Donald et al.	
	28	7948953	B2	2011-05-24	Melkote, Keerti G. et al.	
	29	7969950	B2	2011-06-28	Iyer, Pradeep J. et al.	
	30	8000276	B2	2011-08-16	Scherzer, Shimon et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Andrew J RUDY
	Attorney Docket Number	RALEP007C03

	31	8027339	B2	2011-09-27	Short, Joel E. et al.	
	32	8032409	B1	2011-10-04	Mikurak, Michael G.	
	33	7529204		2009-05-05	Bourlas, Yair et al.	
	34	8078140	B2	2011-12-13	Baker, Matthew Donald et al.	
	35	8090359		2012-01-03	Proctor Jr., James Arthur et al.	
	36	8090616		2012-01-03	Proctor Jr., James Arthur et al.	
	37	8095112	B2	2012-01-10	Chow, Richard et al.	
	38	8116749		2012-02-14	Proctor Jr., James Arthur et al.	
	39	8126476	B2	2012-02-28	Vardi, Yosef et al.	
	40	8134954		2013-03-13	Godfrey, James A. et al.	
	41	8150431		2012-04-03	Wolovitz, Lionel et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Andrew J RUDY
	Attorney Docket Number	RALEP007C03

	42	7756757		2010-07-13	Oakes III, Charles Lee	
	43	8200509	B2	2012-06-12	Kenedy, Andrew Alexander et al.	
	44	8242959	B2	2012-08-14	Mia, Rashidus S. et al.	
	45	8270972	B2	2012-09-18	Otting, Marcia J. et al.	
	46	8285249	B2	2012-10-09	Baker, Matthew Donald et al.	
	47	8307067	B2	2012-11-06	Ryan, Nicholas M.	
	48	8325638		2012-12-04	Jin, Haipeng et al.	
	49	8326319	B2	2012-12-04	Davis, Richard W.	
	50	8356336	B2	2013-01-15	Johnston, Keith et al.	
	51	8358638	B2	2013-01-22	Scherzer, Tamir et al.	
	52	8374592		2013-02-12	Proctor, Jr. James A. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Andrew J RUDY
	Attorney Docket Number	RALEP007C03

	53	8447607	B2	2013-05-21	Weider, Chris et al.	
	54	8472371		2013-06-25	Bari, Farooq et al.	
	55	8483135		2013-07-09	Cai, Yigang et al.	
	56	8495227		2013-07-23	Kaminsky, David L. et al.	
	57	8504729		2013-08-06	Pezzutti, David A.	
	58	7139569		2006-11-21	Kato, Akira	
	59	7930446		2011-04-19	Kesselman, Alex et al.	
	60	8045973		2011-10-25	Chambers, Michael D.	
	61	8068829		2011-11-29	Lemond, Eric et al.	
	62	8078163		2011-12-13	Lemond, Eric et al.	
	63	8086497		2011-12-27	Oakes III, Charles Lee	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Andrew J RUDY
	Attorney Docket Number	RALEP007C03

	64	8116781		2012-02-14	Chen, Xixian et al.	
	65	8126396		2012-02-28	Bennett, James D.	
	66	8166040		2012-04-24	Brindisi, Richard G. et al.	
	67	8351898		2013-01-08	Raleigh, Gregory G.	

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

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20010048738	A	2001-12-06	Baniak, Paul G. et al.	
	2	20020049074	A	2002-04-25	Eisinger, Bernd et al.	
	3	20020161601	A	2002-10-31	Nauer, Bernhard et al.	
	4	20030233332	A	2003-12-18	Keeler, James D. et al.	
	5	20040102182	A	2004-05-27	Reith, Lothar et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Andrew J RUDY
	Attorney Docket Number	RALEP007C03

	6	20060068796	A	2006-03-30	Millen, Stephanie L. et al.	
	7	20060135144	A	2006-06-22	Jothipragasam, Premkumar	
	8	20070033197	A	2007-02-08	Scherzer, Shimon et al.	
	9	20070109983	A	2007-05-17	Shankar, Rohit et al.	
	10	20080022354	A	2008-01-24	Grewal, Karanvir et al.	
	11	20080089295	A	2008-04-17	Keeler, James D. et al.	
	12	20080250053	A	2008-10-09	Aaltonen, Janne et al.	
	13	20090005000	A	2009-01-01	Baker, Matthew et al.	
	14	20090006116	A	2009-01-01	Baker, Matthew et al.	
	15	20090006200	A	2009-01-01	Baker, Matthew et al.	
	16	20110013569	A	2011-01-20	Scherzer, Shimon et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Andrew J RUDY
	Attorney Docket Number	RALEP007C03

	17	20110081881	A	2011-04-07	Baker, Matthew Donald et al.	
	18	20110082790	A	2011-04-07	Baker, Matthew Donald et al.	
	19	20110159818	A	2011-06-30	Scherzer, Shimon et al.	
	20	20120020296	A	2012-01-26	Scherzer, Shimon et al.	
	21	20120196644	A	2012-08-02	Scherzer, Shimon et al.	
	22	20120238287	A	2012-09-20	Scherzer, Shimon	
	23	20130029653	A	2013-01-31	Baker, Matthew Donald et al.	
	24	20130058274	A	2013-03-07	Scherzer, Shimon et al.	
	25	20130065555	A	2013-03-14	Baker, Matthew Donald et al.	
	26	20130084835	A	2013-04-04	Scherzer, Shimon et al.	

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

FOREIGN PATENT DOCUMENTS

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Andrew J RUDY
	Attorney Docket Number	RALEP007C03

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	1998058505	WO		1998-12-23	Sonera Oy		☐
	2	2007097786	WO	A	2007-08-30	Sony Ericsson Mobile Communications AB		☐

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

NON-PATENT LITERATURE DOCUMENTS

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	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)	☐
	2	Office Action Response in U.S. Application No. 13/712,184, August 8, 2013	☐

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

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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Andrew J RUDY
	Attorney Docket Number	RALEP007C03

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		Date (YYYY-MM-DD)	2013-09-06
Name/Print	Krista S. Jacobsen	Registration Number	59374

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.**

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04Q 7/22, H04M 15/00 — A1

(11) International Publication Number: **WO 98/58505**

(43) International Publication Date: 23 December 1998 (23.12.98)

(21) International Application Number: PCT/FI98/00515

(22) International Filing Date: 15 June 1998 (15.06.98)

(30) Priority Data:
972591 17 June 1997 (17.06.97) FI

(71) Applicant *(for all designated States except US)*: SONERA OY [FI/FI]; Sturenkatu 16, FIN–00510 Helsinki (FI).

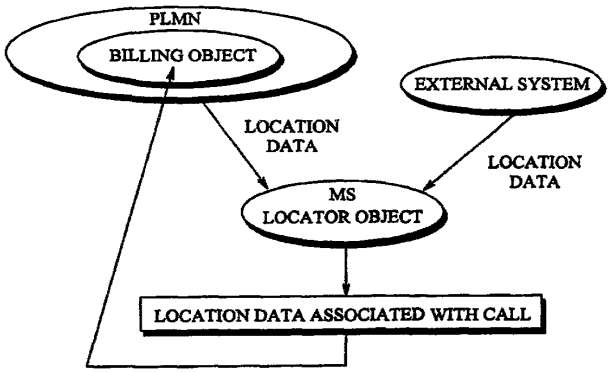
(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: LINKOLA, Janne [FI/FI]; Oikokatu 9 A 3, FIN–00170 Helsinki (FI).

(74) Agent: PAPULA REIN LAHTELA OY; Fredrikinkatu 61 A, P.O. Box 981, FIN–00101 Helsinki (FI).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.
In English translation (filed in Finnish).

(54) Title: CHARGING METHOD IN A MOBILE TELECOMMUNICATION SYSTEM



(57) Abstract

The charging principles regarding mobile calls can be improved by providing the mobile station with a locator object, which at certain intervals determines the cell in which the mobile station is currently located. Stored in the mobile station is also a list of areas permitting application of a special rate. The locator object monitors calls made from the mobile station. When it detects that a call is being started, it checks whether the mobile station was in a special rate area at the time when its location was determined last. If this is the case, then the object will inform the network that the call is entitled to a special rate. As the last location function was executed just before the call setup was started, a special rate call is possible even if the mobile station has moved some distance into the area of a cell applying a normal rate. Placed in a billing centre is a billing object, to which the locator object sends data indicating whether the call was started from a cell or area where a special rate is applicable, as well as data identifying the call. The second object receives the billing records generated by the mobile switching centre, which also contain call identifying data, and compares the call–specific data in them with the data sent by the first object. In this way, the second object can find from the billing records the calls that are entitled to a special rate, regardless of whether the mobile station has moved during call setup from the original cell into a cell where another rate, e.g. a higher rate is applicable.

IPR2025-01571
Apple EX1002 Page 716

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

CHARGING METHOD IN A MOBILE TELECOMMUNICATION SYSTEM

SCOPE OF THE INVENTION

The present invention relates to the formation of the principles of calculation of call price in a cellular mobile communication system.

TECHNOLOGICAL BACKGROUND

In a wired network, the charge for a call depends on whether the call is a local call, a trunk call or an international call, in other words, a geographically defined call, or whether it is a call to a service number. Thus, when dialling the number of a called subscriber, the calling subscriber already knows the principles on which the price of the call will be calculated.

The principles used in a wired network for calculating the call price cannot be directly applied in mobile telephone networks. This is because the mobile subscriber is not tied to a given locality while the called subscriber may be a locality-dependent wired network subscriber or a mobile subscriber in the same mobile communication network or a subscriber in another operator's mobile communication network. Within the mobile communication network, no distinction is made between local calls and long-distance calls regarding pricing; moreover, in distinction from the wired network, even the called subscriber is liable to pay a portion of the price of a received call in certain cases.

In mobile communication networks, a difficulty in locality-dependent determination of price is that the exact locality of neither the calling nor the called subscriber is known. To give an understanding of the principles of calculation of call price, the

IPR2025-01571
Apple EX1002 Page 718

call setup process in a mobile communication network will now be described in general outline, referring to Fig. 1.

When a calling subscriber in cell a1 in location area 1 under mobile switching centre MSC1 makes a call to a subscriber in location area 2 under another mobile switching centre MSC2, he/she will dial the MSISDN number (Mobile Subscriber International ISDN number) of the called subscriber on his/her mobile station MS-A, which sends it in a message to the base transceiver station 1, step 1. Upon receiving the message, MSC1 checks whether the request can be accepted. As a part of this check, the subscriber data of the calling subscriber are retrieved from the visitor location register VLR1 associated with MSC1, where they have been stored in conjunction with the location updating procedure. If the request is accepted, the mobile switching centre MSC1 will send to the home location register HLR an enquiry containing the called subscriber's MSISDN number, step 2. Based on this number, the HLR retrieves the data for the called subscriber, which indicate that the called subscriber has roamed to visitor location register VLR2. Next, the HLR sends the IMSI (International Mobile Subscriber Identity) data to visitor location register VLR2, asking the latter to give the roaming number, step 3, whereupon VLR2 sends the roaming number MSRN to the home location register HLR, step 4, from where it is sent further to MSC1, step 5.

After this, the call can be routed from mobile switching centre MSC1 to mobile switching centre MSC2 on the basis of the MSRN number (Mobile Subscriber Roaming Number) received from VLR2, step 6. Upon receiving the start message, the mobile switching centre MSC2 of the called subscriber retrieves the subscriber data for the called subscriber from the associated VLR2. From the subscriber data, MSC2 learns

IPR2025-01571
Apple EX1002 Page 719

the location area LAI 2 of the called subscriber, so MSC2 is able to send a paging message via the appropriate base station controller 2 (step 7) to the cells b1, b2, b3 in the location area in question. After the called subscriber's mobile station MS-B has responded to the paging, the call is finally set up to the called subscriber. From what was said above, it is obvious that it is only after the called subscriber's mobile station has responded to the paging message that the relevant mobile switching centre MSC2 is informed of the called subscriber's location at the cell level.

The mobile switching centre may also be linked to a service switching point SSP of an intelligent network IN to allow connections from the mobile communication network to the intelligent network. Via an intelligent network, a wide variety of services can be offered to the subscribers of the mobile communication network, including services like follow-me-diversion of calls, call rerouting distribution, premium rate calls, etc.

In a state-of-the-art mobile communication network, the main rule regarding call charging is that the calling subscriber is charged for the connection between him/her and the home network of the called subscriber while the called subscriber is charged for the connection between his/her current locality and his/her home network.

To increase flexibility regarding the billing principles, a known method is to set a special billing parameter that allows calls made from the subscriber number associated with the parameter to be billed at a rate lower than normal at times when the load on the mobile communication network is low and, correspondingly, at a higher rate when the load on the mobile communication network is high. This parameter creates a time-dependent call charging principle, but in other

respects the pricing of calls follows the above-mentioned principles. Another known practice is to charge a lower price for calls between a mobile station and a specified wired network telephone than for normal calls. This can be implemented by assigning for all subscribers to the service a common service number, e.g. 020100, as the called subscriber number, which directs the call to an intelligent network. In the intelligent network, a service program searches a database to find the called subscriber number associated with the calling subscriber number, and the call is routed to this number.

A comparison of the principles of call price calculation used in mobile communication networks with those used in wired networks reveals certain problems. Since all cells are equal with respect to the mobile communication network, it is difficult to offer the various user groups any other principles of call price calculation than e.g. the aforesaid price variation based on the time of the day. At present, there are no special call price calculation principles applicable to calls within the same cell or calls between certain cells. However, it would be attractive for a mobile telephone network operator to be able to provide various services dependent on the locality where the call is started and/or where it is terminated. Such services include e.g. locality-dependent pricing solutions.

Specifications WO-96/20570 and WO/96/20571 present solutions for determining the principles of call price calculation. The price calculation principles can be improved by setting a given cell or a number of cells of a mobile telephone network as a special cell group. During call setup, the mobile switching centre or a service control point SCP in an intelligent network analyses the call to determine whether the cell in whose area the calling subscriber is lo-

cated and/or the cell in whose area the called subscriber is located belong(s) to the group of special cells. When the calling and called subscribers are located in cells belonging to different switching centres, data regarding the cell of the called subscriber is transmitted to the switching centre of the calling subscriber or to an intelligent network before a voice connection is established. Thus, based on whether the subscribers are in a group of special cells or not, it is possible to vary the call charging rates applied.

Specification WO-96/34499 describes a system in which the subscribers are divided into normal subscribers and "fixed" subscribers. A normal subscriber may start a call in any cell, whereas a fixed subscriber has limited access to the network from a subscriber area comprising one or more cells. When a fixed subscriber is at the boundary of his/her area, the call is forcibly directed to the base transceiver station of the subscriber area if possible.

These solutions allow the application of more fine-grained call charging principles than those generally used. A feature common to these solutions is that the right to a differently priced call is determined according to the cell in whose area the subscriber is physically located at the time of the call, i.e. according to the base transceiver station that connects the subscriber to the network. This is because the metering record generated at the start of the call includes, among other data, an identifier of the base transceiver station via which the connection is set up, and the base station identifier again reveals whether the base station belongs to a group of special cells. In other words, the base station identifier functions as a factor that ultimately determines the price of the call.

However, there is a problem associated with these prior-art solutions. In most mobile telephone

systems, it is the network that makes the decision as to which base station is to be used to transmit the subscriber's calls. When the subscriber is in the fringe area of a cell where a lower call charge is applicable, the network may repeatedly command the mobile station to perform a handover between two base stations, which means that the calling end of the connection alternates between the base station of a "cheaper" cell and the base station of an adjacent cell. It the adjacent cell is not one of the cells where a lower call charge is applicable, then the result would be that the call price would vary during the same call as the connection is handed over from one base station to another, the call charge being thus lower at one moment and higher at the next, without the subscriber having any chance to influence the situation in any way.

One solution proposed to cope with this problem is to give the mobile station some of the handover control functions between base stations. In the idle state, the mobile station would remain as long as possible in signalling contact with a cell applying a lower call charge when in the fringe area of the cell, in other words, the mobile station would remain "hanging" in the cell even when a neighbouring cell would provide a better connection quality. During a communication connection, too, the mobile station would continue hanging in the old cell when in the area of another cell, and it would inform the network e.g. in conjunction with a change of base station or the call setup procedure that it gives preference to the old base station providing cheaper service instead of other base stations.

However, this solution has the drawback of increased co-channel interference, which is due to the fact that, when the communication connection is forcibly maintained via the base station of a cheaper cell

although the mobile station is located in the area of an adjacent cell that would provide a better connection, the mobile station has to use a higher transmission power to compensate for the signal attenuation caused by the longer distance. Therefore, the mobile telephone interferes with other mobile stations using the same frequency that are communicating at the reuse distance of this frequency. Another drawback is that changes need to be made in certain network components, such as the base station controller and the telephone itself. Changes must be made at least in the handover criterion and algorithm.

Another solution proposed to deal with the problem is to have information presented on the display of the mobile station in the idle state to indicate the cell in whose area the mobile station is currently located. The idea is to allow the subscriber to move into the area of a cell with a lower call charge at least when the subscriber is at the boundary between cells. A drawback with this solution is that, as the billing record is generated at the beginning of the call when the telephone is already in the active state, the subscriber may move on to the area of a cell with a higher call charge during the call setup procedure although the subscriber has seen from the display before the transmission of the call setup request that the mobile station is still located in the area of a cheap cell.

The object of the present invention is to achieve a system that is free of the drawbacks of prior-art systems and that does not produce co-channel interference. In the system, determination of location of a mobile station should be implemented in a manner that allows a call started from a special cell to continue being charged at the rate applicable in that cell even if the mobile station should move on to a cell with a normal charging rate during call setup. A

further object is to ensure that, even if call setup is started in a cell with a normal charging rate but a moment earlier the mobile station has been in a special cell, the call can still be charged at the rate applicable in the special cell. The length of time of the moment should also be adjustable.

Yet another object is to achieve a system in which the area of a specially priced call is not dependent on the cell coverage area but may consist of any geographic area. The area may even consist of a part of one cell and a part of another cell. Location of the mobile station should therefore be independent of the information transmitted by the base stations.

The objects stated above can be achieved with the attributes defined in the independent claims.

SUMMARY OF THE INVENTION

According to the basic idea of the invention, the mobile station is provided with a first object, a locator object, which determines the location of the mobile station. The location function can be carried out with an accuracy of a cell or a sub-area of a cell, making use of the existing properties of the mobile communication system. By utilising location methods external to the mobile telephone system, completely cell-independent location can be achieved. The location function is executed at certain intervals. The mobile station also contains a stored list of cells and/or areas where a special charging rate is applicable. The locator object monitors the calls originated from the mobile station. When it detects that a call is being started, it checks whether the mobile station was in a cell or area with a special charging rate at the time when the location function was executed last. If this is the case, then the object will inform the network that the call is entitled

to a special rate. The last location function has even been executed before call setup is started, so a call chargeable at a special rate is possible even if the mobile station has moved some distance into the area of a cell applying a normal rate. Channel allocation is done independently of location in accordance with the normal procedures in the system, which means that co-channel interference is avoided.

One of the network elements is provided with a second object, a billing object, to which the first object sends information indicating whether the call has been started from a cell or area where a special rate is applicable. The second object receives the billing records generated by the mobile switching centre and compares the call-specific data in them with the data sent by the first object. In this way, the second object can find those calls in the billing records that are entitled to a special rate, even if the mobile station has moved during the call setup from the original cell or area into a cell where another rate, e.g. a higher rate is applicable.

Cells allowing the application of a special rate can be divided into groups of cells or areas, and each of the groups may have a different rate applicable in that group. Thus, when the final telephone bill is being compiled, the rate applicable in the special rate group can be checked and the call charge can be determined accordingly.

The locator object may send the data regarding a call entitled to a special rate to the network during the call or alternatively it may collect such data for a desired length of time and send the data at once to the billing object. However, the latter method has the drawback that it leads to a more difficult generation of the telephone bill if the data are received after the call records received during the billing period have been subjected to post-processing.

IPR2025-01571
Apple EX1002 Page 726

LIST OF FIGURES

A preferred embodiment of the invention is described by referring to the attached figures, of which

Fig. 1 illustrates call setup in a mobile telephone network,

Fig. 2 illustrates the principle of the invention in a simplified form,

Fig. 3 illustrates the system in a mobile telephone network, and

Fig. 4 presents a flow and signalling diagram consistent with the procedure, applied to a known mobile telephone system.

DETAILED DESCRIPTION OF THE INVENTION

Fig. 2 illustrates the principle of the invention in a simplified form. A mobile telephone system PLMN (Public Land Mobile Network) 22 is provided with a billing object. It is placed in a network element where call data are collected in a centralised manner for billing purposes, so a natural place for it is the billing centre, to which the mobile switching centres send their call data records. Installed in the mobile station, i.e. mobile telephone MS, is a locator object 21, whose function is to establish the location of the mobile station and to send the location data to the billing object 22.

The locator object receives the information required for the determination of location in two ways: either from the mobile telephone network PLMN or from an external system.

The first-mentioned method is based on the fact that the base stations in all known mobile telephone networks transmit information about themselves in a signal that, depending on the system, can be

IPR2025-01571
Apple EX1002 Page 727

called e.g. a beacon signal, a broadcast signal, a pilot signal, or using a corresponding designation. From this signal, the locator object can easily determine its location at least with an accuracy of one cell. In some countries, the regulations by authorities stipulate mobile station location determination with an accuracy beyond the level of the cell coverage area. To meet this requirement, several different methods have been proposed, such as methods based on a timing advance. In these, the network measures timing advance values between several base stations and the mobile station, and since the timing advance between the mobile station and each base station is directly proportional to the distance, three timing advance values will be sufficient to produce coordinates defining the location of the mobile station with a reasonable accuracy. If the PLMN network computes the location data, then these data are transmitted to the locator object.

The second method is based on the principle that the mobile station determines its location in a manner independent of the PLMN network by using some external system. Such a system could be e.g. the previously known GPS (Global Positioning System) satellite location system. In this case, the locator object would contain a GPS receiver.

In both methods, the location data is transmitted during or after the call to the billing object, which uses it as a basis for calculating the charge for the call.

Next, a description will be given of how the invention is applied in the previously known GSM system.

Fig. 3 presents the essential parts of the system, complemented with objects according to the invention. Many of the network elements have already been described in conjunction with Fig. 1. In the state-of-the-art system, when a mobile station MS ini-

IPR2025-01571
Apple EX1002 Page 728

tiates a call, the mobile switching centre MSC generates a call data record CDR, in which a desired amount of information relating to the call is stored. Usually this information comprises at least the call start time, termination time, calling and called numbers and a cell identifier Cell ID. The mobile switching centre MSC transmits a large number of CDR records at a time to the billing centre, where a billing program post-processes the call data records and generates the bills to be sent to the subscribers.

In the GSM system, as in other modern systems, the mobile station MS actually consists of two parts: mobile equipment ME and SIM card (Subscriber Identity Module), so a workable mobile station MS is only obtained by inserting a SIM card into the mobile equipment ME. The SIM card can be used as a storage medium for storing telephone numbers, but above all it is used for subscriber authentication. Identification based on the SIM card inserted by the user into the mobile station MS is designed to prevent illicit use of e.g. stolen equipment and to ensure that only subscribers who pay their bills can use the network. Stored on the card are a user identifier, i.e. PIN code (Personal Identity Number) as well as a subscriber identity code IMSI to be used in the network, the identification algorithm A3 to be used in the authentication and a subscriber-specific identification key K_i.

According to the invention, the mobile station MS is provided with a new function, which in this context is designated as locator object, Fig. 3. The function of the locator object is to establish whether the mobile station is in an area where the charging rate applied to calls originated from that area are different from the rate for calls made from other areas. Usually the rate is lower. For this purpose, the locator object needs to know the location of the mo-

bile station. In the determination of location, the broadcast information sent by the base transceiver stations is utilised. The base transceiver stations keep on sending information about themselves and their environment in their broadcast control channel. This information includes a cell identity code CI, information about adjacent cells and a location area identifier LAI. In its idle state, according to the specification, the mobile station performs frequency measurements on the BCCH (Broadcast Control Channel) channels. From a certain number of BCCH signals, e.g. six signals of highest strength, it decodes the BCCH data block, from which it obtains the BSIC data (Base Transceiver Station Colour Code). Each signal contains a cell identity code CI. The cell identity code and the carrier frequency form a pair that is individual to each base transceiver station. The one of the base transceiver stations that sends the BCCH frequency with the highest signal strength is regarded by the mobile station as its "own" base station. If the mobile station MS detects upon a change of base transceiver station BTS that the location area identifier LAI has changed, then it will send a location update request to the network.

Instead of the actual cell identity code CI, the location data used may consist of almost any unambiguous code obtained from the BSIC and updated at ½ second intervals that allows identification of the network cell or cell area. Such codes include the components of the world-wide CGI identifier (Cell Global Identification), which, according to the GSM recommendations, comprise a Mobile Country Code MCC, a Mobile Network Code MNC, a Location Area Identifier LAI and the above-mentioned Cell Identity code CI.

From the data listed above, a desired item can be selected to be used as the location data monitored by the locator object, so the area permitting

calls at a special charging rate can be defined as the entire network of the operator, as a location area or as a group of one or more cells.

The locator object picks the location data decoded by the mobile equipment and stores it in memory. The picking frequency may be the same as the frequency at which the identifiers are decoded, but since the mobile station cannot advance a long way in half a second, it is preferable to use a lower picking frequency. A suitable frequency is about once in a minute. This length of time is such that the mobile station may start a call setup process in one cell, whose base station identifier it has decoded, but the call setup process is terminated in another cell, whose base station identifier is decoded and placed in the call data record to be generated.

Stored in the memory of the locator object is a list of location data for cells permitting special call charging rates. The locator object compares the decoded location data it has picked with the stored data, and if the location data is found in the storage, then the object may give a command to display the data on the display of the equipment. It may display the cell identity code as it is or it may display e.g. a text saying "special cell" or the like to indicate to the user that calls in the current location area are cheaper. If the decoded location data cannot be found in the storage, this means that calls in the location area are charged for at normal rates, so there is no need to display any information. In this case, a list of special cells has been stored in the memory of the locator object and the locator object compares the located cell identity code with the identifiers in the list, and when this comparison indicates sameness, the above-mentioned texts are displayed.

When the locator object detects that the user is entering a telephone number and that the last loca-

tion check indicates that the mobile station is currently in an area where a special charging rate is applicable, it creates a record of the call data record type, which is designated here as compensation record. The compensation record contains the location data either as such or preferably as a suitable code. Moreover, it contains at least the calling and the called subscriber numbers.

The locator object transmits the compensation record in a special call data message to the billing object 22 in the network, Fig. 3. The billing object is located in the billing centre. The compensation record may be transmitted either during the call or after the call. The locator object may also collect compensation records for a longer time and send the collected compensation records periodically to the billing object. The billing object gathers the call data records sent by the mobile switching centre and the compensation records sent by the locator object and finds the ones of the call data records that are entitled to a different (lower) call charge even if the cell identity code in the call data record should indicate that the call is a normal rate call.

The locator object can be implemented as follows:

In the so-called Phase 2+ of the follow-up specification of the GSM system by ETSI (European Telecommunications Standards Institute), the functions of the SIM card have been considerably increased as compared with the original specifications. The new definitions are presented in detail in specification GSM 11.14 "Digital cellular communications system (Phase 2+): Specification of the SIM Application Toolkit for the Subscriber Identity Module-Mobile Equipment (SIM-ME) Interface. It defines mechanisms that allow applications on the SIM card to cooperate and work with any mobile equipment ME that supports

IPR2025-01571
Apple EX1002 Page 732

these functions. The features that can be utilised in the implementation of the invention include Proactive SIM, which provides mechanisms by means of which, upon initiative by the SIM card, the mobile equipment performs certain functions, such as sending a message of max. 160 characters from the SIM card and displaying it, sending an USSD string (Unstructured Supplementary Service Data) to the network. An important feature in respect of the invention is the Call Control by SIM function described in section 9 in the specification. When this function has been activated on the SIM card, the mobile equipment ME will perform the following functions:

- During each call attempt, the mobile equipment transfers the numbers dialled by the user as well as the associated parameters to the SIM card. The only exception is a redialled attempt, of which only certain details of call setup are transferred to the SIM card.

- The SIM gives a certain response to the mobile equipment, according to which the mobile equipment either starts call setup in accordance with the numbers dialled, does not start call setup at all or uses the data given by the SIM in the call setup procedure.

- If an extra service function is in use, the mobile equipment ME transfers a service control string to the SIM card before the service is implemented.

- The SIM gives the mobile equipment a response of the same type as in the case of dialled numbers, whereupon the mobile equipment either starts the service or does not start it or starts it in accordance with the instructions given by the SIM card.

Moreover, section 6.4.15 of Phase 2+ defines the command PROVIDE LOCAL INFORMATION, which the SIM can use to request the mobile equipment to send current location information. When the SIM issues this

IPR2025-01571
Apple EX1002 Page 733

command to the mobile equipment, the latter responds by giving a TERMINAL RESPONSE, which contains the Mobile Country Code MCC, Mobile Network Code MNC, Location Area Identifier LAI and the Cell Identity code CI.

In addition, Phase 2+ defines the command DISPLAY TEXT. By giving this command, the SIM can cause the mobile equipment to display a desired text on the display of the equipment.

These new features of the SIM-ME interface as defined in Phase 2+ are preferably utilised in the implementation of the invention. Referring to Fig. 4, the operation of the locator object will now be described by using the concepts mentioned above. The figure illustrates the functions of the locator object and the messages exchanged between the SIM card, the mobile equipment ME and the base transceiver station BTS.

The locator object, which is a suitable program, is implemented on the SIM card. At regular time intervals ΔT, the object sends a PROVIDE LOCAL INFORMATION message to the mobile equipment ME. In response to this message, the mobile equipment sends a TERMINAL RESPONSE message, which contains the mobile country code MCC, mobile network code MOBILE NETWORK CODE MNC, location area code LAC and the cell identity code CI (Cell Id). Let us suppose that the object uses the cell identity code CI as location data. Upon receiving the message, the locator object checks whether the cell identity code is included in the list stored on the SIM card. The list has been stored on the card beforehand by the network operator. If it is not found in the list, then the cell identity data last saved is reset and, after the set time interval ΔT, the locator object sends a new request for location data and again compares the cell identity code received with the

list. But if the cell identity code is found in the list, this means that the mobile equipment has received location data from the BCCH carrier while in a cell for which the operator has set a special charging rate for calls originated from that cell. In this case, the location data is stored in memory. Again, after an interval of ΔT, a request for location data is sent and the above-described procedure is repeated. If the cell identity code is not found in the list, then the previously stored cell identity code is reset.

When the location data has been stored, the locator object sends a DISPLAY TEXT message to the mobile equipment, which then displays the cell identity code comprised in the message either as it is or in plain-language form, e.g. "Reduced call charge" or the like.

When the user dials a telephone number to make a call, the mobile equipment transfers the called number dialled by the user in an ENVELOPE message to the SIM card. If the locator object accepts the number, it will send an ALLOWED acknowledgement message. After this, call setup proceeds in the normal manner and ends with a CONNECT message sent by the network, whereupon the speech path is connected. In response to the CONNECT message, the mobile equipment sends a TERMINAL RESPONSE message to the SIM card, letting the locator object know that the speech path has been connected.

The locator object now retrieves the location data from the storage. If it is not zero, which would mean "not a special rate cell", the locator object will start generating a compensation record by placing in the record the location data and call identification data specifying the call so that the billing object will be able to link the compensation record and the call data record generated by the mobile switching

centre together. The call identification data may include at least a running sequence number N, which is reset when it reaches a maximum value M. The sequence number thus changes as moduloM. Each successful call would thus be given a sequence number, but since a compensation record is not generated for every call, the locator object will receive compensation records with a sequence number N that does not grow regularly. For this reason, the mobile switching centre must be provided with a function that adds to the call data record a sequence number N increasing in the same way moduloM. Thus, the billing object will be able to link the compensation records with call data records having the same N value and charge the customer on the basis of the location data given in the compensation record. Of course it is also possible to include the calling and the called numbers in the compensation record.

During the call, the locator object transfers the compensation record to the mobile equipment, which sends it over the network to the billing object during the call. The transmission can also be effected in the form of a short message SMS (Short Message Service), in which case the locator object will give the mobile equipment a Send SMS command, or using the USSD (Unstructured Supplementary Service Data) consistent with the GSM standard, in which case it will give a Send USSD command.

In the foregoing description, the compensation record was sent during the call. As another alternative, the locator object may collect compensation records for some time and send them to the billing object in a larger batch. The limit for the batch size is set by the maximum length of the short message, which is 160 characters. The transmission of the batch can be done in the same way as the transmission of a compensation record during a call. However, if the compensation records are not sent during the call but

periodically in larger batches, there is a risk that the compensation records associated with the calls will be received after the actual billing period. This would be difficult because it would be necessary to send credit notes to the customers. Therefore, real-time transmission of compensation records is a preferable alternative.

In both alternatives, the billing object gathers the call data records sent by the mobile switching centre and the compensation records sent by the locator object together and finds those ones of the call data records which, according to the compensation record, are entitled to a different (lower) call charge, even if the cell identity code in the call data record should indicate that the call is a normal rate call. If the billing object cannot match a call data record produced by the mobile switching centre with a compensation record produced by the locator object, then it will assume that the call has been made in a normal rate area.

For the transmission of the compensation records to the billing object, a reliable data transmission link must be available between the objects. The SMS and USSD used in the GSM system are sufficiently reliable for this purpose.

The invention is not restricted to the example presented in the foregoing, but many different embodiments are possible within the scope of the definitions given in the claims. The locator object may also be implemented in the mobile equipment while only a list of special cells is stored on the SIM card by the operator.

Besides the cell identity code CI, the data used as location data may consist of the mobile country code MCC, the mobile network code MNC or the location area code LAC or a combination of these. In the CDMA system, the base station pilot signal data can be

used as location data because each base station keeps sending its own individual pilot signal. If the mobile communication system comprises, e.g. because required by the authorities, a feature for calculating the location of the mobile station using timing advance values or some other method, then this information is transmitted e.g. in the form of coordinates to the locator object. In this case, the locator object can be provided with tables of special location areas, whose boundaries need not coincide with cell area boundaries. The tables contain e.g. coordinate values and the locator object compares the current location data with the table to establish whether the location is within a special area. It is also possible to provide the mobile station with a location system such as a GPS receiver. The locator object compares the coordinate values obtained from the system with the table values and proceeds as above.

CLAIMS

1. Procedure for forming the principle of calculation of call charge in a cellular mobile telephone network, which comprises

a mobile switching centre, which produces a call data record for each call,

and a plurality of base transceiver stations, each of which transmits the calls of the mobile stations located in the area served by the respective base transceiver station,

and in which at least one special area has been formed and a special charging rate has been set for calls originated from such an area, and in which the mobile station determines its location at time intervals of a predetermined length,

c h a r a c t e r i s e d in that

a list of the location identifiers of the special areas is stored in the mobile station in advance,

and that in the mobile station;

a check is carried out to establish whether the location data of the mobile station is comprised in the special areas on the list,

the location data is stored in memory for said time interval of predetermined length if it is comprised in the list,

a compensation record associated with a call initiated from the mobile station is generated during the call if the location data has been stored in memory, the information placed in said compensation record comprising at least the location data and data identifying the call,

the compensation record is transmitted to the mobile telephone network,

and that in the mobile telephone network;

to determine the charge for the call, the data in the compensation record and the data in the call data record are combined.

2. Procedure as defined in claim 1, characterised in that the determination of location is effected by utilising identifier data sent by the mobile telephone network.

3. Procedure as defined in claim 1, characterised in that the determination of location is effected by utilising data sent by an external system.

4. Procedure as defined in claim 3, characterised in that the external system used is a satellite positioning system.

5. Procedure as defined in claim 1, characterised in that the data identifying the call is a parameter placed in both the compensation record and the call data record, being the same in both records.

6. Procedure for improving the principles of calculation of call charge in a cellular mobile telephone network, in which

the mobile stations order the broadcast channels received from different base transceiver stations according to signal strength and decode at least from the strongest broadcast channel the various identifier data sent by the base transceiver station,

at least one special area has been formed and a special charging rate has been set for calls started from such an area, and

the mobile station determines its location at time intervals of a predetermined length,

characterised in that

a list of special areas is stored in the mobile station,

and that in the mobile station;

a check is carried out to establish whether the mobile station is located in a special area,

the location data is stored in memory for said time interval of predetermined length if the mobile station is in a special area,

a compensation record associated with a call started from the mobile station is generated during the call if the location data has been stored in memory, the information placed in said compensation record comprising at least the location data and data identifying the call,

the compensation record is transmitted to the mobile telephone network.

7. Procedure as defined in claim 6, characterised in that, when the identifier data is stored in memory, information indicating that the mobile station is in a special area is shown on the display of the mobile station.

8. Procedure as defined in claim 6, characterised in that the length of the predetermined time interval is substantially longer than the interval at which the mobile station decodes the signal of the strongest broadcast channel.

9. Procedure as defined in claim 6, characterised in that the special area comprises at least one cell and the list of special areas contains the identifiers of the cells in the special areas.

10. Procedure as defined in claim 6, characterised in that the compensation record is sent during the call.

11. Procedure as defined in claim 6, characterised in that a plurality of compensation records are collected into a batch and the batch is sent to the mobile telephone network.

12. Procedure as defined in claim 6, characterised in that the call data records generated by the mobile switching centre are compared

with the compensation records sent by the mobile station and when, based on the data identifying the call, records corresponding to each other are found, the price of the call is calculated on the basis of the rate set for the special area specified by the background record.

13. Procedure as defined in claim 6, c h a r a c t e r i s e d in that the list of special areas is stored in the Subscriber Identity Module.

14. Cellular mobile telephone system, which comprises

a mobile switching centre,

a plurality of base transceiver stations, each of which keeps sending its own identifier data in its broadcast channel,

mobile stations which consist of a mobile equipment (ME) and a subscriber identity module mounted in it and which order the broadcast channels received from different base transceiver stations according to signal strength and decode at least from the strongest broadcast channel the identifier data sent by the base transceiver station,

and in which system at least one special area has been formed and a special charging rate has been set for calls made from such an area, and

c h a r a c t e r i s e d in that the mobile station contains a list containing data regarding the special areas, and a locator object which

determines the location of the mobile station at time intervals of predetermined length and compares the resulting location data with the list,

stores the location data in memory for said time interval of predetermined length if it is comprised in the list,

during a call started from a mobile telephone, generates a compensation record associated with the call if the location data is currently stored in

memory and places in the compensation record at least the location data and data identifying the call and sends the compensation record to the mobile telephone network,

and that the system contains a billing object, which compares the compensation records with the call data records generated by the mobile switching centre and, when the call identifying data in said records correspond to each other, generates a call charge using the rate set for the special area indicated in the compensation record.

15. System as defined in claim 14, characterised in that the locator object is located in the subscriber identity module (SIM) and the billing object is located in conjunction with a billing centre.

16. System as defined in claim 14, characterised in that the interface between the mobile equipment and the subscriber identity module is consistent with GSM system specification 11.14.

17. System as defined in claim 16, characterised in that the locator object sends to the mobile equipment a Provide Local Information message at time intervals of predetermined length, and in response to a Terminal Response return message the locator object checks whether the decoded identifier data is included in the list.

18. System as defined in claim 17, characterised in that, when the identifier data is included in the list, the locator object sends to the mobile equipment a Display Text message, in response to which the mobile equipment displays the identifier data on its display screen.

19. System as defined in claim 14, characterised in that, in response to a message sent to the subscriber identity module (SIM) indicating es-

IPR2025-01571
Apple EX1002 Page 743

tablishment of a speech connection, the locator object generates a compensation record.

20. System as defined in claim 14, characterised in that the locator object sends to the mobile equipment a Send Short Message message, in response to which the mobile equipment sends the compensation record to the billing object.

21. System as defined in claim 14, characterised in that the locator object sends to the mobile equipment a Send USSD message, in response to which the mobile equipment sends the compensation record to the billing object.

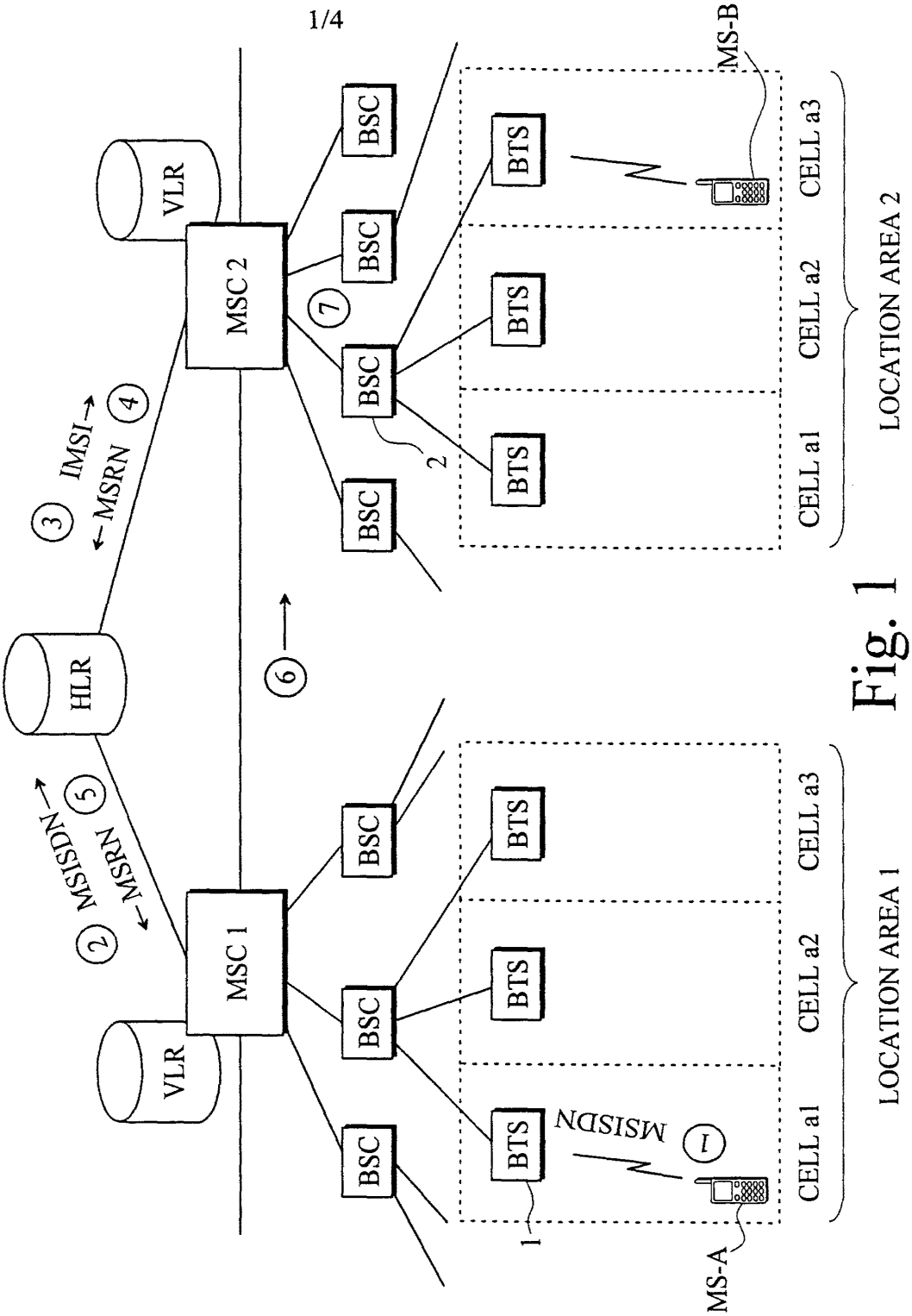

VLR
MSC 2
HLR
VLR
MSC 1
BSC
BTS
MS-B
MS-A
MSISDN
IMSI
MSRN
MSISDN
MSRN
CELL a1
CELL a2
CELL a3
LOCATION AREA 1
LOCATION AREA 2
1
2
3
4
5
6
7

Fig. 1

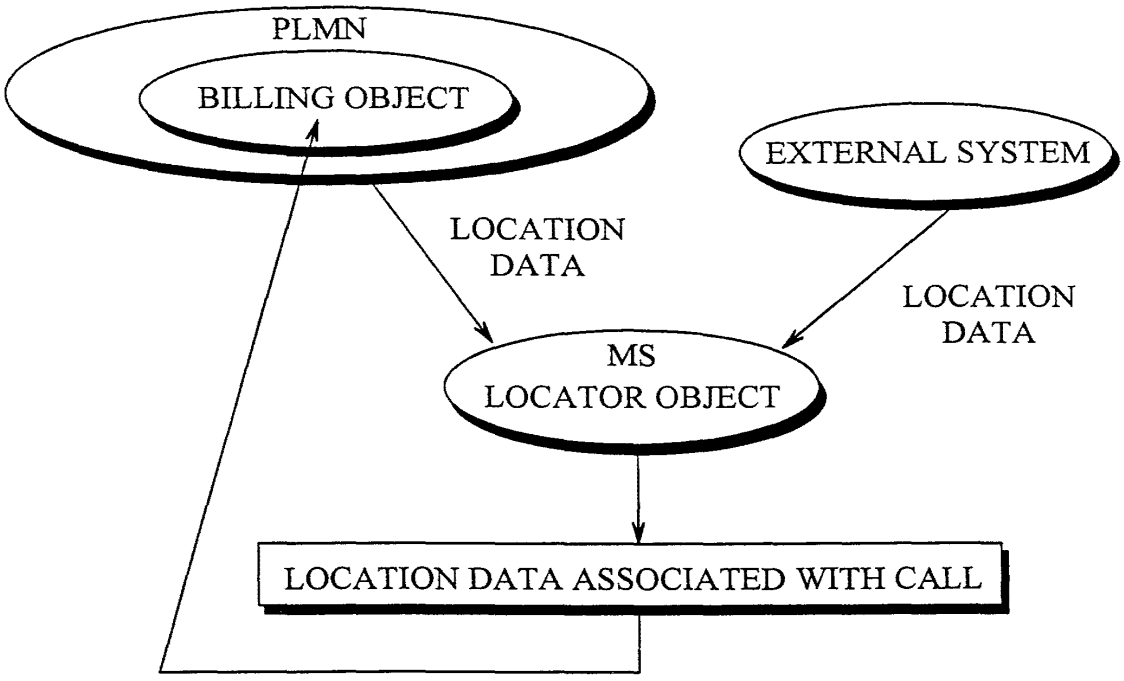

PLMN
BILLING OBJECT
EXTERNAL SYSTEM
LOCATION DATA
LOCATION DATA
MS LOCATOR OBJECT
LOCATION DATA ASSOCIATED WITH CALL

Fig. 2

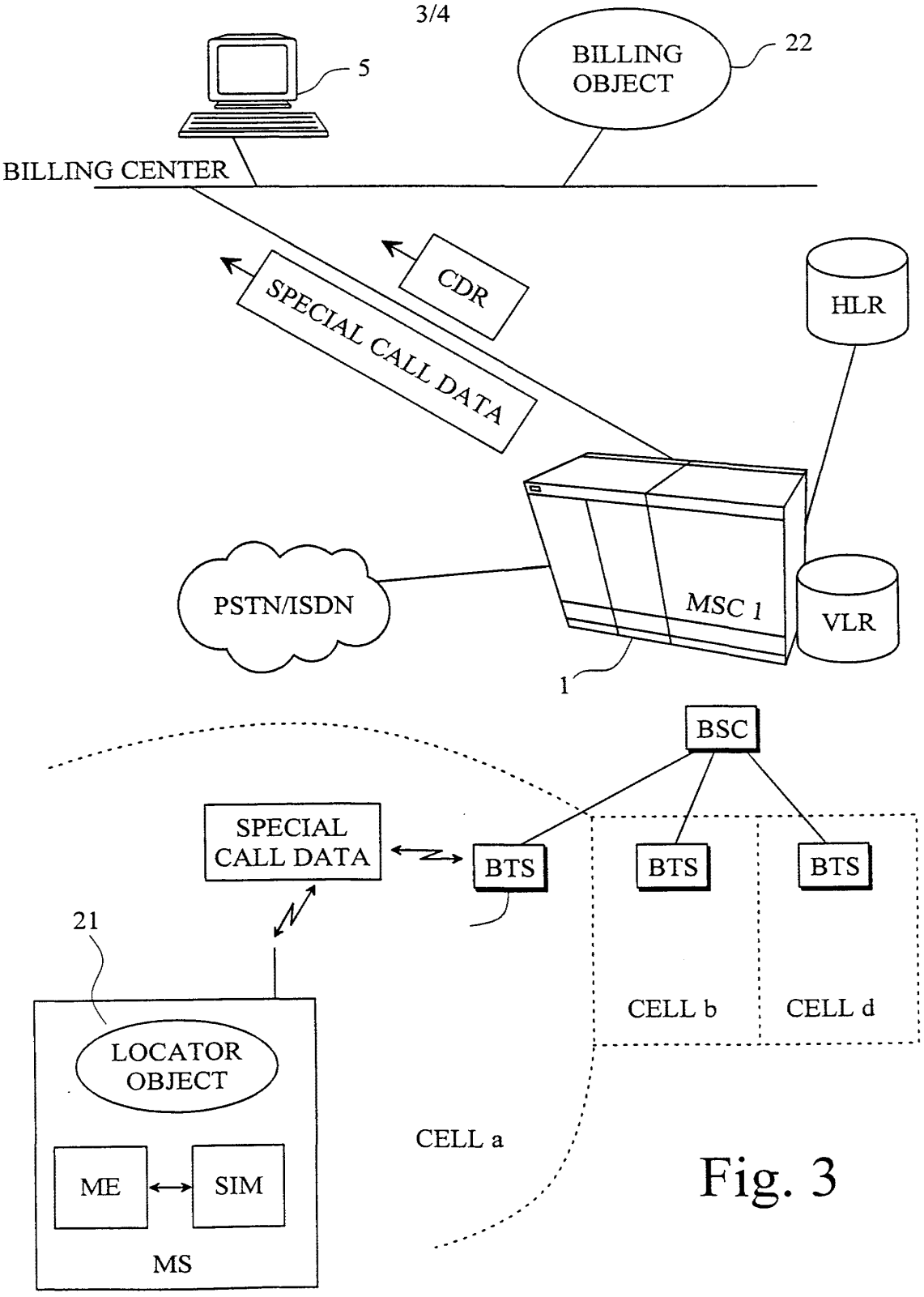

5
BILLING OBJECT
22
BILLING CENTER
CDR
SPECIAL CALL DATA
HLR
PSTN/ISDN
MSC 1
VLR
1
BSC
SPECIAL CALL DATA
BTS
BTS
BTS
21
CELL b
CELL d
LOCATOR OBJECT
CELL a
ME
SIM
MS

Fig. 3

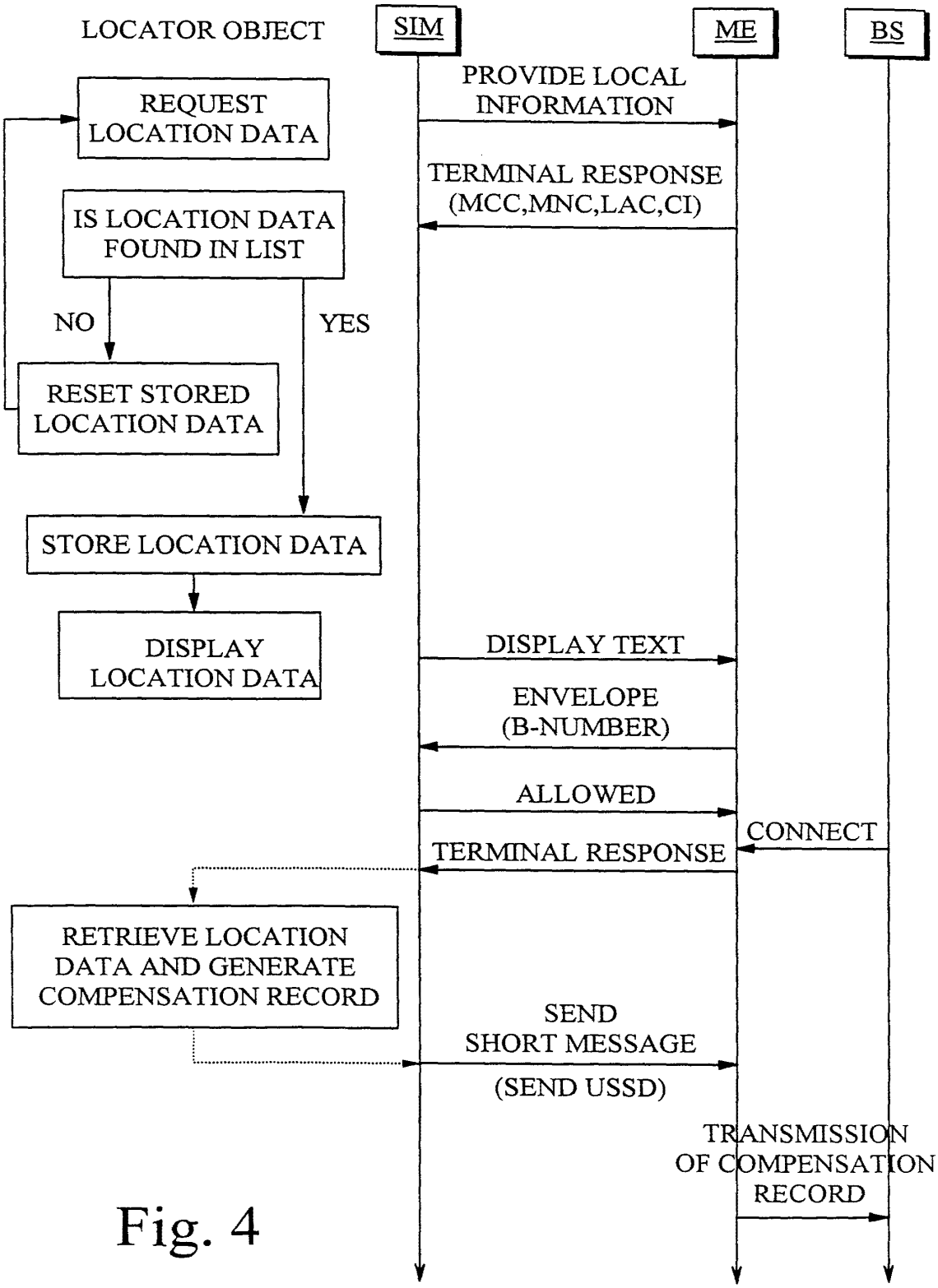

LOCATOR OBJECT
SIM
ME
BS
REQUEST LOCATION DATA
PROVIDE LOCAL INFORMATION
TERMINAL RESPONSE (MCC,MNC,LAC,CI)
IS LOCATION DATA FOUND IN LIST
NO
YES
RESET STORED LOCATION DATA
STORE LOCATION DATA
DISPLAY LOCATION DATA
DISPLAY TEXT
ENVELOPE (B-NUMBER)
ALLOWED
CONNECT
TERMINAL RESPONSE
RETRIEVE LOCATION DATA AND GENERATE COMPENSATION RECORD
SEND SHORT MESSAGE
(SEND USSD)
TRANSMISSION OF COMPENSATION RECORD

Fig. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 98/00515

A. CLASSIFICATION OF SUBJECT MATTER

IPC6: H04Q 7/22, 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)

IPC6: H04Q, H04M, G01S

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)

WPI, EDOC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 0568824 A2 (US WEST, INC.), 10 November 1993 (10.11.93), column 3, line 11 - column 4, line 2; column 4, line 55 - column 6, line 6; column 15, line 10 - line 39, figures 2,10, abstract --	1-21
Y	EP 0734144 A2 (SIEMENS AKTIENGESELLSCHAFT), 25 Sept 1996 (25.09.96), column 3, line 5 - column 5, line 9, figure 3, abstract --	1-21
A	WO 9620570 A1 (NOKIA TELECOMMUNICATIONS OY), 4 July 1996 (04.07.96), cited in the application --	1-21

[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" erlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
2 November 1998	05 -11- 1998
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 Patrik Rydman Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1992)

IPR2025-01571
Apple EX1002 Page 749

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 98/00515

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 9428670 A1 (NOKIA TELECOMMUNICATIONS OY), 8 December 1994 (08.12.94) --	1-21
A	WO 9708884 A1 (TELEFONAKTIEBOLAGET LM ERICSSON), 6 March 1997 (06.03.97), figures 1a,b, abstract, claims --	1-21
A	WO 9620571 A1 (NOKIA TELECOMMUNICATIONS OY), 4 July 1996 (04.07.96), cited in the applications --	1-21
A	WO 9711569 A1 (TELEFONAKTIEBOLAGET LM ERICSSON), 27 March 1997 (27.03.97), abstract --	1-21
A	WO 9634499 A1 (TELEFONAKTIEBOLAGET LM ERICSSON), 31 October 1996 (31.10.96), cited in the application --	1-21
A	US 5546445 A (EVERETT DENNISON ET AL), 13 August 1996 (13.08.96), abstract -- --------	3,4

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

05/10/98

International application No.
PCT/FI 98/00515

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0568824 A2	10/11/93	CA 2083791 A	09/10/93
		JP 6105364 A	15/04/94
		US 5295180 A	15/03/94
		US 5600706 A	04/02/97
		US 5758288 A	26/05/98
EP 0734144 A2	25/09/96	NONE	
WO 9620570 A1	04/07/96	AU 4262396 A	19/07/96
		CA 2207426 A	04/07/96
		CN 1171185 A	21/01/98
		EP 0800748 A	15/10/97
		FI 97510 B,C	13/09/96
		FI 946091 A	24/06/96
		NO 972889 A	20/06/97
WO 9428670 A1	08/12/94	AU 6798194 A	20/12/94
		FI 932480 A	01/12/94
WO 9708884 A1	06/03/97	AU 6892796 A	19/03/97
		DE 19681544 T	20/08/98
WO 9620571 A1	04/07/96	AU 4305796 A	19/07/96
		CA 2207420 A	04/07/96
		CN 1171186 A	21/01/98
		EP 0801874 A	22/10/97
		FI 97511 B,C	13/09/96
		FI 946092 A	24/06/96
		NO 972893 A	20/08/97
WO 9711569 A1	27/03/97	AU 7005096 A	09/04/97
		EP 0852101 A	08/07/98
		US 5754955 A	19/05/98
WO 9634499 A1	31/10/96	AU 5519296 A	18/11/96
US 5546445 A	13/08/96	AU 6772994 A	12/12/94
		WO 9427398 A	24/11/94
		AU 3414193 A	28/07/93
		US 5235633 A	10/08/93
		WO 9313618 A	08/07/93

IPR2025-01571
Apple EX1002 Page 751

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
30 August 2007 (30.08.2007)

PCT

(10) International Publication Number
WO 2007/097786 A1

(51) International Patent Classification:
H04M 15/28 (2006.01)

(21) International Application Number:
PCT/US2006/041665

(22) International Filing Date: 25 October 2006 (25.10.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/363,141 27 February 2006 (27.02.2006) US

(71) Applicant *(for all designated States except US)*: **SONY ERICSSON MOBILE COMMUNICATIONS AB** [SE/SE]; Nya Vattentornet, S-221 88 Lund (SE).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **PANTALONE, Brett, Anthony** [US/US]; 601 Jamestown Road, Pittsboro, North Carolina 27312 (US). **VASA, Yojak** [US/US]; 303 Birdwood Court, Cary, North Carolina 27519 (US).

(74) Common Representative: **SONY ERICSSON MOBILE COMMUNICATIONS AB**; c/o David E. Bennett, Coats & Bennett, P.l.l.c., Post Office Box 5, Raleigh, North Carolina 27602 (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, 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.

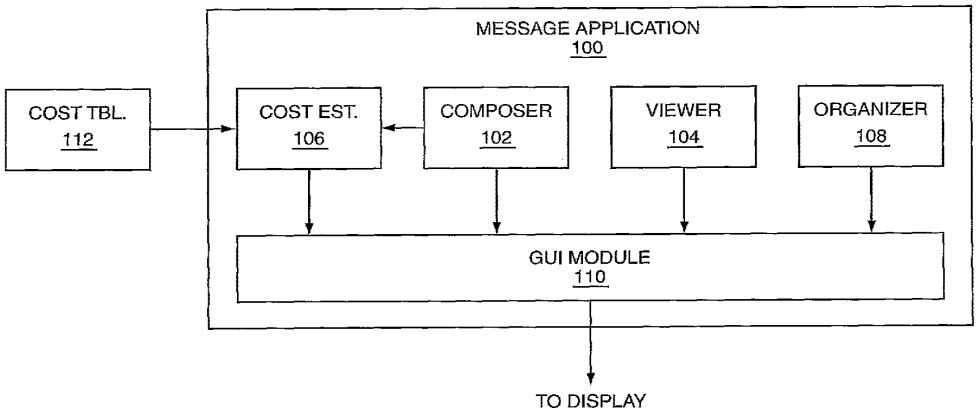
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, 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:
— *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: COST ESTIMATION IN MESSAGING APPLICATION FOR A MOBILE COMMUNICATION DEVICE



(57) Abstract: A messaging application (100) for a mobile communication device (10) comprises an integrated message composer (102) for creating messages of two or more different types, and a cost estimation function (106) for estimating the cost of messages based on the message type and cost data stored in memory (14) and for providing the estimated cost of the message to the user before the message is sent. Providing the user with information about the cost of the message gives the user confidence that messages will not be undesirably expensive and the increased confidence in the cost of messages will encourage use of messaging services.

WO 2007/097786 A1

COST ESTIMATION IN MESSAGING APPLICATION FOR A MOBILE COMMUNICATION DEVICE

BACKGROUND

The present invention relates generally to messaging applications for mobile communication devices, and more particularly, to an integrated messaging application capable of sending text messages, multimedia messages, email messages and instant messages.

Mobile communication devices, such as cellular telephones, offer customers a wide variety of messaging services, enabling customers to send and receive text messages, multimedia messages, email messages and instant messages. To facilitate ease of use, the current trend is to integrate some or all of the available messaging applications into a single integrated application with a common composer for creating messages. The common composer typically includes a set of editing tools for creating and sending messages. The user can thus use the same interface and a consolidated set of editing tools to create different types of messages.

Cellular operators and service providers often have different charging schemes for different types of messages. For example, a service provider may charge on a per message basis for SMS text messages, a flat monthly fee for email, and a cost per bit for multimedia messages. When using an integrated message composer, the user may not realize what type of message the user is creating. Since there may be a substantial cost difference between different types of messages, the user may unknowingly incur undesired expenses to send a message that would have been substantially cheaper using a different service. For example, a simple SMS text message intended for a relatively inexpensive transport may unwittingly become a more expensive multimedia message when the user attaches a sound file or image. Thus, while the integrated message composer is intended as a convenience for the user, it may cause confusion and worry about the cost of messages being sent.

SUMMARY

The present invention relates to a messaging application that provides the user with information about the type and cost of messages to be sent. In one exemplary embodiment, the messaging application includes a common composer for creating messages of two or more different types. For example, the common composer application may be used to create simple text messages, email messages, instant messages, and multimedia messages. The messaging application includes a cost estimation function for estimating the cost of a message and indicating the estimated costs of the message to the user before it is sent. The estimated cost may be displayed to the user in a portion of an application window for the message composer. For example, the type and cost of the message can be displayed to the user in a title bar, menu bar, or

IPR2025-01571
Apple EX1002 Page 753

status bar of an application window. The estimated cost of the message could also be presented to the user in a pop-up window, such as a message box or dialog box. The pop-up window may prompt the user to confirm a previous command to send a message so that the user does not inadvertently send an undesirably expensive message. The user is thus given an opportunity to edit the content of the message before it is sent such that a cheaper transport can be used to send the message if desired. By giving users confidence in the cost of messages being sent, the present invention may encourage otherwise hesitant users to send messages without fear that the messages will incur undesired expenses.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a functional block diagram of a messaging application for a mobile communication device according to one exemplary embodiment.

Fig. 2 illustrates an exemplary GUI for a message composer displayed on a mobile communication device.

Fig. 3A illustrates an exemplary GUI for a message composer displayed on a mobile communication device.

Fig. 3B illustrates an exemplary GUI for a message composer displayed on a mobile communication device.

Fig. 4 illustrates an exemplary GUI for a message composer displayed on a mobile communication device.

Fig. 5 illustrates an exemplary GUI for a message composer displayed on a mobile communication device.

Fig. 6 is a block diagram of an exemplary mobile communication device.

Fig. 7 illustrates an exemplary cost table embodied in XML code.

DETAILED DESCRIPTION

Figure 1 illustrates the main components of a messaging application 100 for a mobile communication device 10. The messaging application 100 includes a message composer 102, a message viewer 104, a cost estimation function 106, an organizer 108, and a graphical user interface (GUI) module 110. The message composer 102 is used to create messages to be sent. The message composer 102 provides a common interface and a common set of editing tools for creating messages of two or more different types. In one exemplary embodiment, the message composer 102 is capable of creating simple text messages, multimedia messages, instant messages and email messages. The message viewer 104 provides tools for viewing messages received by the mobile communication device 10. The cost estimation function 106 estimates the cost of messages to be sent. The cost estimation function 106 receives information from the

IPR2025-01571
Apple EX1002 Page 754

message composer 102 about the type, size and content of messages. The cost estimation function 108 also has access to cost information stored in a cost table 112 in the memory of the mobile communication device 10. The organizer 108 provides a set of management tools to manage messages sent and received. The GUI module 110 creates a GUI for the components of the messaging application 100 that is presented to the user on a display 40 of the mobile communication device 10. In the exemplary embodiment, the GUI is a conventional windowing interface. Those skilled in the art will appreciate, however, that the nature of the software interface is not a material part of the invention and that other types of interfaces may be used with the present invention, including command line interfaces and other types of GUI interfaces.

Figs. 2 – 5 illustrate a GUI for the message composer 102 as it appears on the display 40 of the mobile communication device 10. The GUI for the message composer 102 comprises an application window 150 having a title bar 152 at the top of the window 150, a menu bar 154 at the bottom of the window, and a message field 156 where the message being composed is displayed. In this example, the message field 156 displays a simple text message which the user is composing. The title bar 152 includes information identifying the type and estimated cost of the message. In this example, the information contained in the title bar 152 indicates that the message is a text message using the Short Message Service (SMS) for transport, and that the estimated cost of the message is 10 cents. The menu bar 154 at the bottom of the application window 150 includes one or more menu items 158 that can be selected by pressing the selection keys 32 adjacent to the display. A navigation control 34 is also provided to enable the user to navigate through menus and make selections.

The menu bar 154 in the exemplary embodiment displays two menu items 158 that are used to access pop-up menus as shown in Figs. 3A and 3B. The CONTINUE menu, shown in Fig. 3A, provides a list of options for handling messages, such as SAVE, SEND, and DELETE. The MORE menu, shown in Fig. 3B, provides a set of editing tools for editing messages. In this example, the editing tools allow the user to add or attach images, audio, and video to the message.

As additional content is added to the message, the type and/or cost of the message may change. Referring to Figure 4, the user has added an image of a clock to the original text message. The information contained in the title bar 152 changes to reflect that the message type has changed. The estimated cost has also been updated. Following the addition of the image, the message has become a multimedia message using the Multimedia Messaging Service (MMS) for transport. The estimated cost of the message is 49 cents.

Providing information to the user about the type and cost of the message before it is sent provides more certainty about the cost of messages being sent. Some users that are hesitant to use messaging services because of worries about the cost of such services will be encouraged to

IPR2025-01571
Apple EX1002 Page 755

make more use of messaging services. If a message is considered too costly, the user also has an opportunity to change the content of the message to reduce the cost before the message is sent.

In the exemplary embodiment described above, cost information is provided for individual messages and is not stored. That is, the cost information is discarded after the message is sent. In some embodiments, the messaging application 100 can store historical cost information about the cost of each message sent. Also, some embodiments may track the cumulative cost of all messages sent over a defined period of time. The cumulative cost of all messages sent over a defined period may also be displayed to the user.

In some embodiments of the invention, the messaging application 100 may generate a pop-up window 160 before the message is sent to inform the user of the cost of the message as shown in Fig. 5. The pop-up window 160 may be displayed responsive to a request or command to send the message. The pop-up window 160 may further include a prompt requesting the user to confirm the send command. In Fig. 5, the pop-up window 160 displays information indicating the cost of the message being sent and prompts the user to confirm the send command. In this example, the pop-up window 160 includes two buttons 162, 164. Button 162 is used to confirm the send command. Button 164 is used to cancel the send command. When the send command is canceled, the message may be displayed to the user in the message composer window for editing.

The user may consider the display of the pop-up window 160 with every message to be annoying. Therefore, the messaging application 100 may allow the user to set preferences to control when the pop-up window 160 is displayed. The user preferences may permit the user to suppress the pop-up window 160 for all messages, or for some messages based on a predefined criterion. The pop-up window 160 may be suppressed depending on the type or cost of the message, the time of day, the cumulative cost of messages sent over a defined period, or other criteria. For example, the user may chose to suppress the pop-up window 160 for text messages and to enable the pop-up window 160 for all other messages. In another example, the user may select to suppress the pop-up window 160 where the cost of the individual message is less than a specified amount, e.g. 10 cents, or where the cumulative cost of all messages sent over a defined period is less than a specified amount. In other embodiments, the user may enable the pop-up window for specified times of the day when costs are high and suppress the pop-up window 160 for times of day when the rates are lower.

Fig. 6 is a block diagram illustrating a mobile communication device 10 in which the present invention may be implemented. The mobile terminal 10 may, for example, comprise a cellular telephone for use in a mobile communication network, a personal digital assistant (PDA), a laptop computer, or a hand-held computer. The mobile terminal 10 includes a system controller 12 to control overall operation of the mobile terminal 10 and a memory 14 to store program instructions and data needed for operation. The system controller 12 may comprise one or more processors,

IPR2025-01571
Apple EX1002 Page 756

microcontrollers, hardware, firmware, or a combination thereof. Memory 14 may comprise one or more memory devices, including removable memory devices such as SIM cards and smart cards.

A transceiver 16 coupled to an antenna 18 and under the control of the system controller 12 enables communication with remote devices. The transceiver 16 may, for example, comprise a fully functional cellular transceiver operating according to any known standard. A user interface 20 enables the user to interact with the mobile terminal 10. The user interface 20 includes a microphone 22 for converting audible signals into electrical audio signals, a speaker 24 for converting electrical audio signals into audible sounds, one or more input controls indicated generally by the numeral 30 for receiving user input, and a display 40 to display information for viewing by the user. Any known type of input controls 30 for receiving user input may be used including hard and soft keys, programmable keys, keypads, dials, joysticks, buttons, thumbwheels, touch pads, etc. The selection keys 32 and navigation keys 34 shown in Figs. 2 – 5 are exemplary input controls 30. Display 40 may comprise a color display, such as a liquid crystal display (LCD) or a touchscreen display that can also be used for user input.

The messaging application 100 is stored in memory 14 and executed by the system processor 12. Memory 14 further stores cost information, which may be in the form of a cost table 112, that is accessed by the cost estimation function 106 to estimate the cost of messages. In one exemplary embodiment, the cost table 112 is stored in a SIM card or other removable memory device. The cost table 112 is downloaded into memory 14 during device provisioning, which may occur over-the-air. The service provider can update the cost table 112 whenever the pricing for messaging services changes or when the user changes service plans. The cost table 112 contains cost information for all messaging services, and may include information on roaming costs and time-of-day pricing.

Fig. 7 illustrates an exemplary cost table 112 implemented as an XML script. The cost table 112 in Fig. 7 represents a hypothetical pricing structure for SMS, MMS and IMS services. Between 6:00 am and 9:00 pm, SMS messages cost 10 cents per message, with a 25 cent roaming surcharge for roaming. From 9:00 pm to 6:00 am, SMS messages are free, but the roaming surcharge still applies. IMS is charged at a fixed rate of $6.00 per month. MMS is charged at a fixed rate of $6.00 per month, plus an additional 2 cents per kilobyte. Thus, it can be seen that the present invention accommodates any arbitrarily complex pricing structure.

While the implementation of the cost table as an XML document provides a convenient method for updating the cost table, those skilled in the art will appreciate that the cost table could be implemented in other ways. For example, the cost table could be implemented as a database table, associative hash table, or other data structure.

The present invention may, of course, be carried out in other ways than those specifically set forth herein without departing from essential characteristics of the invention. The present

IPR2025-01571
Apple EX1002 Page 757

embodiments are to be considered in all respects as illustrative and not restrictive, and all changes coming within the meaning and equivalency range of the appended claims are intended to be embraced therein.

IPR2025-01571
Apple EX1002 Page 758

CLAIMS

What is claimed is:

1. A mobile communication device (10), comprising:
   a processor (12);
   a memory (14);
   a messaging application (100) stored in said memory (14) and executed by said processor (12) for sending and receiving messages, said messaging application (100) including a message composer (102) for creating messages to be sent;
   a cost estimation function (106) integrated with said message composer (102) for estimating the cost of said messages and for indicating the cost of said messages to a user.

2. The mobile communication device of claim 1 wherein the mobile communication device (10) further comprises a display (40) and wherein the messaging application (100) includes a graphical user interface that is displayed to the user on said display (40).

3. The mobile communication device of claim 2 wherein the graphical user interface displays the estimated cost of a message to be sent.

4. The mobile communication device of claim 3 wherein the graphical user interface comprises an application window (150) and wherein the estimated cost of the message is displayed in a portion of the application window (150).

5. The mobile communication device of claim 4 wherein the estimated cost is displayed in one of a title bar (152), menu bar (154), or status bar of the application window (150).

6. The mobile communication device of claim 3 wherein the estimated cost is displayed to the user in a pop-up window (160).

7. The mobile communication device of claim 3 wherein the messaging application (100) prompts the user to send the message after displaying the estimated cost.

8. The mobile communication device of claim 7 wherein the estimated cost and prompt are displayed together in a pop-up window (160).

IPR2025-01571
Apple EX1002 Page 759

9. The mobile communication device of claim 8 wherein the messaging application (100) is configured to selectively suppress the pop-up window (160) based on a predefined criterion.

10. The mobile communication device of claim 9 wherein the messaging application (100) suppresses the pop-window (160) when the cost of a message is less than a predetermined amount.

11. The mobile communication device of claim 9 wherein the messaging application (100) suppresses the pop-window (160) based on a type of the message.

12. The mobile communication device of claim 9 wherein the messaging application (100) suppresses the pop-window (160) based on time of day.

13. The mobile communication device of claim 1 further comprising a cost table stored in memory (14) and containing cost information for estimating the cost of message to be sent.

14. The mobile communication device of claim 13 wherein the cost table is stored in a removable memory device.

15. A method of providing information to a user of a mobile communication device (10) about the cost of messages being sent, said method comprising:

storing cost information in a memory (14) in the mobile communication device (10);

estimating the cost of a message to be sent based on said cost information stored in memory (14); and

displaying the estimated cost of the message to the user before the message is sent.

16. The method of claim 15 wherein displaying the estimated cost of the message comprises displaying the estimated cost on a display (40).

17. The method of claim 16 wherein the estimated cost is displayed in a graphical user interface.

18. The method of claim 17 wherein the estimated cost is displayed in a portion of an application window (150) of a graphical user interface.

IPR2025-01571
Apple EX1002 Page 760

19. The method of claim 18 wherein the estimated cost is displayed in one of a title bar (152), menu bar (154), or status bar of the application window (150).

20. The method of claim 17 wherein the estimated cost is displayed to the user in a pop-up window (160).

21. The method of claim 20 further comprising prompting the user to send the message after displaying the estimated cost.

22. The method of claim 21 wherein the cost is displayed together with a user prompt in the pop-up window (160).

23. The method of claim 20 further comprising selectively suppressing the pop-up window (160) based on a predefined criterion.

24. The method of claim 23 wherein the pop-window (160) is suppressed when the cost of a message is less than a predetermined amount.

25. The method of claim 23 wherein the pop-window (160) is suppressed based on a type of the message.

26. The method of claim 23 wherein the pop-window (160) is suppressed based on time of day.

27. The method of claim 15 wherein the cost information is stored in a table.

28. The method of claim 27 wherein the cost table is stored in a removable memory device.

29. A messaging application (100) for a mobile communication device (10) comprising:
a message composer (102) for creating messages of two or more different types;
a cost estimation function (106) for estimating the cost of messages and for indicating the estimated cost to the user.

30. The messaging application of claim 29 wherein the mobile communication device (10) further comprises a display (40) and wherein the messaging application (100) includes a graphical user interface that is displayed to the user on said display (40).

IPR2025-01571
Apple EX1002 Page 761

31. The messaging application of claim 30 wherein the graphical user interface comprises an application window (150) and wherein the estimated cost of the message is displayed in a portion of the application window (150).

32. The messaging application of claim 31 configured to display the estimated cost in one of a title bar (152), menu bar (154), or status bar of the application window (150).

33. The messaging application of claim of 32 configured to display the estimated cost in a pop-up window (160).

34. The messaging application of claim 33 configured to prompt the user to send the message after displaying the estimated cost.

35. The messaging application of claim 34 configured to display the estimated cost and prompt together in the pop-up window (160).

36. The messaging application of claim 33 configured to selectively suppress the pop-up window (160) based on a predefined criterion.

37. The messaging application of claim 36 configured to suppress the pop-window (160) when the cost of a message is less than a predetermined amount.

38. The messaging application of claim 36 configured to suppress the pop-window (160) based on a type of the message.

39 The messaging application of claim 36 configured to suppress the pop-window (160) based on time of day.

40. The messaging application of claim 29 including a cost table stored in memory (14) containing cost information for estimating the cost of message to be sent.

41. The messaging application of claim 40 wherein the cost table is stored in a removable memory device.

IPR2025-01571
Apple EX1002 Page 762

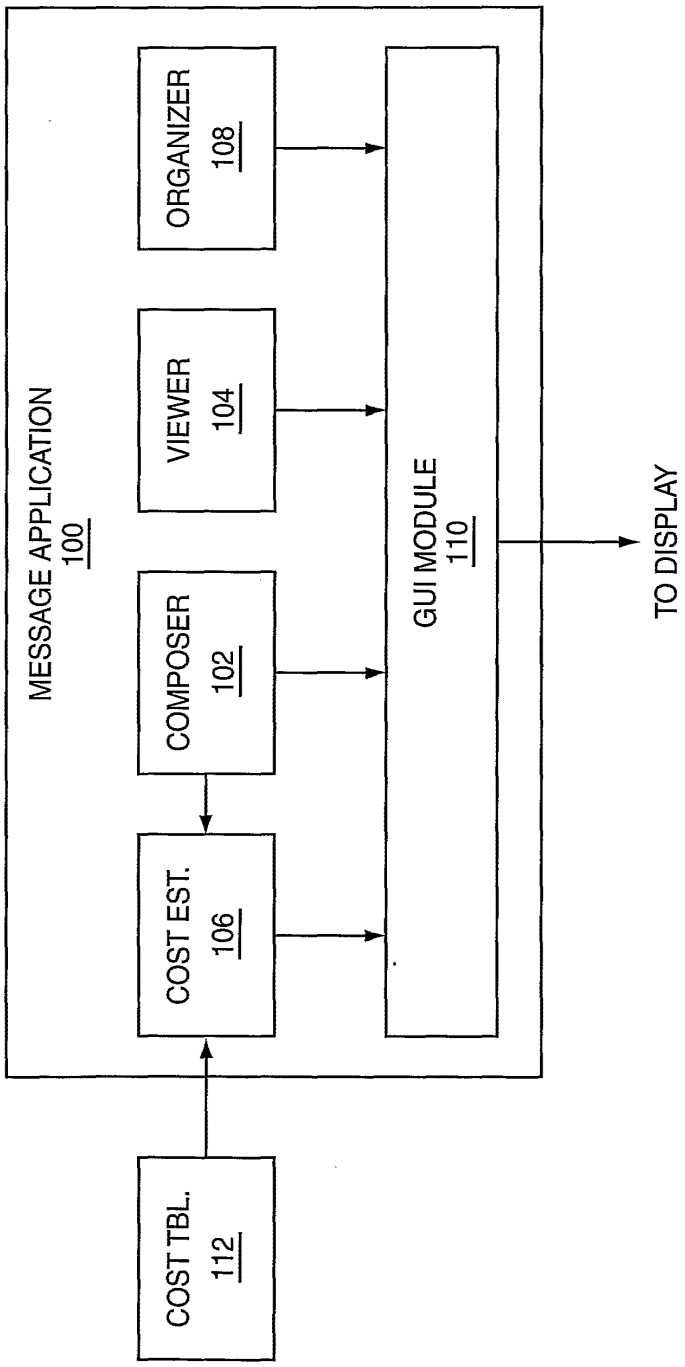


FIG. 1

IPR2025-01571
Apple EX1002 Page 763

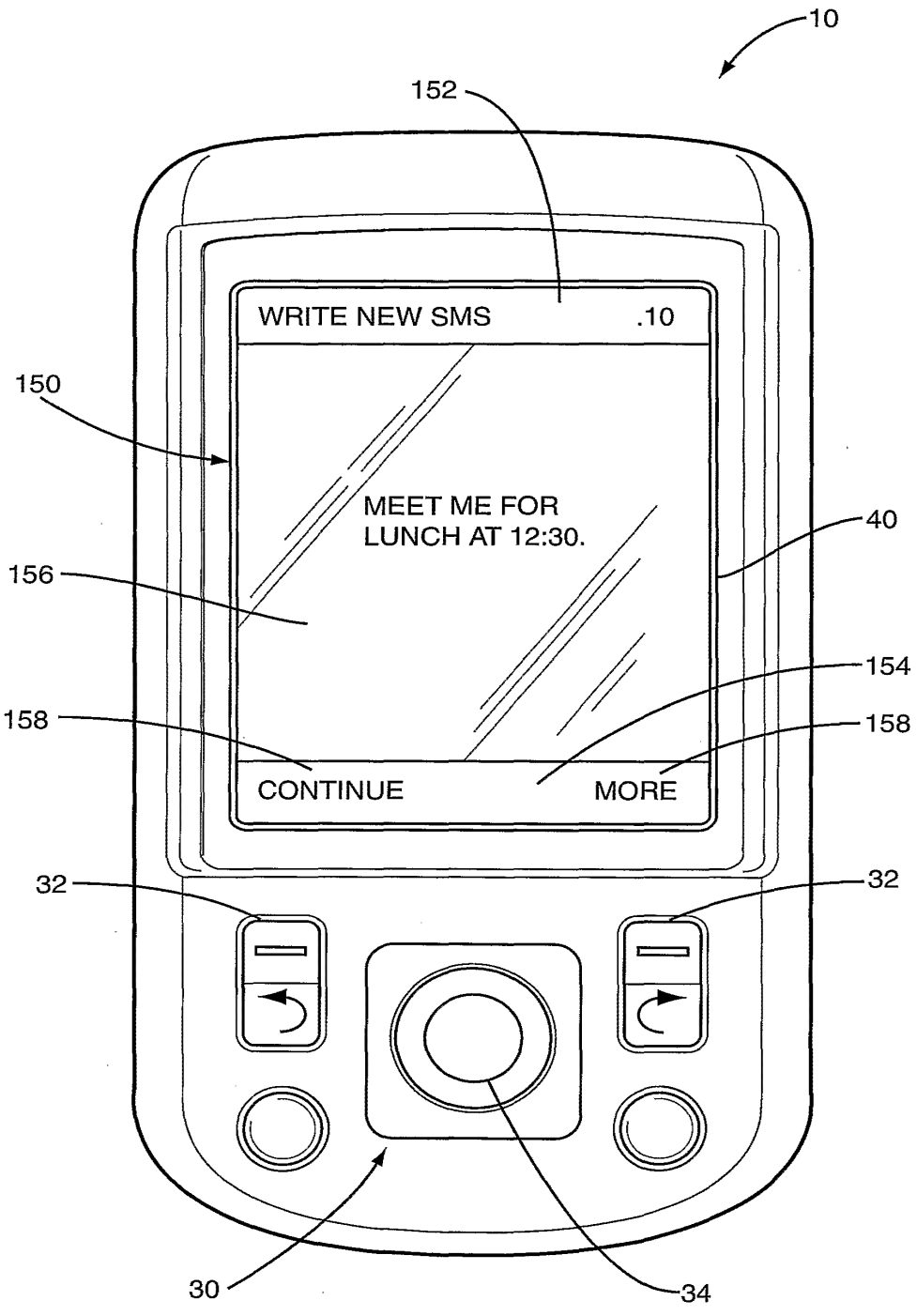


FIG. 2

IPR2025-01571
Apple EX1002 Page 764

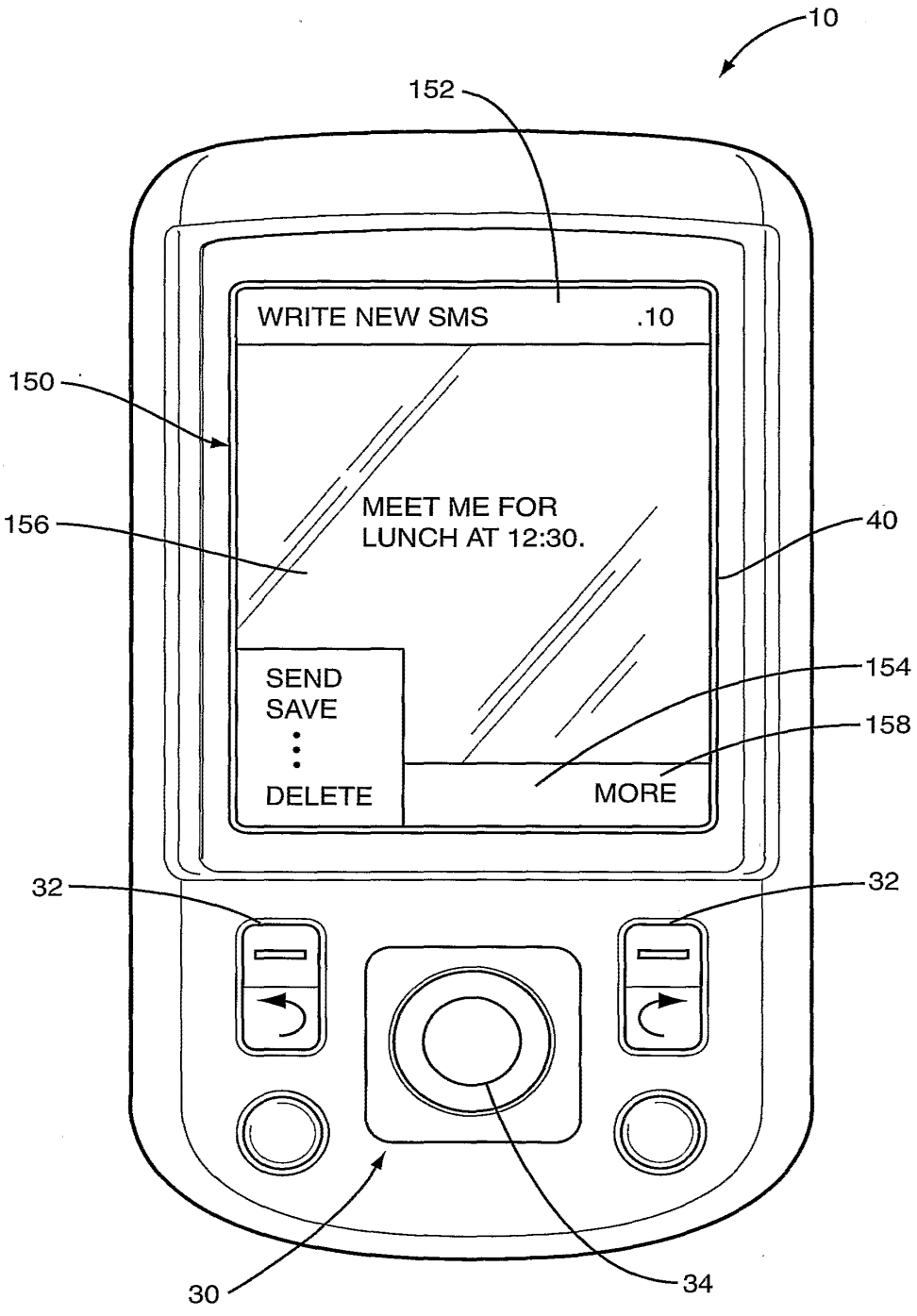


FIG. 3A

IPR2025-01571
Apple EX1002 Page 765

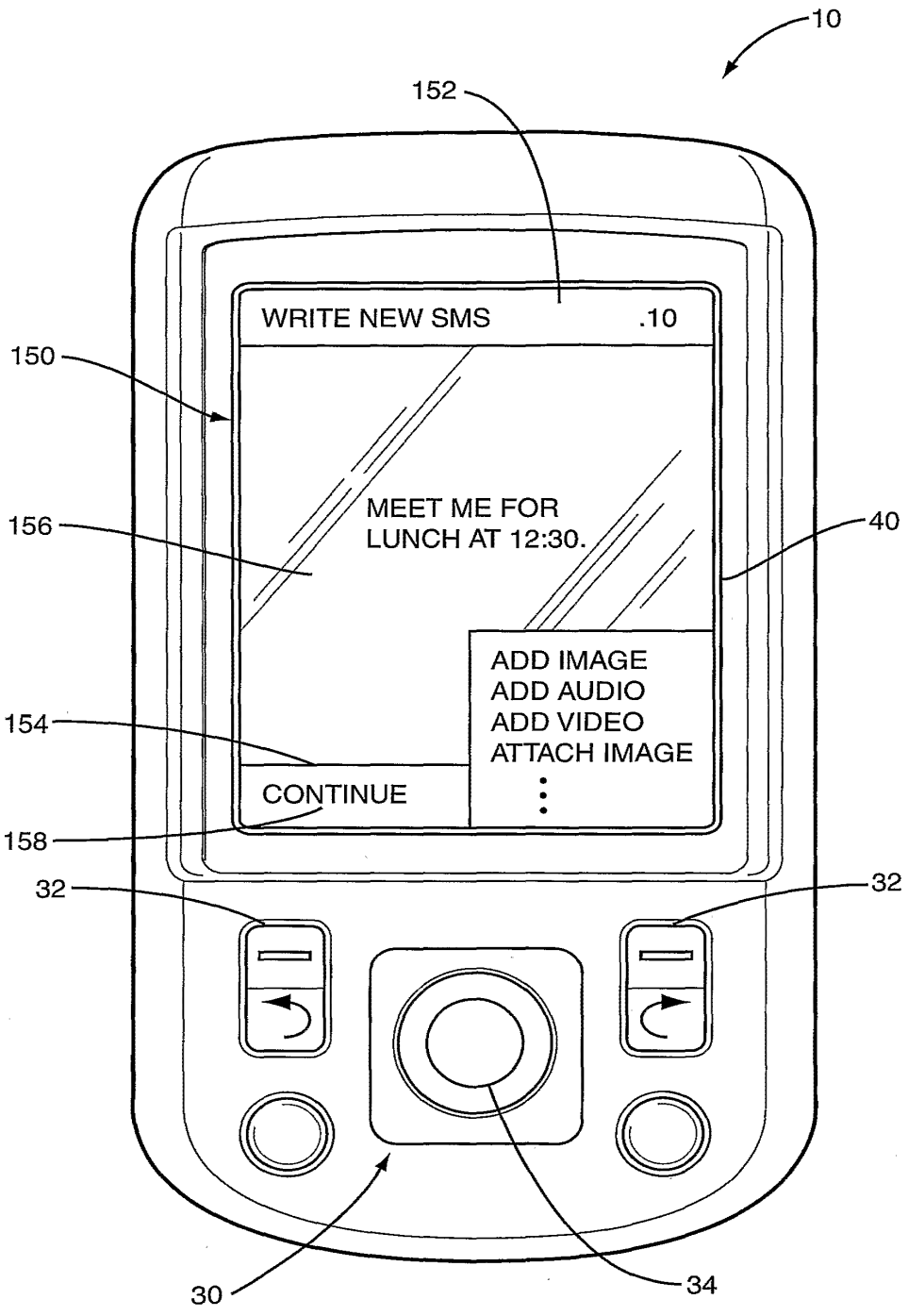


FIG. 3B

IPR2025-01571
Apple EX1002 Page 766

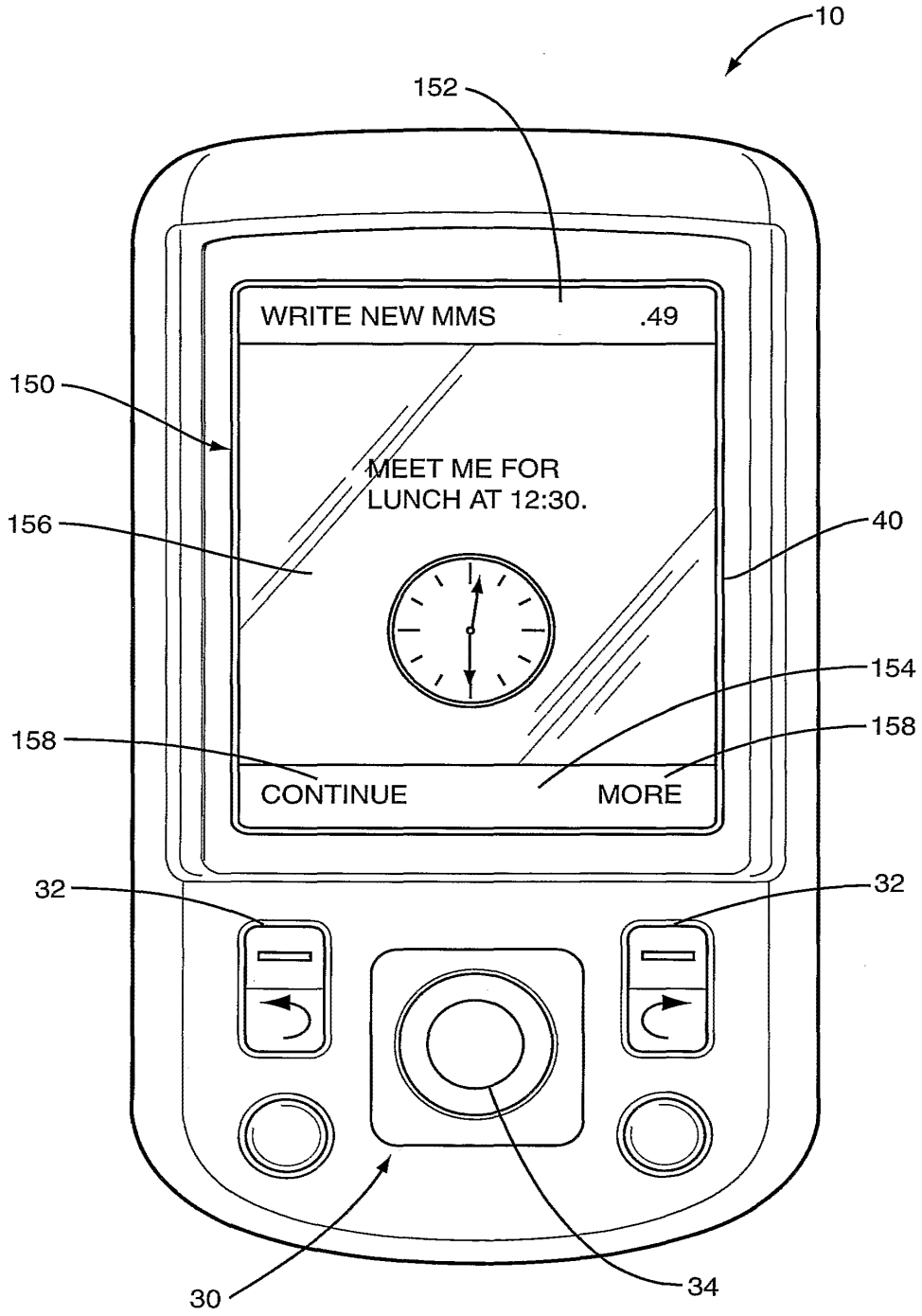


FIG. 4

IPR2025-01571
Apple EX1002 Page 767

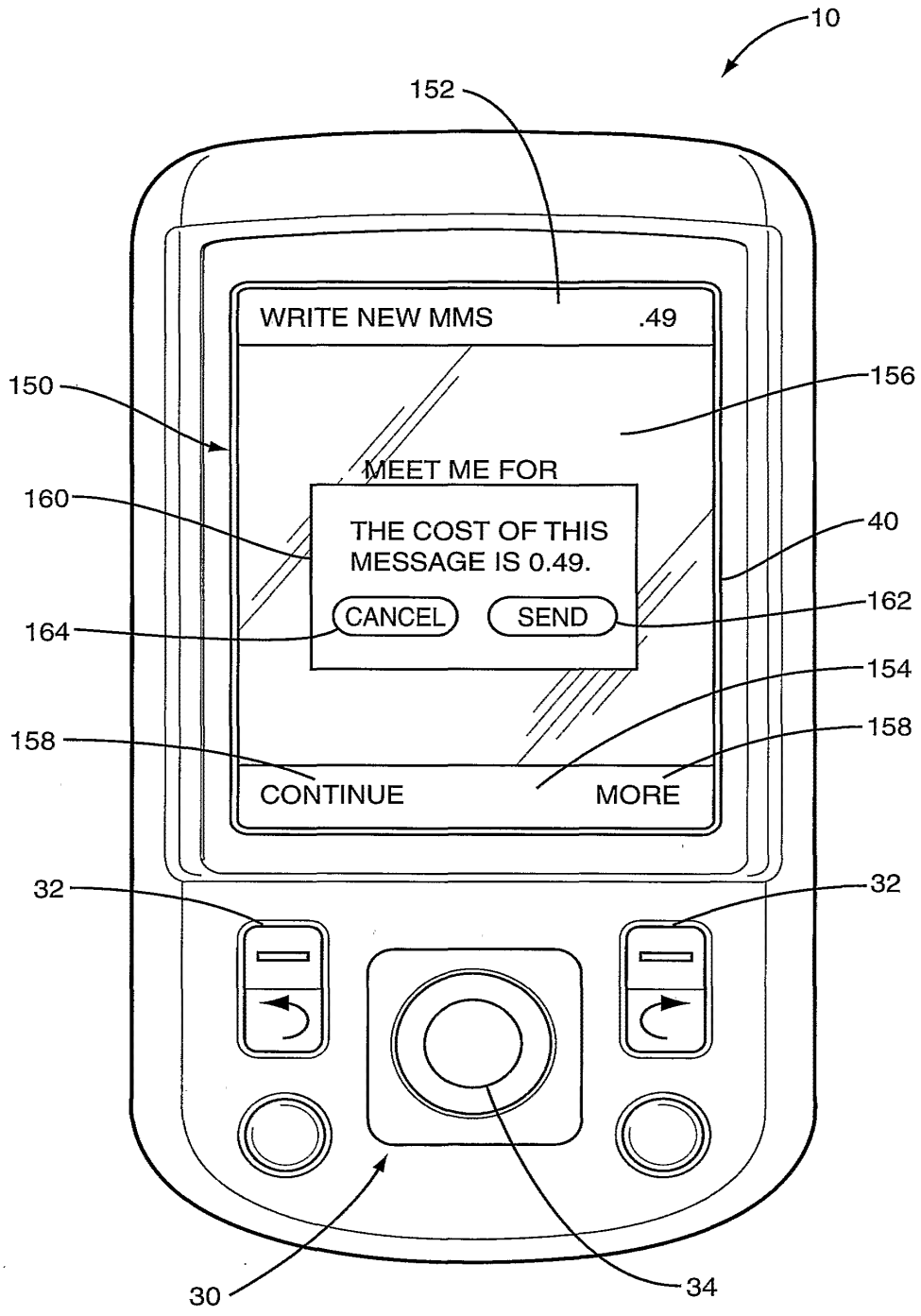


FIG. 5

IPR2025-01571
Apple EX1002 Page 768

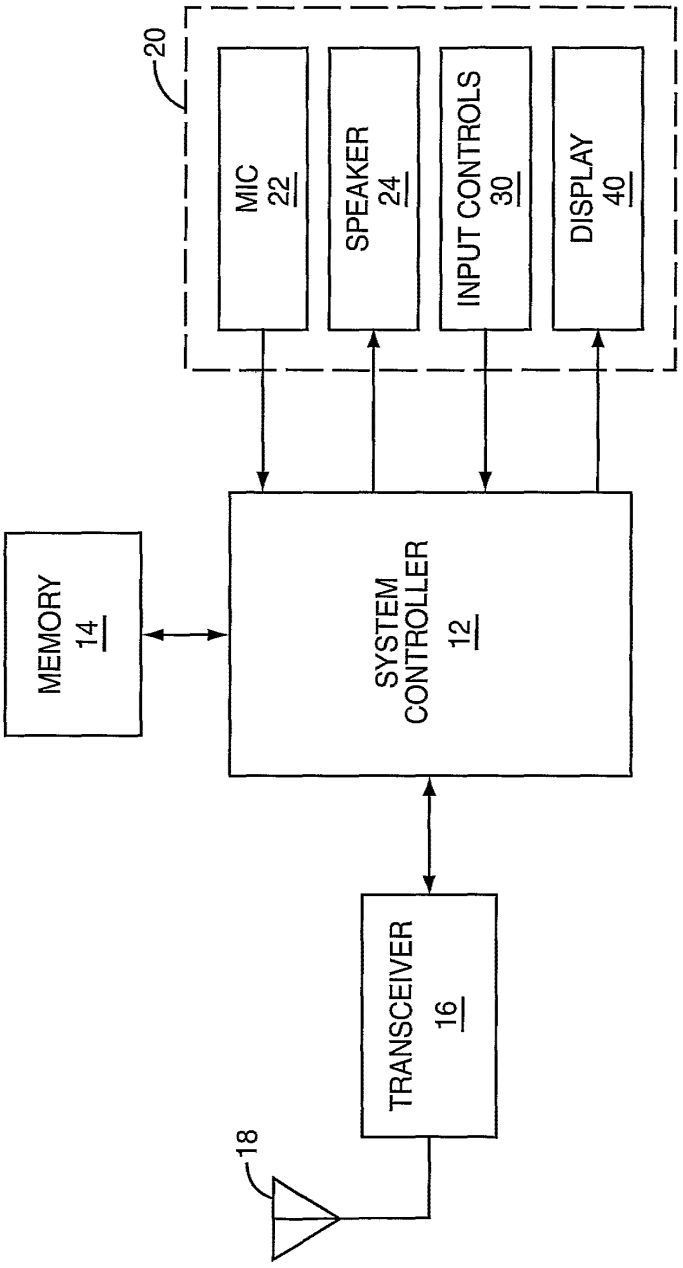


FIG. 6

IPR2025-01571
Apple EX1002 Page 769

```
<?xml version="1.0"?>
<message-price-table>
     <service name="SMS">
          <schemes>
               <scheme>
                    <time-of-day start="0600" end="2100"/>
                    <applies-to>message</applies-to>
                    <price>0.10</price>
                    <roaming-surcharge>0.25</roaming-surcharge>
               </scheme>
               <scheme>
                    <time-of-day start="2100" end="0600"/>
                    <applies-to>message</applies-to>
                    <price>0.00</price>
                    <roaming-surcharge>0.25</roaming-surcharge>
               </scheme>

          </schemes>
     </service>
     <service name="IMS">
          <schemes>
               <scheme>
                    <applies-to>monthly</applies-to>
                    <price>6.00</price>
               </scheme>
          </schemes>
     </service>
     <service name="MMS">
          <schemes>
               <scheme>
                    <applies-to>monthly</applies-to>
                    <price>6.00</price>
               </scheme>
               <scheme>
                    <applies-to>kilobytes</applies-to>
                    <price>0.02</price>
               </scheme>
          </schemes>
     </service>
</message-price-table>
```

FIG. 7

IPR2025-01571
Apple EX1002 Page 770

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2006/041665

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04M15/28

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)
H04M H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2001/038625 A1 (SATOH KAZUNORI [JP]) 8 November 2001 (2001-11-08) abstract figures 1a,1ab,1c,2 paragraphs [0023] - [0034] claims 1-3	1-41
X	US 2004/122684 A1 (KAIKURANTA TERHO [FI]) 24 June 2004 (2004-06-24) figures 2-10 paragraphs [0011] - [0015] paragraphs [0045] - [0079] claims 1-27	1-41

-/--

[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 document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
27 April 2007	09/05/2007

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Maciejewski, Robert

Form PCT/ISA/210 (second sheet) (April 2005)

IPR2025-01571
Apple EX1002 Page 771

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2006/041665

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2005/046197 A (GIESECKE & DEVRIENT GMBH [DE]; LEINEWEBER HARALD [DE]; RANKL WOLFGANG) 19 May 2005 (2005-05-19) abstract page 3, lines 4-28 page 5, line 26 - page 11, line 18 figures 1,2	1-41

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

IPR2025-01571
Apple EX1002 Page 772

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2006/041665

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2001038625 A1	08-11-2001	GB 2365663 A	20-02-2002
		JP 3397196 B2	14-04-2003
		JP 2001257719 A	21-09-2001
US 2004122684 A1	24-06-2004	CN 1520088 A	11-08-2004
WO 2005046197 A	19-05-2005	DE 10351763 A1	09-06-2005

Form PCT/ISA/210 (patent family annex) (April 2005)

Electronic Patent Application Fee Transmittal	
Application Number:	13705055
Filing Date:	04-Dec-2012
Title of Invention:	AUTOMATED DEVICE PROVISIONING AND ACTIVATION
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Filer:	Krista Susan Jacobsen/Ann Taylor
Attorney Docket Number:	RALEP007C03
Filed as Large Entity	

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
		Total in USD ($)		**180**

Electronic Acknowledgement Receipt	
EFS ID:	16791537
Application Number:	13705055
International Application Number:	
Confirmation Number:	3375
Title of Invention:	AUTOMATED DEVICE PROVISIONING AND ACTIVATION
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	Krista Susan Jacobsen/Ann Taylor
Filer Authorized By:	Krista Susan Jacobsen
Attorney Docket Number:	RALEP007C03
Receipt Date:	07-SEP-2013
Filing Date:	04-DEC-2012
Time Stamp:	02:33:20
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$180
RAM confirmation Number	7665
Deposit Account	505876
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees) Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees) Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	P007C03.pdf	2070016 99e4f435c5586104f5c5d370e3c115933725ac30	no	11
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
2	Foreign Reference	2035_SONERA.pdf	1449270 83f568206d53812bd422a23bc97d8efdc212af6a	no	36
Warnings:					
Information:					
3	Foreign Reference	2036_SONY.pdf	831108 a6a0c393147acb9517804ca2ded34f2a1d36d44c	no	22
Warnings:					
Information:					
4	Non Patent Literature	3025_ANTON.PDF	608012 129dd45630f651b9102a169bcfd96b3eb3641016	no	37
Warnings:					
Information:					
5	Non Patent Literature	5094_P007C4OAR.pdf	1772633 f55e8494d2afc97f5b2239e9a45f5acf6ba5c554	no	37
Warnings:					
Information:					
6	Fee Worksheet (SB06)	fee-info.pdf	30272 8bca9fcf3ddada286ba2cfe9d4954d26d27b4168	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	6761311		

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.
13/705,055	12/04/2012	Gregory G. Raleigh	RALEP007C03	3375

106963 7590 09/10/2013

Headwater Partners I LLC
350 Marine Parkway, Suite 300
Redwood Shores, CA 94065

EXAMINER	
RUDY, ANDREW J	
ART UNIT	PAPER NUMBER
3687	

NOTIFICATION DATE	DELIVERY MODE
09/10/2013	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

IPR2025-01571
Apple EX1002 Page 779

Office Action Summary for Applications Under Accelerated Examination	**Application No.** 13/705,055	**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 --

***Since this application has been granted special status under the accelerated examination program, NO extensions of time under 37 CFR 1.136(a) will be permitted and a SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE:* ONE MONTH OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION – if this is a non-final action or a *Quayle* action.**

(Examiner: For **FINAL** actions, please use PTOL-326.)

The objective of the accelerated examination program is to complete the examination of an application within twelve months from the filing date of the application. Any reply must be filed electronically via EFS-Web so that the papers will be expeditiously processed and considered. If the reply is not filed electronically via EFS-Web, the final disposition of the application may occur later than twelve months from the filing of the application.

Status

1)☒ Responsive to communication(s) filed on *29 July 2013*.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

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

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

Disposition of Claims

4)☒ Claim(s) *1-28,31 and 32* is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28,31 and 32* is/are rejected.

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

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

* If any claims have been determined allowable, 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.

Application Papers

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

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

11)☐ 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)).

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

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

IPR2025-01571
Apple EX1002 Page 780

DETAILED ACTION

Election/Restrictions

1. Applicant's election of Group I in the reply filed on July 29, 2013 is acknowledged. Applicant cancelled claims 29 and 30. Applicant added 31 and 32. Thus, claims 1-28, 31 and 32 are pending.

Claim Rejections - 35 USC § 112

2. The following is a quotation of 35 U.S.C. 112(b):

> (b) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

> The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:
> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 1-28, 31 and 32 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention.

Claim 1, lines 3-4, "a first set of one or more wireless networks" is not clear in juxtaposition to the drawing figures and descriptive portion of the specification.

Claim 1, lines 21-22, "at least a portion of the message payload for delivery to the end-user device" is not clear in juxtaposition to the drawing figures and descriptive portion of the specification.

Claim 27, lines 3-4, “a first set of one or more wireless networks” is not clear in juxtaposition to the drawing figures and descriptive portion of the specification.

Claim 27, line 21, “at least a portion of the message payload for delivery to the end-user device” is not clear in juxtaposition to the drawing figures and descriptive portion of the specification.Clarification is required.

Claim Rejections - 35 USC § 103

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

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

5. Claims 1-28, 31 and 32, as understood, are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Falk et al., US 8,495,360 in view of Maes, US 7,546,460.

Falk discloses, e.g. Figs. 1-4 and related text, networks, a wireless device, e.g. MP-A, MP-B, a server message, e.g. col. 4, lines 46-55, encryption protocols, e.g. cols. 3-5, lines 16-40, servers, e.g. cols. 8-9, and a link to a server, e.g. cols. 5-6, lines 55-16. Falk does not explicitly disclose the terminology of a message payload.

Maes discloses, e.g. Figs. 1-6 and related text,a wireless network having a message payload and encryption protocols, e.g. col. 10, lines 56-67. To have provided such for Falk would have been obvious to one of ordinary skill in the art in view of Maes.

The motivation for having done such would have been implementing common knowledge message payloads associated with wireless transmission of data.

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

7. Applicant's seven Information Disclosure Statements (IDS's) have been reviewed. Note the attached IDS's.

8. 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, Matthew S. Gart can be reached on 571-272-3955. 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. 13/705,055	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	Classification
*	A	US-8,521,110	08-2013	Rofougaran, Ahmadreza	455/168.1
*	B	US-8,520,589	08-2013	Bhatt et al.	370/328
*	C	US-8,495,360	07-2013	Falk et al.	713/155
*	D	US-8,379,847	02-2013	Bell et al.	380/44
*	E	US-8,122,249	02-2012	Falk et al.	713/168
*	F	US-7,940,751	05-2011	Hansen, Christopher J.	370/354
*	G	US-7,921,463	04-2011	Sood et al.	726/26
*	H	US-7,546,460	06-2009	Maes, Stephane H.	713/168
*	I	US-7,356,011	04-2008	Waters et al.	370/338
*	J	US-7,310,424	12-2007	Gehring et al.	380/277
*	K	US-6,542,992	04-2003	Peirce et al.	713/153
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

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

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

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	13705055
Filing Date	2012-12-04
First Named Inventor	Raleigh, Gregory G.
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP007C3

U.S.PATENTS

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	8135388		2012-03-13	Gailloux, Michael A. et al.	
	2	6947723		2005-09-20	Gurnani, Roger et al.	
	3	8350700		2013-01-08	Fast, Raymond D. et al.	
	4	8204190		2012-06-19	Bang, Jung-Hee et al.	
	5	7962622		2011-06-14	Friend, John et al.	
	6	7583964		2009-09-01	Wong, Gregory A.	
	7	7565141		2009-07-21	Macaluso, Anthony G.	
	8	7373179		2008-05-13	Stine, Ted 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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C3

	9	7236780		2007-06-26	Benco, David S. et al.	
	10	7039403		2006-05-02	Wong, Gregory A.	
	11	7865182		2011-01-04	Macaluso, Anthony G.	
	12	8370477		2013-02-05	Short, Joel E. et al.	
	13	8364806		2013-01-29	Short, Joel E. et al.	
	14	8279067		2012-10-02	Berger, Thomas R. et al.	
	15	8213296		2012-07-03	Shannon, Frank M. et al.	
	16	8019868		2011-09-13	Rao, Goutham et al.	
	17	8005988		2011-08-23	Maes, Stephane H.	
	18	7978627		2011-07-12	Taylor, William Scott et al.	
	19	7711848		2010-05-04	Maes, Stephane 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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C3

	20	6782412		2004-08-24	Brophy, Kevin et al.	
	21	6081591		2000-06-27	Skoog, Frederick H.	
	22	6064878		2000-05-16	Denker, John Stewart et al.	
	23	7730123		2010-06-01	Erickson, Richard R. et al.	
	24	8024397		2011-09-20	Erickson, Richard R. et al.	
	25	8156206		2012-04-10	Kiley, Kevin J. et al.	
	26	8126722		2012-02-28	Robb, Terence Alan et al.	
	27	8291238		2012-10-16	GINTER, Karl L. et al.	
	28	8068824		2011-11-29	SHAN, Xueshan et al.	
	29	7228354		2007-06-05	CHAMBLISS, David Darden et al.	
	30	5283904		1994-02-01	CARSON, David G. 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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C3

	31	8208919		2012-06-26	KOTECHA, Lalit Ratilal	
	32	8185152		2012-05-22	GOLDNER, Alla	
	33	7844728		2010-11-30	ANDERSON, Thomas W. et al.	
	34	7873344		2011-01-18	BOWSER, Robert et al.	
	35	7856226		2010-12-21	WONG, Ellis L. et al.	
	36	7948952		2011-05-24	HURTTA, Tuija et al.	

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

U.S.PATENT APPLICATION PUBLICATIONS

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	20090299857		2009-12-03	Brubaker, Curtis M.	
	2	20090307746		2009-12-10	DI, Jinwen et al.	
	3	20050009499		2005-01-13	KOSTER, Karl	

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C3

FOREIGN PATENT DOCUMENTS

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

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

NON-PATENT LITERATURE DOCUMENTS

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

EXAMINER SIGNATURE

Examiner Signature	/Andrew Joseph Rudy/	Date Considered	09/05/2013

*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	13705055
Filing Date	2012-12-04
First Named Inventor	Raleigh, Gregory G.
Art Unit	2447
Examiner Name	not yet assigned
Attorney Docket Number	RALEP007C3

U.S.PATENTS

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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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		2012-09-26	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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.	

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

U.S.PATENT APPLICATION PUBLICATIONS

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

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.

FOREIGN PATENT DOCUMENTS

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	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		☐

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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		☐
	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.		☐

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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		☐
	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		☐

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

NON-PATENT LITERATURE DOCUMENTS

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

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	☐
	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	☐

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	☐
	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	☐

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	☐

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

EXAMINER SIGNATURE

Examiner Signature	/Andrew Joseph Rudy/	Date Considered	09/05/2013

*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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C03

U.S.PATENTS

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.

U.S.PATENT APPLICATION PUBLICATIONS

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
/A.R./	1	20100241544		2010-09-23	Benson, Dan et al.	
/A.R./	2	20090157792		2009-06-18	Fiatal, Trevor	

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

FOREIGN PATENT DOCUMENTS

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

NON-PATENT LITERATURE DOCUMENTS

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C03

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

EXAMINER SIGNATURE

Examiner Signature	/Andrew Joseph Rudy/	Date Considered	09/05/2013

*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.

Search Notes

Application/Control No.	Applicant(s)/Patent under Reexamination	
13/705,055	RALEIGH, GREGORY G.	
Examiner	**Art Unit**	
ANDREW JOSEPH RUDY	3687	

SEARCHED			
Class	Subclass	Date	Examiner
455	405-409, 414.1, 422.1,431, 432.1	9/5/2013	AJR
455	456.3	9/5/2013	AJR
709	224,225	9/5/2013	AJR
713	168	9/5/2013	AJR
726	7	9/5/2013	AJR
370	328,338	9/5/2013	AJR
370	354	9/5/2013	AJR

INTERFERENCE SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES (INCLUDING SEARCH STRATEGY)		
	DATE	EXMR
Continuity data reviewed.	9/5/2013	AJR
Inventor name search conducted.	9/5/2013	AJR
Bibliographic data updated.	9/5/2013	AJR

IPR2025-01571
Apple EX1002 Page 817

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. 3375

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
13/705,055	12/04/2012	705	3687	RALEP007C03

APPLICANTS

Gregory G. Raleigh, Woodside, CA;
HEADWATER PARTNERS I LLC, Redwood Shores, CA

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

This application is a CON of 12/380,780 03/02/2009
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 **
01/02/2013

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	30	3

ADDRESS

Headwater Partners I LLC
350 Marine Parkway, Suite 300
Redwood Shores, CA 94065
UNITED STATES

TITLE

AUTOMATED DEVICE PROVISIONING AND ACTIVATION

FILING FEE RECEIVED		
1783	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

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	13705055
Filing Date	2012-12-04
First Named Inventor	Raleigh, Gregory G.
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP007C03

U.S.PATENTS

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	6035281		2000-03-07	Crosskey, James P. et al.	
	2	6996393		2006-02-07	Pyhalammi, Seppo et al.	
	3	7760711		2010-07-20	Kung, Fen-Chung et al.	
	4	8000318		2011-08-16	Wiley, William L. et al.	
	5	8098579		2012-01-17	Ray, Amar N. et al.	
	6	8155670		2012-04-10	Fullam, Scott et al.	
	7	8374090		2013-02-12	Morrill, Robert J. et al.	
	8	7457265		2008-11-25	Julka, Vibhor 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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C03

	9	7729326		2010-06-01	Sekhar, Ramesh	
	10	7929973		2011-04-19	Zavalkovsky, Arthur et al.	
	11	7945945		2011-05-17	Graham, Richard et al.	
	12	8059530		2011-11-15	Cole, Terry L.	
	13	8266681		2012-09-11	Deshpande, Sumit B. et al.	
	14	8280354		2012-10-02	Smith, Christopher et al.	
	15	8331293		2012-12-11	Sood, Kapil	
	16	8019820		2011-09-13	Son, Giyeong et al.	
	17	8155155		2012-04-10	Chow, Albert T. et al.	
	18	8191116		2012-05-29	Gazzard, Daryl	
	19	6292828		2001-09-18	Williams, David 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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C03

	20	7043226		2006-05-09	Yamauchi, Toshiaki	
	21	7472189		2008-12-30	Mallya, Arvind R. et al.	
	22	7944948		2011-05-17	Chow, Albert T. et al.	
	23	8005009		2011-08-23	McKee, Neil et al.	
	24	7760861		2010-07-20	Croak, Marian et al.	
	25	8060463		2011-11-15	Spiegel, Joel R.	
	26	8224773		2012-07-17	Spiegel, Joel R.	
	27	8352980		2013-01-08	Howcroft, Jerald Robert	
	28	8386386		2013-02-26	Zhu, Kevin	
	29	8340718		2012-12-25	Colonna, Massimo et al.	
	30	8385896		2013-02-26	Proctor, Jr., James A. 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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C03

	31	8320949		2012-11-27	Matta, Sudheer Poorna Chandra	
	32	8279864		2012-10-02	Wood, Daniel M.	
	33	8271045		2012-09-18	Parolkar, Satish et al.	
	34	8233883		2012-07-31	De Froment, Eric	
	35	8224382		2012-07-17	Bultman, Michael J.	
	36	8184590		2012-05-22	Rosenblatt, Ariel	
	37	8174970		2012-05-08	Adamczyk, Maria et al.	
	38	8165576		2012-04-24	Raju, Vishwanath et al.	
	39	8073721		2011-12-06	Lewis, Lundy	
	40	8032899		2011-10-04	Archer, Charles J. et al.	
	41	7974624		2011-07-05	Gallagher, Michael 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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C03

	42	7907970		2011-03-15	Park, Vincent D. et al.	
	43	7778176		2010-08-17	Morford, Michael Robert|	
	44	7725570		2010-05-25	Lewis, Lundy	
	45	7634388		2009-12-15	Archer, Charles J. et al.	
	46	7633438		2009-12-15	Tysowski, Piotr Konrad	
	47	7593417		2009-09-22	Wang, James et al.	
	48	7551922		2009-06-23	Roskowski, Steve et al.	
	49	7545782		2009-06-09	Rayment, Stephen G. et al.	
	50	7802724		2010-09-28	Nohr, Steven Paul	
	51	7039037		2006-05-02	Wang, Jiwei R. et al.	
	52	6928280		2005-08-09	Xanthos, 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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C03

	53	6765925		2004-07-20	Sawyer, Wilson et al.	
	54	5889477		1999-03-30	Fastenrath, Ulrich	
	55	8447980		2013-05-21	Godfrey, James A. et al.	
	56	8429403		2013-04-23	Moret, Eric et al.	
	57	8411587		2013-04-02	Curtis, William et al.	
	58	8396929		2013-03-12	Helfman, Nadav et al.	
	59	8363658		2013-01-29	Delker, Jason R. et al.	
	60	8265004		2012-09-11	Toutonghi, Michael J.	
	61	8233895		2012-07-31	Tysowski, Piotr Konrad	
	62	7685254		2010-03-23	Pandya, Ashish A.	
	63	7181017		2007-02-20	Nagel, Robert H. 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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C03

	64	6965872		2005-11-15	Grdina, Jerome M.	
	65	8402540		2013-03-19	Kapoor, Harsh et al.	
	66	8135657		2012-03-13	Kapoor, Harsh et al.	
	67	8271992		2012-09-18	Chatley, Scott P. et al.	
	68	8315999		2012-11-20	Chatley, Scott P. et al.	
	69	8332375		2012-12-11	Chatley, Scott P. et al.	
	70	8468337		2013-06-18	Gaur, Santosh P. et al.	
	71	8477778		2013-07-02	Lehmann, Jr., L. Curtis et al.	
	72	6640097		2003-10-28	Corrigan, Louis et al.	

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

U.S.PATENT APPLICATION PUBLICATIONS

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

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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C03

	1	20080120668		2008-05-22	Yau, Frank Chuen-Foo	
	2	20030171112		2003-09-11	Lupper, Alfred et al.	
	3	20070300252		2007-12-27	Acharya, Swarup et al.	
	4	20050007993		2005-01-13	Chambers, Mahdi et al.	
	5	20020164983		2002-11-07	Raviv, Li-On et al.	
	6	20070280453		2007-12-06	Kelley, Sean S. et al.	

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

FOREIGN PATENT DOCUMENTS

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	1889777A	CN		2006-07-19	Huawei Tech. Co. Ltd.		☐
	2	101155343A	CN		2006-09-29	Huawei Tech. Co. Ltd.		☐
	3	101035308A	CN		2006-03-09	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C03

	4	2007124279	WO		2007-11-01	Cisco Technology, Inc.		☐
	5	2005008995	WO		2005-01-27	Starhub Ltd.		☐

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

NON-PATENT LITERATURE DOCUMENTS

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	2013-05-09 Non-Final Rejection in U.S. Application No. 13/712,184, filed December 12, 2012 and entitled "Automated Device Provisioning and Activation"	☐
	2	2012-10-03 Non-Final Rejection in U.S. Application No. 13/461,141, filed May 1, 2012 and entitled "Automated Device Provisioning and Activation"	☐
	3	2012-10-15 Amendment-Req. Reconsideration-After Non-Final Rejection in U.S. Application No. 13/461,141, filed May 1, 2012 and entitled "Automated Device Provisioning and Activation"	☐

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

EXAMINER SIGNATURE

Examiner Signature	/Andrew Joseph Rudy/	Date Considered	09/05/2013

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

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

EFS Web 2.1.17

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

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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

U.S.PATENTS						
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	7957020		2011-06-07	Mine, Ryuta et al.	
	2	7346410		2008-03-18	Uchiyama, Kenji	
	3	7167078		2007-01-23	Pourchot, Shawn C.	
	4	8102814		2012-01-24	Rahman, Shahriar I. et al.	
	5	7970350		2011-06-28	Sheynman, Arnold et al.	
	6	8094551		2012-01-10	Huber, Kurt Donald et al.	
If you wish to add additional U.S. Patent citation information please click the Add button.						
U.S.PATENT APPLICATION PUBLICATIONS						
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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	1	20010053694		2001-12-20	Igarashi, Yoichiro et al.	
	2	20100041364		2010-02-18	Lott, Robert Wayne et al.	
	3	20100027469		2010-02-04	Gurajala, Ravindra Babu et al.	

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

FOREIGN PATENT DOCUMENTS

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

NON-PATENT LITERATURE DOCUMENTS

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

EXAMINER SIGNATURE

Examiner Signature	/Andrew Joseph Rudy/	Date Considered	09/05/2013

*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.

EFS Web 2.1.17

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	13705055
Filing Date	2012-12-04
First Named Inventor	Raleigh, Gregory G.
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP007C3

U.S.PATENTS

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	6754470		2004-06-22	Hendrickson, Keith et al.	
	2	8122128		2012-02-21	Burke, II, Robert M. et al.	
	3	8149823		2012-04-03	Turcan, Diane Brown et al.	
	4	8131256		2012-03-06	Martti, Jyrki et al.	
	5	6381316		2002-04-30	Joyce, Simon James et al.	
	6	7965983		2011-06-21	Swan, Tim et al.	
	7	8284740		2012-10-09	O'Connor, Dennis M.	
	8	8116223		2012-02-14	Tian, Dan 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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C3

	9	6154738		2000-11-28	Call, Charles Gainor	
	10	8423016		2013-04-16	Buckley, Adrian et al.	

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

U.S.PATENT APPLICATION PUBLICATIONS

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	20110173678		2011-07-14	Kaippallimalil, John et al.	
	2	20080235511		2008-09-25	O'Brien, William G. et al.	
	3	20080240373		2008-10-02	Wilhelm, Robert D.	
	4	20100027559		2010-02-04	LIN, Hung-Ming et al.	
	5	20020116338		2002-08-22	Gonthier, Jean-Charles et al.	
	6	20070061878		2007-03-15	Hagiu, Costin et al.	
	7	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP007C3

	8	20040203755		2004-10-14	Brunet, Jeffrey et al.	
	9	20090172077		2009-07-02	Roxburgh, David et al.	
	10	20080051076		2008-02-28	O'Shaughnessy, John et al.	
	11	20080313730		2008-12-18	Iftimie, Sorin et al.	

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

FOREIGN PATENT DOCUMENTS

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	2006120558A1	WO		2006-11-16	Nokia Corp.		☐

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

NON-PATENT LITERATURE DOCUMENTS

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

EXAMINER SIGNATURE

Examiner Signature	/Andrew Joseph Rudy/	Date Considered	09/05/2013

*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.

EFS Web 2.1.17

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	13705055
Filing Date	2012-12-04
First Named Inventor	Raleigh, Gregory G.
Art Unit	2447
Examiner Name	not yet assigned
Attorney Docket Number	RALEP007C3

U.S.PATENTS

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.

U.S.PATENT APPLICATION PUBLICATIONS

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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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.	

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

FOREIGN PATENT DOCUMENTS

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

NON-PATENT LITERATURE DOCUMENTS

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

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

EXAMINER SIGNATURE

Examiner Signature	/Andrew Joseph Rudy/	Date Considered	09/05/2013

*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./

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Raleigh	Examiner:	RUDY, Andrew J.
Serial No.:	13/705,055	Art Unit:	3687
Filed:	December 4, 2012	Conf. No.:	3375
Title:	Automated Device Provisioning and Activation		

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

AMENDMENT AND RESPONSE

Madam:

In response to the Office Action dated September 10, 2013, the deadline for response being October 10, 2013, please amend the above-identified application as follows:

Amendments to the Claims begin on page 2.

Remarks begin on page 9.

IPR2025-01571
Apple EX1002 Page 854

AMENDMENTS TO THE CLAIMS

Without prejudice and without surrender of any subject matter, please amend the claims as follows:

1. (Currently amended) A method performed by a network system, the method comprising:

providing a first service control link to a first end-user device communicatively coupled to the network system over a first set of one or more wireless networks, the first service control link secured at least in part by at least a first encryption protocol, the first service control link for supporting **first** control-plane communications between the network system and the first end-user device, the first end-user device comprising a first set of two or more device agents, the first set of two or more device agents including a particular device agent;

providing a second service control link to a second end-user device communicatively coupled to the network system over a second set of one or more wireless ~~access~~ networks, the second set of one or more wireless ~~access~~ networks being the same as or different from the first set of one or more wireless ~~access~~ networks, the second service control link secured at least in part by at least a second encryption protocol, the second encryption protocol being the same as or different from the first encryption protocol, the second service control link for supporting **second** control-plane communications between the network system and the second end-user device, the second end-user device comprising a second set of two or more device agents;

receiving a server message from a particular server of a plurality of servers communicatively coupled to the network system, the server message comprising message payload, at least a portion of the message payload for delivery to the first end-user device;

generating an encrypted message comprising the at least a portion of the message payload and an identifier**, the identifier** identifying the particular device agent, the identifier **for** ~~configured to~~ assist**ing** in delivering the at least a portion of the message payload to the particular device agent; and

sending the encrypted message to the first end-user device over the first service control link.

2. (Previously presented) The method of claim 1, wherein the particular server comprises a service usage server, a policy management server, an access control integrity server, a network

IPR2025-01571
Apple EX1002 Page 855

traffic analysis server, a beta test server, a service download control server, a billing event server, an activation server, a transaction server, an authentication server, or a content management server.

3. (Previously presented) The method of claim 1, wherein the at least a portion of the message payload comprises information associated with a service usage or cost.

4. (Currently amended) The method of claim 3, wherein the information associated with a service usage or cost comprises a service usage value, a projected service usage value, a service ~~usage~~ plan limit, a projected service usage overage warning, a projected service cost overage warning, a service plan period time duration, a service plan time remaining before end of period, or information about a service overage.

5. (Previously presented) The method of claim 1, wherein the at least a portion of the message payload is based, at least in part, on a user preference.

6. (Previously presented) The method of claim 1, wherein the at least a portion of the message payload comprises at least an aspect of: a service offer, an advertisement, or a transaction offer.

7. (Currently amended) The method of claim 1, wherein the at least a portion of the message payload comprises a**n** ~~**device agent**~~ instruction **for a first device agent in the first set of two or more device agents**, a setting, **a** ~~**an agent**~~ configuration **for the first device agent in the first set of two or more device agents**, or a software update for the particular device agent.

8. (Previously presented) The method of claim 1, wherein the at least a portion of the message payload comprises information associated with software or a media file.

9. (Previously presented) The method of claim 1, wherein the at least a portion of the message payload comprises information associated with a service policy.

IPR2025-01571
Apple EX1002 Page 856

10. (Previously presented) The method of claim 1, wherein the at least a portion of the message payload comprises an indication of additional data or information available to the particular device agent.

11. (Currently amended) The method of claim 1, wherein the at least a portion of the message payload is configured to assist in causing the first end-user device to present, through a user interface **of the first end-user device**, information associated with the at least a portion of the message payload.

12. (Currently amended) The method of claim 1, wherein the server message is a first server message, and wherein the message payload is a first message payload, and wherein the identifier ~~**identifying the particular device agent**~~ is a first identifier, and further comprising receiving a second server message from the particular server or from another server of the plurality of servers communicatively coupled to the network system, the second server message comprising second message payload, and wherein the encrypted message further comprises at least a portion of the second message payload and a second identifier**, the second identifier for** ~~**configured to**~~ assist**ing** in delivering the at least a portion of the second message payload to a second device agent of the first set of two or more device agents, the second device agent being the particular device agent or another device agent of the first set of two or more device agents.

13. (Currently amended) The method of claim 1, wherein the server message is a first server message, and wherein the particular server is a first server, and wherein the message payload is first message payload, and wherein the particular device agent is a first device agent, and wherein the encrypted message is a first encrypted message, and wherein the identifier is a first identifier, and further comprising:

receiving a second server message from a second server of the plurality of servers communicatively coupled to the network system, the second server message comprising second message payload, at least a portion of the second message payload for delivery to the first end-user device;

generating a second encrypted message comprising the at least a portion of the second message payload and a second identifier**, the second identifier for** ~~**configured to**~~ assist**ing** the

IPR2025-01571
Apple EX1002 Page 857

first end-user device in delivering the at least a portion of the second message payload to a second device agent of the first set of two or more device agents; and

sending the second encrypted message to the first end-user device over the first service control link.

14. (Previously presented) The method of claim 1, wherein the first service control link supports asynchronous transmissions by the network system.

15. (Previously presented) The method of claim 1, further comprising sending a credential, a certificate, or a token to the first end-user device or obtaining the credential, the certificate, or the token from the first end-user device during a service authorization sequence.

16. (Previously presented) The method of claim 15, wherein the credential comprises a phone number, an identification number, a security signature, a security credential, a subscriber identity module (SIM) identifier, a mobile equipment identifier (MEID), or a device identifier.

17. (Previously presented) The method of claim 1, wherein the particular device agent comprises software.

18. (Previously presented) The method of claim 1, further comprising:

triggering a transmission to maintain the first service control link when a time since sending the encrypted message to the first end-user device would otherwise cause the first service control link to terminate.

19. (Previously presented) The method of claim 1, wherein the sending the encrypted message to the first end-user device over the first service control link is not based on whether the particular device agent is running on the first end-user device.

20. (Previously presented) The method of claim 1, wherein the particular server comprises a content transaction server configured to provide an electronic commerce offering and transaction platform to the first end-user device.

IPR2025-01571
Apple EX1002 Page 858

21. (Canceled)

22. (Previously presented) The method of claim 1, wherein a transmission over the first service control link is within an ambient service, the ambient service being provided at no cost to a user or a subscriber associated with the first end-user device.

23. (Previously presented) The method of claim 1, wherein the first service control link enables the particular server to push the at least a portion of the message payload to the particular device agent.

24. (Canceled)

25. (Previously presented) The method of claim 1, wherein providing the first service control link to the first end-user device comprises providing the first service control link to a service control device link agent on the first end-user device, the service control device link agent for delivering agent messages over an agent communication bus to at least the particular device agent.

26. (Previously presented) The method of claim 25, wherein the encrypted message is a first encrypted message, and wherein the identifier is configured to assist the service control device link agent in generating a second encrypted message for delivery to the particular device agent, the second encrypted message comprising the at least a portion of the message payload.

27. (Currently amended) A network system, comprising:

means for providing a first service control link to a first end-user device communicatively coupled to the network system over a first set of one or more wireless networks, the first service control link secured at least in part by at least a first encryption protocol, the first service control link for supporting **first** control-plane communications between the network system and the first end-user device, the first end-user device comprising a first set of two or more device agents, the first set of two or more device agents including a particular device agent;

IPR2025-01571
Apple EX1002 Page 859

means for providing a second service control link to a second end-user device communicatively coupled to the network system over a second set of one or more wireless ~~access~~ networks, the second set of one or more wireless ~~access~~ networks being the same as or different from the first set of one or more wireless ~~access~~ networks, the second service control link secured at least in part by at least a second encryption protocol, the second encryption protocol being the same as or different from the first encryption protocol, the second service control link for supporting **second** control-plane communications between the network system and the second end-user device, the second end-user device comprising a second set of two or more device agents;

means for receiving a server message from a particular server of a plurality of servers communicatively coupled to the network system, the server message comprising message payload, at least a portion of the message payload for delivery to the first end-user device;

means for generating an encrypted message comprising the at least a portion of the message payload and an identifier**, the identifier** identifying the particular device agent, the identifier **for ~~configured to~~** assist**ing** in delivering the at least a portion of the message payload to the particular device agent; and

means for sending the encrypted message to the first end-user device over the first service control link.

28-30. (Canceled)

31. (Previously presented) The method of claim 1, further comprising sending a credential, a certificate, or a token to the particular device agent or obtaining the credential, the certificate, or the token from the particular device agent during a service authorization sequence.

32. (Previously presented) The network system recited in claim 27, wherein the message payload comprises an indication of additional data or information available to the particular device agent.

33. (Currently amended) The network system recited in claim 27, wherein the message payload is configured to assist in causing the first end-user device to present, through a user interface **of**

IPR2025-01571
Apple EX1002 Page 860

the first end-user device, information associated with the at least a portion of the message payload.

34. (Previously presented) The network system recited in claim 27, further comprising means for sending a credential, a certificate, or a token to the particular end-user device or obtaining the credential, the certificate, or the token from the particular end-user device during a service authorization sequence.

35. (Previously presented) The network system recited in claim 27, wherein providing the first service control link to the first end-user device comprises providing the first service control link to a service control device link agent on the first end-user device, the service control device link agent for delivering agent messages over an agent communication bus to at least the particular device agent.

IPR2025-01571
Apple EX1002 Page 861

REMARKS

Claims 1-20, 22, 23, 25-27 and 31-35 are pending and stand rejected by the Office Action dated September 10, 2013.[1] Claims 21, 24, and 28-30 were previously canceled.

In section 3, the Office Action rejects claims 1-28, 31, and 32 [*sic*, claims 1-20, 22, 23, 25-27, and 31-35] under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the applicant regards as the invention.

In section 6, the Office Action rejects claims 1-28, 31, and 32 [*sic*, claims 1-20, 22, 23, 25-27, and 31-35] under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 8,495,360 to Falk *et al.* (hereinafter, "Falk") in view of U.S. Patent No. 7,546,460 to Maes (hereinafter, "Maes").

Applicant is amending claims 1, 4, 7, 11-13, 27, and 33. No new matter is being added.

Applicant respectfully requests reconsideration.

Claim Rejections – 35 U.S.C. § 112

In section 3, the Office Action rejects claims 1-28, 31, and 32 [*sic*, claims 1-20, 22, 23, 25-27, and 31-35] under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the applicant regards as the invention. In particular, the Office Action states that the phrases "a first set of one or more wireless networks" (lines 3-4 of claim 1, and lines 3-4 of claim 27) and "at least a portion of the message payload for delivery to the end-user device" (lines 21-22 of claim 1, and line 21 of claim 27) are not clear in juxtaposition to the drawing figures and descriptive portion of the specification.

---

[1] The Office Action states that claims 1-28, 31, and 32 are pending, but in Applicant's election of claims filed on July 31, 2013, Applicant elected claims 1-27, canceled claims 21, 24, and 28-30, and added claims 31-35. Thus, claims 1-20, 22, 23, 25-27 and 31-35 are now pending.

IPR2025-01571
Apple EX1002 Page 862

Applicant respectfully submits that "a first set of one or more wireless networks" is supported at least by paragraphs [00115]-[00118], [00121], [00123], [00125], and [00128], and by FIGS. 1-8. Applicant respectfully submits that "at least a portion of the message payload for delivery to the end-user device" is supported at least by paragraph [00327] and by FIG. 25.

Therefore, Applicant respectfully submits that all claims comply with 35 U.S.C. § 112, and Applicant respectfully requests that the rejection be withdrawn.

Claim Rejections – 35 U.S.C. § 103

In section 6, the Office Action rejects claims 1-28, 31, and 32 [*sic*, claims 1-20, 22, 23, 25-27, and 31-35] under 35 U.S.C. § 103(a) as being unpatentable over Falk in view of Maes.

Overview of Falk

Falk discloses a method for providing a wireless local network in which both stationary communication devices and mobile communication devices are connected as a sub-network in mesh form and connected to a first infrastructure network via a first communication device in such a way that they can exchange authentication messages with an authentication, authorization, and accounting (AAA) server in the first infrastructure network. Falk at col. 3, ll. 18-29. During a registration procedure, a first procedure is performed in which the first communication device in the role of an authenticator communicates with the AAA server when a second communication device is authenticating itself in the role of a supplicant. *Id.* at col. 3, ll. 29-34. The AAA server generates a set of basic encryption information for the sub-network, the basic encryption information relating to the second communication device and being transmitted to the first communication device. *Id* at col. 3, ll. 35-39. A second procedure is performed in which the first communication device in the role of a supplicant communicates with the second communication device without communicating with the AAA server, with authentication within the second procedure being conducted on the basis of at least some of the basic encryption information. *Id.* at col. 3, ll. 39-46.

According to Falk, the second procedure can take place without security material of another mesh node needing to be configured previously on that mesh node having no link to an

IPR2025-01571
Apple EX1002 Page 863

AAA server. *Id.* at col. 9, ll. 24-27. Thus, it is only necessary to be configured with security material that will enable it to authenticate itself with the central AAA server. *Id.* at col. 9, ll. 27-29. As a result, the AAA server need not be replicated on mesh nodes, which improves security. *Id.* at col. 9, ll. 31-40.

Overview of Maes

Maes discloses systems, methods, and devices for secure communications when a user is communicating with servers outside the wireless network, and the communications transmitted and received by the user's wireless communication device may need to be translated from one protocol to another. Maes at col. 1, ll. 8-11, 42-43. In order to prevent communications from being in the clear while protocol conversion takes place, applications executing on an application server and the wireless communication device may encrypt the payload or message portion of a communication before transmitting the communication. *Id.* at col. 5, ll. 20-25. Another portion of the communication may remain unencrypted so that it may be converted by an intermediate server to the protocol used by the application server (in the case of a message sent by the wireless communication device) or to the protocol used by the application on the wireless communication device (in the case of a message sent by the application server). *Id.* at col. 5, ll. 28-30, 45-54; col. 6, ll. 19-28; col. 10, l. 58 – col. 11, l. 4. Thus, the message or payload portion of the communication may remain encrypted when an intermediate server converts the unencrypted portion between protocols, and end-to-end security of communications sent between the application server and the wireless communication devices may be achieved. *Id.* at col. 5, ll. 32-37.

In the case of communications from an access device, such as wireless communication device, to an application server, the access device receives an encryption key and determines a portion of a communication to encrypt using a first encryption process. *Id.* at col. 3, ll. 50-53. The portion to encrypt may be determined by determining a payload portion or a message portion of the communication, or by determining at least one argument included in the communication, where the argument is shared by a first protocol and a second protocol. *Id.* at col. 1, l. 61 – col. 2, l. 1. An additional portion of the communication is also determined to remain unencrypted by the first encryption process. *Id.* at col. 1, ll. 53-55. The portion of the

IPR2025-01571
Apple EX1002 Page 864

communication is encrypted using the encryption key and the first encryption process, and the communication is then transmitted from the access device. *Id.* at col. 1, ll. 55-58. Transmitting the communication may comprise transmitting an e-mail that includes the encrypted portion and the additional portion, where the encrypted portion includes a message portion of the e-mail, and the additional portion includes commands associated with a mobile e-mail protocol. *Id.* at col. 2, ll. 1-6.

An intermediate server, such as a mobile enabling server, may receive the communication from the access device. *Id.* at col. 2, ll. 7-9; col. 4, ll. 32-35. The intermediate server may be responsible for translating communication between protocols used by the access device and an application server. *Id.* at col. 4, ll. 35-39. The intermediate server converts the additional portion of the communication from a first protocol to a second protocol without decrypting the encrypted portion. *Id.* at col. 2, ll. 9-12. For example, if the communication is an e-mail, converting the second portion may comprise converting the second portion from a mobile e-mail protocol to either an Internet Mail Access Protocol (IMAP) or Post Office Protocol (POP). *Id.* at col. 2, ll. 12-16. The intermediate server then transmits the communication, which includes the encrypted first portion and the converted second portion, to an application server. *Id.* at col. 2, ll. 16-19.

The application server includes an application that provides a service to clients. *Id.* at col. 4, ll. 65-66. The application server may include, for example, an e-mail server application, a database application, a calendar application, an address application, a voice-over-IP application. *Id.* at col. 4, l. 66 – col. 5, l. 2. The application server receives the communication and decrypts the first portion of the communication using a decryption key. *Id.* at col. 2, ll. 20-23.

Maes describes a similar procedure for communications from the application server to the access device. *See, e.g.,* col. 2, ll. 36-60; col. 10, l. 56 – col 11, l.4.

Claim 1

In rejecting claim 1, the Office Action states that Falk discloses, *e.g.*, Figs. 1-4 and related text, networks, a wireless device, *e.g.*, MP-A, MP-B, a server message, *e.g.*, col. 4, lines 46-55, encryption protocols, *e.g.*, cols. 3-5, lines 16-40, servers, *e.g.*, cols. 8-9, and a link to a

IPR2025-01571
Apple EX1002 Page 865

server, *e.g.*, cols. 5-6, lines 55-16. The Office Action acknowledges that Falk does not disclose a message payload, but the Office Action asserts that Maes fills this gap. In particular, the Office Action states that Maes discloses, *e.g.*, Figs. 1-6 and related text, a wireless network having a message payload and encryption protocols, *e.g.*, col. 10, lines 56-67. The Office Action states that to have provided such for Falk would have been obvious to one of ordinary skill in the art in view of Maes, and that the motivation for having done such would have been implementing common knowledge message payloads associated with wireless transmission of data.

Applicant respectfully submits that claim 1 is patentable over Falk in view of Maes at least because neither Falk nor Maes discloses several of the limitations of claim 1, and a rejection of a claim under 35 U.S.C. § 103 based on a combination of references cannot stand unless each of the limitations of the claim is disclosed by at least one of the references in the combination. MPEP § 2143(A) (35 U.S.C. § 103 rejection that combines references only proper if Examiner makes "a finding that the prior art included each element claimed, although not necessarily in a single prior art reference, with the only difference between the claimed invention and the prior art being the lack of actual combination of the elements in a single prior art reference."). If a claim recites a limitation X, and the Office Action combines references A and B in a rejection under 35 U.S.C. § 103, the claim limitation X must be present in at least one of the references for it to be present in the combination of references. In other words, a limitation that is not present in reference A or in reference B cannot be present in the combination of A and B, and a rejection of the claim under 35 U.S.C. § 103 based on the combination of references A and B necessarily fails.

Applicant respectfully submits that claim 1 is patentable over the combination of Falk and Maes at least because neither Falk nor Maes discloses at least "receiving a server message from a particular server of a plurality of servers communicatively coupled to the network system, the server message comprising message payload, at least a portion of the message payload for delivery to the first end-user device," "generating an encrypted message comprising the at least a portion of the message payload and an identifier, the identifier identifying the particular device agent, the identifier for assisting in delivering the at least a portion of the message payload to the particular device agent," or "sending the encrypted message to the first end-user device over the first service control link."

IPR2025-01571
Apple EX1002 Page 866

"receiving a server message from a particular server of a plurality of servers communicatively coupled to the network system, the server message comprising message payload, at least a portion of the message payload for delivery to the first end-user device"

Applicant respectfully submits that neither Falk nor Maes discloses a network system receiving a server message from a particular server of a plurality of servers communicatively coupled to the network system. Falk does not disclose this limitation because Falk does not disclose a plurality of servers communicatively coupled to a network system. Although Falk discloses a network system that includes a AAA server, Falk at col. 5, l. 67 – col. 6, l. 11, Falk does not disclose that the AAA server is communicatively coupled to a plurality of servers, nor does Falk disclose the AAA server receiving a message from a particular server of such a plurality of servers.

Maes likewise does not disclose a network system receiving a server message from a plurality of servers communicatively coupled to the network system. Maes discloses an application server that may provide its services to users of wireless communication devices by communicating with a mobile enabling server. Maes at col. 5, ll. 3-5. The mobile enabling server may need to convert communications that are sent to wireless communication devices from the application server between different protocols. *Id.* at col. 5, ll. 17-20. Assuming, *arguendo*, that the mobile enabling server is the network system recited in claim 1, Maes discloses that the mobile enabling server receives communications only from one server: the application server. Maes nowhere discloses that the mobile enabling server is communicatively coupled to any server other than the application server, or that it receives a message from any server other than the application server.

Thus, Applicant respectfully submits that neither Falk nor Maes discloses "receiving a server message from a particular server of a plurality of servers communicatively coupled to the network system, the server message comprising message payload, at least a portion of the message payload for delivery to the first end-user device." For at least this reason, Applicant respectfully submits that claim 1 is patentable over Falk in view of Maes.

IPR2025-01571
Apple EX1002 Page 867

"generating an encrypted message comprising the at least a portion of the message payload and an identifier, the identifier identifying the particular device agent, the identifier for assisting in delivering the at least a portion of the message payload to the particular device agent"

Applicant respectfully submits that neither Falk nor Maes discloses "generating an encrypted message comprising the at least a portion of the message payload and an identifier, the identifier identifying the particular device agent, the identifier for assisting in delivering the at least a portion of the message payload to the particular device agent." Falk does not disclose this limitation at least because Falk does not disclose "receiving a server message from a particular server of a plurality of servers communicatively coupled to the network system, the server message comprising message payload, at least a portion of the message payload for delivery to the first end-user device." Falk cannot disclose generating an encrypted message comprising at least a portion of a message payload that it did not receive and thus does not have available to it.

Moreover, if even Falk did disclose a network system receiving a server message from a particular server of a plurality of servers communicatively coupled to the network system—which, Applicant respectfully submits, it does not—Falk still would not disclose "generating an encrypted message comprising the at least a portion of the message payload and an identifier, the identifier identifying the particular device agent, the identifier for assisting in delivering the at least a portion of the message payload to the particular device agent" because Falk does not disclose an encrypted message comprising an identifier that identifies a particular device agent and assists in delivering the at least a portion of the message payload to the particular device agent. Indeed, Falk does not disclose that any node of the mesh network comprises two or more device agents. Thus, Falk does not disclose or contemplate that any encrypted message sent to a node comprises an identifier identifying a particular device agent.

Maes likewise does not disclose "generating an encrypted message comprising the at least a portion of the message payload and an identifier, the identifier identifying the particular device agent, the identifier for assisting in delivering the at least a portion of the message payload to the particular device agent." As explained above, Maes does not disclose "receiving a server message from a particular server of a plurality of servers communicatively coupled to the

IPR2025-01571
Apple EX1002 Page 868

network system, the server message comprising message payload, at least a portion of the message payload for delivery to the first end-user device." Consequently, Maes cannot disclose generating an encrypted message comprising at least a portion of a message payload that it did not receive.

Furthermore, Maes does not disclose that the intermediate server generates an encrypted message. Maes discloses that the intermediate server receives a communication that includes an already-encrypted portion and an unencrypted portion, where the unencrypted portion is converted to the protocol used by the element that will be receiving the communication from the intermediate server. Maes at col. 5, ll. 20-30. Maes is clear that the intermediate server operates only on the unencrypted portion of the communication. *See, e.g., id.* at col. 5, ll. 32-37 (message/payload portion of communication remains encrypted when mobile e-mail enabling server converts unencrypted portion between protocols). Indeed, Maes's objective is for the intermediate server to perform the protocol conversion without disturbing the encrypted portion of the communication. *Id.* at col. 1, ll. 33-38; col. 5, ll. 20-25. Therefore, the intermediate server does not generate an encrypted message.

Moreover, Maes does not disclose that any communication from the intermediate server comprises an identifier that identifies a particular device agent and assists in delivering the at least a portion of the message payload to the particular device agent. Maes discloses that the intermediate server converts communications sent to a wireless communication device by an application server between different protocols. *Id.* at col. 5, ll. 17-20. As an example, Maes discloses that the intermediate server may be a mobile e-mail enabling server that translates e-mail communications between the protocol used by an e-mail server (*e.g.*, IMAP or POP) and the protocol used by a mobile e-mal client on the wireless communication device. *Id.* at col. 6, ll. 19-27. Thus, communications from the mobile enabling e-mail server are always e-mail communications destined for or received from the e-mail client on the wireless communication device. Consequently, Maes does not disclose, and has no need for, generating an encrypted message comprising the at least a portion of the message payload and an identifier that identifies the particular device agent and assists in delivering the at least a portion of the message payload to the particular device agent.

IPR2025-01571
Apple EX1002 Page 869

Thus, neither Falk nor Maes discloses "generating an encrypted message comprising the at least a portion of the message payload and an identifier, the identifier identifying the particular device agent, the identifier for assisting in delivering the at least a portion of the message payload to the particular device agent." For at least this reason, Applicant respectfully submits that claim 1 is patentable over Falk in view of Maes.

"sending the encrypted message to the first end-user device over the first service control link"

Applicant respectfully submits that neither Falk nor Maes discloses "sending the encrypted message to the first end-user device over the first service control link" because, as explained above, neither Falk nor Maes discloses generating the encrypted message as recited in claim 1, and, therefore, neither reference can disclose sending something it has not generated.

For at least this reason and for the reasons provided above, Applicant respectfully submits that claim 1 is patentable over Falk in view of Maes. Therefore, Applicant respectfully requests that the rejection of claim 1 under 35 U.S.C. § 103(a) be withdrawn.

Claim 27

The limitations of claim 27 parallel the limitations of claim 1. Therefore, claim 27 is patentable over Falk in view of Maes for at least the same reasons that claim 1 is patentable over Falk in view of Maes, and Applicant respectfully requests that the rejection of claim 27 under 35 U.S.C. § 103(a) be withdrawn.

Claims 2-20, 22, 23, 25, 26, 31-35

Claims 2-20, 22, 23, 25, 26, and 31 depend, directly or indirectly, from claim 1 and are therefore patentable over Falk in view of Maes for at least the same reasons that claims 1 and 27 are patentable over Falk in view of Maes. Therefore, Applicant respectfully requests that the rejections of claims 2-20, 22, 23, 25, 26, and 31 under 35 U.S.C. § 103(a) be withdrawn.

Claims 32-35 depend directly from claim 27 and are therefore patentable over Falk in view of Maes for at least the same reasons that claim 27 is patentable over Falk in view of Maes.

IPR2025-01571
Apple EX1002 Page 870

Therefore, Applicant respectfully requests that the rejections of claims 32-35 under 35 U.S.C. § 103(a) be withdrawn.

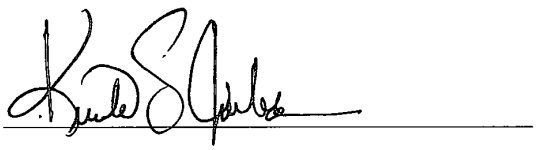
IPR2025-01571
Apple EX1002 Page 871

CONCLUSION

Applicant respectfully requests entry of these amendments as provided herein. The application is believed to be in condition for allowance, and a Notice of Allowance is hereby respectfully requested. 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.

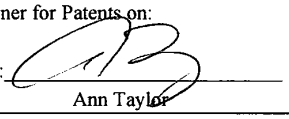
Respectfully submitted,

Date: October 10, 2013 By: 

Krista S. Jacobsen
Reg. No. 59,374
Head Counsel
Headwater Partners I LLC
350 Marine Parkway, Suite 300
Redwood Shores, CA 94065
(650) 517-2798

CERTIFICATE OF ELECTRONIC TRANSMISSION

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being filed electronically via EFS-Web addressed to the Commissioner for Patents on:

Date: Oct. 10, 2013 By: 
Ann Taylor

IPR2025-01571
Apple EX1002 Page 872

Electronic Acknowledgement Receipt	
EFS ID:	17097933
Application Number:	13705055
International Application Number:	
Confirmation Number:	3375
Title of Invention:	AUTOMATED DEVICE PROVISIONING AND ACTIVATION
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	Krista Susan Jacobsen/Ann Taylor
Filer Authorized By:	Krista Susan Jacobsen
Attorney Docket Number:	RALEP007C03
Receipt Date:	10-OCT-2013
Filing Date:	04-DEC-2012
Time Stamp:	17:01:16
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		P007C03OAR.pdf	307565 ff5405868b01250a72b3bef45511892c6a1f39c1	yes	19

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Claims	2	8
	Applicant Arguments/Remarks Made in an Amendment	9	19
Warnings:			
Information:			
	Total Files Size (in bytes):	307565	

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.

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 13/705,055	Filing Date 12/04/2012	☐ 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 **10/10/2013**

	(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))	* 30	Minus	** 30	= 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
/MARCIA GORDON/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

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

NOTICE OF ALLOWANCE AND FEE(S) DUE

106963 7590 11/20/2013

Headwater Partners I LLC
350 Marine Parkway, Suite 300
Redwood Shores, CA 94065

EXAMINER
RUDY, ANDREW J

ART UNIT	PAPER NUMBER
3687	

DATE MAILED: 11/20/2013

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/705,055	12/04/2012	Gregory G. Raleigh	RALEP007C03	3375

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	$890	$0	$0	$890	02/20/2014

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

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

HOW TO REPLY TO THIS NOTICE:

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

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

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

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

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

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

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

PTOL-85 (Rev. 02/11)

IPR2025-01571
Apple EX1002 Page 876

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 11/20/2013
Headwater Partners I LLC
350 Marine Parkway, Suite 300
Redwood Shores, CA 94065

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

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

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/705,055	12/04/2012	Gregory G. Raleigh	RALEP007C03	3375

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	$890	$0	$0	$890	02/20/2014

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

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
- ❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 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 credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

PTOL-85 (Rev. 02/11)

IPR2025-01571
Apple EX1002 Page 877

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

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

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

IPR2025-01571
Apple EX1002 Page 878

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.
13/705,055	12/04/2012	Gregory G. Raleigh	RALEP007C03	3375

106963 7590 11/20/2013

Headwater Partners I LLC
350 Marine Parkway, Suite 300
Redwood Shores, CA 94065

EXAMINER	
RUDY, ANDREW J	
ART UNIT	**PAPER NUMBER**
3687	

DATE MAILED: 11/20/2013

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

The Patent Term Adjustment to date is 0 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 0 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

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

PTOL-85 (Rev. 02/11)

IPR2025-01571
Apple EX1002 Page 879

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.

Notices of Allowance and Fee(s) Due mailed between October 1, 2013 and December 31, 2013

(Addendum to PTOL-85)

If the "Notice of Allowance and Fee(s) Due" has a mailing date on or after October 1, 2013 and before January 1, 2014, the following information is applicable to this application.

If the issue fee is being timely paid on or after January 1, 2014, the amount due is the issue fee and publication fee in effect January 1, 2014. On January 1, 2014, the issue fees set forth in 37 CFR 1.18 decrease significantly and the publication fee set forth in 37 CFR 1.18(d)(1) decreases to $0.

If an issue fee or publication fee has been previously paid in this application, applicant is not entitled to a refund of the difference between the amount paid and the amount in effect on January 1, 2014.

Notice of Allowability	Application No. 13/705,055	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 *10 October 2013*.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on_____.
2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are *1-20,22,23,25-27 and 31-35*. 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 _____.

IPR2025-01571
Apple EX1002 Page 882

DETAILED ACTION

1. Applicant cancelled claims 21, 24 and 28-30.

Allowable Subject Matter

2. Pursuant to Applicant's October 10, 2013 Amendment and REMARKS, claims 1-20, 22, 23, 25-27 and 31-35 are allowed.

3. The following is an examiner's statement of reasons for allowance: The prior art of record, either alone or in combination, does not disclose, or suggest, Applicant's claim language.

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."

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

5. Applicant's Information Disclosure Statement (IDS) submitted September 7, 2013 has been reviewed. Note the attached IDS.

6. 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, Matthew S. Gart can be reached on 571-272-3955. 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. 13/705,055	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	Classification
*	A	US-8,228,818	07-2012	Chase et al.	370/253
*	B	US-7,940,685	05-2011	Breslau et al.	370/251
*	C	US-7,574,509	08-2009	Nixon et al.	709/228
*	D	US-6,873,988	03-2005	Herrmann et al.	1/1
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

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

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

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	13705055
Filing Date	2012-12-04
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Andrew J RUDY
Attorney Docket Number	RALEP007C03

U.S.PATENTS

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	5630159	A	1997-05-13	Zancho, William F.	
	2	5633484	A	1997-05-27	Zancho, William F. et al.	
	3	5814798	A	1998-09-29	Zancho, William F.	
	4	5915008	A	1999-06-22	Dulman, Scott	
	5	6654814		2003-11-25	Britton, Kathryn H. et al.	
	6	6934249	B1	2005-08-23	Bertin, Olivier et al.	
	7	6957067		2005-10-18	Iyer, Pradeep J. et al.	
	8	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Andrew J RUDY
	Attorney Docket Number	RALEP007C03

	9	7039713	B1	2006-05-02	Van Gunter, David et al.	
	10	7286848	B2	2007-10-23	Vireday, Richard P. et al.	
	11	7313237	B2	2007-12-25	Bahl, Paramvir et al.	
	12	7444669	B1	2008-10-28	Bahl, Paramvir et al.	
	13	7493659	B1	2009-02-17	Wu, Handong et al.	
	14	7496652		2009-02-24	Pezzutti, David	
	15	7499438		2009-03-03	Hinman, Brian L. et al.	
	16	7535880		2009-05-19	Hinman, Brian L. et al.	
	17	7548976	B2	2009-06-16	Bahl, Paramvir et al.	
	18	7478420		2009-01-13	Wright, Michael et al.	
	19	7593730	B2	2009-09-22	Khandelwal, Deepak 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	13705055
Filing Date	2012-12-04
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Andrew J RUDY
Attorney Docket Number	RALEP007C03

	20	7502672		2009-03-10	Kolls, H. Brock	
	21	7720960	B2	2010-05-18	Pruss, Richard Manfred et al.	
	22	7774456	B1	2010-08-10	Lownsbrough, Derek Leigh et al.	
	23	7801985	B1	2010-09-21	Pitkow, Jim et al.	
	24	7881697	B2	2011-02-01	Baker, Matthew Donald et al.	
	25	7899438	B2	2011-03-01	Baker, Matthew Donald et al.	
	26	7929959	B2	2011-04-19	DeAtley, Dallas et al.	
	27	7945238	B2	2011-05-17	Baker, Matthew Donald et al.	
	28	7948953	B2	2011-05-24	Melkote, Keerti G. et al.	
	29	7969950	B2	2011-06-28	Iyer, Pradeep J. et al.	
	30	8000276	B2	2011-08-16	Scherzer, Shimon 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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Andrew J RUDY
	Attorney Docket Number	RALEP007C03

	31	8027339	B2	2011-09-27	Short, Joel E. et al.	
	32	8032409	B1	2011-10-04	Mikurak, Michael G.	
	33	7529204		2009-05-05	Bourlas, Yair et al.	
	34	8078140	B2	2011-12-13	Baker, Matthew Donald et al.	
	35	8090359		2012-01-03	Proctor Jr., James Arthur et al.	
	36	8090616		2012-01-03	Proctor Jr., James Arthur et al.	
	37	8095112	B2	2012-01-10	Chow, Richard et al.	
	38	8116749		2012-02-14	Proctor Jr., James Arthur et al.	
	39	8126476	B2	2012-02-28	Vardi, Yosef et al.	
	40	8134954		2013-03-13	Godfrey, James A. et al.	
	41	8150431		2012-04-03	Wolovitz, Lionel 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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Andrew J RUDY
	Attorney Docket Number	RALEP007C03

	42	7756757		2010-07-13	Oakes III, Charles Lee	
	43	8200509	B2	2012-06-12	Kenedy, Andrew Alexander et al.	
	44	8242959	B2	2012-08-14	Mia, Rashidus S. et al.	
	45	8270972	B2	2012-09-18	Otting, Marcia J. et al.	
	46	8285249	B2	2012-10-09	Baker, Matthew Donald et al.	
	47	8307067	B2	2012-11-06	Ryan, Nicholas M.	
	48	8325638		2012-12-04	Jin, Haipeng et al.	
	49	8326319	B2	2012-12-04	Davis, Richard W.	
	50	8356336	B2	2013-01-15	Johnston, Keith et al.	
	51	8358638	B2	2013-01-22	Scherzer, Tamir et al.	
	52	8374592		2013-02-12	Proctor, Jr. James A. 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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Andrew J RUDY
	Attorney Docket Number	RALEP007C03

	53	8447607	B2	2013-05-21	Weider, Chris et al.	
	54	8472371		2013-06-25	Bari, Farooq et al.	
	55	8483135		2013-07-09	Cai, Yigang et al.	
	56	8495227		2013-07-23	Kaminsky, David L. et al.	
	57	8504729		2013-08-06	Pezzutti, David A.	
	58	7139569		2006-11-21	Kato, Akira	
	59	7930446		2011-04-19	Kesselman, Alex et al.	
	60	8045973		2011-10-25	Chambers, Michael D.	
	61	8068829		2011-11-29	Lemond, Eric et al.	
	62	8078163		2011-12-13	Lemond, Eric et al.	
	63	8086497		2011-12-27	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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Andrew J RUDY
	Attorney Docket Number	RALEP007C03

	64	8116781		2012-02-14	Chen, Xixian et al.	
	65	8126396		2012-02-28	Bennett, James D.	
	66	8166040		2012-04-24	Brindisi, Richard G. et al.	
	67	8351898		2013-01-08	Raleigh, Gregory G.	

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

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20010048738	A	2001-12-06	Baniak, Paul G. et al.	
	2	20020049074	A	2002-04-25	Eisinger, Bernd et al.	
	3	20020161601	A	2002-10-31	Nauer, Bernhard et al.	
	4	20030233332	A	2003-12-18	Keeler, James D. et al.	
	5	20040102182	A	2004-05-27	Reith, Lothar 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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Andrew J RUDY
	Attorney Docket Number	RALEP007C03

	6	20060068796	A	2006-03-30	Millen, Stephanie L. et al.	
	7	20060135144	A	2006-06-22	Jothipragasam, Premkumar	
	8	20070033197	A	2007-02-08	Scherzer, Shimon et al.	
	9	20070109983	A	2007-05-17	Shankar, Rohit et al.	
	10	20080022354	A	2008-01-24	Grewal, Karanvir et al.	
	11	20080089295	A	2008-04-17	Keeler, James D. et al.	
	12	20080250053	A	2008-10-09	Aaltonen, Janne et al.	
	13	20090005000	A	2009-01-01	Baker, Matthew et al.	
	14	20090006116	A	2009-01-01	Baker, Matthew et al.	
	15	20090006200	A	2009-01-01	Baker, Matthew et al.	
	16	20110013569	A	2011-01-20	Scherzer, Shimon 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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Andrew J RUDY
	Attorney Docket Number	RALEP007C03

	17	20110081881	A	2011-04-07	Baker, Matthew Donald et al.	
	18	20110082790	A	2011-04-07	Baker, Matthew Donald et al.	
	19	20110159818	A	2011-06-30	Scherzer, Shimon et al.	
	20	20120020296	A	2012-01-26	Scherzer, Shimon et al.	
	21	20120196644	A	2012-08-02	Scherzer, Shimon et al.	
	22	20120238287	A	2012-09-20	Scherzer, Shimon	
	23	20130029653	A	2013-01-31	Baker, Matthew Donald et al.	
	24	20130058274	A	2013-03-07	Scherzer, Shimon et al.	
	25	20130065555	A	2013-03-14	Baker, Matthew Donald et al.	
	26	20130084835	A	2013-04-04	Scherzer, Shimon et al.	

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

FOREIGN PATENT DOCUMENTS

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Andrew J RUDY
	Attorney Docket Number	RALEP007C03

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	1998058505	WO		1998-12-23	Sonera Oy		☐
	2	2007097786	WO	A	2007-08-30	Sony Ericsson Mobile Communications AB		☐

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

NON-PATENT LITERATURE DOCUMENTS

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	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)	☐
	2	Office Action Response in U.S. Application No. 13/712,184, August 8, 2013	☐

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

EXAMINER SIGNATURE

Examiner Signature	/Andrew Joseph Rudy/	Date Considered	10/31/2013

*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	
13/705,055	RALEIGH, GREGORY G.	
Examiner	**Art Unit**	
ANDREW JOSEPH RUDY	3687	

SEARCHED			
Class	Subclass	Date	Examiner
prior			
search	updated	11/12/2013	AJR
726	3-5,26	11/12/2013	AJR
709	227,228	11/12/2013	AJR
705	14.4	11/12/2013	AJR
705	26.1,30	11/12/2013	AJR

INTERFERENCE SEARCHED			
Class	Subclass	Date	Examiner
726	**3-7,26**	**11/12/2013**	**AJR**
709	224,228	11/12/2013	AJR
713	168	11/12/2013	AJR
455/405 370/328,338 705/14.4,30		11/12/2013	AJR

SEARCH NOTES (INCLUDING SEARCH STRATEGY)		
	DATE	EXMR
Continuity data searched.	11/12/2013	AJR
Inventor name searched.	11/12/2013	AJR
Bibliographic data reviewed.	11/12/2013	AJR

IPR2025-01571
Apple EX1002 Page 896

Issue Classification	Application/Control No.	Applicant(s)/Patent under Reexamination	
	13/705,055	RALEIGH, GREGORY G.	
	Examiner	Art Unit	
	ANDREW JOSEPH RUDY	3687	

ISSUE CLASSIFICATION

ORIGINAL			CROSS REFERENCE(S)						
CLASS	SUBCLASS	CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)						
726	7	709	224						
INTERNATIONAL CLASSIFICATION									
G 0 6 F	17/30								
	/								
	/								
	/								
	/								

XXXXXXXXXXXXXXXXXXXXXX (Assistant Examiner) (Date)	/Andrew Joseph Rudy/ 11/12/13 (Primary Examiner) (Date)	Total Claims Allowed: 30
(Legal Instruments Examiner) (Date)		O.G. Print Claim(s): 1 / O.G. Print Fig.: 25

☐ 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
1	1	21	31		61		91		121		151		181
2	2	27	32		62		92		122		152		182
3	3	28	33		63		93		123		153		183
4	4	29	34		64		94		124		154		184
5	5	30	35		65		95		125		155		185
6	6		36		66		96		126		156		186
7	7		37		67		97		127		157		187
8	8		38		68		98		128		158		188
9	9		39		69		99		129		159		189
10	10		40		70		100		130		160		190
11	11		41		71		101		131		161		191
12	12		42		72		102		132		162		192
13	13		43		73		103		133		163		193
14	14		44		74		104		134		164		194
15	15		45		75		105		135		165		195
16	16		46		76		106		136		166		196
17	17		47		77		107		137		167		197
18	18		48		78		108		138		168		198
19	19		49		79		109		139		169		199
20	20		50		80		110		140		170		200
	21		51		81		111		141		171		201
22	22		52		82		112		142		172		202
23	23		53		83		113		143		173		203
	24		54		84		114		144		174		204
24	25		55		85		115		145		175		205
25	26		56		86		116		146		176		206
26	27		57		87		117		147		177		207
	28		58		88		118		148		178		208
	29		59		89		119		149		179		209
	30		60		90		120		150		180		210

IPR2025-01571
Apple EX1002 Page 897

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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Andrew J RUDY
	Attorney Docket Number	RALEP007C03

U.S.PATENTS						
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	5983270	A	1999-11-09	Abraham et al.	
	2	6104700	A	2000-08-15	Haddock, Stephen R. et al.	
	3	6598034	B1	2003-07-22	Kloth, Axel K.	
	4	6748195	B1	2004-06-08	Phillips, W. Garland	
	5	7013469	B2	2006-03-14	Smith et al.	
	6	7032072	B1	2006-04-18	Quinn et al.	
	7	7043268	B2	2006-05-09	Yukie et al.	
	8	7113780	B2	2006-09-26	Mckenna Daniel et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Andrew J RUDY
	Attorney Docket Number	RALEP007C03

	9	7203169	B1	2007-04-10	Okholm, Jon et al.	
	10	7286834	B2	2007-10-23	Walter	
	11	7460837	B2	2008-12-02	Diener, Neil R.	
	12	7540408	B2	2009-06-02	Levine, Judah et al.	
	13	7555757	B2	2009-06-30	Smith et al.	
	14	7580356	B1	2009-08-25	Mishra et al.	
	15	7596373	B2	2009-09-29	Mcgregor, Christopher et al.	
	16	7610396	B2	2009-10-27	Taglienti et al.	
	17	7616962	B2	2009-11-10	Oswal, Anand K. et al.	
	18	7653394	B2	2010-01-26	McMillin, Brian K.	
	19	7697540	B2	2010-04-13	Haddad et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Andrew J RUDY
	Attorney Docket Number	RALEP007C03

	20	7742406	B1	2010-06-22	Muppala, Suresh	
	21	7774323	B2	2010-08-10	Helfman, Nadav	
	22	7826427	B2	2010-11-02	Sood et al.	
	23	7826607	B1	2010-11-02	De Carvalho Resende et al.	
	24	7953877	B2	2011-05-31	Vemula et al.	
	25	7957381	B2	2011-06-07	Clermidy et al.	
	26	7958029	B1	2011-06-07	Bobich et al.	
	27	7984511	B2	2011-07-19	Kocher Paul et al.	
	28	7987510	B2	2011-07-26	Kocher et al.	
	29	8031601	B2	2011-10-04	Feroz et al.	
	30	8130793	B2	2012-03-06	Edwards, Stephen K. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Andrew J RUDY
	Attorney Docket Number	RALEP007C03

	31	8166554	B2	2012-04-24	John, Pramod	
	32	8185093		2012-05-22	Jheng, Yu-Syuan et al.	
	33	8185127	B1	2012-05-22	Cai, Zheng et al.	
	34	8195163	B2	2012-06-05	Gisby, Doug et al.	
	35	8196199	B2	2012-06-05	Hrastar et al.	
	36	8204505	B2	2012-06-19	Jin et al.	
	37	8255534	B2	2012-08-28	Assadzadeh, Alireza	
	38	8296404		2012-10-23	McDysan, Dave et al.	
	39	8320244	B2	2012-11-27	Muqattash et al.	
	40	8351592	B2	2013-01-08	Freeny Jr et al.	
	41	8352360	B2	2013-01-08	De Judicibus et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Andrew J RUDY
	Attorney Docket Number	RALEP007C03

	42	8411691	B2	2013-04-02	Aggarwal	
	43	8437734		2013-05-07	Ray, Amar N. et al.	
	44	8461958	B2	2013-06-11	Saenz et al.	
	45	8463232	B2	2013-06-11	Tuli et al.	
	46	8483694	B2	2013-07-09	Lewis et al.	
	47	8484327	B2	2013-07-09	Werner et al.	
	48	8489720	B1	2013-07-16	Morford, Michael et al.	
	49	8509082	B2	2013-08-13	Heinz, John M. et al.	
	50	8522039	B2	2013-08-27	Hyndman et al.	
	51	8526329	B2	2013-09-03	Mahany, Ronald L. et al.	
	52	8526350	B2	2013-09-03	Xue, Qi et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Andrew J RUDY
	Attorney Docket Number	RALEP007C03

	53	8543265	B2	2013-09-24	Ekhaguere et al.	
	54	8544105	B2	2013-09-24	Mclean et al.	
	55	8561138	B2	2013-10-15	Rothman, Michael M. et al.	
	56	8571474	B2	2013-10-29	Chavez et al.	
	57	8571993	B2	2013-10-29	Kocher et al.	
	58	8583499		2013-11-12	De Judicibus, Dario et al.	

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

U.S.PATENT APPLICATION PUBLICATIONS

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	20060174035	A	2006-08-03	Tufail, Mudassir	
	2	20070025301	A	2007-02-01	Petersson et al.	
	3	20070140145	A	2007-06-21	Kumar et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Andrew J RUDY
	Attorney Docket Number	RALEP007C03

	4	20070147324		2007-06-28	McGary, Faith	
	5	20070155365	A	2007-07-05	Kim, Sung-Jun et al.	
	6	20070168499	A	2007-07-19	Chu, Jing-Long	
	7	20080120129	A	2008-05-22	Seubert et al.	
	8	20100080202		2010-04-01	Hanson, Mark	
	9	20100131584		2010-05-27	Johnson, William J.	
	10	20110264923	A	2011-10-27	Kocher et al.	
	11	20130144789		2013-06-06	Aaltonen, Janne et al.	

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

FOREIGN PATENT DOCUMENTS

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	101115248A	CN		2008-01-30	Lenovo Beijing Ltd.		☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Andrew J RUDY
	Attorney Docket Number	RALEP007C03

	2	101341764A	CN		2009-01-07	Telefonaktiebolaget LM Ericsson		☐
	3	1538730A	CN		2004-10-20	Zhongxing Communication Co., Ltd.		☐
	4	2007068288	WO		2007-06-21	Telefonaktiebolaget LM Ericsson		☐

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

NON-PATENT LITERATURE DOCUMENTS

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	"The Construction of Intelligent Residential District in Use of Cable Television Network," Shandong Science, Vol. 13, No. 2, June 2000	☐
	2	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	☐

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

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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Andrew J RUDY
	Attorney Docket Number	RALEP007C03

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		Date (YYYY-MM-DD)	2013-11-25
Name/Print	Krista S. Jacobsen	Registration Number	59374

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.

IPR2025-01571
Apple EX1002 Page 907

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	13705055
Filing Date	2012-12-04
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Andrew J RUDY
Attorney Docket Number	RALEP007C03

U.S.PATENTS

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.

U.S.PATENT APPLICATION PUBLICATIONS

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.

FOREIGN PATENT DOCUMENTS

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	1802839A	CN		2006-07-12	Motorola Inc.		☐
	2	2004064306	WO		2004-07-29	Motorola Inc.		☐

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

NON-PATENT LITERATURE DOCUMENTS

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Andrew J RUDY
	Attorney Docket Number	RALEP007C03

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	9/30/2013 First Office Action in Chinese Patent Application No. 201080013732.4	☐

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

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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Andrew J RUDY
	Attorney Docket Number	RALEP007C03

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).

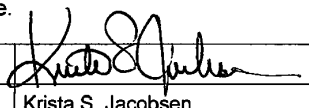
☐ See attached certification statement.

☒ 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		Date (YYYY-MM-DD)	2013-11-25
Name/Print	Krista S. Jacobsen	Registration Number	59374

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

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

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

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

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

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

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

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

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

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

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

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

[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04M 11/06
H04M 15/00 H04M 17/00
H04L 9/32 H04L 12/14

[12] 发明专利申请公开说明书

[21] 申请号 03113227.8

[43] 公开日 2004 年 10 月 20 日

[11] 公开号 CN 1538730A

[22] 申请日 2003.4.15 [21] 申请号 03113227.8

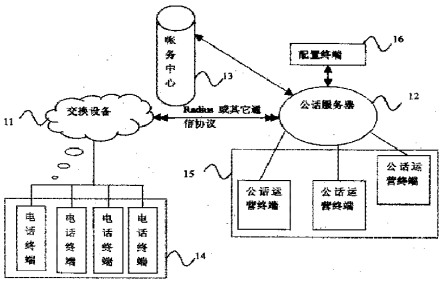
[71] 申请人 中兴通讯股份有限公司
地址 518057 深圳市南山区高新技术产业园科技南路中兴通讯大厦法律部
[72] 发明人 贾廷尧 潘红兵 朱 越

权利要求书 2 页 说明书 5 页 附图 3 页

[54] 发明名称 一种宽带公话系统及其实现方法

[57] 摘要

本发明提供一种宽带公话系统及其实现方法，该系统包括交换设备、公话服务器、帐务中心、公话运营终端和电话终端，其中所述电话终端挂接在所述交换设备上，在所述公话运营终端的数据控制下，与所述公话服务器之间进行通讯；该实现方法包含以下步骤：对用户发起的呼叫进行认证；以及对用户资费结帐。 采用本发明提供的宽带公话系统，能够提供具有良好的开放性、易于扩充规模的公话系统，可跨地域运行，很好地适应了现代通信网的高度智能化的要求，降低了投资，易于维护，具有良好的性价比；其实现方法可对多个公话运营点进行集中控制和管理，防止了人为违规资费发生，具有较高的可靠性、安全性，不易被攻击，同时还可达到计费准确度高的效果。



ISSN1008-4274

知识产权出版社出版

IPR2025-01571
Apple EX1002 Page 912

1．一种宽带公话系统，该系统包括交换设备、公话服务器、帐务中心、公话运营终端和电话终端，其中电话终端挂接在交换设备上，在公话运营终端的数据控制下，与公话服务器之间进行通讯。

2．如权利要求1所述的宽带公话系统，其中所述交换设备和所述公话服务器之间采用标准的RADIUS协议，或其他等效通信协议。

3．如权利要求 1 所述的宽带公话系统，其中所述公话服务器和所述公话运营终端 15 之间采用标准的 RADIUS 协议，或其他等效通信协议。。

4．如权利要求 1 所述的宽带公话系统，其特征在于所述系统还可采用一个交换设备带多个公话服务器的连接方式。

5．如权利要求 1 所述的宽带公话系统，其特征在于所述系统还采用多个交换设备共用一个公话服务器的连接方式。

6．如权利要求 1 所述的宽带公话系统，对于在网上不具有支持 RADIUS 协议功能的交换设备，可将这些设备接入软交换系统，从而获得支持这些通信协议的能力。

7．一种宽带公话系统实现方法，其特征在于该方法包含以下步骤：

对用户发起的呼叫进行认证；及

对用户资费结帐。

8．如权利要求 7 所述的宽带公话系统实现方法，其特征在于所述对用户发起的呼叫进行认证的步骤，还包括以下步骤：

用户到运营终端申请使用公话业务；

管理员在运营终端指定的所述电话终端，并输入该终端的信用额度；

公话服务器接受运营终端的输入，指定电话终端处于开启状态；

用户使用终端发起呼叫；

交换设备向公话服务器进行该终端信用认证；

若认证不能通过，则终端话机被置于闭锁状态，用户不能使用业务；

若认证通过，则公话服务器向交换设备传递信用额度；

用户开始使用该终端，进行呼叫业务；

如果用户结束业务使用，或信用额度不足，则业务结束。

9．如权利要求 7 所述的宽带公话系统实现方法，其特征在于所述对用户发起的呼叫进行认证的步骤，还包括以下步骤：

授权认证业务结束后，交换设备向公话服务器发出业务结束指示；

公话服务器向帐务中心(或独立的计费服务器)传递详细通话记录；

公话服务器从帐务中心(或独立的计费服务器)获得该此通话的费用帐单；

IPR2025-01571
Apple EX1002 Page 913

公话服务器将此帐单传递给指定的公话运营终端；

公话运营终端向用户输出通话帐单，整个公话系统业务结束。

IPR2025-01571
Apple EX1002 Page 914

一种宽带公话系统及其实现方法

技术领域

本发明涉及电信网络运营系统，特别是涉及该系统中的有人值守宽带公话系统及其实现方法。

背景技术

在现代电信固话运营业务中，公用电话（以下简称公话）系统是运营商获得利润的一个重要手段。特别是随着目前 IP 电话的广泛使用，宽带公话运营已是运营商重要的利润增长点，通过提供这种立即付费的公话业务，可以为广大用户提供方便。

现有技术的公话系统大致可分为无人值守和有人值守两种模式：其中对于无人值守公话系统，常见的为磁卡、IC 卡电话；而有人值守公话系统，常见的为电信营业厅或者写字楼的商务中心中使用的公用电话系统，对于有人值守公话系统，其主要的功能为：

1. 由控制终端设备发起呼叫，防止未授权用户使用业务；

2. 用户使用终端通话结束后输出通话费用.运营商获得收入.

本发明正是针对有人值守公话系统，而提出的一种新的公话系统及其实现方法。

目前的宽带公话系统的实现一般独立于交换系统，只是在交换终端对终端设备予以计量控制，一般采用以下几种模式：

1. 使用公话计费器来提供服务

只需配置计费器，将话机和计费器连接即可，由计费器对话机进行控制，并在通话结束后显示通话费用。 这种模式的实现较为简单，但存在着计费精度低，易引发用户话费纠纷等缺点，特别是如遇资费调整则存在着巨大的数据配置工作量，平时也具有较大的维护工作量；

2. 使用公话计费服务器

增加硬件设备，将若干用户线进行转接集成，（或在环路中继上进行控制，）由服务器对终端设备进行控制，采用内置计费服务器的办法，因此可能于帐务中心的帐单输出有差异，并且同样存在着计费精度低的缺点；

3.使用小交换系统完成

在需要配置为公话的终端话机上接入小交换设备，从而使其接入交换网，在

IPR2025-01571
Apple EX1002 Page 915

小交换设备上对话机终端控制，利用小交换设备的计费系统完成资费计算。这和第二种实现方式本质相同，存在计费精度底、投资成本高的缺点。

并且，当运营商需要设置多个营业点时，利用现有的以上这些系统，需要相应的投资多套软硬件设备，因此其成本较高，维护工作量较大。

并且这些实现方式，普遍存在以下缺点：

1. 智能化较低，不能高效进行集中管理；
2. 在资费政策变化时，数据修改工作量巨大；
3. 内部接口不具有很好的开放性；
4. 由于计算电话费用的设备一般配置较低，无法获得精确计费；
5. 在运营规模扩大时需要投入多套设备，投资成本高，维护工作量大；
6. 系统运营受地域限制，一套系统一般集中在一个城市的一个地域，不能跨地域城市运营。

经检索，“ 深圳市冠日高科技发展有限公司”申请获得了“公用电话网的构成及其实现方法”专利，其核心内容是建立独立的公话交换系统，并对其予以公话网管，接入到运营电信网上，其思想内容类似于上述第三种实现方式，该发明需要建立独立的公话交换网，不能充分利用网上的现有设备，同时， 需要建立独立的计费模块，不能从已有的帐务中心获取计费信息，存在着投资大、实际建设困难的弱点。

上述现有的公话系统的实现都是基于运营的交换系统，其具有相对的封闭性，和第三方设备不具有开放的通信能力，因此第三方设备无法控制交换设备的动作，不便于直接从交换设备采集话单. 因此其实现基于对交换终端附以另外的设备，或加以计价设备，或建立另外的交换设备从而达到控制终端话机，采集话单的目的.

随着电信网的演变，宽带交换系统（例如软交换系统）已经推向市场，这种系统以 IP 协议为基石，其系统具有良好的开放性和扩充性，也为新的公话系统的实现提供了基础。

本发明正是在现代交换网络（特别使软交换网络）的智能化程度越来越高的情况下，充分运用电信网上的已有资源，使得交换设备和第三方设备更易于进行信息交流，保护运营商的已有投资；采用灵活的框架结构,实现公话系统。

发明内容

本发明的目的是针对上述背景技术中存在的缺陷，提供一种宽带公话系统及其实现方法，即在公话服务器的控制下，利用交换设备完成对电话终端的控制，实现通话，并由公话服务器提供费用帐单，由公话运营终端来完成和用户的界面交互。

IPR2025-01571
Apple EX1002 Page 916

为了达到上述目的，本发明提供一种宽带公话系统，该系统包括交换设备、公话服务器、帐务中心、信令处理模块，公话运营终端和电话终端，其中所述电话终端挂接在所述交换设备上，在所述公话运营终端的数据控制下，与所述公话服务器之间进行通讯。

本发明还提供一种宽带公话系统实现方法，其特征在于该方法包含以下步骤：

对用户发起的呼叫进行认证，；

对用户资费结帐。

采用本发明提供的宽带公话系统，能够提供具有良好的开放性、易于扩充规模的公话系统，可跨地域运行，很好地适应了现代通信网的高度智能化的要求，降低运营商投资，且该系统易于操作维护，具有良好的性价比；其实现方法可对多个公话运营点进行集中控制和管理，防止了人为违规资费发生，具有较高的可靠性、安全性，不易被攻击，同时还可达到计费准确度高的效果。

下面将结合实施例并参照附图对该发明的技术方案进行详细说明。

附图说明

图 1 为本发明的系统结构图。

图 2 为本发明的实现方法流程图。

图 3 为本发明系统结构扩充形态图一。

图 4 为本发明系统结构扩充形态图二。

具体实施方式

如图 1 所示，为本发明系统结构图，也是本发明系统结构的基本形态，它由一个公话服务器接入一个交换设备，带有多个运营终端，系统规模可以为某一城市地域，，可为跨地域模式，即系统不受地域限制，该系统由以下几部分组成：交换设备 11，它是电话业务的提供者，主要用于实现电话业务，在实际应用中一般是指运营商网上运营的交换设备，具有支持鉴权认证通信协议的能力；公话服务器 12，用于控制并完成话机终端的认证、授权操作，通过帐务中心（或计费服务器）13 完成通话资费，并将帐单传递给公话运营终端；在公话服务器 12 上，可通过配置终端 16 配置不同的策略服务，以便对由不同运营终端控制的话机终端提供不同的控制方式，实现个性化的服务（例如指定有的用户可先打电话后付费；有的需要交付押金后才可打电话；有的可以进行通话累计优惠活动）；公话运营终端 15，它是运营商的业务使用界面，用于指定话机的开放/闭锁状态、

IPR2025-01571
Apple EX1002 Page 917

录入指定终端的信用额度、配合公话服务器完成终端话机的认证，实现授权操作，以及在通话输出后,从公话服务器获得通话帐单，完成电信运营收入；电话终端14，它是用户使用终端，用于完成用户通话，可以是普通的电话机或其他智能终端，它在本发明的系统可以有任意多个；

以上各单元的连接关系是：电话终端14挂接在交换设备11上，在公话运营终端的数据控制下，与公话服务器12之间进行通讯，其中交换设备11和公话服务器之间可采用标准的RADIUS协议（或其他通信协议）；公话服务器12和公话运营终端15之间也采用标准的RADIUS协议（或其他通信协议）。

图2所示为为本发明公话系统的实现方法流程图，该流程的具体步骤包括：首先，对用户发起的呼叫进行认证，以防止未授权的用户使用业务，步骤201；对用户资费结帐，步骤202。

本发明所采用的系统结构除了如图1所示的基本形态外，还可以有如图3和图4所示的两种扩充形态，其中图3所示的扩充形态一，系统可由一个交换设备11带多个公话服务器32组成,这些公话服务器分布在不同地域,以不同的策略提供个性化的服务；图4所示的扩充形态二，采用多个交换设备41共用一个公话服务器12的连接方式，并且此时的交换设备可以为异种交换设备(如交换机、软交换设备等)。

下面试举一具体实例，更进一步说明本发明的技术方案：

在实际应用中，本发明所提到的宽带公话系统，其硬件部分包括帐务中心、交换设备、公话服务器、公话运营终端、电话终端设备，其中帐务中心和交换设备为运营商已有的系统，公话服务器可根据运营规模选用市场上的商用服务器，公话运营终端可为普通的PC机；该系统的实现方法可通过执行以下步骤来完成：

1．在交换设备上指定若干话机为公话话机终端，并指定受控公话服务器地址；

2．在公话服务器的配置终端上，对公话服务器进行配置,将所控制的公话终端，分配到相应的公话运营终端作用域；

3．用户使用公话终端进行通话，需到该终端的公话运营终端进行业务使用申请；

4．公话运营终端受理用户申请，并向服务器报告该终端当前的信用情况；

5．用户摘机发起呼叫，交换设备判断为公话服务，则向指定的公话服务器发起认证请求；

6．公话服务器依据该用户的信用情况，控制认证结果，如果信用不足以发起呼叫,则通知交换设备，闭锁话机；

IPR2025-01571
Apple EX1002 Page 918

7. 如果该用户有足够的信用，则判断用户可使用业务的时间长度（或字节流量）；

8. 当用户主动结束业务，或用户业务使用耗尽其信用额度，则交换设备主动中止业务.此时业务结束；

9.业务结束后,公话服务器向计费中心,或指定的计费服务器索取通话帐单,并安全传递给公话运营终端；

10. 运营终端接受帐单和用户结算；

11. 运营商可在公话服务器侧对各运营终端进行业务统计，决定各运营点设备的增加或减少。

该系统的软件部分分为：用户认证和资费结账两部分。

其中用户认证步骤具体还包括以下处理内容：（在本过程中可使用 RADIUS 协议，或其他通信协议）

用户到运营终端申请使用公话业务；

管理员在运营终端指定的电话终端，并输入该终端的信用额度；

公话服务器接受运营终端的输入，指定电话终端处于开启状态；

用户使用终端发起呼叫；

交换设备向公话服务器进行该终端信用认证；

认证不能通过则终端话机被置于闭锁状态，用户不能使用业务；

认证通过则公话服务器向交换设备传递信用额度；

用户开始使用该终端，进行呼叫业务；

如果用户结束业务使用，或信用额度不足，则业务结束，至此，认证授权步骤结束。

资费结帐部分：

授权认证业务结束后，交换设备指示公话服务器业务结束；

公话服务器向帐务中心(或独立的计费服务器)传递详细通话记录；

公话服务器从帐务中心(或独立的计费服务器)获得该此通话的费用帐单；

公话服务器将此帐单传递给指定的公话运营终端；

公话运营终端向用户输出通话帐单，整个公话系统业务结束。

很明显本系统要求交换系统能够支持一定的通信协议,比如 RADIUS 协议,以实现和公话服务器的通讯,对于网上不具有此功能的交换设备,运营商可将这些设备接入软交换系统,从而获得支持这些通信协议的能力。

IPR2025-01571
Apple EX1002 Page 919

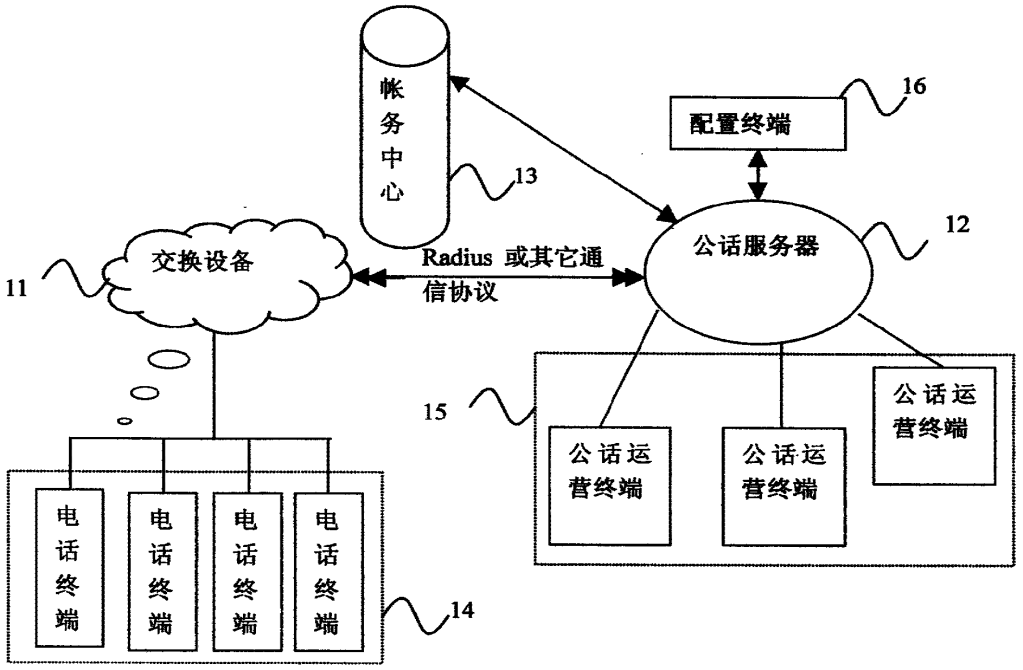


图 1

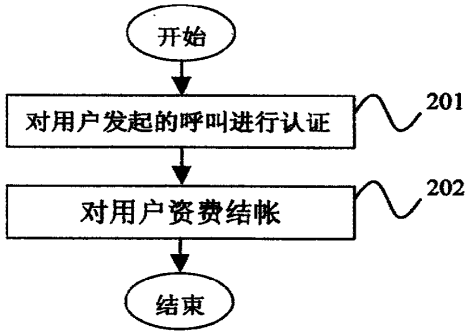


图 2

IPR2025-01571
Apple EX1002 Page 920

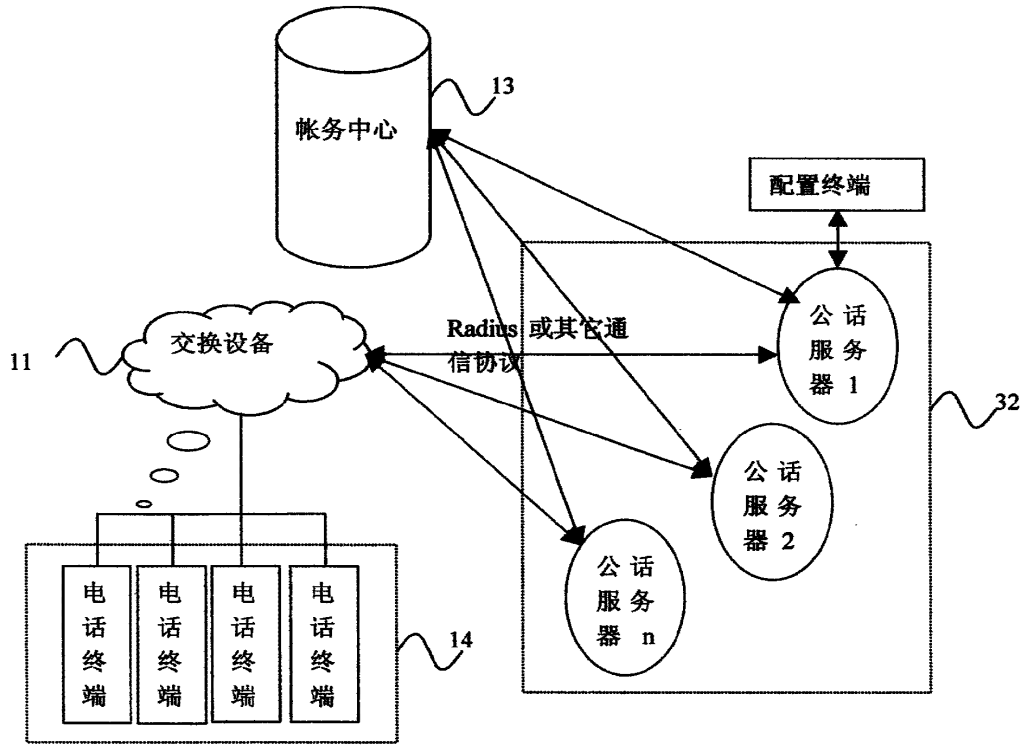


图 3

IPR2025-01571
Apple EX1002 Page 921

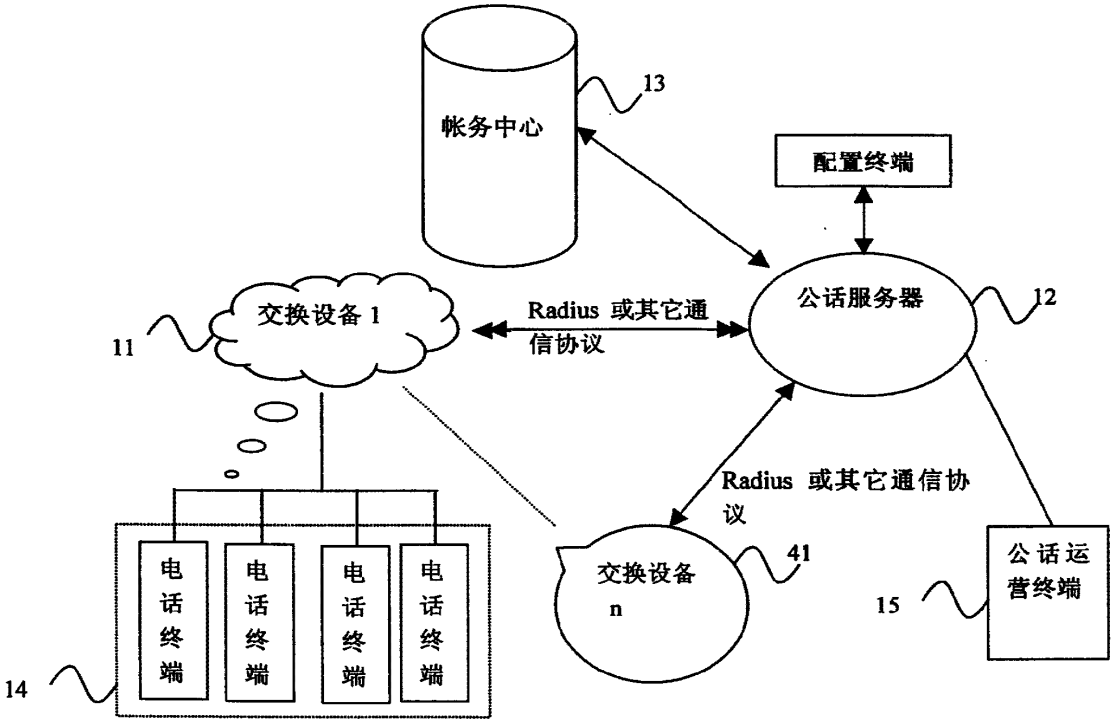


图 4

IPR2025-01571
Apple EX1002 Page 922

(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101115248 B
(45)授权公告日 2010.05.12

(21)申请号 200610107772.0

(22)申请日 2006.07.25

(73)专利权人 联想(北京)有限公司
地址 100085 北京市海淀区上地信息产业基地创业路6号

(72)发明人 周阳霖

(74)专利代理机构 北京银龙知识产权代理有限公司 11243
代理人 许静

(51)Int.Cl.
H04W 28/14(2009.01)
H04W 84/12(2009.01)
H04W 88/06(2009.01)

(56)对比文件
CN 1625868 A,2005.06.08, 全文.
WO 2006023108 A2,2006.03.02, 全文.
EP 1662726 A1,2006.05.31, 全文.
CN 1496171 A,2004.05.12, 全文.
CN 1653499 A,2005.08.10, 全文.

审查员 刘宁

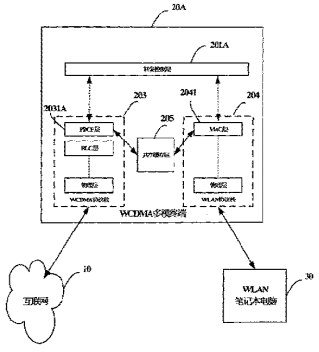
权利要求书 2 页 说明书 7 页 附图 5 页

(54)发明名称

多模终端及其数据转发方法

(57)摘要

本发明公开了一种多模终端及其数据转发方法。本发明的多模终端,具有至少一个移动通信协议栈,至少一个无线局域网协议栈,共享缓存区以及转发控制器。其中,移动通信协议栈用于将从互联网接收到的IP数据包存放到共享缓存区后通知转发控制层;转发控制层用于将IP数据包在共享缓存区中的存放地址通知无线局域网协议栈;无线局域网协议栈用于从共享缓存区取出IP数据包并将其发送到无线设备,移动通信协议栈、转发控制层、无线局域网协议栈中的任何一个将IP数据包的目的IP地址修改为无线设备在无线局域网连接中的IP地址。本发明的多模终端及其数据转发方法可以有效的提高数据传输效率。



CN 101115248 B

IPR2025-01571
Apple EX1002 Page 923

1. 一种多模终端，具有至少一个移动通信协议栈，至少一个无线局域网协议栈，以及转发控制层，其特征在于，多模终端进一步包括共享缓存区，其中，

移动通信协议栈用于将从互联网接收到的 IP 数据包存放到共享缓存区后通知转发控制层；

转发控制层用于将 IP 数据包在共享缓存区中的存放地址通知无线局域网协议栈；

无线局域网协议栈用于从共享缓存区取出 IP 数据包并将其发送到无线设备，

移动通信协议栈、转发控制层、无线局域网协议栈中的任何一个将 IP 数据包的目的 IP 地址修改为无线设备在无线局域网连接中的 IP 地址。

2. 根据权利要求 1 所述的多模终端，其特征在于，

无线局域网协议栈，进一步用于将从无线设备接收到的 IP 数据包转送到共享缓存区，并通知所述转发控制层；

转发控制层，进一步用于将从无线设备接收到的 IP 数据包在共享缓存区中的存放地址通知移动通信协议栈；

移动通信协议栈，进一步用于从共享缓存区取出从无线设备接收到的 IP 数据包，将该 IP 数据包发送到互联网，

移动通信协议栈、转发控制层、无线局域网协议栈中的任何一个将 IP 数据包的源地址修改为多模终端在互联网中对应的 IP 地址。

3. 根据权利要求 1 或 2 所述的多模终端，其特征在于，无线局域网协议栈为 WiFi、WiMax、BlueTooth、UWB、Zigbee、RFID 中的一个。

4. 根据权利要求 1 或 2 所述的多模终端，其特征在于，移动通信协议栈为 TD-SCDMA、WCDMA、GSM、CDMA 1x、CDMA2000、GPRS 中的一个。

5. 一种多模式终端的数据转发方法，其特征在于，包括以下步骤：

移动通信协议栈将从互联网接收到的 IP 数据包存放到共享缓存区后通知转发控制层；

转发控制层将 IP 数据包在共享缓存区中的存放地址通知无线局域网协议栈；

无线局域网协议栈从共享缓存区取出 IP 数据包并将其发送到无线设备，

移动通信协议栈、转发控制层、无线局域网协议栈中的任何一个将 IP 数据包的目的 IP 地址修改为无线设备在无线局域网连接中的 IP 地址。

6. 根据权利要求 5 所述的方法，其特征在于，所述方法进一步包括以下步骤：

无线局域网协议栈将从无线设备接收到的 IP 数据包转送到共享缓存区，并通知所述转发控制层；

转发控制层将从无线设备接收到的 IP 数据包在共享缓存区中的存放地址通知移动通信协议栈；

移动通信协议栈从共享缓存区取出从无线设备接收到的 IP 数据包，将该 IP 数据包发送到互联网，

移动通信协议栈、转发控制层、无线局域网协议栈中的任何一个将 IP 数据包的源地址修改为多模终端在互联网中对应的 IP 地址。

7. 根据权利要求 5 或 6 所述的方法，其特征在于，无线局域网协议栈为 WiFi、WiMax、BlueTooth、UWB、Zigbee、RFID 中的一个。

IPR2025-01571
Apple EX1002 Page 924

8. 根据权利要求 5 或 6 所述的方法，其特征在于，移动通信协议栈为 TD-SCDMA、WCDMA、GSM、CDMA 1x、CDMA2000、GPRS 中的一个。

9. 一种多模终端，具有至少一个移动通信协议栈，至少一个无线局域网协议栈，以及转发控制层，其特征在于，多模终端进一步包括共享缓存区，其中，

无线局域网协议栈用于将从无线设备接收到的 IP 数据包转送到共享缓存区，并通知转发控制层；

转发控制层用于将从无线设备接收到的 IP 数据包在共享缓存区中的存放地址通知移动通信协议栈；

移动通信协议栈用于从共享缓存区取出从无线设备接收到的 IP 数据包，将该 IP 数据包发送到互联网，

移动通信协议栈、转发控制层、无线局域网协议栈中的任何一个将 IP 数据包的源地址修改为多模终端在互联网中对应的 IP 地址。

10. 根据权利要求 9 所述的多模终端，其特征在于，无线局域网协议栈为 WiFi、WiMax、BlueTooth、UWB、Zigbee、RFID 中的一个。

11. 根据权利要求 9 所述的多模终端，其特征在于，移动通信协议栈为 TD-SCDMA、WCDMA、GSM、CDMA 1x、CDMA2000、GPRS 中的一个。

12. 一种多模终端的数据转发方法，其特征在于，包括以下步骤：

无线局域网协议栈将从无线设备接收到的 IP 数据包转送到共享缓存区，并通知转发控制层；

转发控制层将从无线设备接收到的 IP 数据包在共享缓存区中的存放地址通知移动通信协议栈；

移动通信协议栈从共享缓存区取出从无线设备接收到的 IP 数据包，将该 IP 数据包发送到互联网，

移动通信协议栈、转发控制层、无线局域网协议栈中的任何一个将 IP 数据包的源地址修改为多模终端在互联网中对应的 IP 地址。

13. 根据权利要求 12 所述的方法，其特征在于，无线局域网协议栈为 WiFi、WiMax、BlueTooth、UWB、Zigbee、RFID 中的一个。

14. 根据权利要求 12 所述的方法，其特征在于，移动通信协议栈为 TD-SCDMA、WCDMA、GSM、CDMA 1x、CDMA2000、GPRS 中的一个。

IPR2025-01571
Apple EX1002 Page 925

多模终端及其数据转发方法

技术领域

[0001] 本发明涉及一种移动通信技术，特别是一种多模终端及其数据转发方法。

背景技术

[0002] 当今科技的发展带来了多种无线接入技术和蜂窝通信技术，下一代网络将出现由多种不同无线技术支撑的混合网络环境。能在多种不同的蜂窝移动通信网络或无线接入网络中使用或支持多种无线网络的移动通信终端称为“多模移动通信终端”，以下简称“多模终端”。目前，移动终端多模融合已经成为移动通信终端发展的趋势。

[0003] 现有多模终端一般包括蜂窝移动通信网络 (PLMN) 模块，例如 TD-SCDMA、WCDMA、GSM、CDMA1x、CDMA2000，GPRS 等，以及无线接入网络 (RAN) 模块，例如 WiFi、WiMax、BlueTooth、UWB、Zigbee、RFID 等。多模终端可以通过不同的模块执行不同的业务，例如，用户可以通过蜂窝移动通信网络模块连接到移动通信网络来进行语音或者数据业务，也可以通过无线接入网络模块连接无线接入网络，构成无线局域网 (WLAN) 来连接其它设备进行无线业务。

[0004] 目前，多模终端的各个模块之间主要采用多模分离协议栈。例如移动通信协议栈和无线接入协议栈（为了说明的目的，本发明中将多模终端的蜂窝移动通信协议栈简称为移动通信协议栈，将多模终端的无线接入协议栈称为 WLAN 协议栈），分别处理移动通信业务和无线接入业务。

[0005] 当用户通过蜂窝移动通信网络模块连接到移动通信网络来进行数据业务时，移动通信协议栈中的分组数据集中协议 (Packet Data ConvergenceProtocol，PDCP) 层将下层解压的数据进行 PDCP 数据包的解包操作，将恢复出来的 IP 数据包提交给移动通信协议栈的上层用户，例如 TCP/IP 协议层，进行 TCP/IP 数据包的解包等操作，再由互联网浏览器之类的用户应用程序使用；或者，移动通信协议栈中的 PDCP 层将上层用户要发送的 TCP/IP 数据包进行 PDCP 数据包的打包，转发到移动通信协议栈下层的协议层，最终通过移动通信网络发送出去。

[0006] 当用户通过 WLAN 与其它设备建立连接时，数据以 MAC 帧格式进行传递。WLAN 协议栈中的 MAC 层从下层收到的 MAC 帧数据中恢复出 IP 数据包，并提交给 WLAN 协议栈的上层用户，例如 TCP/IP 协议层，进行 TCP/IP 数据包的解包等操作，再由其它用户应用程序使用；或者，WLAN 协议栈中的 MAC 层将上层用户要发送的 TCP/IP 数据包进行 MAC 数据帧的打包，转发到 WLAN 协议栈下层的协议层，最终通过 WLAN 网络发送出去。

[0007] 然而，不同目前多模终端的各种无线协议栈之间的用户面之间没有交互，因此对于移动通信协议栈和 WLAN 协议栈之间的业务数据的传递，需要在两套协议栈的上层增加一个转发控制层来协调处理两套协议栈的数据转发。

[0008] 例如，在火车上使用 WLAN 笔记本电脑通过身边的 3G/WLAN 双模手机上网时，手机通过 3G 网络从互联网下载的数据，经过手机的移动通信网络协议栈处理之后，解压出互联网 IP 数据包，发送到手机的互联网通信协议栈，由手机的互联网通信协议栈从互联网 IP 数

IPR2025-01571
Apple EX1002 Page 926

据包中解压出原始数据，转发到手机用户面控制层，再由手机用户面控制层调用 IP 层再次进行数据打包之后，交给手机的 WLAN 协议栈，通过 WLAN 微网络发送到笔记本电脑的 WLAN 协议栈。

[0009] 或者，手机的 WLAN 协议栈在收到笔记本电脑通过 WLAN 微网络发送的数据之后，解压出 IP 数据包，交给用户面控制层，由用户面控制层调用 IP 层再次进行数据打包之后，交给手机的互联网通信协议栈，通过手机的移动通信网络协议栈发送出去。

[0010] 以上是一种协议栈之间松耦合的方式，这种方式的问题是分组交换域（PS 域）的用户数据需要经过两套协议栈的数据处理，进行了两次 IP 数据的打包，并需要单独开发一个用户面控制层进行数据转发，效率比较低。

发明内容

[0011] 本发明的目的在于提供一种多模终端。

[0012] 本发明的另一目的在于提供上述多模终端的数据转发方法。

[0013] 本发明的一种多模终端，具有至少一个移动通信协议栈，至少一个无线局域网协议栈，共享缓存区以及转发控制器。其中，移动通信协议栈用于将从互联网接收到的 IP 数据包存放到共享缓存区后通知转发控制层；转发控制层用于将修改后的 IP 数据包在共享缓存区中的存放地址通知无线局域网协议栈；无线局域网协议栈用于从共享缓存区取出修改后的 IP 数据包并将其发送到无线设备，移动通信协议栈、转发控制层、无线局域网协议栈中的任何一个将 IP 数据包的目的 IP 地址修改为无线设备在无线局域网连接中的 IP 地址。

[0014] 在上述多模终端中，无线局域网协议栈进一步用于将从无线设备接收到的 IP 数据包转送到共享缓存区，并通知所述转发控制层；转发控制层进一步用于将从无线设备接收到的 IP 数据包在共享缓存区中的存放地址通知移动通信协议栈；移动通信协议栈进一步用于从共享缓存区取出从无线设备接收到的 IP 数据包，将该 IP 数据包发送到互联网，移动通信协议栈、转发控制层、无线局域网协议栈中的任何一个将 IP 数据包的的源地址修改为互联网中对应的 IP 地址。

[0015] 本发明的一种多模式终端的数据转发方法，包括以下步骤：

[0016] 移动通信协议栈将从互联网接收到的 IP 数据包存放到共享缓存区后通知转发控制层；

[0017] 转发控制层将 IP 数据包在共享缓存区中的存放地址通知无线局域网协议栈；

[0018] 无线局域网协议栈从共享缓存区取出 IP 数据包并将其发送到无线设备，

[0019] 移动通信协议栈、转发控制层、无线局域网协议栈中的任何一个将 IP 数据包的目的 IP 地址修改为无线设备在无线局域网连接中的 IP 地址。

[0020] 在上述方法中，可以进一步包括以下步骤：

[0021] 无线局域网协议栈将从无线设备接收到的 IP 数据包转送到共享缓存区，并通知所述转发控制层；

[0022] 转发控制层将从无线设备接收到的 IP 数据包在共享缓存区中的存放地址通知移动通信协议栈；

[0023] 移动通信协议栈从共享缓存区取出从无线设备接收到的 IP 数据包，将该 IP 数据

IPR2025-01571
Apple EX1002 Page 927

包发送到互联网，

[0024] 移动通信协议栈、转发控制层、无线局域网协议栈中的任何一个将 IP 数据包的的源地址修改为互联网中对应的 IP 地址。本发明的另一种多模终端，具有至少一个移动通信协议栈，至少一个无线局域网协议栈，共享缓存区以及转发控制器。其中，无线局域网协议栈用于将从无线设备接收到的 IP 数据包转送到共享缓存区，并通知转发控制层；转发控制层用于将从无线设备接收到的 IP 数据包在共享缓存区中的存放地址通知移动通信协议栈；移动通信协议栈用于从共享缓存区取出从无线设备接收到的 IP 数据包，将该 IP 数据包发送到互联网，移动通信协议栈、转发控制层、无线局域网协议栈中的任何一个将 IP 数据包的的源地址修改为互联网中对应的 IP 地址。

[0025] 本发明的另一种多模终端的数据转发方法，包括以下步骤：

[0026] 无线局域网协议栈将从无线设备接收到的 IP 数据包转送到共享缓存区，并通知转发控制层；转发控制层将从无线设备接收到的 IP 数据包在共享缓存区中的存放地址通知移动通信协议栈；移动通信协议栈从共享缓存区取出从无线设备接收到的 IP 数据包，将该 IP 数据包发送到互联网，移动通信协议栈、转发控制层、无线局域网协议栈中的任何一个将 IP 数据包的的源地址修改为互联网中对应的 IP 地址。

[0027] 在上述多模终端及其数据转发方法中，无线局域网协议栈为 WiFi、WiMax、BlueTooth、UWB、Zigbee、RFID 中的一个，移动通信协议栈为 TD-SCDMA、WCDMA、GSM、CDMA1x、CDMA2000，GPRS 中的一个。

[0028] 应用本发明提供的技术，通过将 IP 数据包的目的 IP 地址修改为无线设备在无线局域网连接中的 IP 地址，实现了在将数据从互联网转发到无线局域网的过程中，仅对数据进行一次打包；通过将 IP 数据包的源地址修改为多模终端在互联网中对应的 IP 地址，实现了在将数据从无线局域网转发到互联网的过程中，仅对数据进行一次打包；本发明通过修改 IP 地址的方式避免了现有技术中数据转发需要两次打包，从而可以有效的提高数据传输效率。

附图说明

[0029] 图 1 所示为根据现有技术，笔记本电脑通过连接互联网的多模终端从互联网获取数据或者发送数据到互联网时数据移动路径的示意图；

[0030] 图 2 所示为描述根据现有技术笔记本电脑通过连接互联网的多模终端从互联网获取数据的过程的流程图；

[0031] 图 3 所示为描述根据现有技术笔记本电脑通过连接互联网的多模终端发送数据到互联网的过程的流程图；

[0032] 图 4 所示为根据本发明的一种实施方式，笔记本电脑通过连接互联网的多模终端从互联网获取数据或者发送数据到互联网时数据移动路径的示意图；

[0033] 图 5 所示为描述根据本发明一种实施方式，笔记本电脑通过连接互联网的多模终端从互联网获取数据的过程的流程图；

[0034] 图 6 所示为描述根据本发明的一种实施方式，笔记本电脑通过连接互联网的多模终端发送数据到互联网的过程的流程图。

IPR2025-01571
Apple EX1002 Page 928

具体实施方式

[0035] 实际上，当多模手机通过移动通信协议栈与互联网建立 IP 连接，并同时通过 WLAN 协议栈与诸如笔记本的其它终端建立 IP 连接时，两个连接之间传递的底层数据格式都是 IP 数据包，因此，有可能通过 IP 地址映射，找到一种数据包之间简单的转换方法。

[0036] 根据本发明的方法，当笔记本通过 WLAN 微网络连接多模手机，通过多模手机进行互联网业务时，在多模手机的移动通信协议栈的 PDCP 层解压出互联网 IP 数据包之后，进行 IP 地址转换，将 IP 数据包的目的 IP 地址转换为笔记本在 WLAN 微网络中的 IP 地址，并直接调用 WLAN 协议栈的接口发送给笔记本；或者，手机的 WLAN 协议栈在收到笔记本发送的微网络 IP 数据包之后，将微网络 IP 数据包转发给移动通信协议栈的 PDCP 层，由 PDCP 层将该数据包的源 IP 地址转换为手机在互联网中的 IP 地址，并通过移动通信协议栈发送出去。本发明的方法可以实现 3G 移动通信协议栈和 WLAN 无线接入协议栈用户面数据直接交互，提高数据传输效率。

[0037] 移动通信协议栈中的 PDCP 层的主要功能是 IP 数据流的头部压缩与解压缩，用于从移动通信协议栈下层的无线链路层 (RLC) 接收无线数据之后，使用 RFC25.07 算法进行解压缩之后传递给移动通信协议栈的上层用户，例如 TCP/IP 等高层网络协议；或者将从移动通信协议栈的上层用户接收的数据按照 RFC25.07 算法进行压缩，再发送到移动通信协议栈下层转发出去。

[0038] 另外，WLAN 协议栈中的 MAC 层的主要功能是 IP 数据流的 MAC 帧打包或者解包，用于从 WLAN 协议栈下层的基带层接收 MAC 帧格式的无线数据之后，进行 MAC 帧解包之后传递给 WLAN 栈的上层用户，例如 TCP/IP 等高层网络协议；或者将从 WLAN 协议栈的上层用户接收的数据打包为 MAC 帧数据，再发送到 WLAN 协议栈的下层转发出去。

[0039] 当例如在上面所述的场景中，即多模终端通过移动通信协议栈连接互联网，笔记本电脑通过 WLAN 微网络与多模终端连接从而连接到互联网的场景下，此时多模终端在互联网中具有 IP 地址，而在 WLAN 微网络中，多模终端与笔记本电脑也分别具有该 WLAN 微网络中的 IP 地址。

[0040] 图 1 所示为根据现有技术，笔记本电脑通过连接互联网的多模终端从互联网获取数据或者发送数据到互联网的数据移动路径的示意图。

[0041] 现在首先参考图 2 的流程图并结合图 1 来描述根据现有技术笔记本电脑通过连接互联网的多模终端从互联网获取数据的过程。

[0042] 从图 1 可见具有 WCDMA 协议栈 203 的 WCDMA 多模终端 20 同时具有 WLAN（可以是 WiFi、WiMax、BlueTooth、UWB、Zigbee、RFID 中任何一种）协议栈 204。

[0043] 当多模终端 20 在 WLAN 连接中利用 ad hoc 模式建立了与附近的 WLAN 笔记本电脑 30 的联系，完成了 WLAN 节点之间的链路建立工作，并且同时已经使用 WCDMA 移动链路建立流程，完成了与互联网 10 之间的空中链路的建立。

[0044] 此时，当笔记本电脑 30 通过多模终端 20 从互联网下载数据时，数据移动过程如下：

[0045] 在步骤 S1，多模终端 20 中的 WCDMA 协议栈 203 中的 PDCP 层 2031 将从 WCDMA 协议栈 203 下层的无线链路层（RLC 层）接收来自互联网的无线数据之后，使用 RFC25.07 算法进行解压缩，得到以多模终端 20 在互联网中的 IP 地址为目标地址的 IP 数据包，并传递给

IPR2025-01571
Apple EX1002 Page 929

WCDMA 协议栈的上层用户，即 TCP/IP 协议层 202。

[0046] 在步骤 S2，TCP/IP 协议层 202 对 IP 数据包进行解包操作，恢复出 IP 数据包的内容并转交给转发控制层 201。

[0047] 在步骤 S3，转发控制层 201 调用 TCP/IP 协议层，按照 WLAN 笔记本电脑 30 在 WLAN 微网络中的 IP 地址（作为目的地址）再次将原 IP 数据包的内容打包为新的 IP 数据包并发送到 WLAN 协议栈 204。

[0048] 之后，在步骤 S4 中，由 WLAN 协议栈 204 中的 MAC 层 2041 将新打包的 IP 数据包再次打包为 MAC 帧的格式之后通过 WLAN 协议栈 204 的下层发送出去由 WLAN 笔记本电脑 30 接收。

[0049] 可以看到，由于多模终端的移动通信协议栈与 WLAN 协议栈之间不能进行数据交互，数据在多模终端 20 中进行了多次转发，并且有一次 IP 数据包的解包操作以及一次 IP 数据包的打包操作。这很大的占用了多模终端的系统资源并且效率很低。

[0050] 下面参考图 3 描述根据现有技术笔记本电脑通过连接互联网的多模终端发送数据到互联网的过程。

[0051] 在步骤 R1，笔记本电脑 30 通过 WLAN 将要发送的数据发送到多模终端 20 的 WLAN 协议栈 204。

[0052] 在步骤 R2，WLAN 协议栈 204 的 MAC 层从 MAC 帧数据中恢复出 IP 数据包，并交给 TCP/IP 层 202，该 IP 数据包的源地址为 WLAN 笔记本电脑 30。

[0053] 在步骤 R3，TCP/IP 协议层 202 对 IP 数据包进行解包操作，恢复出 IP 数据包中的数据并转交给转发控制层 201。

[0054] 在步骤 R4，转发控制层 201 调用 TCP/IP 层，按照多模终端 20 在互联网中的 IP 地址（作为源地址）再次将原 IP 数据包中的内容打包为新 IP 数据包并发送到 WCDMA 协议栈 203。

[0055] 在步骤 R5，WCDMA 协议栈 203 中的 PDCP 层 2031 将新 IP 数据包按照 RFC25.07 算法进行压缩之后，再通过 WCDMA 协议栈下层转发出去。

[0056] 可以看到，与前面一样，由于多模终端的移动通信协议栈与 WLAN 协议栈之间不能进行数据交互，数据在多模终端 20 中进行了多次转发，并且有一次 IP 数据包的解包操作以及一次 IP 数据包的打包操作。

[0057] 而根据本发明的方法，在多模终端移动通信协议栈的 PDCP 层和 WLAN 协议层的 MAC 协议层之间直接进行数据传递，在数据转发过程中对 IP 数据包进行 IP 地址变化，从而避免多余的 IP 数据包解压和压缩操作，以及多次的数据转发，从而避免资源的浪费。

[0058] 图 4 所示为根据本发明，笔记本电脑通过连接互联网的多模终端从互联网获取数据或者发送数据到互联网的数据移动路径的示意图。

[0059] 可以看到，本发明的多模终端 20A 中，使多模终端 20A 的 WCDMA 协议栈 203 的 PDCP 层 2031A 具备了 IP 地址变化的功能，PDCP 层 2031A 和 WLAN 协议栈 204 的 MAC 协议层 2041 之间通过共享缓存区 205 进行数据传递。可以使多模终端 20A 在执行数据转发的状态下，在多模终端 20A 中设定一个网络协同工作模式，使其按照本发明的方法进行数据的转发。

[0060] 下面参考图 5 的流程图并结合图 4 来描述根据本发明的一种实施方式，笔记本电脑通过连接互联网的多模终端从互联网获取数据的过程。

IPR2025-01571
Apple EX1002 Page 930

[0061] 当多模终端 20A 在 WLAN 连接中利用 ad hoc 模式建立了与附近的 WLAN 笔记本电脑 30 的联系，完成了 WLAN 节点之间的链路建立工作，并且同时已经使用 WCDMA 移动链路建立流程，完成了与互联网 10 之间的空中链路的建立。

[0062] 并且，假定此时多模终端 20A 设定了网络协同工作模式。

[0063] 此时，当笔记本电脑 30 通过多模终端 20A 从互联网下载数据时，数据移动过程如下：

[0064] 在步骤 M1，多模终端 20A 中的 WCDMA 协议栈 203 中的 PDCP 层 2031A 从 WCDMA 协议栈 203 下层的无线链路层（RLC 层）接收来自互联网的无线数据后，使用 RFC25.07 算法进行解压缩，得到以多模终端 20 在互联网中的 IP 地址为目标地址的 IP 数据包之后，由于设定了网络协同工作模式，因此 PDCP 层 2031A 将 IP 数据包的目标 IP 地址变化为笔记本在 WLAN 微网络中的 IP 地址，存放在共享缓存区 205，并通知转发控制层 201A。

[0065] 在步骤 M2，转发控制层 201 将 IP 数据包在缓存区的地址通知 WLAN 协议栈 204 的 MAC 层 2041。

[0066] 在步骤 M3，MAC 层 2041 从共享缓存区取出经过地址改变的 IP 数据包再次打包为 MAC 帧的格式之后通过 WLAN 协议栈 204 的下层发送出去由 WLAN 笔记本电脑 30 接收。

[0067] 可以看到，数据直接由 PDCP 层发送到 MAC 层，并且没有 IP 数据包的解包操作和打包操作。

[0068] 上面的实施方式中由 PDCP 层改变接收到的 IP 数据包的目标 IP 地址，然而，PDCP 层也可以不改变接收到的 IP 数据包的 IP 地址而直接将它存放到共享缓存区中，由转发控制层来将 IP 数据包的目标 IP 地址变化为笔记本在 WLAN 微网络中的 IP 地址，再通知 MAC 层将数据包从共享缓存区取出发送出去；或者 PDCP 层和转发控制层都不改变 IP 数据包的目标 IP 地址，由 MAC 层在将 IP 数据包发送出去之前将 IP 数据包的目标 IP 地址变化为笔记本在 WLAN 微网络中的 IP 地址。

[0069] 下面参考图 6 描述根据本发明的一种实施方式，笔记本电脑通过连接互联网的多模终端发送数据到互联网的过程。

[0070] 在步骤 N1，笔记本电脑 30 通过 WLAN 将要发送的数据发送到多模终端 20 的 WLAN 协议栈 204。

[0071] 在步骤 N2，WLAN 协议栈 204 的 MAC 层 2041 从 MAC 帧数据中恢复出 IP 数据包，该 IP 数据包的源 IP 地址为 WLAN 笔记本电脑 30 在 WLAN 微网络中的 IP 地址，由于设置了网络协同工作模式，因此 MAC 层 2041 将数据存放在共享缓存区之后，通知转发控制层 201A。

[0072] 在步骤 N3，转发控制层 201 将 IP 数据包在缓存区的地址通知 WCDMA 协议栈 203 中的 PDCP 层 2031A。

[0073] 在步骤 N4，WCDMA 协议栈 203 中的 PDCP 层 2031 将 IP 数据包从共享缓存区中取出，将数据包的源 IP 地址修改为多模终端 20 在互联网中的 IP 地址，之后按照 RFC25.07 算法进行压缩，再通过 WCDMA 协议栈下层转发出去。

[0074] 可以看到，数据直接由 MAC 层发送到 PDCP 层，而不需要进行多次的转发，并且没有 IP 数据包的解包操作和打包操作。

[0075] 上面的实施方式中由 PDCP 层改变要发送的 IP 数据包的源 IP 地址，然而，也可以由转发控制层在 MAC 层将 IP 数据包存放在共享缓存区之后改变 IP 数据包的源 IP 地址，或

IPR2025-01571
Apple EX1002 Page 931

者由MAC层将通过无线局域网协议栈接收的IP数据包改变源IP地址之后放到共享缓存区中，再由转发控制层通知PDCP层取出源IP地址改变的IP数据包发送出去。

[0076] 另外，以上以多模终端的移动通信协议栈为WCDMA协议栈为例进行了说明，然而，本领域技术人员应该可以理解，多模终端的移动通信协议栈还可以是具有PDCP层的任何一种移动通信协议栈，例如TD-SCDMA、GSM、CDMA 1x、CDMA2000，GPRS等。

[0077] 根据本发明的数据转发方式可以让多模手机在后台完成网络数据传递功能，同时手机可以进行提供其它如打电话、收发短信等通信服务，不占用前台人机操作界面。

IPR2025-01571
Apple EX1002 Page 932

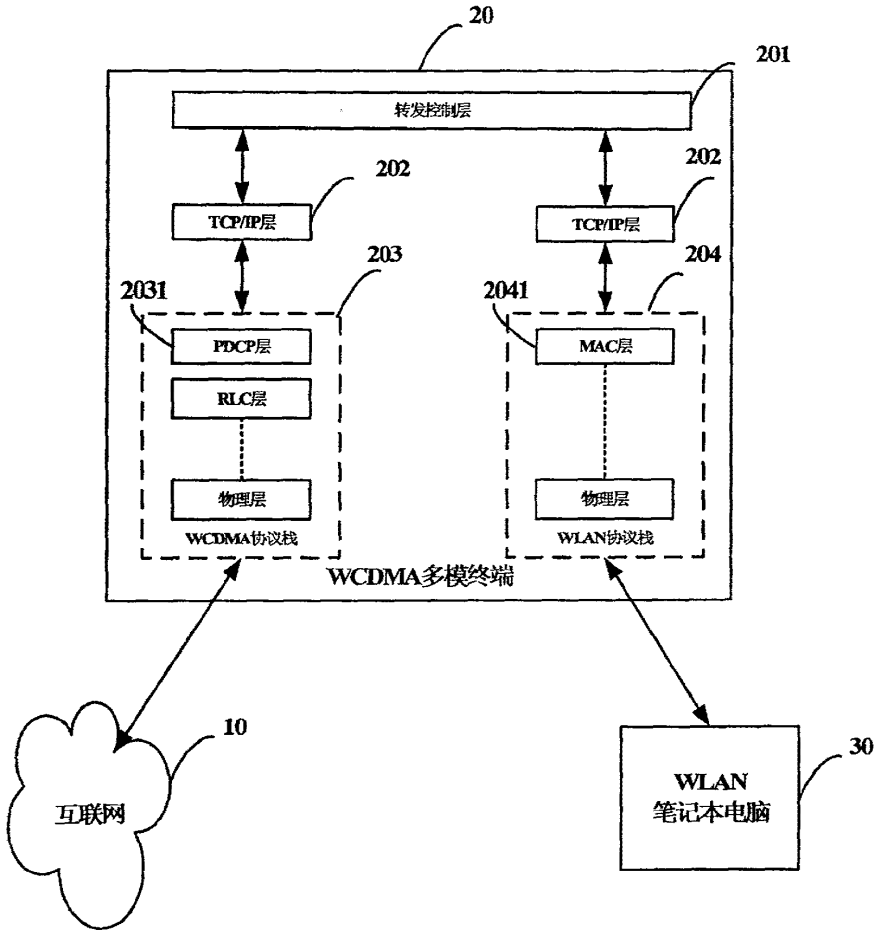


图 1

IPR2025-01571
Apple EX1002 Page 933

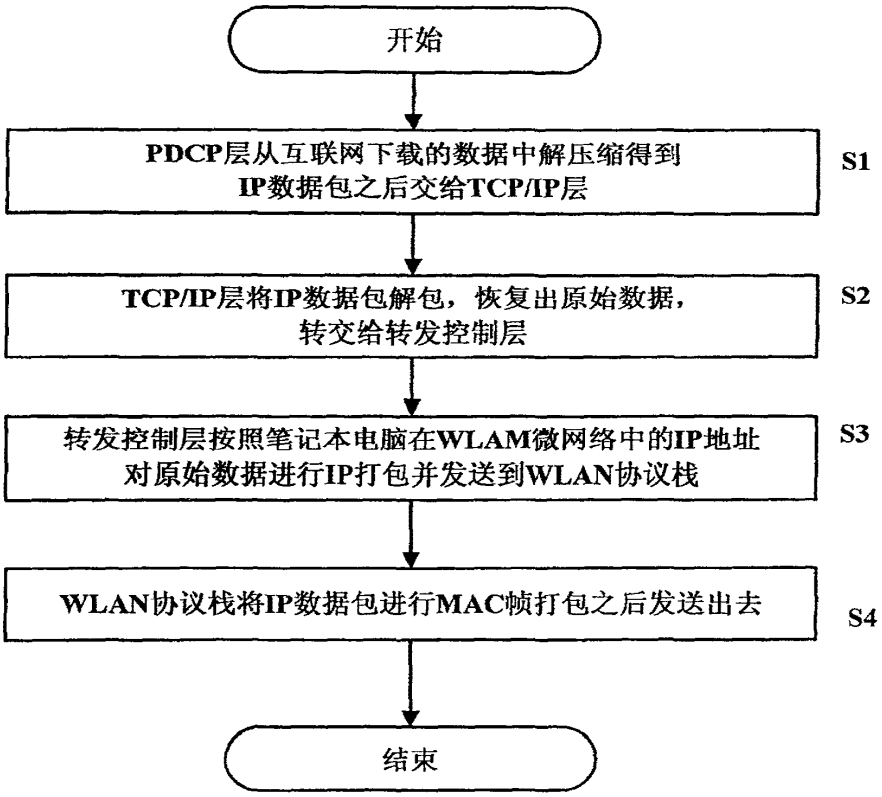


图 2

IPR2025-01571
Apple EX1002 Page 934

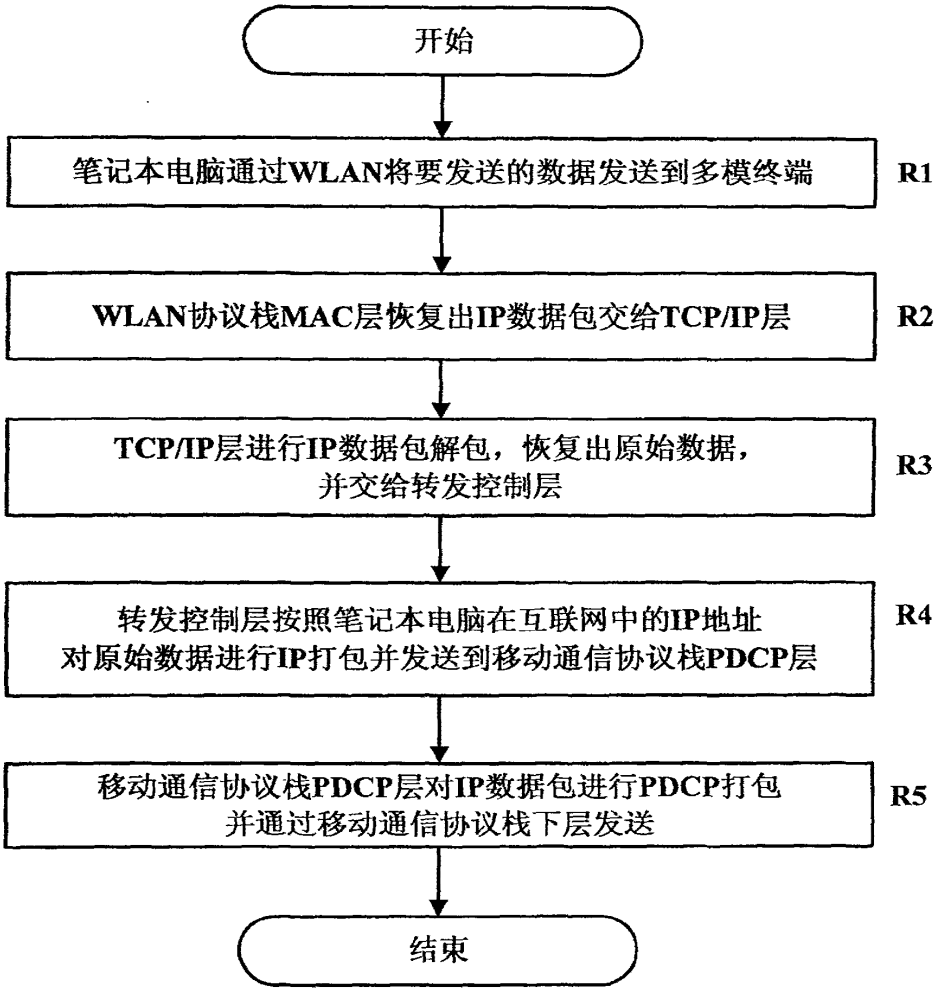


图 3

IPR2025-01571
Apple EX1002 Page 935

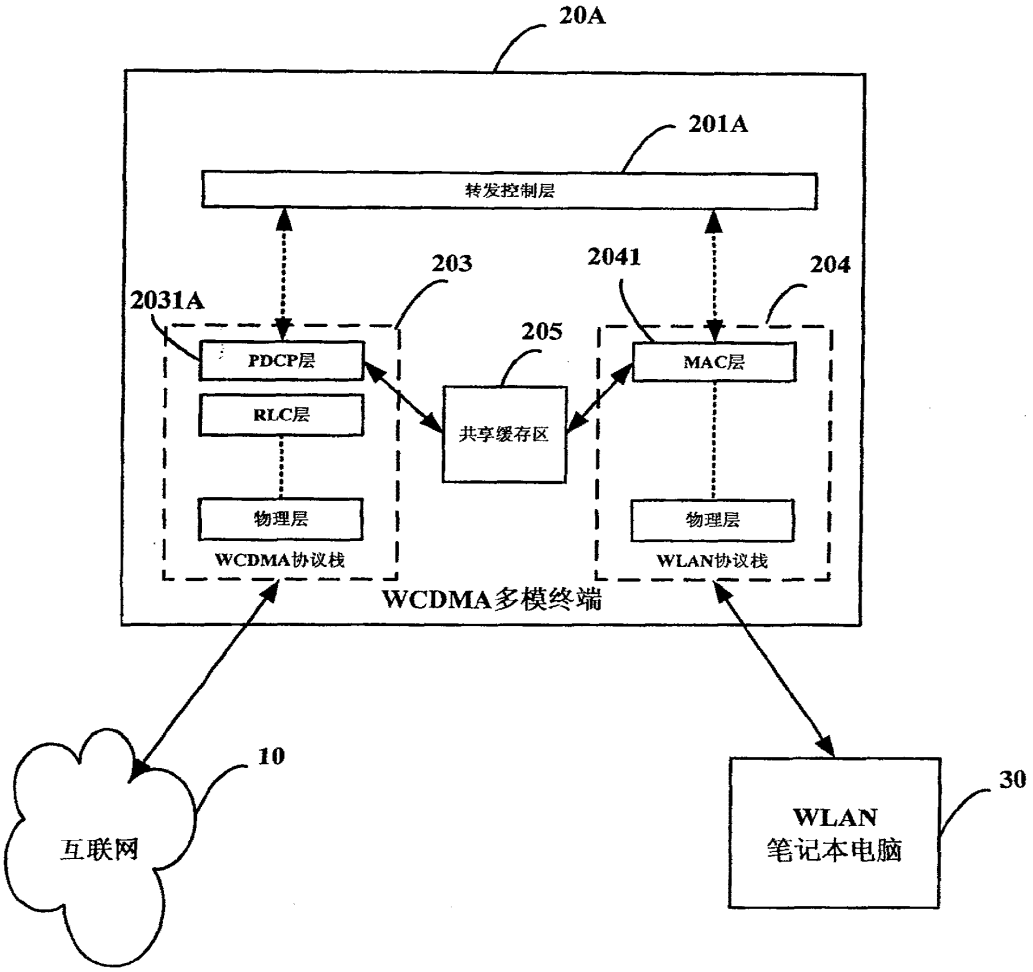


图 4

IPR2025-01571
Apple EX1002 Page 936

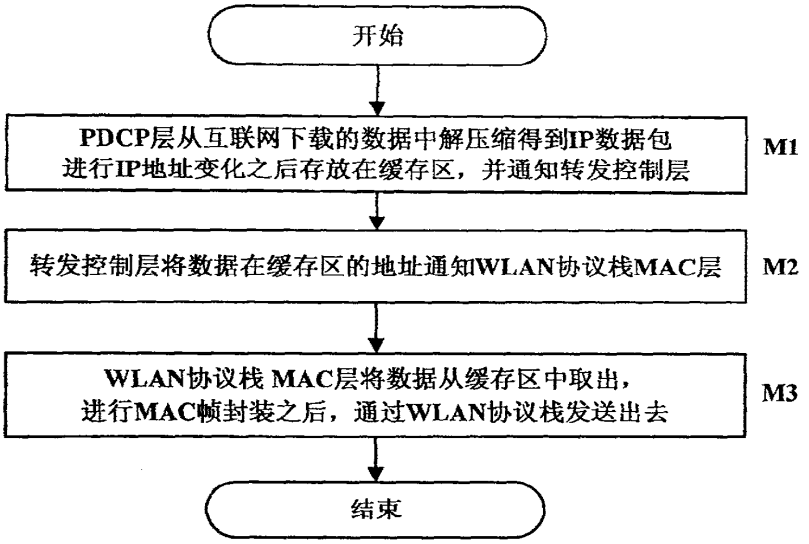


图 5

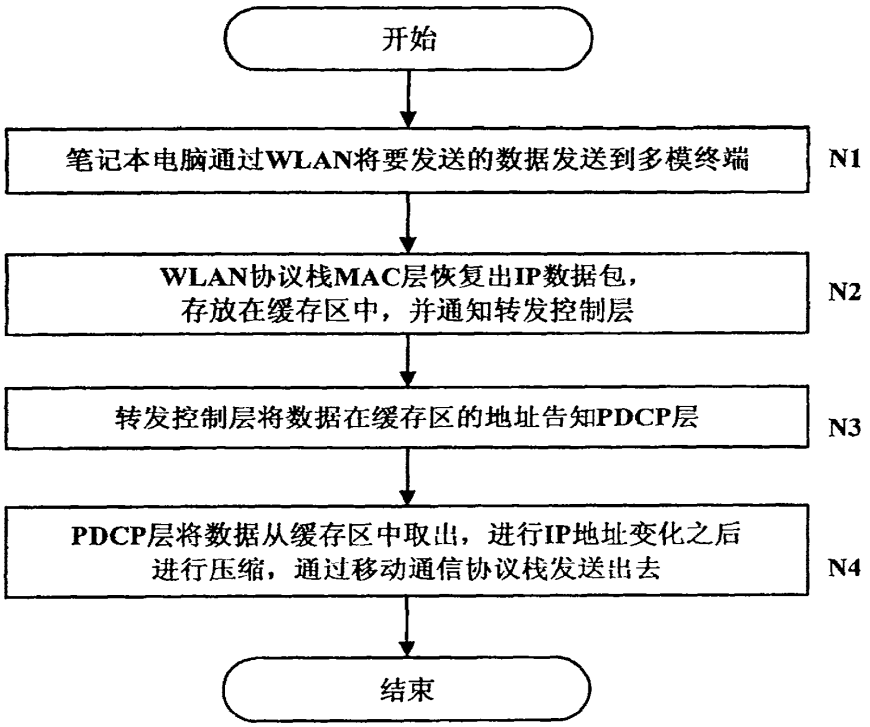


图 6

IPR2025-01571
Apple EX1002 Page 937

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04Q 3/00 (2006.01)
H04Q 7/24 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200580052316.4

[43] 公开日 2009 年 1 月 7 日

[11] 公开号 CN 101341764A

[22] 申请日 2005.12.16
[21] 申请号 200580052316.4
[86] 国际申请 PCT/EP2005/056843 2005.12.16
[87] 国际公布 WO2007/068288 英 2007.6.21
[85] 进入国家阶段日期 2008.6.16
[71] 申请人 艾利森电话股份有限公司
地址 瑞典斯德哥尔摩
[72] 发明人 R·诺尔杜斯 A·沙马

[74] 专利代理机构 中国专利代理(香港)有限公司
代理人 王 岳 张志醒

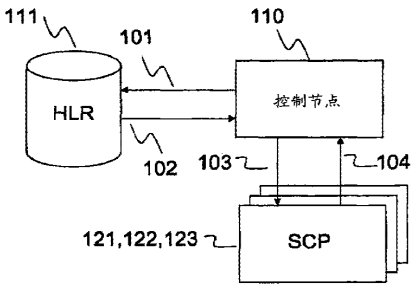
权利要求书 3 页 说明书 15 页 附图 6 页

[54] 发明名称

智能网服务

[57] 摘要

公开了用于处理与对移动电信网络的订户的呼叫相关联的智能网服务的方法、控制节点(110)和计算机程序，该网络包括所述控制节点(110)、HLR 5(111)和一个或多个 SCP(121、122、123)。所述控制节点(110)a)向所述 HLR(111)发送(101)与所述呼叫相关的路由信息的一个或多个请求；b)从所述 HLR(111)接收(102)与所述服务相关联的服务触发元素；c)使用所述触发元素在所述一个或多个(SCP)(121、122、123)中调用(103)所述服务；和 d)从所述一个或多个 SCP(121、122、123)接收与所述触发元素所关联的服务相关的信息。



IPR2025-01571
Apple EX1002 Page 938

1. 一种用于处理与对移动电信网络的订户的呼叫相关联的智能网服务的方法，该网络包括控制节点（110）、归属位置寄存器（111）和一个或多个服务控制点（121、122、123），该方法包括以下步骤：

a. 所述控制节点（110）向所述归属位置寄存器（111）发送（101）与所述呼叫相关的路由信息的一个或多个请求；

b. 所述控制节点（110）从所述归属位置寄存器（111）接收（102）与所述服务相关联的服务触发元素；

c. 所述控制节点（110）使用所述触发元素在所述一个或多个服务控制点（121、122、123）中调用（103）所述服务；

d. 所述控制节点（110）从所述一个或多个服务控制点（121、122、123）接收（104）与所述触发元素所关联的所述服务相关的信息。

2. 根据权利要求 1 所述的方法，其中所述归属位置寄存器（111）响应于路由信息的第一请求发送所述多个服务触发元素中的第一服务触发元素，并且响应于路由信息的第二请求发送所述多个服务触发元素中的第二服务触发元素。

3. 根据权利要求 1 所述的方法，其中所述归属位置寄存器（111）响应于路由信息的第一请求发送所述多个服务触发元素。

4. 根据权利要求 2 或 3 所述的方法，其中所述归属位置寄存器（111）响应于路由信息的第二请求发送所请求的路由信息。

5. 根据权利要求 2-4 中任何一个权利要求所述的方法，其中所述路由信息的第二请求与所述控制节点（110）和被访问移动服务交换中心（112）之间信令连接的建立相关联。

6. 根据前面任何一个权利要求所述的方法，其中所述请求的路由信息包括用于对所述订户的呼叫的移动站漫游号码。

7. 根据前面任何一个权利要求所述的方法，其中多个所述服务触发元素包括在一个移动应用部分消息中。

8. 根据权利要求 7 所述的方法，其中由于移动应用部分的分段，所述一个移动应用部分消息在多个信令连接控制部分消息中从所述归属位置寄存器（111）发送到所述控制节点。

9. 根据权利要求 1-6 中任何一个权利要求所述的方法，其中所述一个或多个所述服务触发元素作为前缀或后缀包括在移动站漫游号码

IPR2025-01571
Apple EX1002 Page 939

中。

10. 根据权利要求 1-6 中任何一个权利要求所述的方法，其中所述服务触发元素包括分离的参数。

11. 根据前面任何一个权利要求所述的方法，其中所述服务的第一服务在所述一个或多个服务控制点（121、122、123）中的第一服务控制点（121）中执行，并且所述服务的第二服务在所述一个或多个服务控制点（121、122、123）中的第二服务控制点（122）中执行。

12. 根据权利要求 11 所述的方法，其中所述服务的第一服务是预付费计费服务。

13. 根据权利要求 11 或 12 所述的方法，其中所述服务的第二服务是诸如个人问候服务的移动被叫服务。

14. 根据前面任何一个权利要求所述的方法，其中所述控制节点（110）是网关移动交换中心（110）。

15. 根据权利要求 2-14 中任何一个权利要求所述的方法，其中所述第一请求包含所述订户的移动站 ISDN 号码。

16. 根据权利要求 2-15 中任何一个权利要求所述的方法，其中所述第二请求包含所述订户的移动站 ISDN 号码和“抑制 T-CSI”参数。

17. 根据前面任何一个权利要求所述的方法，其中所述路由信息的一个或多个请求中的第一或第二请求包括移动应用部分发送路由信息消息。

18. 一种用于处理与对移动电信网络的订户的呼叫相关联的智能网服务的控制节点（110），该网络包括控制节点（110）、归属位置寄存器（111）和一个或多个服务控制点（121、122、123）；控制节点（110）配置用于向所述归属位置寄存器（111）发送对与所述呼叫相关联的路由信息的一个或多个请求；控制节点（110）还配置用于从所述归属位置寄存器(111)接收与所述服务相关联的多个服务触发元素，并且用于通过使用所述触发元素在所述一个或多个服务控制点（121、122、123）中调用所述服务；控制节点还配置用于从所述一个或多个服务控制点（121、122、123）接收与所述触发元素所关联的所述服务相关的信息。

19. 一种计算机程序，其包括致使计算机执行依照权利要求 1-17 中任何一个所述的方法的程序指令。

IPR2025-01571
Apple EX1002 Page 940

20. 一种载体上的计算机程序，其包括致使计算机执行依照权利要求 1-17 的方法的计算机可执行指令。

21. 根据权利要求 19 所述的计算机程序，其中所述载体是记录介质、计算机存储器、只读存储器或电载体信号。

IPR2025-01571
Apple EX1002 Page 941

智能网服务

技术领域

本发明涉及用于处理与对移动电信网络的订户的呼叫相关的智能网服务的方法和控制节点。

背景技术

在当前的电信网络技术诸如 GSM（全球移动通信系统）中，智能网服务是众所周知的。

GSM 网络的核心网络子系统的中央部件是移动服务交换中心（MSC）。它起类似于 PSTN 或 ISDN 的交换节点的作用，并且另外提供用于处理移动订户所需的所有功能，诸如注册、鉴权、位置更新、移交和到漫游订户的呼叫路由。这些服务连同几个功能实体一起被提供，它们一起构成了核心网络子系统。网关 MSC（GMSC）提供到固定网络（诸如 PSTN 或 ISDN）的连接。核心网络子系统中的功能实体之间的信令使用 7 号信令系统，7 号信令系统在 ISDN 中用于中继信令并且在当前的公共网络中广泛使用。

归属位置寄存器（HLR）和访问位置寄存器（VLR）与 MSC 一起提供 GSM 的呼叫路由和漫游能力。HLR 包含在相应的 GSM 网络中注册的每个订户的所有管理信息，以及该移动站的当前位置。移动站的位置通常是与该移动站相关联的 VLR 的信令地址的形式。在逻辑上说，每个 GSM 网络一个 HLR，尽管它可以实现为分布式数据库。

VLR 为当前位于由该 VLR 控制的地理区域内并且当前由该 VLR 服务的每个移动站包含对于呼叫控制和提供预订的服务所必须的来自 HLR 的选定管理信息。尽管每个功能实体可以实现为独立的单元，当前所有的交换设备制造商将 VLR 与 MSC 一起实现，这样由 MSC 控制的地理区域与 VLR 所控制的地理区域相对应，从而简化了所需的信令。MSC 不包含关于特定移动站的信息；这个信息在位置寄存器中存储。

接下来，将描述 GSM 网络中典型的入局呼叫建立（移动被叫（mobile terminating call））。

当订户对移动电话发起呼叫，它拨打与该电话用户相关联的电话号

IPR2025-01571
Apple EX1002 Page 942

码，即所谓的移动站 ISDN（MSISDN）号码，并且该呼叫被路由到该移动电话运营商的网关 MSC。网关是用于互连两个网络的节点。网关通常在 MSC 中实现，在这种情况下 MSC 称为 GMSC。GMSC 作为从公共交换电话网络的外面部分到供应商网络的入口。

如上所述，电话可以自由地漫游到运营商网络之中或漫游合作商的网络上的任何地方，包括其它国家。因此，网关 MSC 的第一个任务是确定移动电话的当前位置以便连接该呼叫。它通过咨询 HLR 来做到这一点，如上所述 HLR 知道在该时刻该电话与哪个访问位置寄存器（VLR）相关联（如果有的话）。

当 HLR 接收到这个查询消息，它确定是否应该将该呼叫路由到另一个号码（称为转移）或者应该将该呼叫直接路由到被呼叫订户的移动站。

如果电话的所有者先前已经请求将所有的入局呼叫转接到另一个号码，该补充服务也称为到被转接号码（FTN）的无条件呼叫转接（CFU），那么这个 FTN 被存储在 HLR 中。如果是这种情况，那么将 FTN 返回该网关 MSC 以便立即路由到那个目的地。

如果移动站当前不与 VLR 相关联（例如因为电话已经关机），那么 HLR 返回称为呼叫不可转接（CFNR）号的号码给 GMSC，并且该呼叫被转接到那里。许多运营商可以将这个值自动设置为该电话的语音邮箱号码，这样呼叫者可以留下消息。

最后，如果 HLR 知道该电话在特定 VLR 的管辖范围之内，那么它将从该 VLR 请求一个临时号码，即所谓的移动站漫游号（MSRN）。这个号码被中继到 GMSC，GMSC 使用它将该呼叫路由到称为被访问 MSC（VMSC）的另一个 MSC。

当 VMSC 接收到该呼叫时，使用 MSRN 在 VLR 中寻找该电话的记录。这个记录标识该电话的位置区域。对该区域中的所有移动电话杆（mobile phone mast）发生寻呼。当订户的移动电话响应时，该电话的确定位置被返回给 VMSC。VMSC 随后将呼叫转接到合适的电话杆，并且该电话响铃。如果订户应答，通过该 VMSC 和 GMSC 创建回到人进行呼叫的网络的语音通路，并且随后是一般的电话呼叫。

也可能呼叫没有被应答。如果订户在忙于另一个呼叫（并且没有使用呼叫等待），那么 VMSC 将呼叫路由到预定的遇忙呼叫转接（CFB）

IPR2025-01571
Apple EX1002 Page 943

号码。类似的 ，如果订户在一段时间（通常是 30 秒）之后没有应答呼叫，那么 VMSC 将该呼叫路由到预定的无应答呼叫转接（CFNRy）号码。再次的，运营商可以决定默认将这个值设置为该电话的语音邮箱，以便呼叫者能够留下消息。

智能网（IN）是与电信网络耦合的使得运营商能够采用运营商特有的增值服务（VAS）的网络。通过来自智能网的智能增加了交换机中驻留的智能，智能网中的智能安置在分布在网络中各处的计算机节点中。这给网络运营商提供了更有效地开发、采用和控制服务的方式。新的服务可以快速引入到电信网络中。一旦引入，服务可以容易地定制以满足个体客户的需求。

IN 服务通常由服务控制点（SCP）提供。SCP 是与电信网络中的其它节点和实体通信的控制计算机。SCP 包括一个或多个 IN 服务的服务逻辑，并且可选包括 IN 服务预订数据，该预订数据允许 SCP 依照订户的特定设置执行 IN 服务，即特制对该订户的服务执行。当建立了呼叫时，电信网络可以询问 SCP 并且请求处理这个呼叫的指令。例如，SCP 被咨询提供 800 号码到实际电话号码的翻译，并且为该呼叫对该 800 号码的所有者计费。SCP 在物理上可以与智能网的其它组件分离，或者可以与这些其它组件组合到单个节点中。

在 GSM 网络中，IN 服务预订信息在 HLR 中存储。HLR 中驻留两个类型的信息：（1）静态订户信息和（2）动态订户信息。后者例如需要允许将入局呼叫路由到该移动订户。HLR 存储以下信息及其它：

- 国际移动订户身份（IMSI）；只由该网络使用的内部订户身份；
- MSISDN 号码；
- VLR 地址；
- 关于补充服务的订户数据。

IN 服务可以分为两个种类。一个种类包括为发起呼叫（终端发起呼叫-MOC）的订户调用的服务。这些服务称为终端发起（MO）服务。MO 服务的一个例子是出局呼叫屏蔽。

每个 IN 服务订户在他的 HLR 中用发起 CAMEL 预订信息（O-CSI）元素标记，该元素用于在SCP标识特定服务。一旦订户启动 MO呼叫，O-SCI 启动MOC 服务的触发。在上述例子中采用了 CAMEL，其代表“用于移动网络增强逻辑的定制应用”。CAMEL 发展为用于扩展陆地线路 IN 电话

IPR2025-01571
Apple EX1002 Page 944

服务的标准，诸如呼叫等待和到 GSM 移动电话的呼叫转接。

另一种类包括为接收呼叫（移动被叫-MTC）的订户调用的服务。这些服务称为移动被叫（mobile terminating,MT）服务。移动被叫服务的例子是呼叫转移服务和个人问候服务（PGS）。PGS 是与漫游支线相关的服务。PGS 使得当在 GMSC 和 VMSC 之间（所谓的漫游支线）建立了信令连接，向呼叫方显示个人化的问候。个人化问候替换了传统的警报音调（“响铃音调”）。这样，个人化问候主要与漫游支线的建立相关；只有当漫游支线建立并且警报了被呼叫方的时候响铃音调才变得有效。每个 IN 服务订户在他的 HLR 中利用终止 CAMEL 预订信息（T-SCI）标志来标记，该标记用于在 SCP 标识特定服务。这在试图对订户呼叫期间启动 MTC 服务的触发。

依照当前技术，控制节点在 MTC 处理期间可以询问 HLR 以便获得来自 HLR 的指令。控制节点可以是 GMSC。响应于控制节点的询问，HLR 可以发送用于被叫的 IN 触发信息。在 HLR 和控制节点之间交换的 IN 触发信息已经被标准化。例如，如在 3GPP TS 29.002 中由 3GPP（第三代合作伙伴计划）指定的，T-CSI 是 GSM 标准化的用于被叫的 IN 触发信息。IN 触发信息包括 IN 服务所驻留的 SCP 的地址和标识该 SCP 内的特定 IN 服务的服务关键字。

按照在 IN 触发信息中为订户指定的，控制节点使用该 IN 触发信息来调用 SCP 中的 IN 服务。响应于服务调用，SCP 依赖于该服务执行的结果向控制节点发送指令，例如继续建立呼叫或被叫。当前网络通常设置为为一个 MTC 处理 IN 服务的单个调用。但是近来的发展显示，在被叫处理期间需要调用两个或更多 IN 服务。

专利申请 WO00/25528 公开了在 SCP 中包含的服务交互管理器。服务交互管理器的任务是确定应该为订户执行 SCP 中的哪些可用服务并且以特定顺序调用这些服务。

发明内容

本发明的目的是提供通过允许订户对于一个呼叫拥有多于一种 IN 服务来克服当前技术的缺点的方法和设备。

在本发明的第一方面，提出了一种处理与对移动电信网络的订户的呼叫相关的智能网服务的方法，该网络包括控制节点、归属位置寄存

IPR2025-01571
Apple EX1002 Page 945

器和一个或多个服务控制点，该方法包括以下步骤：

a. 所述控制节点向所述归属位置寄存器发送与所述呼叫相关的路由信息的一个或多个请求；

b. 所述控制节点从所述归属位置寄存器接收与所述服务相关的服务触发元素；

c. 所述控制节点使用所述服务触发元素在所述一个或多个服务控制点中调用所述服务；

d. 所述控制节点从所述一个或多个服务控制点接收与所述触发元素所关联的所述服务相关的信息。

以此方式，可以为预订了属于订户的一个呼叫的一个或多个 IN 服务的该订户处理多个服务触发元素。IN 服务不需知道在用于该呼叫的控制节点中一个或多个其它 IN 服务的存在。换句话说，第一服务不需知道是否将调用第二服务，反之亦然。因为服务不要求关于为这个呼叫可能调用其它 IN 服务的知识，服务可以运行在不同平台上并且可以由不同的卖主供应。

存在本发明的若干实施例。

例如，本发明可以规定归属位置寄存器响应于路由信息的第一请求而发送所述多个服务触发元素中的第一服务触发元素，并且响应于路由信息的第二请求而发送所述多个服务触发元素中的第二服务触发元素。

所述路由信息的第一请求可以包括：

- 订户的 MSISDN 号码。

对路由信息的第一请求的响应可以包括：

- 第一服务触发元素。

路由信息的第二请求可以包括：

- 订户的 MSISDN 号码；
- HLR 应该在所述响应中抑制第一服务触发元素的指示。这个指示可以是例如“抑制 T-SCI”参数。

对路由信息的第二请求的响应可以包括：

- 用于呼叫被服务订户的 MSRN；
- 第二服务触发元素；
- 订户的 MSRN 的前缀或后缀。

IPR2025-01571
Apple EX1002 Page 946

由于 MAP 分段，MAP 消息可以在多个信令连接控制部分消息中被从 HLR 发送给 GMSC。第一服务，例如预付费计费服务，在第一服务控制点中执行，第二服务，例如 PGS，在第二 SCP 中执行。

以此方式，可以将预付费服务和 PGS 提供给相同订户；预付费服务和 PGS 可以在不同平台上运行并且彼此不相关。

当本发明用于 PGS 时，呼叫订户可以收听任何呼叫进程消息，即使当利用最优路由的早期呼叫转接或晚期呼叫转接发生的时候。

本发明的另一个优点是可以将 PGS 提供给虚拟私人网（VPN）订户。

在本发明的第二方面，提出了一种处理与对移动电信网络的订户的呼叫相关的智能网服务的控制节点，该网络包括所述控制节点、HLR 和一个或多个 SCP；控制节点配置用于向所述 HLR 发送与所述呼叫相关的路由信息的一个或多个请求；控制节点还配置用于从所述 HLR 接收与所述服务相关联的多个服务触发元素，并且用于通过使用所述触发元素在所述一个或多个 SCP 中调用所述服务；控制节点进一步配置用于从所述一个或多个 SCP 接收与所述触发元素所关联的服务相关的信息。

在优选实施例中，控制节点包括 GMSC。无论如何，控制节点也可以包括诸如 MSC 或 SCP 的设备。

本发明的第三方面提出了一种计算机程序，该计算机程序包括致使计算机执行依照本发明的方法的程序指令。

计算机程序可以存储在载体上，并且可以包括致使计算机执行依照本发明的方法的计算机可执行指令。

计算机程序的载体可以是记录介质、计算机存储器、只读存储器或电载体信号。

本发明提出可以为对订户的特定呼叫类型提供多种 IN 服务。至此，HLR 可以已经注册了特定 IN 呼叫类型预订的多个指示（此后称为 IN 触发元素）。

附图说明

图 1 是移动电信网络中设备的当前技术配置的框图。

图 2 是依照本发明的方法和设备的信令图。

图 3 是依照本发明的设备的框图。

图 4 是本发明的方法实施例的信令图。

IPR2025-01571
Apple EX1002 Page 947

图 5 是本发明的方法实施例的信令图。

图 6 是本发明的方法实施例的信令图。

具体实施方式

为了本发明的目的，GMSC 中的 MT 呼叫处理可以分为两个逻辑部分：

（1） 被叫处理；

（2） 漫游支线处理。

被叫处理包括从 HLR 获取 T-CSI 并且调用第一 CAMEL 服务。第一 CAMEL 服务可以强加呼叫限制或者可以施加呼叫转接。通常，对于被呼叫订户漫游的情况，第一 CAMEL 服务也可以用于终止计费。HLR 也可以与 T-CSI 一起返回其它 IN 触发元素。

漫游支线处理包括从 HLR 获取 MSRN 并且将呼叫从 GMSC 路由到终止 MSC，在终止 MSC 被呼叫方在该时刻注册。注意“漫游支线”同等适用于订户在被访问公共陆地移动网络（VPLMN）和订户在归属公共陆地移动网络（HPLMN）中的情况。也就是说，在这个例子中“漫游”不与“在另一个网络或另一个国家中”相关联。

本发明提出了沿着上述区别的线路，为 MT 呼叫进行两个 IN 服务的调用。依照本发明，可以定义用于 MT 呼叫的两种类型的 IN 服务：

（1）需要对 MT 呼叫的控制并且可能需要影响该呼叫的路由的能力的 IN 服务。这些类型的 IN 服务还需要知道目的地订户的位置，从而可以施加计费。

（2）只要求到目的地订户的漫游支线的 IN 服务。这类 IN 服务只有在建立了漫游支线，即 GMSC 已经从 HLR 接收到 MSRN 的时候，才被调用。

如果 HLR 返回转接号码（FTN）而不是 MSRN，那么将不存在漫游支线，并且随后将不会调用与漫游支线相关的 IN 服务。

图 1 是移动电信网络中的设备的当前技术配置的框图。所示的实体至少在概念上属于不同于移动通信网络的智能网。智能网包括 HLR 111、SCP1 121、SCP2 122 和 GMSC 110。GMSC 110 与 SCP1 和 SCP2 以及 HLR 111 对接，以执行众所周知的 IN 触发功能。SCP1 和 SCP2 包括在处理移动被叫期间可以被顺序调用的智能网服务。

图 2 是依照本发明的方法和设备的信令图，其具有各种元件之间的

IPR2025-01571
Apple EX1002 Page 948

关系的概览。该方法包括以下步骤:

步骤 101 控制节点 110 向 HLR 111 发送与所述呼叫相关的路由信息的一个或多个请求;

步骤 102 HLR 111 向所述控制节点 110 发送与所述服务相关联的多个服务触发元素;

步骤 103 控制节点 110 使用所述触发元素在一个或多个服务控制点 121、122、123 中调用一个或多个服务;

步骤 104 所述一个或多个服务控制点 121、122、123 向所述控制节点 110 发送与所述触发元素所关联的一个或多个服务相关的信息。

图 3 是依照本发明的设备和它们的相互关系的框图。

所述块(设备)之间的线表示通信路径。HLR 111 可以与 GMSC 110 和 VMSC 112 通信。GMSC 可以与 SCP1 121 和其它随后被调用的 SCP(SCPn) 122 通信。GMSC 110 可以与 VMSC 112 通信。

图 4 是本发明的方法实施例的信令图,该实施例包括图 3 所示的设备之间的通信序列,所述设备包括 GMSC 110、HLR 111、多个 SCP121、122 和 VMSC 112。在这个例子中,订户预订了 CAMEL 服务并且另外预订了可能是 IN 服务的至少一个服务。对于这个例子,只示出了与两个 SCP 121、122 的通信。但是,可以为第三个 SCP 重复步骤 6-11,并且以此类推。以下步骤发生:

步骤 401 ISUP 初始地址消息(IAM)到达 GMAC 110; GMSC 110 分析 ISUP IAM 中的被呼叫方号码并且推导出该被呼叫方号码是属于它自己的网络的 MSISDN。

步骤 402 GMSC 110 向 HLR 111 发送 MAP 发送路由信息(SRI)。GMSC 110 在 MAP SRI 中指示它支持 CAMEL。

步骤 403 被呼叫方具有对用于 MT 呼叫处理的 CAMEL 服务的预订。结果是,HLR 111 向 GMSC 110 发送 MAP SRI-Res,其包括用于 MT 呼叫的 IN 触发信息,T-CSI。

步骤 404 GMSC 110 使用 T-CSI 来调用 CAMEL 服务。GMSC 110 例示内部 GSM 服务交换功能(gsmSSF)实体; gsmSSF 向 SCP 发送 CAP 初始检测点(IDP)。SCP1 121 的地址和与这个 IN 对话相关的其它数据从 T-CSI 获得。GsmSSF 功能与 GMSC 交互工作。基于在用户的预订中定义的并且从 HLR 发送给 GMSC 的信息,设置 GMSC 和 gsmSSF 内的服务触发。

IPR2025-01571
Apple EX1002 Page 949

这些触发用于指示 gsmSSF 何时应该与 gsmSCF 通信。这接下来将确定如何处理基于 IN 的服务。

步骤 405 SCP1 121 以 CAP 继续（CUE）响应，以便通知 GMSC 110 MT 呼叫处理可以继续，即可以将呼叫传递给被呼叫订户。SCP1 121 和 GMSC 110 之间的控制会话可以保持。SCP1 121 中的 CAMEL 服务不需要具有关于除了该 CAMEL 服务外当前执行的其它 IN 服务的知识。

步骤 406 GMSC110 向 HLR 111 发送第二询问，即向 HLR 111 发送第二 MAP SRI。第二 MAP SRI 包括“抑制 T-CSI”标志。

步骤 407 HLR 111 通过“抑制 T-CSI”的存在识别出该 MAP SRI 是第二 SRI，并且通过向被呼叫方当前所注册的 VMSC 112 发送 MAP 提供漫游号码（PRN）来响应。

步骤 408 VMSC 112 分配用于这个呼叫的 MSRN，并且通过向 HLR 111 发送 MAP PRN-Res 而向 HLR 111 返回该 MSRN。

步骤 409 HLR 111 通过向 GMSC 110 发送 MAP SRI 响应（SRI-Res）而将该 MSRN 转发给 GMSC 110。被呼叫订户预订了用于 MT 呼叫处理的第二 IN 服务。第二 IN 服务是如前面本发明的公开部分所述的漫游支线处理类型。HLR 111 在所述 MAP SRI-Res 中包括与这个第二 IN 服务相关联的 IN 触发信息。为了本发明的目的，这个第二 IN 触发信息命名为“RICK”（漫游支线 IN 种类关键字）。RICK 可以具有如 T-CSI 或 TICK（终止 IN 种类关键字）的结构。为了能够接收 RICK，GMSC 110 在第二 MAP SRI（步骤 6）中指示它支持这个信息元素，即它支持 RICK。“支持 RICK”的指示类似于“支持 TICK”的指示。从 GMSC 向 HLR 发送的“支持 TICK”向 HLR 表明它支持 TICK。TICK 具有与 T-CSI 可比的功能性；但是，TICK 不是标准化的。

步骤 410 GMSC 110 认识到 MSRN 伴随有 RICK。RICK 对于 GMSC 110 作为表明漫游支线应该服从 IN 服务的指示。因此，GMSC 110 通过向 SCPn 122 发送 CAP IDP，使用 RICK 调用 IN 服务。SCPn 122 的地址和与这个 IN 对话相关的其它数据从 RICK 获得。

步骤 411 SCPn 122 以 CAP CUE 响应，通知 GMSC 110 该 MT 呼叫处理可以继续，即可以建立到被呼叫订户的漫游支线。

步骤 412 GMSC 110 通过向目的地交换机发送 ISUP IAM，建立到被叫订户的漫游支线。该 ISUP IAM 包含从 HLR 111 接收到的 MSRN。

IPR2025-01571
Apple EX1002 Page 950

步骤 401-408 表示一般 GSM 呼叫处理。

步骤 409 表示对现有 MT 呼叫处理的改进。HLR 111 一般将只返回 MSRN 给 GMSC 110。步骤 409 对 MAP SRI-Res 添加了 RICK。

步骤 410 和 411 在现有漫游支线处理中不存在。这些步骤表示在 GMSC 110 中对用于 MT 呼叫处理的第二 IN 服务的调用。

当该呼叫被传递到被呼叫订户时，两个 IN 服务可以维持有效。作为向 GMSC 110 发送 T-CSI 的结果而触发的第一 IN 服务可以对整个呼叫维持有效，并且按照用于那个服务的 IN 协议所允许的具有完全可用的能力。

作为向 GMSC 110 发送 RICK 的结果而触发的第二 IN 服务也可以对整个呼叫维持有效。但是，这个 IN 服务应该使用具有某些限制的 IN 能力。作为一个例子，这个服务不应该应用呼叫转接，因为那将影响该呼叫的预付费服务。

本发明可以应用在不同类型的 GSM 呼叫转接上。通过取类似于个人问候服务（PGS）的服务作为例子，可以充分显示出这一点。在呼叫转接的情况下，呼叫的目的地发生变化。一些运营商要求当到语音邮箱的呼叫转接发生时，PGS 服务终止。

关于在呼叫转接的情况下终止 PGS 服务，基本存在两种类型的呼叫转接：早期呼叫转接（ECF）和晚期呼叫转接（LCF），当在 GMSC 110 中发生早期呼叫转接的时候，GMSC 110 没有从 HLR 111 接收用于这个呼叫的 MSRN 并且没有建立漫游支线。GMSC 110 将不建立到被呼叫方的漫游支线，并且作为结果，将不调用漫游支线 IN 服务。

在早期呼叫转接的情况中，HLR 111 不在第二 SRI 结果中返回 MSRN 并且依照本发明不返回 RICK。GMSC 110 现在将该呼叫转接到转接目的地，其可以是例如语音邮箱或者是呼叫结束服务。因为 HLR 111 没有返回 RICK，将不存在 PGS 调用。呼叫订户现在可以收听语音邮箱播放的任何通告，即使语音邮箱将 ISUP 应答消息（ISUP ANM）的生成推迟了限定的持续时间。

当在 VMSC 112 中发生晚期转接的时候，随后可以应用晚期呼叫转接的最佳路由（ORLCF）以便将呼叫处理返回给 GMSC 110。GMSC 110 终止该漫游支线，并且因而漫游支线 IN 服务同样将被终止。在晚期呼叫转接的情况下，所述呼叫已经被路由到被呼叫订户的目的地 MSC。当晚

IPR2025-01571
Apple EX1002 Page 951

期呼叫转接的情况发生，VMSC 112 可以向 GMSC 110 发送 MAP 恢复呼叫处理（RCH）；MAP RCH 的发送是 ORLCF 的一部分。

当 GMSC 110 接收到 MAP RCH 并且批准对 ORLCF 的请求，它释放漫游支线并且创建转接支线。呼叫方可以收听由转接目的地生成的任何通告。

一些运营商采用语音邮箱系统，由此初始通告是免费的。这可以通过令语音邮箱推迟 ISUP ANM 的生成来实现。如果 PGS 在这样的情况下保持有效，那么呼叫方将不会收听到在 ISUP 地址完成消息（ACM）和 ISUP ANM 之间播放的任何通告。原因是个人问候服务保持有效，直到检测到 ISUP ANM。在那种情况下将不会收听到语音邮箱的初始通告。

本发明解决了那个问题，因为在晚期呼叫转接联合 ORLCF 的情况下 PGS 将被终止。

如果晚期呼叫转接没有经受 ORLCF，那么漫游支线服务可以监视诸如呼叫进程（CPG）和 ACM 的 ISUP 消息。这些 ISUP 消息可以指示转接正在发生。

一些运营商应用 PGS 的服务节点解决方案。这意味着对于 PGS 订户，漫游支线需要通过特殊的服务节点（位于内嵌在用于漫游支线的 ISUP 通信链路内）路由。服务节点将把该呼叫广播给目的地 MSC。依照本发明可以实现通过服务节点的漫游支线的路由。利用 RICK 调用的 IN 服务可以为 MSRN 提供前缀，导致呼叫被通过所述服务节点路由。

可替换地，包括在 SRI-Res 中的 RICK 可以具有数字前缀的形式；诸如 GMSC 的交换节点在将该呼叫转接到下一个交换节点之前，将该 RICK 放置在 MSRN 的前面。

可以配置在这个转换节点中的 B-号码分析，使得 RICK 导致选择到所述服务节点的路由。

漫游支线的预订的或一般的 IN 服务的概念可以用于以下类型的服务：

- 个人问候：只有当漫游支线成功建立的时候需要播放个人问候；如果由于无论什么原因，漫游支线没有能够建立或者在应答之前终止，那么不需要个人问候。运营商可以希望在为呼叫分配 MSRN 之前调用 PGS。那样的效果可能是，当到第二被呼叫方的转接发生时，呼叫方将仍然听到第一方的个人问候。另外，这样的配置将具有可能没有收听

IPR2025-01571
Apple EX1002 Page 952

到呼叫转接通告的效果。

- 服务节点路由：对于特定订户，漫游支线可能需要通过服务节点被路由。

- 载体选择：订户可以预订只适用于漫游支线的载体选择服务。

当 HLR 111 向 GMSC 110 发送包括 MSRN 的 SRI-Res 时，它可以包括 RICK。作为可选的实施方式，HLR 111 可以应用在 SRI-Res 中包括 RICK 的标准，类似于借此 HLR 111 应用在第一 SRI-Res 中包括 T-CSI 的标准的情况。这些标准可以是例如：

- 只有当订户在 HPLMN 中的时候在 SRI-Res 中包括 RICK;
- 只有当入局呼叫是语音呼叫的时候在 SRI-Res 中包括 RICK。

不是所有的 MT 呼叫需要终止 IN 服务。类似的，不是所有的 MT 呼叫需要 RICK 服务。作为一个例子，当预付费订户在 HPLMN 中的时候，HLR 111 可以在 SRI 中抑制 T-CSI。结果是，将没有 MT 呼叫服务被触发。如果在这种情况下仍然需要调用漫游支线服务，那么 HLR 111 可以在第一 SRI-Res 中包括 RICK。GMSC 110 中对 RICK 的进一步处理如前所述。

图 5 是本发明的方法实施例的信令图，其中通过在 GMSC 110 建立漫游支线之前由 GMSC 110 向 HLR 111 询问多个（IN）服务来执行对多个服务的调用。在这个实施例中，HLR 111 在第一询问发送所述 IN 服务的所有信息。步骤 501-502 依照当前技术执行。在这里例子中涉及 3 个 SCP，尽管本发明可以应用于多个 SCP。

步骤 501 ISUP IAM 到达 GMSC 110。

步骤 502 GMSC 110 分析 ISUP IAM 中的被呼叫方号码并且推导出该被呼叫方号码是属于它自己的网络的 MSISDN。GMSC 110 向 HLR 111 发送 MAP SRI。GMSC 110 在 MAP SRI 中指示它支持 CAMEL。GMSC 可以支持多个 CAMEL 阶段。

步骤 503 被呼叫方具有对用于 MT 呼叫处理的 CAMEL 服务的预订。结果是，HLR 111 向 GMSC 110 发送 MAP SRI-Res，其包括用于 MT 呼叫的 IN 触发信息，T-CSI。

步骤 504 GMSC 110 使用 T-CSI 来调用 CAMEL 服务。GMSC 110 例示内部 gsmSSF 实体；gsmSSF 向 SCP 121 发送 CAP IDP。SCP1 121 的地址和与这个 IN 对话相关的其它数据从 T-CSI 获得。

IPR2025-01571
Apple EX1002 Page 953

步骤 505 SCP1 121 以 CAP 继续（CUE）或 CAP 连接（CON）响应，以便通知 GMSC 110 MT 呼叫处理可以继续，即可以将呼叫传递给被呼叫订户。依赖于 IN 服务的要求，SCP1 121 和 GMSC 110 之间的控制会话可以保持或者终止。SCP1 121 中的 CAMEL 服务不具有关于除了该 CAMEL 服务外当前执行的其它 IN 服务的知识。

步骤 506 GSMC 110 基于 T-CSI 通过调用第二 IN 服务响应，第二 IN 服务可以仍是 CAMEL 服务。SCPn 122 的地址从第二 T-CSI 获得。

步骤 507 SCP 以 CAP CUE 或 CAP CON 响应，以便通知 GMSC 110 该呼叫处理可以继续，即可以将呼叫传递给被呼叫订户。这里，同样的，SCP2 122 中的 CAMEL 服务不具有关于这个呼叫的第一服务和第三服务的知识。

步骤 508 GMSC 110 检查是否为该订户提供了其它 IN 服务；如果提供的有，那么它基于 T-CSI 通过调用第三 IN 服务进行响应，该第三 IN 服务还可以是 CAMEL 服务。SCP3 123 的地址从第三 T-CSI 获得。

步骤 509 SCP 123 以 CAP CUE 或 CAP CON 响应，以便通知 GMSC 110 该呼叫处理可以继续，即可以将呼叫传递给被呼叫订户。SCP3 123 中的 CAMEL 服务不具有关于这个呼叫的第一服务和第二服务的知识。

步骤 510 GMSC 110 检查是否为该订户提供了其它 IN 服务；如果没有用于该订户的更多 IN 服务，那么 GMSC 110 通过向 HLR 111 发送第二询问进行响应，即向 HLR 111 发送第二 MAP SRI。

步骤 511 HLR 111 识别出该 MAP SRI 是第二 SRI 并且通过向被呼叫方当前被注册的 VMSC 112 发送 MAP 提供漫游号码（PRN）进行响应。

步骤 512 VMSC 112 分配 MSRN，并且通过向 HLR 111 发送 MAP PRN-Res 而向 HLR 111 返回该 MSRN。

步骤 513 HLR 111 通过向 GMSC 110 发送 MAP RSI-Res 将 MSRN 转发给 GMSC 110。

步骤 514 GMSC 110 通过向目的地交换机发送 ISUP IAM 建立到被呼叫订户的漫游支线。ISUP IAM 包含从 HLR 111 接收到的 MSRN。

图 6 是本发明的方法实施例的信令图，由此为 MO 呼叫调用多个 IN 服务。在这个实施例中发生以下步骤：

步骤 601 订户 621 利用 MSC 623 在被访问 GSM 网络中注册。

步骤 602 MSC 623 联系订户 621 的归属 PLMN 中的 HLR 111。

IPR2025-01571
Apple EX1002 Page 954

步骤 603 HLR 111 向 MSC 623 发送用于 IN 服务的多个触发元素。这些触发元素与用于终端发起呼叫和移动转接呼叫的 IN 服务相关联。

步骤 604 订户 621 建立 MO 呼叫。

步骤 605 MSC 623 使用第一触发元素以调用在与所述第一触发元素相关联的 SCP1 121 中的第一 IN 服务。

步骤 606 SCP1 121 中的第一 IN 服务通过发送 CAP 继续消息或 CAP 连接消息将呼叫的控制交回 MSC 623。

步骤 607 MSC 623 使用来自触发元素列表的第二触发元素在 SCP2 122 中调用第二 IN 服务。

对 SCP2 122（步骤 607 和 608）和 SCP3 123（609、610）重复步骤 605 和 606，并且直到调用了所有指示的 IN 服务。MSC 623 中的呼叫处理一般继续步骤 611:

步骤 611 MSC 623 将该呼叫路由到目的地 627。任何调用的 IN 服务可以在该呼叫的整个持续时间保持有效，或者可以在较早的阶段终止。

本发明覆盖以下情景:

1） GMSC 中用于 MT 呼叫处理的 IN 服务调用后跟随 GMSC 中用于漫游支线的 IN 服务调用。

2） GMSC 中用于漫游支线的 IN 服务调用。

3） 如同（1），由此 HLR 在第一询问响应中发送多个 IN 服务触发元素，目的是这些多个触发元素用于与所述 MT 呼叫相关联的多个 IN 服务的调用。

4） 如同（1），由此 HLR 在第二询问响应中发送多个 IN 服务触发元素，目的是这些多个触发元素用于与所述漫游支线相关联的多个 IN 服务的调用。

5） 如同（2），由此 HLR 在第二询问响应中发送多个 IN 服务触发元素，目的是这些多个触发元素用于与所述漫游支线相关联的多个 IN 服务的调用。

6） 如同（1），由此（3）和（4）组合。

7） 如同（1），由此 HLR 在第一询问响应中发送多个 IN 服务触发元素，目的是这些多个触发元素中的一些用于与所述 MT 呼叫相关联的多个 IN 服务的调用，并且这些多个触发元素中的一些用于与所述漫游支线相关联的多个 IN 服务

IPR2025-01571
Apple EX1002 Page 955

的调用。

8） 只有当漫游支线建立的时候需要用于 MT 呼叫的某些 IN 服务。本发明提供实现这一点的工具。

9） 本发明可以用于在预订的基础上或者对于所有服务的订户通过 ISUP 服务节点路由漫游支线。

IPR2025-01571
Apple EX1002 Page 956

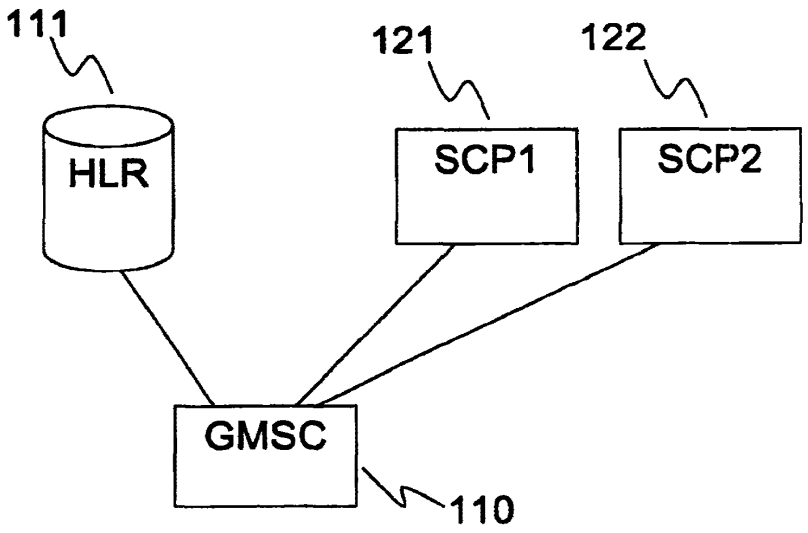


图 1

IPR2025-01571
Apple EX1002 Page 957

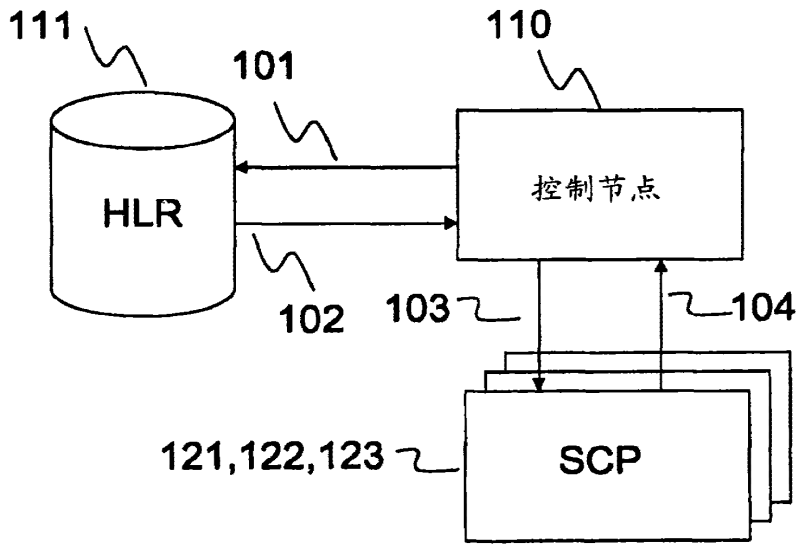


图 2

IPR2025-01571
Apple EX1002 Page 958

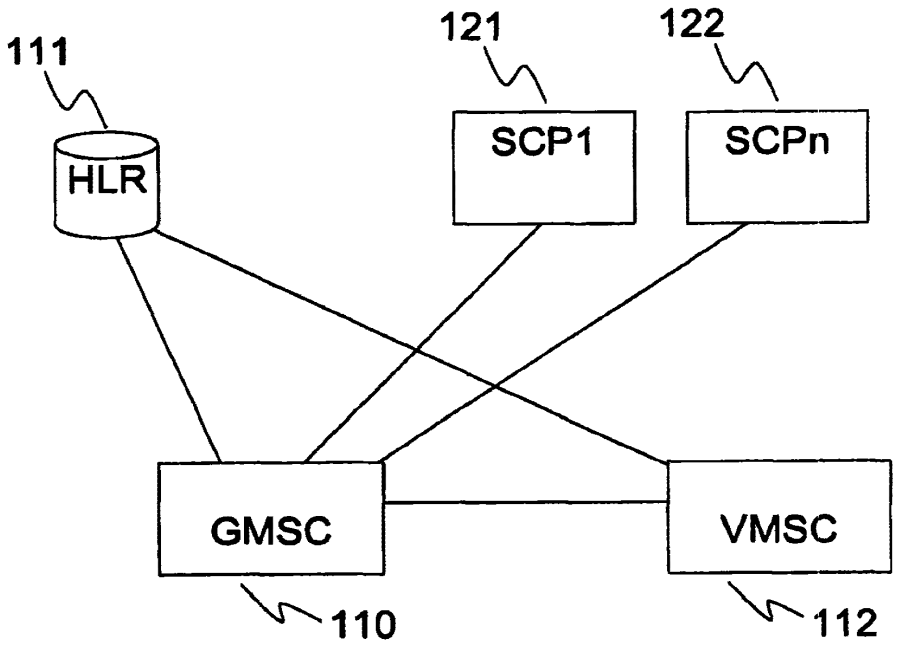


图 3

IPR2025-01571
Apple EX1002 Page 959

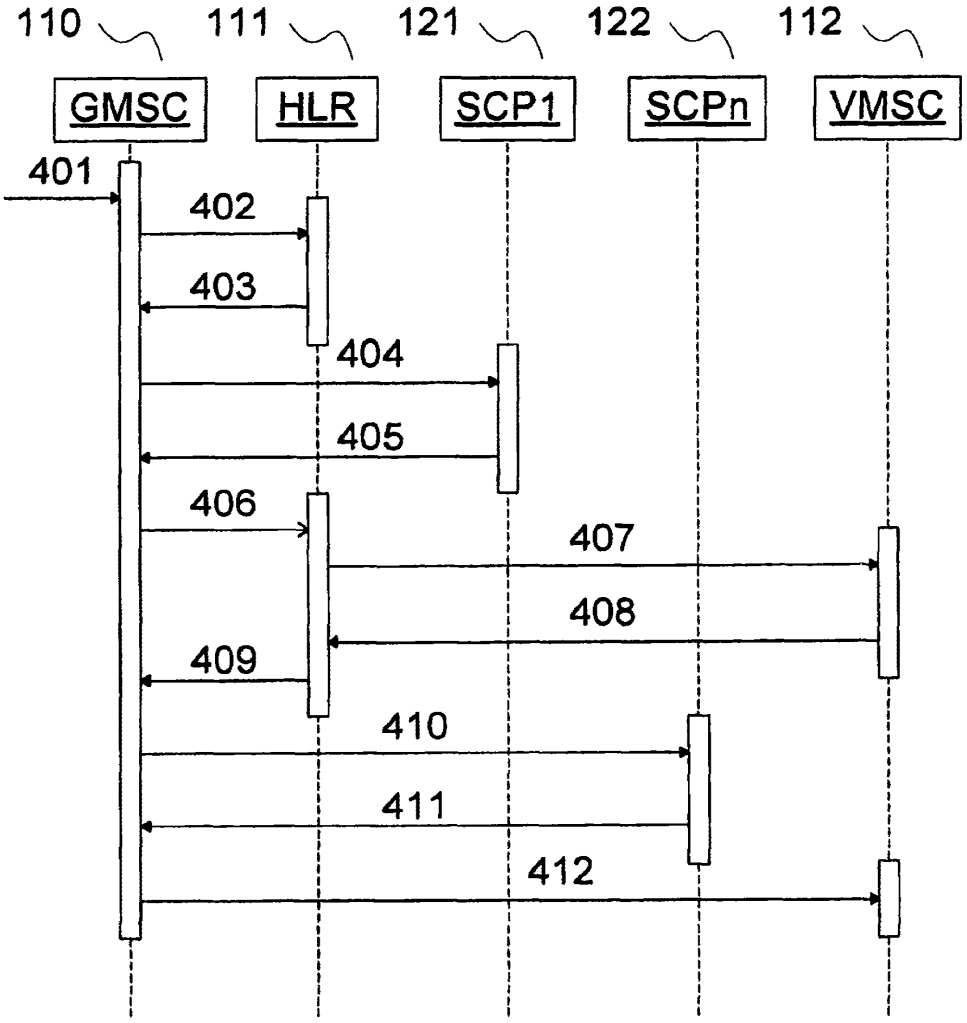


图 4

IPR2025-01571
Apple EX1002 Page 960

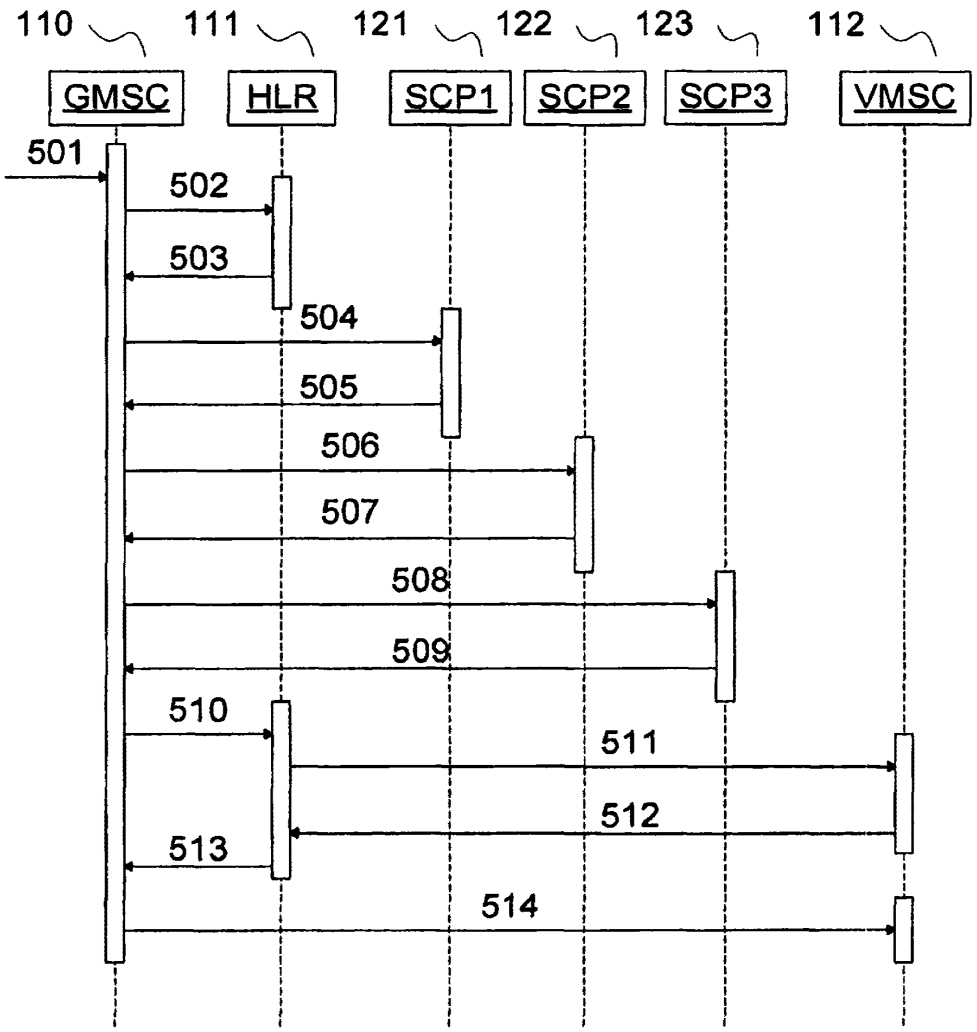


图 5

IPR2025-01571
Apple EX1002 Page 961

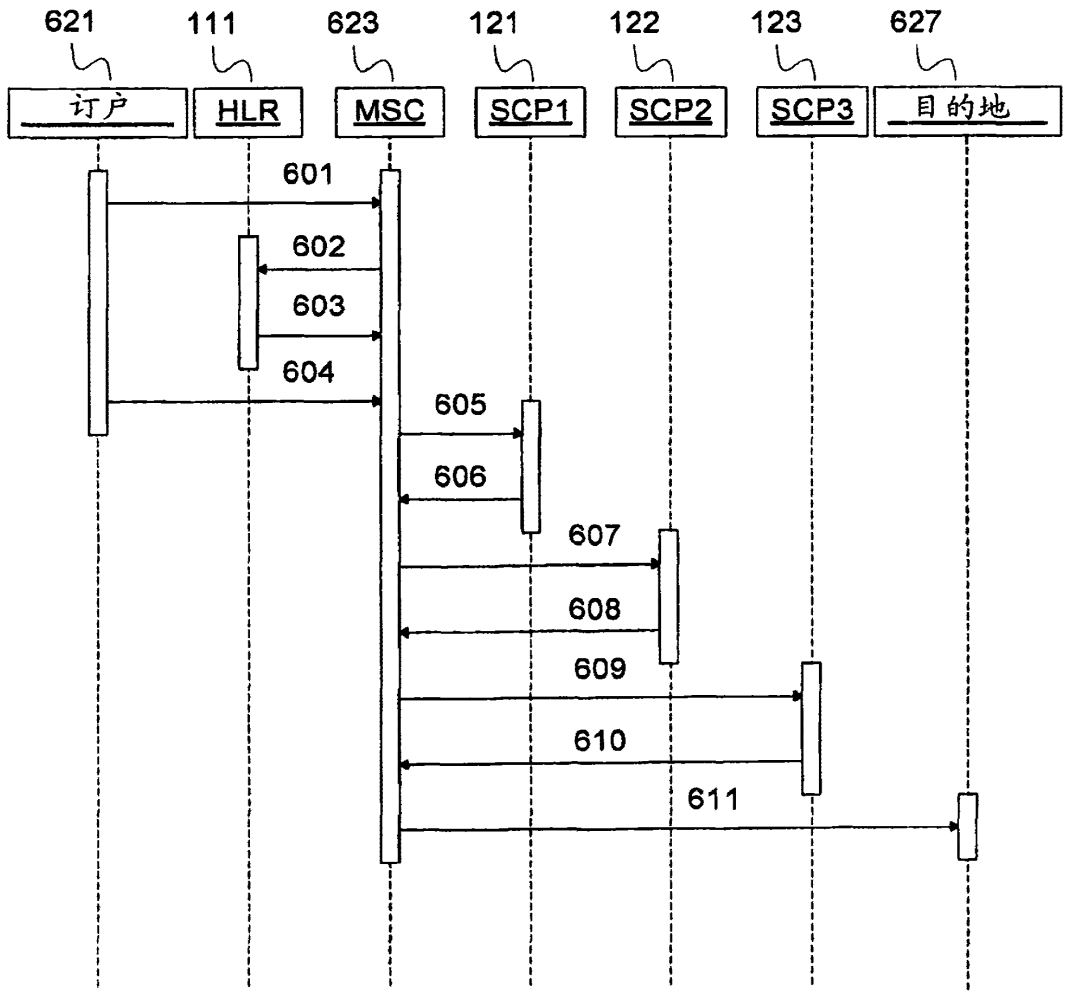


图 6

IPR2025-01571
Apple EX1002 Page 962

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 June 2007 (21.06.2007)

PCT

(10) International Publication Number
WO 2007/068288 A1

(51) International Patent Classification:
H04Q 3/00 (2006.01) *H04Q 7/24* (2006.01)

(21) International Application Number:
PCT/EP2005/056843

(22) International Filing Date:
16 December 2005 (16.12.2005)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **TELEFONAKTIEBOLAGET LM ERICSSON (publ)** [SE/SE]; S-16483 Stockholm (SE).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **NOLDUS, Rogier** [NL/NL]; Naardenstraat 46, NL-5045 ML Tilburg (NL). **SHARMA, Arvind** [NL/NL]; Esperenkamp 21, NL-5632 PX Eindhoven (NL).

(74) Agent: **NORIN, Klas**; Ericsson AB, Patent Unit Core Networks Kista, S-16480 Stockholm (SE).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

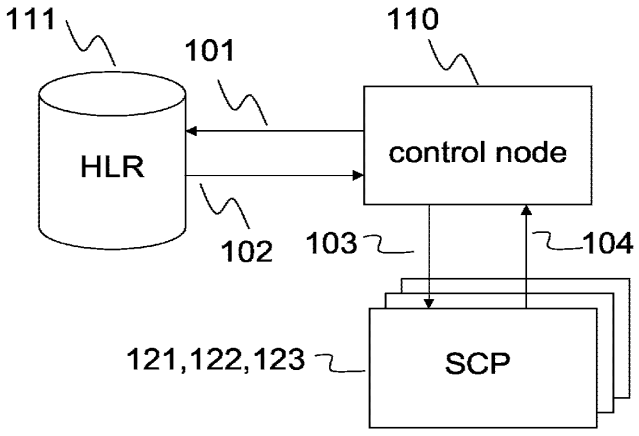
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, 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).

Declaration under Rule 4.17:
— *of inventorship (Rule 4.17(iv))*

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: INTELLIGENT NETWORK SERVICES



(57) Abstract: A method and control node (110) and computer program are disclosed for handling Intelligent Network services associated with a call to a subscriber of a mobile telecommunications network, the network comprising said c ontrol node (110), a HLR 5 (111) and one or more SCPs (121, 122, 123). Said control node (110) a) sends (101) to said HLR (111) one or more requests for routing information associated with said call; b) receives (102) from said HLR (111) service trigger elements associated with said services; c) uses said trigger elements for invoking (103) said services in said one ore more SCPs (121, 122, 123); and d) receives (104) from said one or more 10 SCPs (121, 122, 123) information related to said services associated with said trigger elements.

WO 2007/068288 A1

IPR2025-01571
Apple EX1002 Page 963

INTELLIGENT NETWORK SERVICES

FIELD OF INVENTION

The invention relates to a method and control node for handling Intelligent Network services associated with a call to a subscriber of a mobile telecommunications network.

BACKGROUND

Intelligent Network services are well known in the state of the art telecommunications networks such as GSM (Global System for Mobile communications).

The central component of the Core Network subsystem of a GSM network is the Mobile services Switching Center (MSC). It acts like a switching node of the PSTN or ISDN, and additionally provides all the functionality needed to handle a mobile subscriber, such as registration, authentication, location updating, handovers, and call routing to a roaming subscriber. These services are provided in conjunction with several functional entities, which together form the Core Network subsystem. A Gateway MSC (GMSC) provides the connection to the fixed networks (such as the PSTN or ISDN). Signaling between functional entities in the Core Network subsystem uses Signaling System Number 7 (SS7), used for trunk signaling in ISDN and widely used in current public networks.

The Home Location Register (HLR) and Visitor Location Register (VLR), together with the MSC, provide the call-routing and roaming capabilities of GSM. The HLR contains all the administrative information of each subscriber registered in the corresponding GSM network, along with the current location of the mobile station. The location of the mobile station is typically in the form of the signaling address of the VLR associated with the mobile station. There is logically one HLR per GSM network, although it may be implemented as a distributed database.

The VLR contains selected administrative information from the HLR, necessary for call control and provision of the subscribed services, for each mobile station currently located in the geographical area controlled by the VLR and currently served by that VLR. Although each functional entity can be implemented as an independent unit, currently all manufacturers of switching equipment implement the VLR together with the MSC, so that the geographical area controlled by the MSC corresponds to that controlled by the VLR, thus simplifying the signaling required. The MSC contains no information about particular mobile stations; this information is stored in the location registers.

Next, a typical incoming call setup (mobile terminating call) in a GSM network is described.

When a subscriber places a call to a mobile phone, he dials the telephone number associated with the phone user, the so-called Mobile Station ISDN (MSISDN) number, and the call is routed to the mobile phone operator's Gateway MSC. A gateway is a node used to interconnect two networks. The gateway is often implemented in an MSC, in which case the MSC is referred to as the GMSC. The GMSC acts as the "entrance" from exterior portions of the Public Switched Telephone Network onto the provider's network.

As noted above, the phone is free to roam anywhere in the operator's network or on the networks of roaming partners, including in other countries. So the first job of the Gateway MSC is to determine the current location of the mobile phone in order to connect the call. It does this by consulting the HLR, which, as described above, knows which Visited Location Register (VLR) the phone is associated with at the moment, if any.

When the HLR receives this query message, it determines whether the call should be routed to another number (called a divert), or the call should be routed directly to the mobile station of the called subscriber.

If the owner of the phone has previously requested that all incoming calls be diverted to another number, which supplementary service is also known as Call Forwarding Unconditional (CFU) to a Forwarded-to-Number (FTN), then this FTN is stored in the HLR. If that is the case, then the FTN is returned to the Gateway MSC for immediate routing to that destination.

If the mobile station is not currently associated with a VLR (e.g. because the phone has been turned off), then the HLR returns a number known as the Call Forwarding Not Reachable (CFNRc) number to the GMSC, and the call is forwarded there. Many operators may set this value automatically to the phone's voice mail number, so that callers may leave a message.

Finally, if the HLR knows that the phone is in the jurisdiction of a particular VLR, then it will request a temporary number, a so called Mobile Station Roaming Number (MSRN) from that VLR. This number is relayed to the GMSC, which uses it to route the call to another MSC, called the Visited MSC (VMSC).

When the call is received by the VMSC, the MSRN is used to find the phone's record in the VLR. This record identifies the phone's location area. Paging occurs to all mobile phone masts in that area. When the subscriber's mobile responds, the exact location of the mobile is returned to the VMSC. The VMSC then forwards the call to the appropriate phone mast, and the phone rings. If the subscriber answers, a speech path is created through the VMSC and GMSC back to the network of the person making the call, and a normal telephone call follows.

It is also possible that the phone call is not answered. If the subscriber is busy on another call (and call waiting is not being used), then the VMSC routes the call to a pre-determined Call Forwarding Busy (CFB) number. Similarly, if the subscriber does not answer the call after a period of time (typically 30 seconds), then the VMSC routes the call to a pre-determined Call Forwarding No Reply (CFNRy) number. Once again, the operator may decide to set this value by default to the voice mail of the mobile so that callers can leave a message.

An Intelligent Network (IN) is a network that is coupled to a telecommunications network that enables operators to deploy operator-specific Value Added Services (VAS). The intelligence that resides in the switch is augmented by intelligence from the Intelligent Network, which is placed in computer nodes that are distributed throughout the network. This provides the network operator with the means to develop, deploy and control services more efficiently. New services can be rapidly introduced into the telecommunications network. Once introduced, services are easily customized to meet individual customers' needs.

IN services are typically provided by a Service Control Point (SCP). An SCP is a control computer that communicates with other nodes and entities in the telecommunications network. The SCP comprises the service logic of one or more IN services and optionally IN service subscription data that allows the SCP to execute an IN service in accordance with the specific settings of a subscriber, i.e. tailor the service execution to the subscriber. When a call is established, the telecommunications network may query the SCP and ask for instructions for handling this call. For instance, an SCP is consulted to provide the translation of an 800 number to an actual phone number and to bill the owner of the 800 number for the call. SCPs may be physically separated from other components of the Intelligent Network or may be combined with these other components into a single node.

In a GSM network the IN service subscription information is stored in the HLR. Two types of information reside in the HLR: (1) static subscriber information and (2) dynamic subscriber information. The latter is e.g. needed to allow incoming calls to be routed to the mobile subscriber. The HLR stores, amongst others:

- the International Mobile Subscriber Identity (IMSI); an internal subscriber identity used only by the network;
- MSISDN number;
- VLR address;
- subscriber data on supplementary services.

IN services may be divided into two categories. One category comprises services to be invoked for subscribers who initiate a call (Mobile Originated Call – MOC). These services are called Mobile Originating (MO) services. An example of an MO service is outgoing call screening.

Each IN service subscriber is marked in his HLR with an Originating CAMEL Subscription Information (O-CSI) element, which is used to identify a specific service at the SCP. The O-CSI initiates the triggering of the MOC service as soon as the subscriber initiates a MO call. In the above example CAMEL is deployed, which stands for “Customised Applications for Mobile network Enhanced Logic”. CAMEL was developed as a standard for extending landline IN telephony services such as call waiting and call forwarding to GSM mobile phones.

The other category comprises services to be invoked for subscribers who receive a call (Mobile Terminated Call – MTC). These services are called mobile terminating (MT) services. Examples of mobile terminating services are call diversion services and Personal Greeting Service (PGS). PGS is a service that is associated with a roaming leg. PGS entails that when a signalling connection is established between a GMSC and VMSC (a so called "roaming leg"), then a personalised greeting is played to the calling party. The personalised greeting replaces the conventional alerting tone ("ring tone"). As such, the personalised greeting is primarily related to the establishment of the roaming leg; the ring tone becomes active only when the roaming leg is established and the called party is alerted. Each IN service subscriber is marked in his HLR with a Terminating CAMEL Subscription Information (T-CSI) flag, which is used to identify a specific service at the SCP. This initiates the triggering of the MTC service during a call attempt to the subscriber.

According to the state of the art, a control node may query a HLR during MTC handling to obtain instructions from the HLR. The control node may be a GMSC. In response to the query by the control node, the HLR may send IN trigger information for the terminating call. The IN trigger information exchanged between the HLR and the control node has been standardized. For example T-CSI is the GSM standardized IN trigger information for terminating calls, as specified by 3GPP (3rd Generation Partnership Project) in 3GPP TS 29.002. IN trigger information comprises among others the address of the SCP where the IN service resides and the service key, which identifies a particular IN service within the SCP.

The control node uses the IN trigger information to invoke the IN service in the SCP as specified for the subscriber in the IN trigger information. In response to the service invocation, the SCP sends an instruction to the control node to e.g. continue call set up or to terminate the call depending on the outcome of the service execution.

Current networks are typically arranged to handle a single invocation of an IN service for an MTC. Recent developments show however, that there is a need to invoke two or more IN services during terminating call handling.

Patent application WO00/25528 discloses a Service Interaction Manager, which is included in an SCP. The task of the Service Interaction Manager is to determine which

of the available services in the SCP should be executed for a subscriber and to invoke those services in a particular sequence.

SUMMARY

It is an object of the invention to provide a method and devices that overcome the drawbacks of the state of the art by permitting subscribers to have more than one IN Service for one call.

In a first aspect of the invention a method is proposed for handling Intelligent Network services associated with a call to a subscriber of a mobile telecommunications network, the network comprising a control node, a Home Location Register and one or more Service Control Points, the method comprising the steps of:

a. said control node sending to said Home Location Register, one or more requests for routing information associated with said call;
b. said control node receiving from said Home Location Register service trigger elements associated with said services;
c. said control node using said trigger elements for invoking said services in said one ore more Service Control Points;
d. said control node receiving from said one or more Service Control Points information related to said services associated with said trigger elements.

In this way multiple service trigger elements may be handled for a subscriber who is subscribed to one or more IN services pertaining to one call of the subscriber. IN Services need not be aware of the existence of one or more other IN services in that control node for that call. In other words, a first service does not need to know whether a second service will be invoked and vice versa. Since the services do not require knowledge about the possible invocation of other IN services for this call, the services may run on different platforms and may be supplied by different vendors.

There are several embodiments of the invention.

For example, the invention may provide for a Home Location Register to send a first service trigger element of said multiple service trigger elements, in response to a first request for routing information and a second service trigger element of said multiple service trigger elements in response to a second request for routing information.

The first request for routing information may comprise:

- MSISDN number of the subscriber.

The response to the first request for routing information may comprise:

- the first service trigger element.

The second request for routing information may comprise:

- MSISDN number of the subscriber;
- an indication that the HLR shall suppress the first service trigger element in the response. This indication may e.g. be the "suppress T-CSI" parameter.

The response to the second request for routing information may comprise:

- an MSRN to be used for the call to the served subscriber;
- the second service trigger element;
- a prefix or a suffix to the MSRN of the subscriber.

The MAP message may be sent from the HLR to a GMSC in multiple Signalling Connection Control Part messages, due to MAP segmentation. A first service, for example a pre-paid charging service, is executed in a first service control point and a second service, for example PGS, is executed in a second SCP.

In this way the pre-paid service and PGS may be offered to the same subscriber; the pre-paid service and PGS may run on different platforms and are not related to one another.

When the present invention is used for PGS, the calling subscriber may hear any call progress message even when early call forwarding or late call forwarding with optimal routing takes place.

Another advantage of the invention is, that PGS may be offered to Virtual Private Network (VPN) subscribers.

In a second aspect of the invention a control node is proposed for handling Intelligent Network services associated with a call to a subscriber of a mobile telecommunications network, the network comprising said control node, an HLR and one or more SCPs; the control node configured to send to said HLR one or more requests for routing information associated with said call; the control node further configured to receive from said HLR multiple service trigger elements associated with said services, and for invoking said services in said one ore more SCPs by using said trigger elements;

the control node further configured to receive from said one or more SCPs information related to said services associated with said trigger elements.

In a preferred embodiment the control node comprises a GMSC. The control node may however also comprise a device such as an MSC or an SCP.

A third aspect of the invention proposes a computer program, comprising program instructions for causing a computer to perform the method according to the invention.
The computer program may be stored on a carrier and may comprise computer executable instructions for causing a computer to perform the method according to invention.
The carrier of the computer program may be a record medium, computer memory, read-only memory or an electrical carrier signal.

The present invention proposes that multiple IN services may be provided for a particular call type to a subscriber. Hereto, an HLR may have registered multiple indications of particular IN call type subscriptions (hereinafter referred to as IN trigger elements).

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a block diagram of a prior art configuration of devices in a mobile telecommunications network.
Figure 2 is a signalling diagram of the method and devices according to the present invention.
Figure 3 is a block diagram of devices according to the present invention.
Figure 4 is a signalling diagram of an embodiment of the method of the present invention.
Figure 5 is a signalling diagram of an embodiment of the method of the present invention.
Figure 6 is a signalling diagram of an embodiment of the method of the present invention.

DETAILED DESCRIPTION

For the purpose of the present invention, MT call handling in the GMSC may be divided in two logical parts:

(1) Terminating call handling;

(2) Roaming leg handling.

The terminating call handling includes the retrieving of T-CSI from the HLR and the invocation of the first CAMEL service. The first CAMEL service may enforce call restriction or may apply call forwarding. Typically, this first CAMEL service is also used for terminating charging, for the case that the called subscriber is roaming. The HLR may also return other IN trigger elements in combination with T-CSI.

The roaming leg handling includes the retrieving of the MSRN from HLR and the routing of the call from the GMSC to the terminating MSC, where the called party is registered at that moment. It is noticed that "roaming leg" is equally applicable for the case that the subscriber is in the Visited Public Land Mobile Network (VPLMN) and for the case that the subscriber is in the Home Public Land Mobile Network (HPLMN). I.e. "roaming" shall in this case not be associated with "being in another network or in another country".

The present invention proposes that the invocation of two IN services for an MT call is done along the line of above-described distinction. According to the present invention, two types of IN services for MT call may be defined:

(1) IN services that need control over the MT call and that may need the capability to influence the routing of the call. These kind of IN services also need to know the location of the destination subscriber, so charging may be applied.

(2) IN services that are required only for the roaming leg to the destination subscriber. This type of IN service is invoked only when a roaming leg is established, i.e. the GMSC has received an MSRN from the HLR.

If the HLR returns a Forwarded-to-Number (FTN) instead of an MSRN, then there will not be a roaming leg and consequently, no roaming leg-associated IN service will be invoked.

Figure 1 is a block diagram of a prior art configuration of devices in a mobile telecommunications network. The shown entities belong, at least conceptually, to an intelligent network that is distinct from the mobile communications network. The intelligent network includes HLR 111, SCP1 121, SCP2 122 and GMSC110. GMSC 110 interfaces to SCP1 and SCP2 as well as to HLR 111 for performing well known IN triggering functions. SCP1 and SCP2 contain intelligent network services that may be invoked sequentially during the handling of a mobile terminating call.

Figure 2 is a signalling diagram of the method and devices according to the present invention with a general overview of relations between various elements. The method comprises next steps:

Step 101 A control node 110 sends to a HLR 111, one or more requests for routing information associated with said call;

Step 102 The HLR 111 sends to said control 110 node multiple service trigger elements associated with said services;

Step 103 The control node 110 uses said trigger elements to invoke one or more services in one ore more Service Control Points 121, 122, 123;

Step 104 The one or more Service Control Points 121, 122, 123 sends to said control node 110 information related to on one or more services associated with said trigger elements.

Figure 3 is a block diagram of devices and their interrelations according to the present invention.

The lines between the blocks (devices) represent communication paths. HLR 111 may communicate with GMSC 110 and to VMSC 112. GMSC may communicate with SCP1 121 and other subsequently invoked SCPs (SCPn) 122. GMSC 110 may communicate with VMSC 112.

Figure 4 is a signalling diagram of an embodiment of the method of the present invention comprising a communication sequence between the devices as shown in figure 3, comprising GMSC 110, HLR 111, multiple SCPs 121, 122 and a VMSC 112. In this example a subscriber is subscribed to a CAMEL service and additionally to at least one service, which may be an IN, service. For this example only the communication with two

SCPs 121, 122 is shown. However, steps 6-11 may be repeated for a third SCP and so on. The following steps occur:

Step 401 ISUP Initial Address Message (IAM) arrives at the GMSC 110; the GMSC 110 analyses the Called Party Number in ISUP IAM and deduces that the Called Party Number is an MSISDN belonging to its own network.

Step 402 The GMSC 110 sends MAP Send Routing Information (SRI) to the HLR 111. The GMSC 110 indicates in MAP SRI that it supports CAMEL.

Step 403 The called subscriber has a subscription to a CAMEL service for MT call handling. As a result, the HLR 111 sends MAP SRI-Res to the GMSC 110, including the IN trigger information for MT calls, T-CSI.

Step 404 The GMSC 110 uses T-CSI to invoke a CAMEL service. The GMSC 110 instantiates an internal GSM Service Switching Function (gsmSSF) entity; the gsmSSF sends CAP Initial Detection Point (IDP) to the SCP. The address of the SCP1 121, and other data related to this IN dialogue, is obtained from T-CSI. The gsmSSF function interworks with the GMSC. Based on information defined in the user's subscription, and sent from the HLR to the GMSC, service triggers within the GMSC and gsmSSF are set. These triggers are used to dictate when the gsmSSF shall communicate with the gsmSCF. This in turn will determine how IN based services are handled.

Step 405 The SCP1 121 responds with CAP Continue (CUE), to inform the GMSC 110 that MT call handling may continue, i.e. the call may be delivered to the called subscriber. The control dialogue between SCP1 121 and GMSC 110 may be retained. The CAMEL service in SCP1 121 does not need to have knowledge about other IN services than the CAMEL service it's currently executing.

Step 406 The GMSC 110 sends a second interrogation to the HLR 111, i.e. sends a second MAP SRI to the HLR 111. The second MAP SRI includes the flag "suppress T-CSI".

Step 407 The HLR 111 recognizes the MAP SRI as a second SRI, by virtue of the presence of "suppress T-CSI", and responds by sending MAP Provide

Roaming Number (PRN) to the VMSC 112 where the called party is currently registered.

Step 408 The VMSC 112 allocates an MSRN for this call and returns the MSRN to the HLR 111, by sending MAP PRN-Res to the HLR 111.

Step 409 The HLR 111 forwards the MSRN to the GMSC 110, by sending MAP SRI Response (SRI-Res) to the GMSC 110. The called subscriber subscribes to a second IN service for MT call handling. The second IN service is of the type Roaming Leg handling, as described in an earlier part of the present invention disclosure. The HLR 111 includes the IN trigger information associated with this second IN service, in the MAP SRI-Res. For the purpose of the present invention, this second IN trigger information is named "RICK" (Roaming leg IN Category Key). RICK may have the structure as T-CSI or TICK (Terminating IN Category Key). In order to be able to receive RICK, the GMSC 110 would have indicated in the 2nd MAP SRI (step 6) that it supports this information element, i.e. it supports RICK. This indication of "RICK support" is similar to the indication of "TICK support". The "TICK support", which is sent from GMSC to HLR, indicates to HLR that it supports the TICK. The TICK has functionality that may be compared with T-CSI; TICK is, however, not standardised.

Step 410 The GMSC 110 recognizes that the MSRN is accompanied by a RICK. The RICK serves as an indication for the GMSC 110 that the roaming leg shall be subject to an IN service. The GMSC 110 therefore uses RICK to invoke an IN service, by sending CAP IDP to the SCPn 122. The address of the SCPn 122, and other data related to this IN dialogue, is obtained from RICK.

Step 411 The SCPn 122 responds with CAP CUE, to inform the GMSC 110 that MT call handling may continue, i.e. the roaming leg towards the called subscriber may be established.

Step 412 The GMSC 110 establishes the roaming leg towards the called subscriber, by sending ISUP IAM towards the destination exchange. The ISUP IAM contains the MSRN that was received from the HLR 111.

Steps 401 – 408 represent normal GSM call handling.

Step 409 represents an enhancement to the existing MT call handling. The HLR 111 will normally return only the MSRN to the GMSC 110. Step 409 adds the RICK to the MAP SRI-Res.

Step 410 and step 411 do not exist in existing Roaming Leg handling. These steps represent the invocation of the second IN service for the MT call handling in the GMSC 110.

When the call is delivered to the called subscriber, the two IN services may remain active. The first IN service, triggered as a result of the sending of T-CSI to the GMSC 110, may remain active for the entire call and has the full capability available as allowed by the IN protocol used for that service.

The second IN service, triggered as a result of the sending of RICK to the GMSC 110, may also remain active for the entire call. This IN service shall, however, use the IN capability with certain restrictions. As an example, this service shall not apply call forwarding, as that would affect a pre-paid service for the call.

The present invention may be applied on various types of GSM call forwarding. This may be shown most adequately by taking a service like Personal Greeting Service (PGS) as an example. In the case of call forwarding, the destination of the call changes. Some operators require that the PGS service be terminated when call forwarding to a voice mailbox takes place.

With regard to terminating a PGS service in a call forwarding situation there are basically two types of call forwarding: Early call forwarding (ECF) and Late Call Forwarding (LCF)

When early call forwarding takes place in the GMSC 110, the GMSC 110 does not receive an MSRN form the HLR 111 for this call and no roaming leg is established. The GMSC 110 will not establish a roaming leg to the called party and as a result, no roaming-leg IN service will be invoked.

In the case of early call forwarding, the HLR 111 does not return an MSRN in the second SRI Result and, according to the present invention, does not return the RICK. The GMSC 110 now forwards the call to the forwarded-to destination, which may e.g. be a voice mailbox or call completion service. Since the HLR 111 has not returned RICK,

there will not be a PGS invocation. The calling subscriber may now hear any announcement that is played by the voice mailbox, even when the voice mailbox defers the generation of the ISUP Answer Message (ISUP ANM) for a defined duration.

When late call forwarding takes place in the VMSC 112, then Optimal Routing of Late Call Forwarding (ORLCF) may be applied to return the call handling to the GMSC 110. The GMSC 110 terminates the roaming leg and hence, the roaming-leg IN service will be terminated as well. In the case of late call forwarding, the call is already routed to the destination MSC of the called subscriber. When the late call forwarding condition occurs, the VMSC 112 may send MAP Resume Call Handling (RCH) to the GMSC 110; the sending of MAP RCH is part of ORLCF.

When the GMSC 110 receives MAP RCH and approves the request for ORLCF, it releases the roaming leg and creates a forwarded leg. The calling party may hear any announcement generated by the forwarded-to destination.

Some operators deploy a voice mailbox system whereby the initial announcement is free of charge. This may be accomplished by having the voice mailbox defer the generation of the ISUP ANM. If PGS remains active in such situation, then the calling party will not hear any announcement that is played between ISUP Address Complete Message (ACM) and ISUP ANM. Reason is that the personal greeting remains active until the ISUP ANM is detected. The initial announcement of the voice mail would in that case not be heard.

The present invention resolves that problem, since PGS will be terminated in the case of late call forwarding in combination with ORLCF.

If late call forwarding is not subject to ORLCF, then the Roaming Leg service may monitor for ISUP messages such as Call Progress (CPG) and ACM. These ISUP messages may indicate that forwarding is taking place.

Some operators apply a service node solution for PGS. This means that for PGS subscribers, the roaming leg needs to be routed through a special service node (located in-line with the ISUP traffic link for the roaming leg). The service node will propagate the call to the destination MSC. The routing of the roaming leg through a service node may be accomplished in accordance with the present invention. The IN service that is

invoked with RICK may provide a prefix for the MSRN, resulting in that the call is routed through the service node.

Alternatively, the RICK that is included in the SRI-Res may have the form of a number prefix; a switching node such as a GMSC places the RICK in front of the MSRN, prior to forwarding the call to a next switching node.

The B-number analysis in this transition node may be configured such that the RICK results in the selection of a route to the service node.

The concept of a subscribed or generic IN service for a roaming leg may be used for the following type of services:

- Personal greeting: the playing of the personal greeting is required only when the roaming leg is successfully established; if the roaming leg can, for whatever reason, not be established or is terminated before answer, then the personal greeting is not required. An operator may wish to invoke PGS prior to the allocation of a MSRN for the call. The effect of that may be that when forwarding to a second called party takes place, the calling party will still hear a first party's personalised greeting. In addition, such configuration would have the effect that call forwarding announcements may not be heard.
- Service-node routing: for a particular subscriber, the roaming leg may need to be routed through a service node.
- Carrier selection: a subscriber may subscribe to a carrier selection service that is applicable for roaming leg only.

When the HLR 111 sends SRI-Res to GMSC 110 including MSRN, it may include RICK. As an implementation option, the HLR 111 may apply criteria for the inclusion of RICK in SRI-Res, similar to the case whereby the HLR 111 applies criteria for the inclusion of T-CSI in the first SRI-Res. These criteria may e.g. be:

- include RICK in SRI-Res only when subscriber is in HPLMN;
- include RICK in SRI-Res only when the incoming call is a speech call

Not all MT calls need a terminating IN service. Likewise, not all MT calls need a RICK service. As an example, when a pre-paid subscriber is in the HPLMN, the HLR

111 may suppress T-CSI in SRI. As a result, there will not be a MT call service triggered. If the invocation of the Roaming leg service is still required in this case, then the HLR 111 may include RICK in the first SRI-Res. The further handling of RICK in the GMSC 110 is as described earlier.

Figure 5 is a signalling diagram of an embodiment of the method of the present invention, wherein the invocation of multiple services is performed by a GMSC 110 interrogating an HLR 111 for multiple (IN) services before the GMSC 110 sets up the roaming leg. In this embodiment the HLR 111 sends all the information of the IN services at the first interrogation. Steps 501-502 are performed according to the current state of the art. In this example 3 SCPs are involved, although the invention is applicable to multiple SCPs.

Step 501 ISUP IAM arrives at the GMSC 110.

Step 502 The GMSC 110 analyses the Called Party Number in ISUP IAM and deduces that the Called Party Number is an MSISDN belonging to its own network. The GMSC 110 sends MAP SRI to the HLR 111. The GMSC 110 indicates in MAP SRI that it supports CAMEL. The GMSC may support multiple CAMEL phases.

Step 503 The called subscriber has a subscription to a CAMEL service for MT call handling. As a result, the HLR 111 sends MAP SRI-Res to the GMSC 110 including IN trigger information for MT calls, T-CSI.

Step 504 The GMSC 110 uses T-CSI to invoke a CAMEL service. The GMSC 110 instantiates an internal gsmSSF entity; the gsmSSF sends CAP IDP to the SCP 121. The address of the SCP1 121, and other data related to this IN dialogue, is obtained from T-CSI.

Step 505 The SCP1 121 responds with CAP Continue (CUE) or CAP Connect (CON), to inform the GMSC 110 that MT call handling may continue, i.e. the call may be delivered to the called subscriber. The control dialogue between SCP1 121 and GMSC 110 may be retained or terminated, depending on IN service requirements. The CAMEL service in SCP1 121 has no knowledge about other IN services than the CAMEL service that it is currently executing.

Step 506 The GMSC 110 responds by invoking a second IN service, which could again be a CAMEL service, based on T-CSI. The address of SCPn 122 is obtained from the second T-CSI.

Step 507 The SCP responds with CAP CUE or CAP CON, to inform the GMSC 110 that call handling may continue, i.e. the call may be delivered to the called subscriber. Here as well, the CAMEL service in SCP2 122 has no knowledge about the first service and the third service for this call.

Step 508 The GMSC 110 checks whether further IN services are provisioned for the subscriber; if they are, then it responds by invoking the third IN service, which could again be a CAMEL service, based on T-CSI. The address of SCP3 123 is obtained from the third T-CSI.

Step 509 The SCP 123 responds with CAP CUE or CAP CON, to inform the GMSC 110 that call handling may continue, i.e. the call may be delivered to the called subscriber. The CAMEL service in SCP3 123 has no knowledge about the first service and the second service for this call.

Step 510 The GMSC 110 checks whether further IN services are provisioned for the subscriber; if there are no more IN services for the subscriber, then the GMSC 110 responds by sending a second interrogation to the HLR 111, i.e. sends a second MAP SRI to the HLR 111.

Step 511 The HLR 111 recognises the MAP SRI as a second SRI and responds by sending MAP Provide Roaming Number (PRN) to the VMSC 112 where the called party is currently registered.

Step 512 The VMSC 112 allocates an MSRN and returns the MSRN to the HLR 111, by sending MAP PRN-Res to the HLR 111.

Step 513 The HLR 111 forwards the MSRN to the GMSC 110, by sending MAP SRI-Res to the GMSC 110.

Step 514 The GMSC 110 establishes the roaming leg towards the called subscriber, by sending ISUP IAM towards the destination exchange. The ISUP IAM contains the MSRN that was received from the HLR 111.

Figure 6 is a signalling diagram of an embodiment of the method of the present invention, whereby multiple IN services are invoked for an MO call. The following steps occur in this embodiment.

Step 601 A subscriber 621 registers with an MSC 623 in a visited GSM network.

Step 602 The MSC 623 contacts the HLR 111 in the Home PLMN of the subscriber 621.

Step 603 HLR 111 sends multiple trigger elements for IN services to the MSC 623. These trigger elements are associated to IN services for mobile originating calls and mobile forwarding calls.

Step 604 The subscriber 621 establishes an MO call.

Step 605 The MSC 623 uses a first trigger element to invoke a first IN service in SCP1 121 associated with the first trigger element.

Step 606 The first IN service in SCP1 121 gives control of the call back to the MSC 623, by sending a CAP Continue message or a CAP Connect message

Step 607 The MSC 623 uses the second trigger element from the list of trigger elements to invoke a second IN service in SCP2 122.

The steps 605 and 606 are repeated with SCP 2 122 (steps 607, 608) and SCP3 123 (609, 610) and further, until all indicated IN services are invoked. Call processing in MSC 623 continues with step 611 as normal:

Step 611 The MSC 623 routes the call to the destination 627. Any of the invoked IN services may remain active for the entire duration of the call, or may terminate at an earlier stage.

The following scenarios are covered by the invention:

1) IN service invocation in GMSC for MT call handling, followed by IN service invocation in GMSC for roaming leg.
2) IN service invocation in GMSC for roaming leg.

3) As (1), whereby the HLR sends multiple IN service trigger elements in the first interrogation response, with the purpose that these multiple trigger elements are used for the invocation of multiple IN services associated with the MT call.
4) As (1), whereby the HLR sends multiple IN service trigger elements in the second interrogation response, with the purpose that these multiple trigger elements are used for the invocation of multiple IN services associated with the roaming leg.
5) As (2), whereby the HLR sends multiple IN service trigger elements in the second interrogation response, with the purpose that these multiple trigger elements are used for the invocation of multiple IN services associated with the roaming leg.
6) As (1), whereby (3) and (4) are combined.
7) As (1), whereby the HLR sends multiple IN service trigger elements in the first interrogation response, with the purpose that some of these multiple trigger elements are used for the invocation of multiple IN services associated with the MT call and some of these multiple trigger elements are used for the invocation of multiple IN services associated with the roaming leg.
8) Certain IN services for MT calls are required only when a roaming leg is established. The present invention offers the tools to accomplish this.
9) The present invention may be used to route a roaming leg through an ISUP service node on a subscription basis or generically for all served subscribers.

CLAIMS

1. A method for handling Intelligent Network services associated with a call to a subscriber of a mobile telecommunications network, the network comprising a control node (110), a Home Location Register (111) and one or more Service Control Points (121, 122, 123) , the method comprising the steps of:
   a. said control node (110) sending (101) to said Home Location Register (111), one or more requests for routing information associated with said call;
   b. said control node (110) receiving (102) from said Home Location Register (111) service trigger elements associated with said services;
   c. said control node (110) using said trigger elements for invoking (103) said services in said one ore more Service Control Points (121, 122, 123);
   d. said control node (110) receiving (104) from said one or more Service Control Points (121, 122, 123) information related to said services associated with said trigger elements.

2. The method according to claim 1, wherein said Home Location Register (111) sends a first service trigger element of said multiple service trigger elements in response to a first request for routing information and a second service trigger element of said multiple service trigger elements in response to a second request for routing information.

3. The method according to claim 1, wherein said Home Location Register (111) sends said multiple service trigger elements in response to a first request for routing information.

4. The method according to claim 2 or 3, wherein said Home Location Register (111) sends the requested routing information in response to a second request for routing information.

5. The method according to any of the claims 2-4, wherein said second request for routing information is associated with the establishment of a signalling

connection between said control node (110) and a Visited Mobile services Switching Center (112).

6. The method according to any one of the preceding claims, wherein said requested routing information comprises a Mobile Station Roaming Number to be used for the call to said subscriber.

7. The method according to any one of the preceding claims, wherein a plurality of said service trigger elements is comprised in one Mobile Application Part message.

8. The method according to claim 7, wherein said one Mobile Application Part message is sent from said Home Location Register (111) to said Control Node in multiple Signalling Connection Control Part messages, due to Mobile Application Part segmentation.

9. The method according to any of the claims 1-6, wherein one or more of said service trigger elements is included in a Mobile Station Roaming Number as a prefix or a suffix.

10. The method according to any of the claims 1-6, wherein said service trigger elements comprise separate parameters.

11. The method according to any one of the preceding claims, wherein a first service of said services is executed in a first Service Control Point (121) of said one or more Service Control Points (121, 122, 123) and a second service of said services is executed in a second Service Control Point (122) of said one or more Service Control Points (121, 122, 123).

12. The method according to claim 11, wherein a first service of said services is a pre-paid charging service.

13. The method according to claim 11 or 12, wherein a second service of said services is a mobile terminating service such as a personal greeting service.

14. The method according to any one of the preceding claims, wherein said control node (110) is a Gateway Mobile Switching Centre (110).

15. The method according to any of the claims 2-14, wherein said first request contains a Mobile Station ISDN number of said subscriber.

16. The method according to any of the claims 2-15, wherein said second request contains a Mobile Station ISDN number of said subscriber and a "Suppress T-CSI" parameter.

17. The method according to any one of the preceding claims, wherein a first or a second request of said one or more requests for routing information comprises a Mobile Application Part Send Routing Information message.

18. A control node (110) for handling Intelligent Network services associated with a call to a subscriber of a mobile telecommunications network, the network comprising said control node (110), a Home Location Register (111) and one or more Service Control Points (121, 122, 123); the control node (110) configured to send to said Home Location Register (111) one or more requests for routing information associated with said call; the control node (110) further configured to receive from said Home Location Register (111) multiple service trigger elements associated with said services, and for invoking said services in said one ore more Service Control Points (121, 122, 123) by using said trigger elements; the control node further configured to receive from said one or more Service Control Points (121, 122, 123) information related to said services associated with said trigger elements.

19. A computer program comprising program instructions for causing a computer to perform the method according to of any of the claims 1-17.

20. A computer program on a carrier and comprising computer executable instructions for causing a computer to perform the method according to claims 1-17.

21. A computer program according to claim 19, wherein said carrier is a record medium, computer memory, read-only memory or an electrical carrier signal.

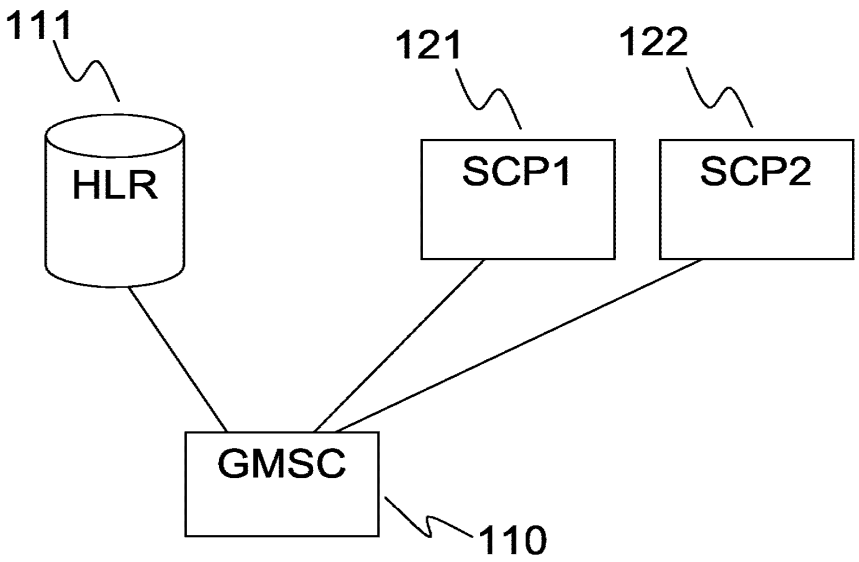


Fig. 1

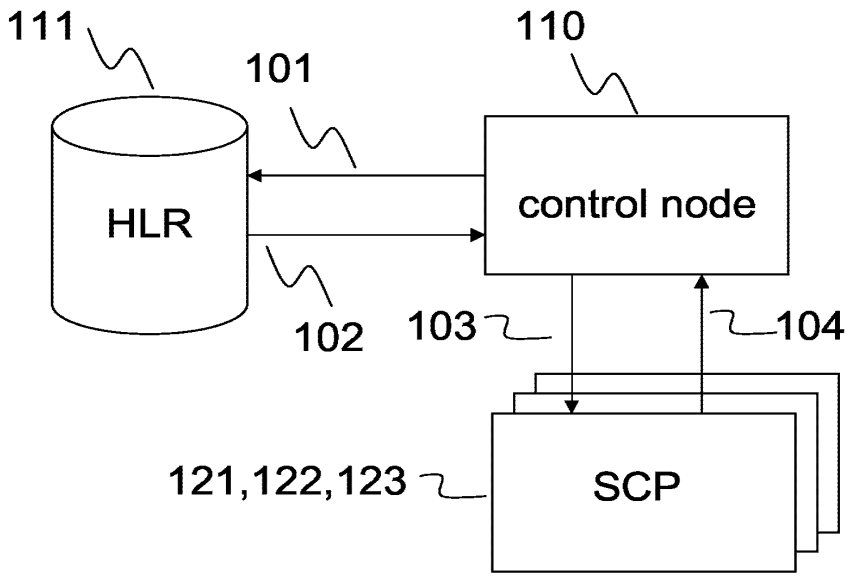


Fig. 2

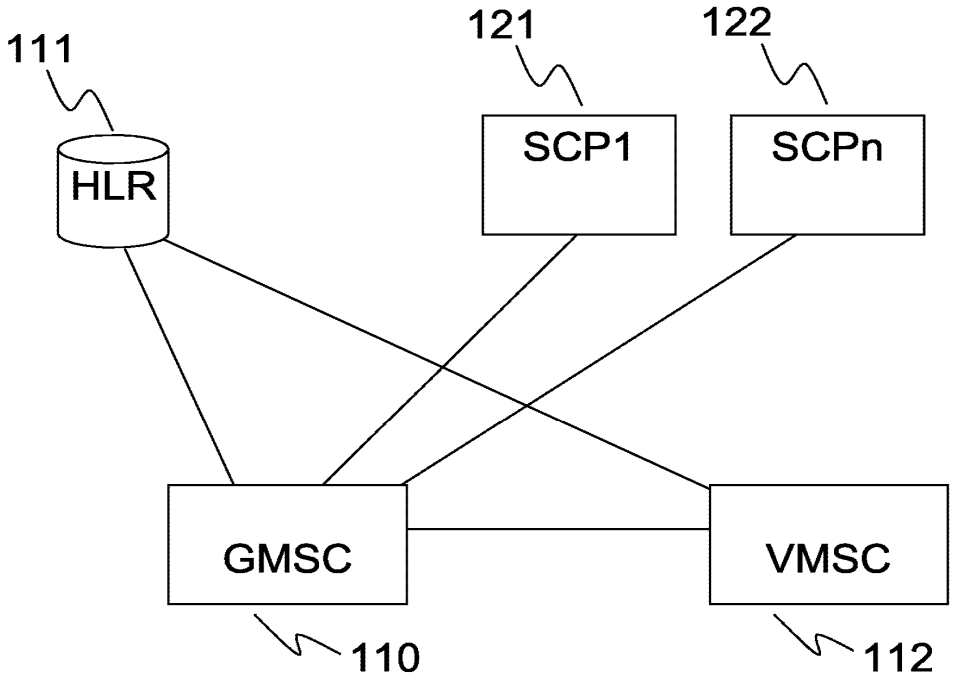


Fig. 3

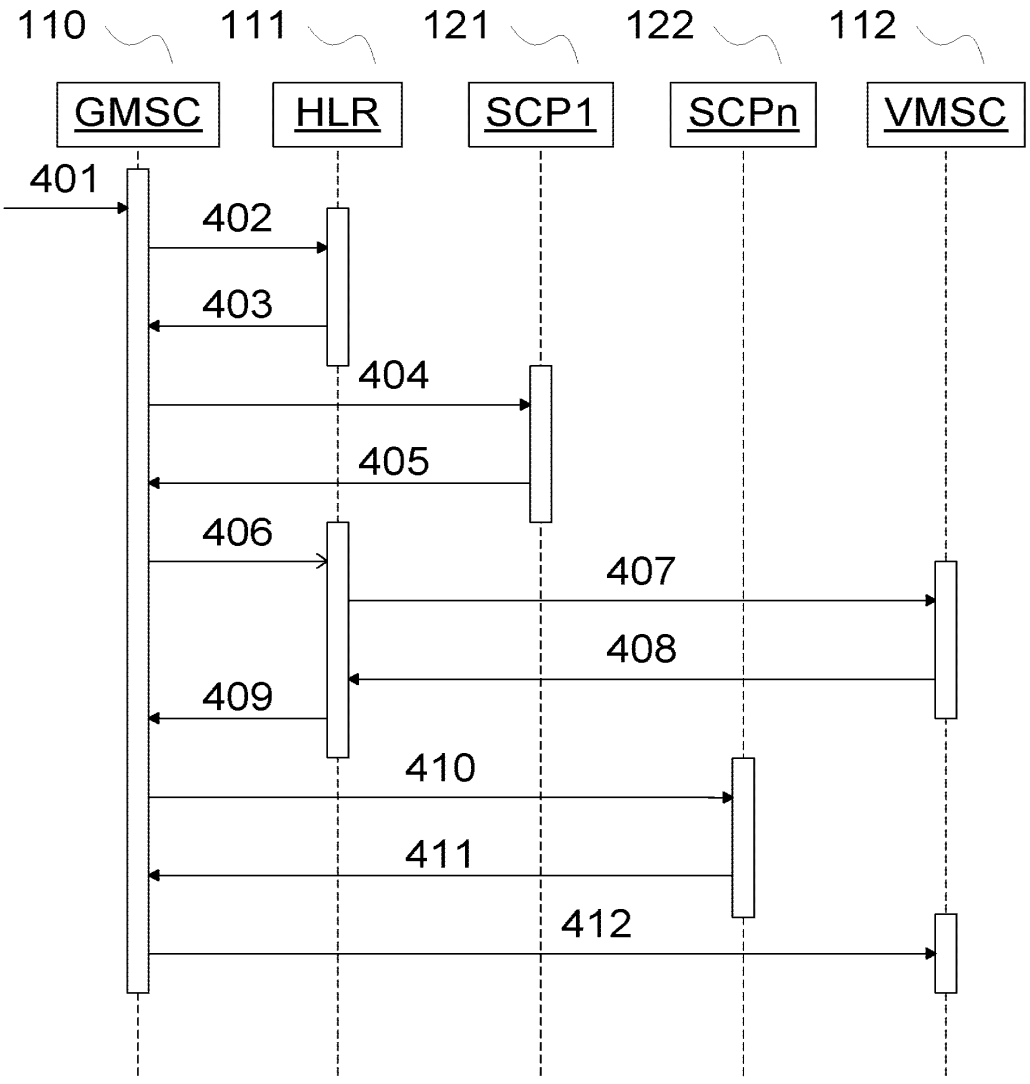

110
111
121
122
112
GMSC
HLR
SCP1
SCPn
VMSC
401
402
403
404
405
406
407
408
409
410
411
412

Fig. 4

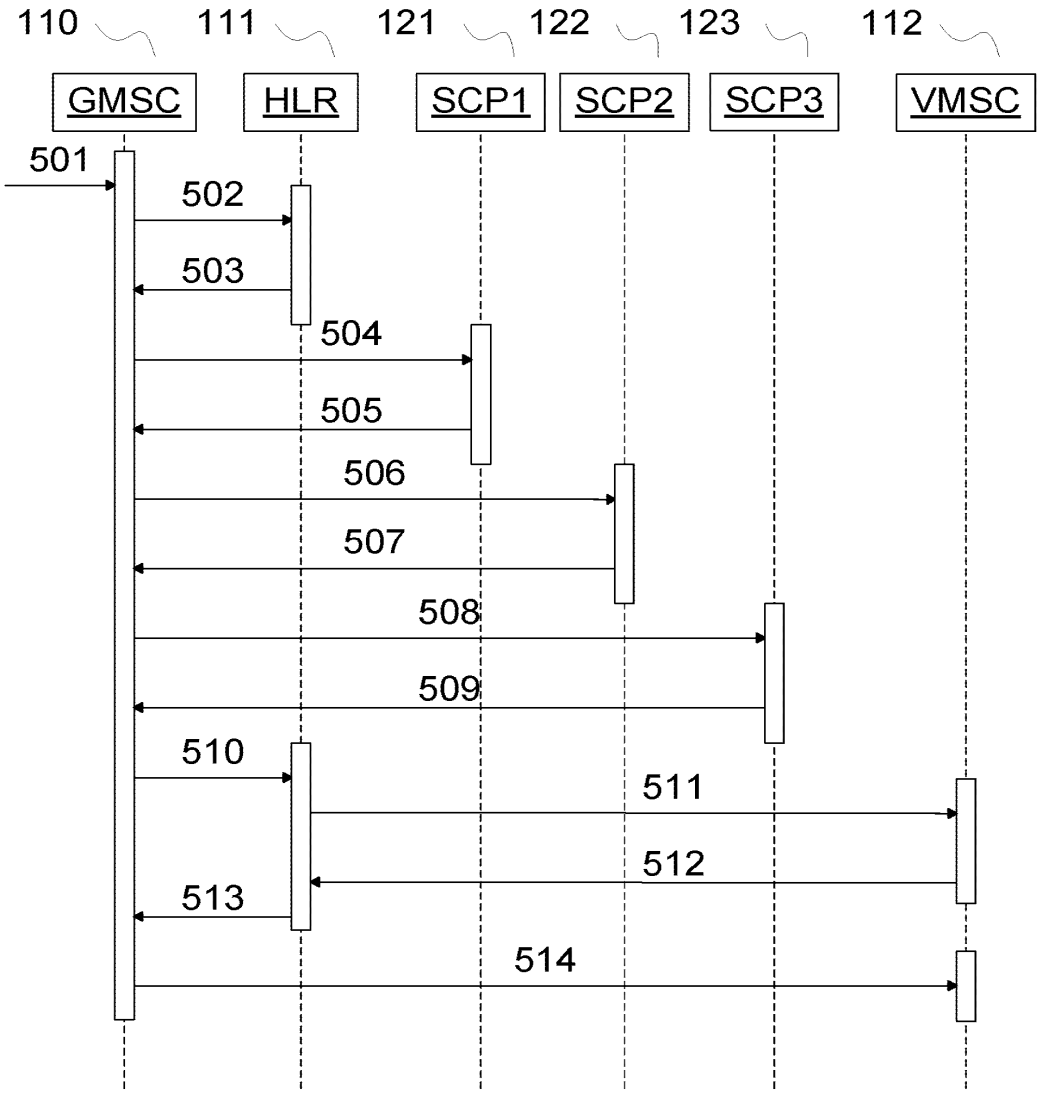

110
111
121
122
123
112
GMSC
HLR
SCP1
SCP2
SCP3
VMSC
501
502
503
504
505
506
507
508
509
510
511
512
513
514

Fig. 5

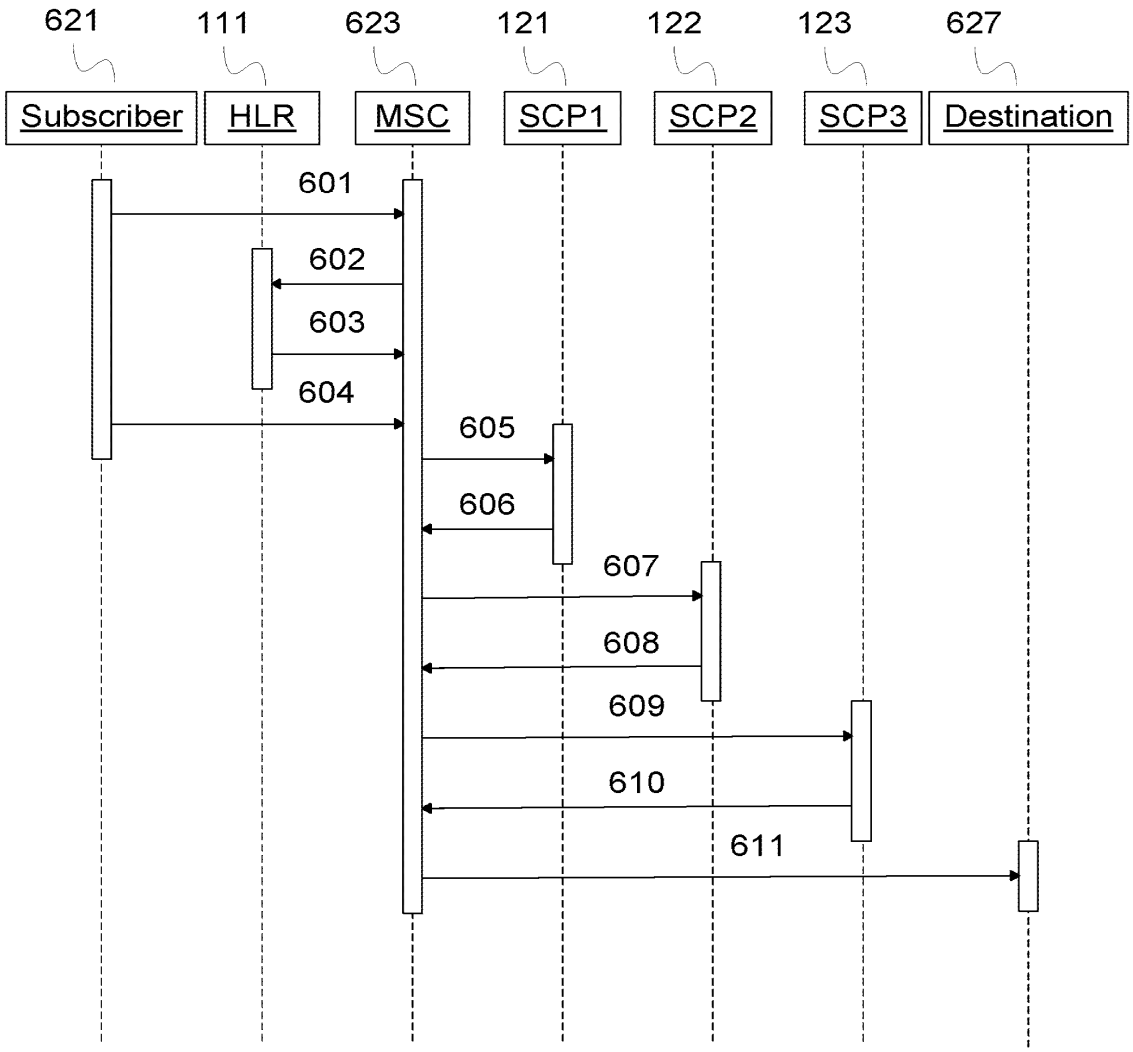

621
111
623
121
122
123
627
Subscriber
HLR
MSC
SCP1
SCP2
SCP3
Destination
601
602
603
604
605
606
607
608
609
610
611

Fig. 6

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2005/056843

A. CLASSIFICATION OF SUBJECT MATTER
H04Q3/00 H04Q7/24

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)
H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2004/103012 A (SIEMENS AKTIENGESELLSCHAFT; KASTL, PETRA; WOELKNER, CHRISTIAN) 25 November 2004 (2004-11-25) page 9, line 7 - page 10, line 37	1-21
X	WO 97/07637 A (MOTOROLA LTD; CHAMBERS, DAVID; CRICHTON, PAUL; DODD, ADRIAN) 27 February 1997 (1997-02-27) page 3, line 26 - page 5, line 24 figure 1	1-21

☐ 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 document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
8 February 2006	27/02/2006

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Chassatte, R

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2005/056843

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2004103012 A	25-11-2004	AU 2003242558 A1	03-12-2004
WO 9707637 A	27-02-1997	CA 2229447 A1	27-02-1997
		CN 1194079 A	23-09-1998
		DE 69631888 D1	22-04-2004
		DE 69631888 T2	05-08-2004
		EP 0846399 A1	10-06-1998
		GB 2304491 A	19-03-1997
		HK 1016400 A1	01-08-2003
		JP 2000502217 T	22-02-2000

IPR2025-01571
Apple EX1002 Page 994

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04M 1/66 (2006.01)

[12] 发明专利申请公开说明书

[21] 申请号 200480002062.0

[43] 公开日 2006 年 7 月 12 日

[11] 公开号 CN 1802839A

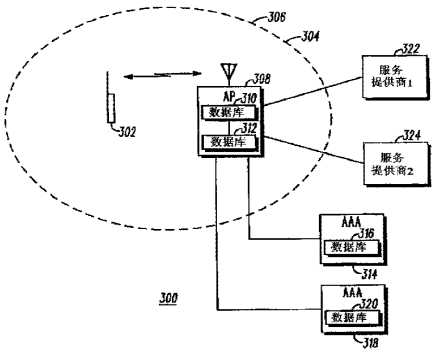
[22] 申请日 2004.1.13
[21] 申请号 200480002062.0
[30] 优先权
[32] 2003.1.13 [33] US [31] 60/439,743
[32] 2004.1.12 [33] US [31] 10/755,800
[86] 国际申请 PCT/US2004/000870 2004.1.13
[87] 国际公布 WO2004/064306 英 2004.7.29
[85] 进入国家阶段日期 2005.7.11
[71] 申请人 摩托罗拉公司（在特拉华州注册的公司）
地址 美国伊利诺斯州
[72] 发明人 约翰纳·维尔德
拉杰什·帕日亚努尔
[74] 专利代理机构 中原信达知识产权代理有限责任公司
代理人 李 涛 钟 强
权利要求书 2 页 说明书 11 页 附图 4 页

[54] 发明名称

通过无线局域网向移动站提供网络服务信息的方法和装置

[57] 摘要

一种无线局域网(WLAN)通信系统(300)，包括与移动站(302)通信的接入点(308)以及至少一个鉴别、授权、结算(AAA)服务器(314、318)，提供鉴别过程，由此移动站用户可以在被鉴别之前从一个或多个 WLAN 服务提供商和/或一个或多个 3GPP 服务提供商(322、324)中选择 WLAN 服务提供商，进而根据与所选服务提供商相关联的、除了服务集标识符(SSID)之外的网络服务信息来作出订制所选服务提供商的服务的决定。



IPR2025-01571
Apple EX1002 Page 995

1. 一种用于提供网络服务信息给接入无线局域网的移动站用户的方法，包括：

接收鉴别移动站的请求；和

作为对接收到上述请求的响应，传送关于多个服务提供商中每个服务提供商的网络识别和服务信息到移动站。

2. 如权利要求 1 所述的方法，其中，鉴别移动站的请求与网络识别和服务信息每个都是在媒介接入控制层消息中传送的。

3. 如权利要求 1 所述的方法，进一步包括：

请求鉴别信息；和

接收包括对从多个服务提供商中选择服务提供商的选择的鉴别信息。

4. 如权利要求 3 所述的方法，进一步包括：

根据接收到的鉴别信息来确定鉴别、授权、结算服务器；和

通过确定的鉴别、授权、结算服务器来请求对移动站的授权。

5. 一种用于接入无线局域网的方法，包括：

传送鉴别移动站的请求；

接收关于服务提供商的网络识别和服务信息；和

根据接收到的网络识别和服务信息来确定是否接入无线局域网。

6. 如权利要求 5 所述的方法，其中，鉴别移动站的请求与网络识别和服务信息每个都是在媒介接入控制层消息中传送的。

7. 如权利要求 5 所述的方法，其中，接收关于服务提供商的网络识别和服务信息包括接收关于多个服务提供商中的每个服务提供商

IPR2025-01571
Apple EX1002 Page 996

的网络识别和服务信息，并且其中，该方法进一步包括：

接收对鉴别信息的请求；和

传送对从多个服务提供商中选择服务提供商的选择。

8. 一种无线局域网中的接入点，包括：

存储器，储存关联于多个服务提供商中每个服务提供商的服务提供商标识符和网络服务信息；和

处理器，连接到存储器，组装一个或多个消息，所述消息包括与多个服务提供商中每个服务提供商相关联的服务提供商标识符和网络服务信息，并将这一个或多个消息传送到移动站。

9. 如权利要求 8 所述的接入点，其中，所述一个或多个消息包括第一一个或多个消息，并且其中，所述处理器接收鉴别移动站的请求，作为对接收到该请求的响应，组装所述第一一个或多个消息，进而组装包括对鉴别信息的请求的第二消息，然后将所述第二消息传送到移动站。

10. 如权利要求 9 所述的接入点，其中，所述处理器进而响应于传送对鉴别信息的请求，接收所请求的鉴别信息，而且，作为对接收到所请求的鉴别信息的响应，组装请求对移动站的授权的第三消息，然后将所述第三消息传送到服务器。

11. 如权利要求 10 所述的接入点，其中，所述存储器，关联于服务器，储存服务提供商标识符，其中，所接收到的鉴别信息包括服务提供商标识符，并且其中，所述处理器根据所接收到的服务提供商标识符来确定所述服务器。

IPR2025-01571
Apple EX1002 Page 997

通过无线局域网向移动站提供网络服务信息的方法和装置

技术领域

本发明一般涉及无线局域网，具体涉及由无线局域网基础设施向移动站提供网络覆盖、网络可接入性和网络服务信息。

背景技术

局域网（LAN）允许组织在高速网络上共享信息，其可以由相对便宜的硬件组件来组装。LAN 还通过允许 LAN 内的多用户通过对所有用户公用的接口连接到 LAN 外多个网络中的每个，来提供相对便宜的硬件连接给超出 LAN 的网络。直到近来，LAN 受限于硬连线的基础设施，需要用户通过有线连接物理上连接到 LAN。但是，随着无线技术和无线消息传递的近来的发展，无线通信也被用于 LAN 领域，导致无线局域网（WLAN）的发展。

图 1 是现有技术的示例无线局域网（WLAN）通信系统 100 的框图。通信系统 100 包括 WLAN，其包括基本服务集（BSS）104，BSS 又包括一个或多个接入点（AP）106、108（示出了两个）。与 BSS 104 相关联的是服务集标识符（SSID），该 SSID 为 BSS 104 中每个 AP 106、108 所公有，并由 BSS 104 中每个 AP 106、108 储存，起到 BSS 的标识符的作用。WLAN，尤其是一个或多个 AP 106、108 中的每个，连接到鉴别（Authentication）、授权（Authorization）、结算（Accounting）（AAA）服务器 110，AAA 服务器 110 向 WLAN 提供鉴别、授权、结算服务。AAA 服务器 110 包括数据库 112，其储存与授权接入 WLAN 的每个移动站（MS）相关联的标识符，并且进一步储存与每个标识符相关联的密码。

当 MS 102 希望接入 WLAN 时，MS 首先必须建立和配置与一个

IPR2025-01571
Apple EX1002 Page 998

或多个 AP 106、108 中的一个 AP 的链路，通常通过主动或被动扫描 WLAN 来完成。在主动扫描中，MS 102 通过广播探测请求（Probe Request）来开始建立和配置链路。探测请求包括服务集标识符（SSID）以及 MS 所支持的功能和数据率。一旦接收到探测请求，一个或多个 AP 106、108 中的每个 AP 确定探测请求中包含的 SSID 是否同与 AP 相关联的 SSID 相同。当 SSID 相同时，AP 响应探测请求，发送探测响应回到 MS，其包括与 AP 相关联的 SSID 以及 AP 所支持的功能和数据率。基于接收到的探测响应，MS 102 从一个或多个 AP 106、108 中选择最佳 AP，诸如 AP 106，并且发送关联请求到所选的 AP 106，其包括 SSID，还包括 MS 所支持的功能和数据率。一旦接收到关联请求，AP 106 发送关联响应到 MS 102，其包括唯一关联于 AP 的标识符，即 AP 地址，和 AP 将要支持的功能和数据率，并且建立 MS 和所选 AP 之间的链路。

在被动扫描中，不利用探测请求和探测响应，MS 102 可以选择 AP 并发送关联请求到所选 AP，以响应于接收到一个或多个 AP 106、108 中每个断断续续地发射的信标（Beacon）。类似于探测响应，每个信标包括与 AP 相关联的 SSID 以及 AP 所支持的功能和数据率。

在建立了 MS 102 和 AP 106 之间的链路之后，在对 MS 102 授权发送数据业务到 AP 106（即，不封锁对 WLAN 的接入）之前必须鉴别 MS 102。图 2 是现有技术的 WLAN 鉴别过程的信号流图 200。鉴别过程开始于 MS 102 发送 EAPOL（Extensible Application Protocol Over LAN，局域网可扩展应用协议）-开始消息 202 到 AP 106。响应于接收到 EAPOL-开始消息 202，AP 106 发送 EAPOL-EAP（Extensible Application Protocol，可扩展应用协议）-请求/识别消息 204 到 MS 102。EAPOL-EAP-请求/识别消息 204 从 MS 请求鉴别信息，诸如唯一关联于 MS 的标识符和密码。一旦接收到 EAPOL-EAP-请求/识别消息 204，MS 102 发送 EAPOL-EAP-响应/识别消息 206 到 AP 106，其提供了所请求的信息。

IPR2025-01571
Apple EX1002 Page 999

一旦接收到 EAPOL-EAP-响应/识别消息 206，AP 106 将 MS 102 所提供的标识符和密码通过半径（RADIUS）-EAP-响应/识别消息 208 转发到 AAA 服务器。一旦接收到识别消息，AAA 服务器 110 选择 EAP 鉴别方法。该方法包括一轮或多轮的 EAP 鉴别请求消息 210、212，从 AAA 服务器 110 传送到 MS 102，以及作为响应的 EAP 鉴别响应消息 214、216，从 MS 传送到 AAA 服务器。EAP 消息在 AAA 服务器 110 和 AP 106 之间携带在半径消息中，在 AP 106 和 MS 102 之间携带在 EAPOL 消息中。在鉴别请求和鉴别响应的最终交换的结束处，AAA 服务器 110 基于储存在数据库 112 中的一个或多个公知的用户标识符，诸如密码、共享秘密、公钥或数字证书，来鉴别 MS 102。如果 AAA 服务器 110 能够成功地鉴别 MS 102，那么 AAA 110 将半径-EAP-成功消息 218 传送到 AP 106。一旦接收到半径-EAP-成功消息 218，AP 106 将 EAPOL-EAP-成功消息 220 传送到 MS 102，并且不再封锁对 MS 102 的接入。如果 AAA 服务器 110 不能成功鉴别 MS 102，则 AAA 服务器将半径-EAP-失败消息传送到 AP 106，AP 106 继续封锁对 MS 102 的接入。

随着 WLAN 逐渐普及，WLAN 建立在更多数量的商业设施和公共场所中，诸如咖啡馆、机场、图书馆、学校以及会议中心。由于订制不同服务提供商的服务的不同人群在这些场所表达了希望接入 WLAN 服务的需求，因此对于提供商来说，将发展需要以提供交叠服务。但是，当前对于 AP 的共享并没有规定任何过程。相反地，在当前最新技术中，每个提供商提供独立的 AP，其配置以自己的 SSID 并且广播该 SSID。这样的系统十分浪费，因为它迫使服务提供商提供冗余的系统。而且，提供 WLAN 服务的可用带宽是有限的，主要的 WLAN 场所，诸如机场和会议中心，可能不具有足够的带宽来支持多个服务提供商中每个所使用的交叠 AP。

此外，当前最新技术仅仅允许用户根据 SSID 来选择服务提供商。

IPR2025-01571
Apple EX1002 Page 1000

当用户能够接入多个服务提供商的每个的网络时，SSID 独自不可能向用户提供足够的信息来作出有关使用哪个服务提供商的充分有见识（fully informed）的决定。而且，当用户执行被动扫描时，用户可能不得不在选择与所需服务提供商相关联的 SSID 之前扫描和处理多个信标，消耗了向 MS 供电的有限寿命电池的过多的电量。

因此，需要一种方法和装置，允许接入 WLAN 的 MS 用户根据一个或多个标准，诸如每个服务提供商所支持的服务、服务价格、付费方法、访问的网络提供商和用户的归属网络之间的关系，从多个服务提供商中选择服务提供商，并进一步允许多个服务提供商共享 AP。

附图说明

图 1 是现有技术的示例无线局域网的框图。

图 2 是现有技术鉴别过程的信号流图。

图 3 是根据本发明实施例的无线通信系统的框图。

图 4 是根据本发明实施例的图 3 的移动站的框图。

图 5 是根据本发明实施例的图 3 的无线通信系统所执行的鉴别过程的信号流图。

具体实施方式

为了解决上述需要，即一种方法和装置，用于允许接入无线局域网（WLAN）的 MS 用户根据一个或多个标准，诸如每个服务提供商所支持的服务、服务价格、付费方法、访问的网络提供商和用户的归属网络之间的关系，从多个服务提供商中选择服务提供商，并进一步允许多个服务提供商共享 AP，提供一种 WLAN 通信系统，其包括与移动站通信的接入点，至少一个鉴别、授权、结算（AAA）服务器提供鉴别过程，由此移动站用户可以在被鉴别之前从一个或多个 WLAN 服务提供商和/或一个或多个 3GPP 服务提供商中选择 WLAM 服务提供商，进一步根据与所选服务提供商相关联的、除了服务集标识符（SSID）之外的网络服务信息来作出订制所选服务提供商的服务的决

IPR2025-01571
Apple EX1002 Page 1001

定。

一般地，本发明的实施例包括一种用于向接入无线局域网的移动站用户提供网络服务信息的方法。该方法包括接收鉴别移动站的请求，作为对接收到请求的响应，传送关于多个服务提供商中每个服务提供商的网络识别和服务信息到移动站。

本发明的另一个实施例包括一种用于接入无线局域网的方法。该方法包括传送鉴别移动站的请求，接收关于服务提供商的网络识别和服务信息，以及根据接收到的网络识别和服务信息来确定是否接入该无线局域网。

本发明又一个实施例包括一种无线局域网中的接入点。接入点包括存储器和连接到存储器的处理器。存储器储存与多个服务提供商中的每个服务提供商相关联的标识符和网络服务信息，并将一个或多个消息传送到移动站。

通过参考图 3-5 可更加全面地描述本发明。图 3 是根据本发明实施例的无线通信系统 300 的框图。通信系统 300 包括无线局域网（WLAN）304，其包括具有一个或多个接入点（AP）308（示出了一个）的基本服务集（BSS）306。AP 308 提供无线通信服务给用户设备（UE），也就是，移动站（MS），诸如 MS 302，其位于 AP 所服务的覆盖区域内。优选地，MS 302 是便携、移动、或蜂窝通信设备，诸如但不限于蜂窝电话、无线电话、或无线调制解调器，其包括在数据终端设备内或连接到数据终端设备，诸如个人电脑、笔记本电脑、工作站、打印机、或传真机，其能够在 WLAN 通信系统中工作。BSS 306 和 AP 308 是由能够与 WLAN 网络交互的多个公共和/或专用网络服务提供商 322、324（示出了两个）所共享的，也就是说，代表这多个公共和/或专用网络服务提供商 322、324 来提供无线通信服务，这些服务提供商诸如但不限于，3GPP（第三代合作项目）、3GPP2、和企业

IPR2025-01571
Apple EX1002 Page 1002

网络服务提供商，其允许 MS 与有效连接到 AP 的相应的外部网络进行通信。

通信系统 300 还包括一个或多个鉴别、授权、结算（AAA）服务器 314、318（示出了两个），其有效连接到 WLAN 304，具体连接到 AP 308，并且提供鉴别、授权和结算服务给 WLAN。多个 AAA 服务器 314、318 的每个 AAA 服务器都与关联于 BSS 306 和 AP 308 的多个服务提供商 322、324 之一相关联。每个 AAA 服务器 314、318 包括各自的数据库 316、320，其储存与被授权接入 WLAN 304 的每个移动站（MS）相关联的标识符，进一步地，关联于每个标识符，储存密码和相关付费信息，诸如与 MS 相关联的归属服务提供商。在本发明的另一实施例中，AP 308，或 BSS 306 和 AP 308，可以仅代表单一的 WLAN 服务提供商，诸如服务提供商 322，来提供无线通信服务。

AP 308 包括处理器 310，诸如一个或多个微处理器、微控制器、数字信号处理器（DSP）、其组合或者本领域普通技术人员已知的这样的其他设备。AP 308 还包括与处理器相关联的一个或多个存储设备 312，诸如随机存取存储器（RAM）、动态随机存取存储器（DRAM）、和/或只读存储器（ROM）或其等价物，其储存可由处理器执行的数据和程序。存储设备 312 还关联于与 AP 相关的每个服务提供商 322、324，储存服务提供商标识符或网络标识符、优选储存服务集标识符（SSID），以及网络服务信息，诸如关于服务提供商所支持的服务的信息、服务提供商所支持的每项服务的价格、为所提供的服务付费的方法、以及每个服务提供商与用户的归属服务提供商之间的关系，诸如其他服务提供商（即，归属网络）的订户使用该服务提供商网络（即访问网络）时该服务提供商所征收的任何额外费用。

图 4 是根据本发明实施例的 MS 302 的框图。MS 302 包括连接到处理器 404 的用户接口 402，处理器 404 诸如一个或多个微处理器、微控制器、数字信号处理器（DSP）、其组合或者本领域普通技术人

IPR2025-01571
Apple EX1002 Page 1003

员已知的这样的其他设备。用户接口 402 向 MS 的用户提供与 MS 交互的能力，包括输入指令到 MS。在本发明的一个实施例中，用户接口 402 包括显示屏幕，其包括触摸屏，触摸屏能够确定用户在触摸屏上触摸的位置(即 X 坐标和 Y 坐标)，并把位置数据传送到处理器 404。根据位置数据，处理器 404 随后将用户的触摸转换成指令。在本发明的另一个实施例中，用户接口 402 可包括显示屏幕和键盘。

MS 302 还包括与处理器 404 相关联的一个或多个存储设备 406，诸如随机存取存储器（RAM）、动态随机存取存储器（DRAM）、和/或只读存储器（ROM）或其等价物，其储存可由处理器执行的数据和程序。存储设备 406 还储存唯一关联于 MS 的 MS 标识符以及 SSID 和相应的鉴别标识符，诸如密码、共享秘密、公钥、数字证书等等，关联于每个服务提供商，诸如 MS 302 所订制的一个或多个服务提供商 322、324。此外，存储设备 406 储存用于组装 MS 与 WLAN 304 所交换的消息的指令。

优选地，通信系统 300 根据用于 WLAN 通信系统的电气电子工程师协会（IEEE）802.11 标准、尤其是根据 IEEE P802.1X/D11 和 802.11i/D2 标准来工作，该标准在此整体结合进来，其可以从 IEEE 行政办公机构（Piscataway, NJ）或者通过 standards.ieee.org 在线获得。此外，通信系统 300 优选还根据第三代合作项目（3GPP）对于 WLAN-蜂窝交互标准(TR 22.934 和 TR 23.934)的要求工作，该标准可从 ETSI 的 3GPP 处（Mobile Competence Centre, 650, route des Lucioles, 06921 Sophia-Antipolis Cedex, France）或通过 3gpp.org 在线获得，还有因特网工程任务组（IETF）RFC（请求注解）2284，其可以从 IETF 办公机构（Reston, VA）或者通过 ietf.org/rfc 在线获得，其描述了媒介接入控制（MAC）层可扩展鉴别协议（EAP），提供了鉴别协议的 MAC 层协商，用于在允许网络层协议通过链路发送之前鉴别对等设备，这些标准和协议，以及 IETF 备忘录“EAP AKA Authentication”, H. Haverinen, February 2002, 和“EAP SIM Authentication”, H. Haverinen,

IPR2025-01571
Apple EX1002 Page 1004

June 2002 都在这里整体结合进来。

为了让 MS 302 接入 WLAN 304，MS 首先根据公知的链路建立和配置技术建立与 WLAN 的链路。一旦建立了这条链路，通信系统 300 在授权 MS 发送数据业务之前鉴别 MS 302。在现有技术中，为了订制 WLAN 的服务，鉴别过程仅仅允许 MS 用户根据相关服务提供商的 SSID 作出订制决定。跟现有技术不同，通信系统 300 提供了鉴别过程，从而 MS 302 的用户可以在被鉴别之前从一个或多个 WLAN 服务提供商和/或一个或多个 3GPP 服务提供商中选择 WLAN 服务提供商，进而根据与所选服务提供商相关联的、除了服务集标识符（SSID）之外的网络服务信息作出订制所选服务提供商的服务的决定。

图 5 是根据本发明实施例的通信系统 300 所执行的鉴别过程的信号流图 500。鉴别过程开始于 MS 发送鉴别步骤开始消息 502，优选为 EAPOL（局域网可扩展应用协议）-开始消息，到 WLAN 304，具体是到 AP 308。一旦接收到鉴别步骤开始消息 502，AP 308，具体是 AP 的处理器 310，从存储器 312 中提取关于与 AP 相关联的每个服务提供商（诸如服务提供商 322 和 324）的网络识别和服务信息。AP 308 随后在网络识别和服务信息消息 504、优选为 EAPOL-EAP-请求/信息消息中将提取的网络识别和服务信息传送到 MS 302。

一旦接收到网络识别和服务信息消息 504，MS 302 在用户接口 402 的显示屏幕中显示 508 关联于相应服务提供商 322、324 的至少一部分的接收到的网络识别和服务信息。通过显示网络识别和服务信息，MS 302 允许 MS 用户作出关于订制服务提供商用于特定通信会话的有见识的（informed）选择，而不是局限于仅仅根据 SSID 就作出选择。而且，通过在鉴别过程的开始处向 MS 302 提供对应于与 AP 308 相关联的每个服务提供商 322、324 的网络识别和服务信息，系统 300 减少了 MS 302 通过向 AP 提供单一 SSID 并反过来接收对应于所提供的 SSID 的网络服务信息而单独恳请与 BSS 相关联的每个服务提供商的

IPR2025-01571
Apple EX1002 Page 1005

网络服务信息的需要。

根据在 MS 302 的用户接口 402 上显示的信息，MS 用户随后能够决定是否接入 WLAN 304。一旦确定接入 WLAN，用户向 MS 302 输入，同时 MS 从用户接收 508，对服务提供商的选择。例如，用户可能通过选择用户接口的显示屏幕上显示的软按键或者文本消息或者通过按下用户接口的键盘上的按键来输入他或她的选择。在本发明的另一个实施例中，其中，AP 308 只代表单一的服务提供商提供无线通信服务，MS 302 用户可能不需要输入服务提供商的选择，而是输入希望接入 WLAN 304 的指示。在本发明又一个实施例中，MS 的用户或卖家可能在 MS 302 的存储设备 406 中储存服务偏好。储存的偏好可能随后由 MS 302 用于自动选择服务提供商或根据 MS 从 AP 308 所接收到的网络和服务信息确定是否接入 WLAN 304。

一旦接收到网络服务信息消息 504，MS 302 通过传送确认 510、优选为 EAPOL-EAP-响应/信息/ACK 消息回到 AP 308 来确认消息的接收。一旦接收到确认 510，AP 308 将消息 512 传送到 MS 302，从 MS 请求鉴别信息，诸如唯一关联于 MS 的标识符、与所选服务提供商相关联的 SSID、和密码。优选地，请求鉴别信息的消息 512 是 EAPOL-EAP-请求/识别消息。一旦接收到请求鉴别信息的消息 512 并且一旦从 MS 用户接收到对服务提供商的选择、接收到用户希望接入 WLAN 304 的指示、或自动选择了服务提供商或确定接入 WLAN 304，MS 302 就发送提供请求的鉴别信息的消息 514，优选为 EAPOL-EAP-响应/识别消息，其包括所选网络的标识符、即 SSID，以及至少一部分的接收到的网络识别和服务信息。通过提供 SSID 和至少一部分的接收到的网络识别和服务信息，MS 302 向 WLAN 304、具体是 AP 308 提供所选的服务提供商。根据从 MS 接收的 SSID 和信息，WLAN 能够确定合适的 AAA 服务器 314、318 用于鉴别 MS。

一旦接收到请求的鉴别信息，AP 308 能够确定合适的 AAA 服务

IPR2025-01571
Apple EX1002 Page 1006

器 314、318 来进行鉴别。AP 308 随后在鉴别信息消息 516、优选为半径-EAP-响应/识别消息中将 MS 302 所提供的标识符和密码转发给与所选服务提供商相关联的 AAA 服务器，诸如 AAA 服务器 314。类似于通信系统 100，一旦接收到鉴别信息消息 516，AAA 服务器 314 就选择 EAP 鉴别方法，AAA 服务器就要通过该方法鉴别 MS 302。EAP 鉴别方法包括一轮或多轮的 EAP 鉴别请求消息 518、520，其分别从 AAA 服务器 314 传送到 AP 308 和从 AP 308 传送到 MS 302，而作为响应，还包括 EAP 鉴别响应消息 522、524，分别从 MS 到 AP 和从 AP 到 AAA 服务器。在本发明的一个实施例中，EAP 消息是 MAC 层消息或数据链路层消息，其携带在 AAA 服务器 314 和 AP 308 之间的半径协议消息以及 AP 308 和 MS 302 之间的 EAPOL 消息中。在本发明的另一实施例中，在 AAA 服务器 314 和 AP 308 之间交换的 EAP 消息是 MAC 层消息或数据链路层消息，其携带在直径（Diameter）协议消息中。

在鉴别请求和鉴别响应的最终交换的结尾处，AAA 服务器 314 根据储存在 AAA 数据库 316 中的一个或多个公知鉴别标识符，诸如密码、共享秘密、公钥、或数字证书，来鉴别 MS 302。如果 AAA 服务器 314 能够成功鉴别 MS 302，则 AAA 服务器 314 传送授权消息 526、优选为半径-EAP-成功消息，到 AP 308，用于授权 AP 不再封锁对 MS 302 的接入。一旦接收到授权消息 526，AP 308 传送授权消息 528、优选为 EAPOL-EAP-成功消息，到 MS 302，用于授权 MS 接入 WLAN 304 并解除对 MS 302 的接入的封锁。如果 AAA 服务器 314 不能成功鉴别 MS 302 的话，则 AAA 服务器传送授权失败消息 532、优选为半径-EAP-失败消息，到 AP 308。在此情况下，AP 308 继续到框 534 接入 MS 302。

总而言之，WLAN 通信系统 300 提供了鉴别过程，由此 MS 302 用户可以在被鉴别之前从共享 WLAN 的一个或多个 WLAN 服务提供商和/或一个或多个 3GPP 服务提供商 322、324 中选择 WLAN 服务提

IPR2025-01571
Apple EX1002 Page 1007

供商，进而根据与所选服务提供商相关联的、除服务集标识符（SSID）之外的网络服务信息，作出订制所选服务提供商的服务的决定。作为鉴别过程的一部分，WLAN 304 向 MS 提供关于一个或多个服务提供商的网络识别和服务信息，诸如每个服务提供商所支持的服务、服务价格、付费方法、以及访问的网络提供商和用户的归属网络之间的关系，从而允许 MS 用户作出关于 WLAN 服务提供商的有见识的选择。MS 可随后从这一个或多个服务提供商中选择服务提供商并且通过向 WLAN 传送相关 SSID 和至少一部分的接收到的网络识别和服务信息来通知 WLAN 所选的服务提供商。根据从 MS 接收到的 SSID 和信息，WLAN 能够确定合适的 AAA 服务器 314、318，用于鉴别 MS。

尽管本发明具体通过结合特定其实施例而显示和描述，但本领域技术人员将理解，可以作出各种变化以及进行要素的等价替换，这并不偏离本发明如权利要求所述的范围。因此，说明书和附图都应被视为说明性的而非限制性的，所有这样的变化和替换都包括在本发明的范围之内。

上面已经关于特定实施例描述了益处、其他优点、和问题的解决方案。但是，益处、优点、问题的解决方案，以及任何能够引起任何益处、优点或解决方案，或者使之出现或变得更显著的要素都不应被视作是任意或所有权利要求的决定性的、必需的或者关键的特征或要素。如这里所使用的，术语“包括、包含”或其任何变形，都意欲覆盖非排他性的包含，因此，包括一系列要素的过程、方法、物品或装置不仅仅包括那些列出的要素，还有可能包括其他未明确列出或者这样的过程、方法、物品或装置所固有的其他要素。还应当理解，关系术语的使用（如果有的话），诸如第一和第二、顶和底等等，都仅仅是用来区分一个实体或行为与另一个实体或行为，而不必要求或暗示这样的实体或行为之间的任何实际的这样的关系或顺序。

IPR2025-01571
Apple EX1002 Page 1008

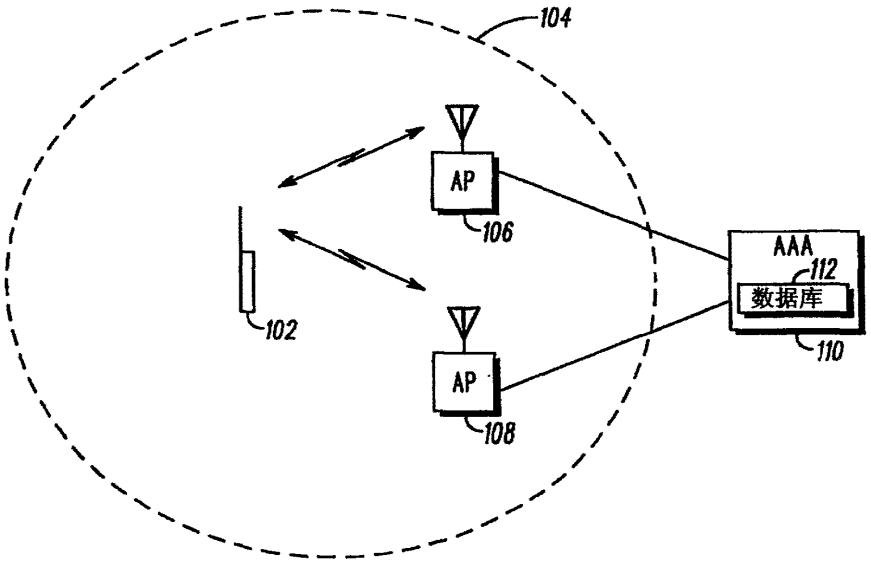


图1
现有技术

IPR2025-01571
Apple EX1002 Page 1009

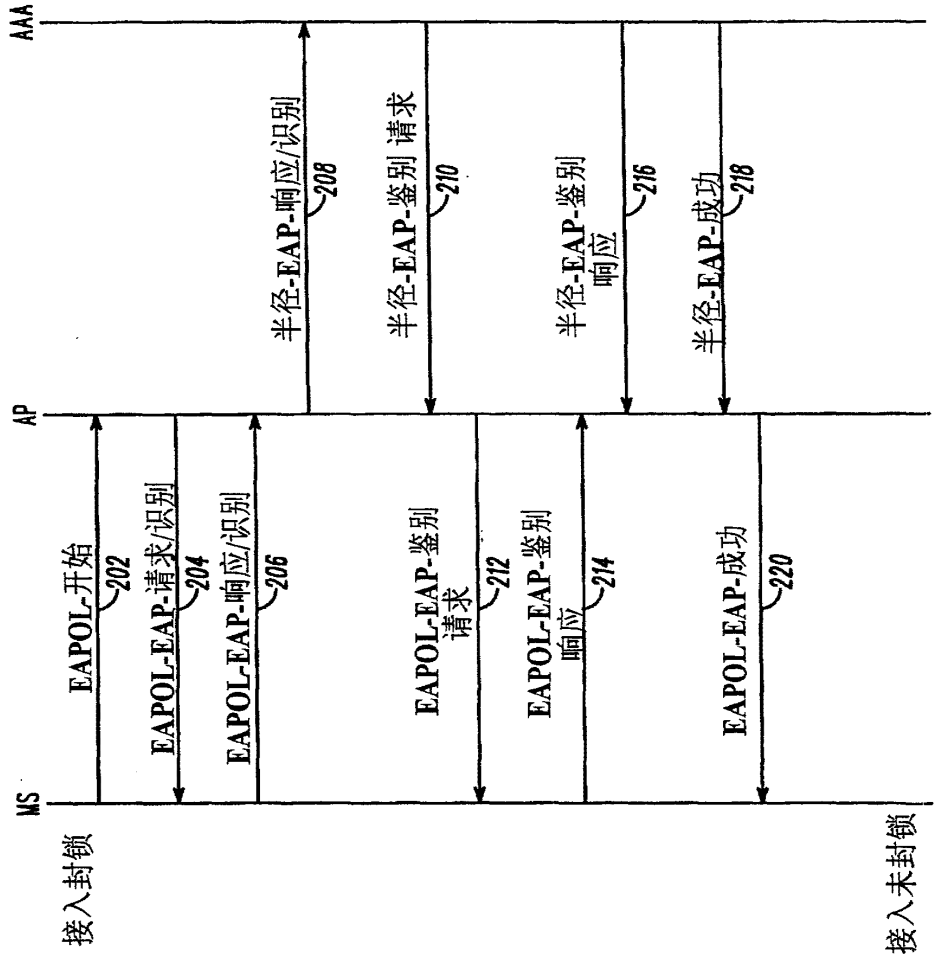


图2
现有技术

IPR2025-01571
Apple EX1002 Page 1010

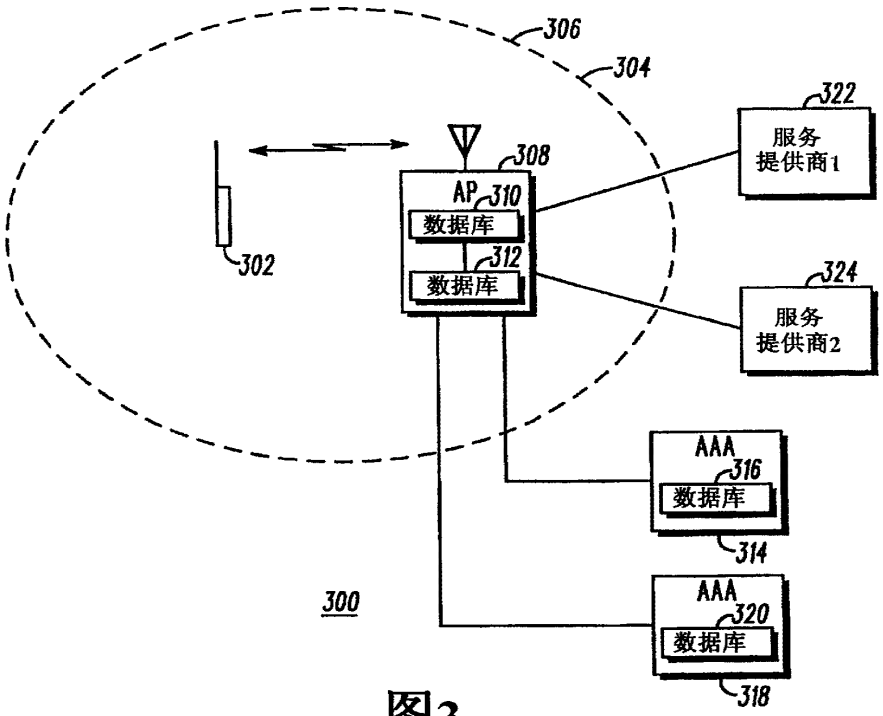


图3

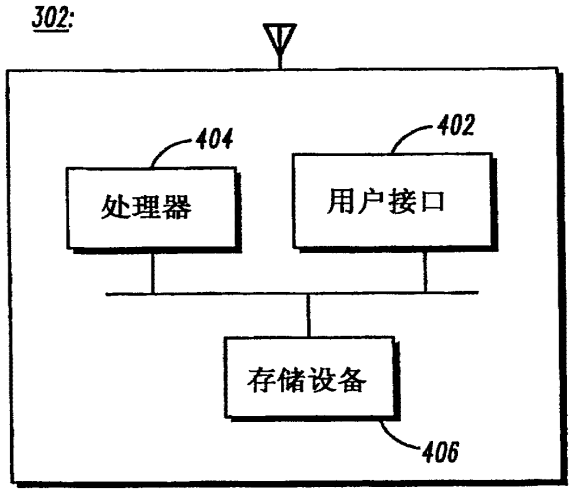


图4

IPR2025-01571
Apple EX1002 Page 1011

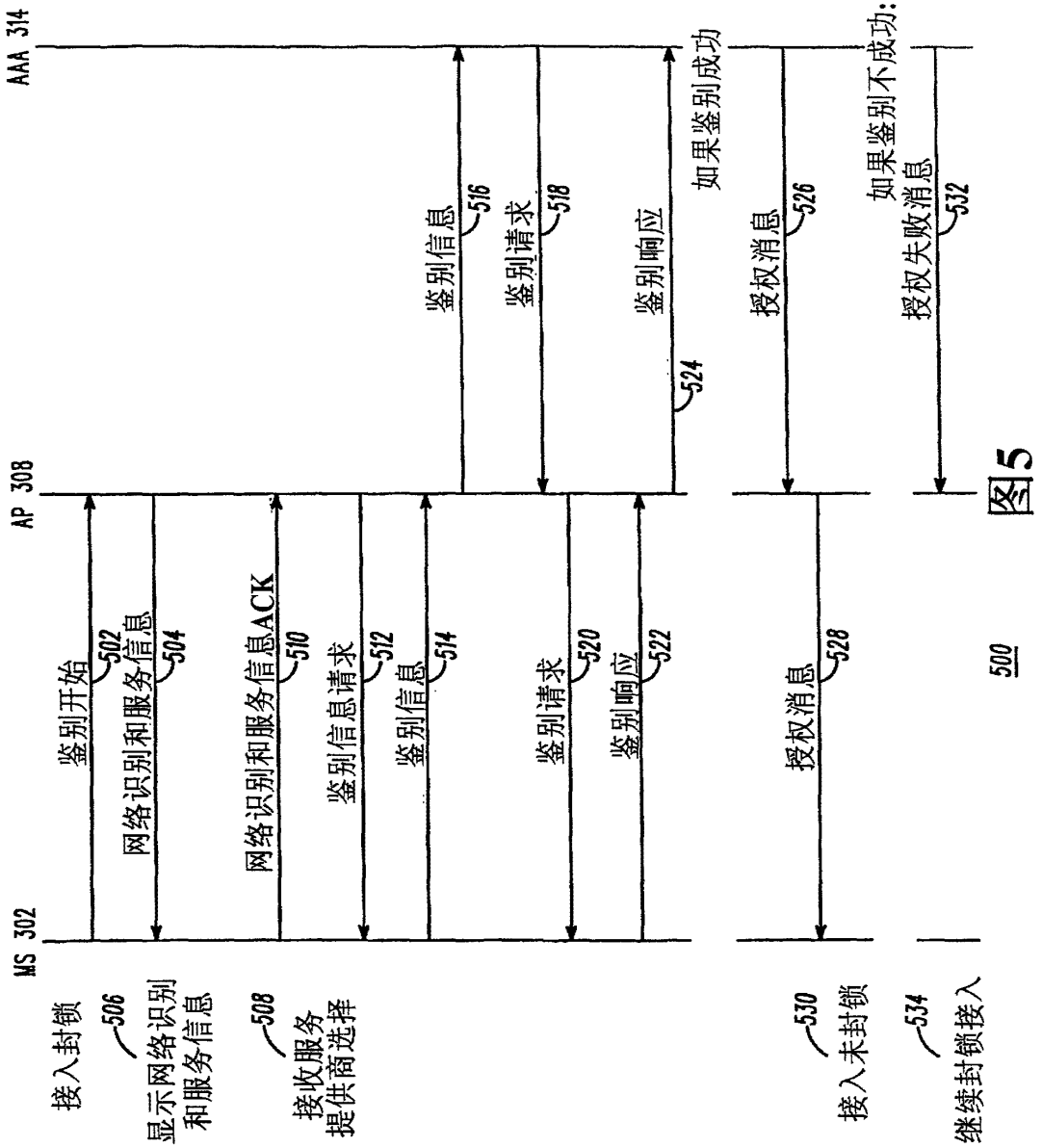


图5

IPR2025-01571
Apple EX1002 Page 1012

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 July 2004 (29.07.2004)

PCT

(10) International Publication Number
WO 2004/064306 A2

(51) International Patent Classification[7]: H04L

(21) International Application Number:
PCT/US2004/000870

(22) International Filing Date: 13 January 2004 (13.01.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/439,743	13 January 2003 (13.01.2003)	US
10/755,800	12 January 2004 (12.01.2004)	US

(71) Applicant *(for all designated States except US)*: **MOTOROLA INC. A CORPORATION OF THE STATE OF DELAWARE** [US/US]; 1303 East Algonquin Road, Schaumburg, Illinois 60196 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **WILD, Johanna,** [DE/DE]; Seitzstr. 17, Bavaria, 80538 Muenchen (DE). **PAZHYANNUR, Rajesh,** [IN/US]; 1204 East Algonquin Road, Schaumburg, Illinois 60173 (US).

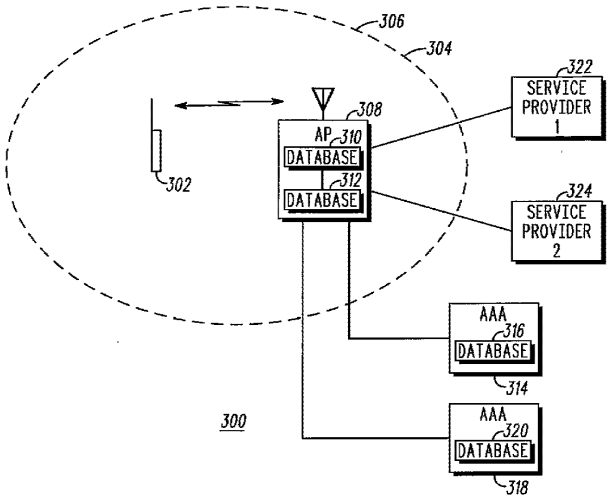
(74) Agents: **MAY, Steven A.,** et al.; 1303 East Algonquin Road, Schaumburg, Illinois 60196 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR PROVIDING NETWORK SERVICE INFORMATION TO A MOBILE STATION BY A WIRELESS LOCAL AREA NETWORK



(57) Abstract: A wireless local area network (WLAN) communication system (300) that includes an access point (308) in communication with a mobile station (302) and at least one Authentication, Authorization, and Accounting (AAA) server (314, 318) provides an authentication process whereby a user of the mobile station may select a WLAN service provider from among one or more WLAN service providers and/or one or more 3GPP service providers (322, 324) before being authenticated and further to make a decision to subscribe to the services of the selected service provider based on network service information, other than or in addition to an Service Set Identifier (SSID), associated with the selected service provider.

WO 2004/064306 A2

IPR2025-01571
Apple EX1002 Page 1013

Published:
— *without international search report and to be republished upon receipt of that report*

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

METHOD AND APPARATUS FOR PROVIDING NETWORK SERVICE INFORMATION TO A MOBILE STATION BY A WIRELESS LOCAL AREA NETWORK

Field of the Invention

The present invention relates generally to wireless local area networks and, in particular, to provision of network coverage, network accessibility, and network service information by a wireless local area network infrastructure to a mobile station.

Background of the Invention

Local area networks (LANs) allow organizations to share information over a high speed network that may be assembled with relatively inexpensive hardware components. LANs also provide for relatively inexpensive hardware connections to networks beyond the LAN by allowing multiple users within the LAN to connect to each of multiple networks outside of the LAN through an interface common to all users. Until recently, LANs were limited to hardwired infrastructure, requiring the user to physically connect to the LAN via a wired connection. However, with the recent growth of wireless telephony and wireless messaging, wireless communications have also been applied to the realm of LANs, resulting in the development of wireless local area networks (WLANs).

FIG. 1 is a block diagram of an exemplary wireless local area network (WLAN) communication system 100 of the prior art. Communication system 100 includes a WLAN that comprises a Basic Service Set (BSS) 104, which BSS in turn comprises one or more Access Points (APs) 106, 108 (two shown). Associated with BSS 104 is a Service Set Identifier (SSID), which SSID is common to, and stored by, each AP 106, 108 in BSS 104 and functions as an identifier of the BSS. The WLAN, and in particular each of the one or more APs 106 and 108, is coupled to an Authentication, Authorization, and Accounting (AAA) server 110 that provides authentication, authorization, and

IPR2025-01571
Apple EX1002 Page 1015

accounting services to the WLAN. AAA server 110 includes a database 112 that stores identifiers associated with each mobile station (MS) that is authorized to access the WLAN and further stores a password in association with each identifier.

When an MS 102 wishes to access the WLAN, the MS must first establish and configure a link with an AP of the one or more APs 106, 108, typically by actively or passively scanning the WLAN. In an active scan, MS 102 initiates the establishment and configuration of a link by broadcasting a Probe Request. The Probe Request includes a Service Set Identifier (SSID) and capabilities and data rates supported by the MS. Upon receiving the Probe Request each AP of the one or more APs 106, 108 determines whether the SSID included in the Probe Request is the same as the SSID associated with the AP. When the SSIDs are the same, the AP responds to the Probe Request by transmitting a Probe Response back to the MS that includes the SSID associated with the AP and capabilities and data rates supported by the AP. Based on the received Probe Responses, MS 102 selects a best AP, such as AP 106, of the one or more APs 106, 108 and transmits an Association Request to the selected AP 106 that includes the SSID and further includes the capabilities and data rates supported by the MS. Upon receiving the Association Request, AP 106 transmits an Association Response to MS 102 that includes an identifier uniquely associated with the AP, that is, an AP address, and the capabilities and data rate that will be supported by the AP, and establishes a link between the MS and the selected AP.

In a passive scan, instead of utilizing a Probe Request and a Probe Response, MS 102 may select an AP and transmit an Association Request to the selected AP in response to receiving a Beacon that is intermittently transmitted by each of the one or more APs 106, 108. Similar to the Probe Response, each Beacon includes the SSID associated with the AP and capabilities and data rates supported by the AP.

After a link is established between MS 102 and AP 106, MS 102 must be authenticated before the MS is authorized to transmit data traffic to AP 106, that is, is access to the WLAN is unblocked. FIG. 2 is a signal flow diagram 200 of a WLAN authentication process of the prior art. The authentication process begins when MS 102 transmits an EAPOL (Extensible Application Protocol Over LAN)-Start message 202 to

the AP 106. In response to receiving EAPOL-Start message 202, AP 106 transmits an EAPOL-EAP (Extensible Application Protocol)-Request/Identity message 204 to the MS 102. EAPOL-EAP-Request/Identity message 204 requests authentication information from the MS, such as an identifier uniquely associated with the MS and a password. Upon receiving EAPOL-EAP-Request/Identity message 204, MS 102 transmits an EAPOL-EAP-Response/Identity message 206 to AP 106 that provides the requested information.

Upon receiving EAPOL-EAP-Request/Identity message 206, AP 106 forwards the identifier and password provided by MS 102 to AAA server 110 in a RADIUS-EAP-Response/Identity message 208. On receiving the identity message AAA server 110 chooses an EAP authentication method. The method involves one or more rounds of EAP authentication request messages 210, 212 that are conveyed from AAA server 110 to MS 102 and, in response, EAP authentication response messages 214, 216 that are conveyed from the MS to the AAA server. The EAP messages are carried in RADIUS messages between AAA server 110 and AP 106 and in EAPOL messages between AP 106 and MS 102. At the end of the final exchange of authentication requests and authentication responses, AAA server 110 authenticates MS 102 based on one or more well known user identifiers, such as a password, a shared secret, a public key, or a digital certificate, that is stored in database 112. If AAA server 110 can successfully authenticate MS 102, then AAA 110 conveys a RADIUS-EAP-Success message 218 to AP 106. Upon receiving the RADIUS-EAP-Success message 218, AP 106 conveys an EAPOL-EAP-Success message 220 to MS 102 and unblocks access to the MS 102. If AAA server 110 cannot successfully authenticate MS 102, then the AAA server conveys a RADIUS-EAP-Failure message to the AP 106. In this case, AP 106 continues to block access to MS 102.

With the increasing popularity of WLANs, WLANs are being set up in an increasing number of commercial establishments and public places, such as coffee houses, airports, libraries, schools, and convention centers. As diverse groups of people who subscribe to the services of a diversity of service providers express their desire to access WLAN services in such places, the need will evolve for the providers to provide overlapping services. However, currently no process is prescribed for a sharing of an AP.

Instead, in the current state of the art, each provider provides a separate AP that is configured with, and broadcasts, its own SSID. Such a system is wasteful in that it forces service providers to provide redundant systems. Furthermore, the bandwidth available for provision of WLAN services is limited and prime WLAN locations, such as airports and convention centers, may not have sufficient bandwidth to support overlapping APs employed by each of multiple service providers.

In addition, the current state of the art permits a user to select a service provider based only on SSID. When a user is capable of accessing the networks of each of multiple service providers, the SSID alone may not provide the user with sufficient information to make a fully informed decision concerning which service provider to use. Furthermore, when the user performs a passive scan, the user may have to scan and process multiple beacons before selecting an SSID associated with a desired service provider, consuming an excessive amount of power of a limited life battery powering an MS.

Therefore a need exists for a method and apparatus that permits a user of an MS accessing a WLAN to select a service provider from among multiple service providers based on one or more criterion, such as services supported by each service provider, service costs, methods of billing, and a relationship between the visited network provider and the user's home network, and that further allows multiple service providers to share an AP.

Brief Description of the Drawings

FIG. 1 is a block diagram of an exemplary wireless local area network of the prior art.

FIG. 2 is a signal flow diagram of a prior art authentication process.

FIG. 3 is a block diagram of a wireless communication system in accordance with an embodiment of the present invention.

FIG. 4 is a block diagram of the mobile station of FIG. 3 in accordance with an embodiment of the present invention.

FIG. 5 is a signal flow diagram of an authentication process performed by the wireless communication system of FIG. 3 in accordance with an embodiment of the present invention.

Detailed Description of the Invention

To address the need for a method and an apparatus that that permits a user of an MS accessing a wireless local area network (WLAN) to select a service provider from among multiple service providers based on one or more criterion, such as services supported by each service provider, service costs, methods of billing, and a relationship between the visited network provider and the users home network, and that further allows multiple service providers to share an AP, a WLAN communication system that includes an access point in communication with a mobile station and at least one Authentication, Authorization, and Accounting (AAA) server provides an authentication process whereby a user of the mobile station may select a WLAN service provider from among one or more WLAN service providers and/or one or more 3GPP service providers before being authenticated and further to make a decision to subscribe to the services of the selected service provider based on network service information, other than or in addition to an Service Set Identifier (SSID), associated with the selected service provider.

Generally, an embodiment of the present invention encompasses a method for providing network service information to a user of a mobile station accessing a wireless local area network. The method includes receiving a request to authenticate the mobile station and, in response to receiving the request, conveying network identification and service information with respect to each service provider of a plurality of service providers to the mobile station.

Another embodiment of the present invention encompasses a method for accessing a wireless local area network. The method includes conveying a request to authenticate a mobile station, receiving network identification and service information with respect to a service provider, and determining whether to access the wireless local area network based on the received network identification and service information.

Yet another embodiment of the present invention encompasses an Access Point in a wireless local area network. The Access Point includes a memory and a processor coupled to the memory. The memory stores an identifier and network service information in association with each service provider of a plurality of service providers. The processor assembles one or more messages comprising the service provider identifier and the network service information associated with each service provider of a plurality of service providers and conveys the one or more messages to a mobile station.

The present invention may be more fully described with reference to FIGs. 3-5. FIG. 3 is a block diagram of a wireless communication system 300 in accordance with an embodiment of the present invention. Communication system 300 comprises a wireless local area network (WLAN) 304 that includes a Basic Service Set (BSS) 306 comprising one or more Access Points (APs) 308 (one shown). AP 308 provides wireless communication services to user equipment (UEs), that is, mobile stations (MSs), such as MS 302, located in a coverage area serviced by the AP. Preferably MS 302 is a portable, mobile, or cellular communication device, such as but not limited to a cellular telephone, a radiotelephone, or a wireless modem that is included in or coupled to data terminal equipment, such as a personal computer, a laptop computer, a workstation, a printer, or a facsimile machine, that is capable of operating in a WLAN communication system. BSS 306 and AP 308 are shared by, that is, provide wireless communication services on behalf of, multiple public and/or private network service providers 322, 324 (two shown) capable of interworking with a WLAN network, such as but not limited to 3GPP (Third Generation Partnership Project), 3GPP2, and enterprise network service providers, that allow the MS to communicate with a corresponding external network operably coupled to the AP.

Communication system 300 further includes one or more Authentication, Authorization, and Accounting (AAA) servers 314, 318 (two shown) that are operably coupled to WLAN 304, and in particular to AP 308, and that provide authentication, authorization, and accounting services to the WLAN. Each AAA server of the multiple AAA servers 314, 318 is associated with one of the multiple service providers 322, 324 associated with BSS 306 and AP 308. Each AAA server 314, 318 includes a respective database 316, 320 that stores identifiers associated with each mobile station (MS) that is

authorized to access WLAN 304 and further stores, in association with each identifier, a password and related billing information, such as a home service provider associated with the MS. In another embodiment of the present invention, AP 308, or BSS 306 and AP 308, may provide wireless communication services on behalf of only a single WLAN service provider, such as service provider 322.

AP 308 includes a processor 310, such as one or more microprocessors, microcontrollers, digital signal processors (DSPs), combinations thereof or such other devices known to those having ordinary skill in the art. AP 308 further includes one or more memory devices 312 associated with processor such as random access memory (RAM), dynamic random access memory (DRAM), and/or read only memory (ROM) or equivalents thereof, that store data and programs that may be executed by the processor. Memory devices 312 further store, in association with each service provider 322, 324 associated with the AP, an address of an AAA server 314, 318 associated with the service provider, a service provider identifier or network identifier, preferably a Service Set Identifier (SSID), and network service information, such as information concerning services supported by the service provider, a cost of each service supported by the service provider, methods of billing for the provided services, and a relationship between each service provider and users' home service providers, such as any extra fees the service provider may assess for use of the service provider's network, that is, a visited network, by subscribers to other service providers, that is, a home network.

FIG. 4 is a block diagram of MS 302, in accordance with an embodiment of the present invention. MS 302 includes a user interface 402 coupled to a processor 404, such as one or more microprocessors, microcontrollers, digital signal processors (DSPs), combinations thereof or such other devices known to those having ordinary skill in the art. User interface 402 provides a user of the MS with the capability of interacting with the MS, including inputting instructions into the MS. In one embodiment of the present invention, user interface 402 includes a display screen that comprises a touch screen that is able to determine a position (i.e., an X-coordinate and a Y-coordinate) of a user's touch on the touch screen and convey the position data to processor 404. Based on the position data, processor 404 then translates the user's touch into an instruction. In another embodiment of the present invention, user interface 402 may include a display screen and

a keypad.

MS 302 further includes one or more memory devices 406 associated with processor 404, such as random access memory (RAM), dynamic random access memory (DRAM), and/or read only memory (ROM) or equivalents thereof, that store data and programs that may be executed by the processor. Memory devices 406 further store an MS identifier that is uniquely associated with the MS and an SSID and a corresponding authentication identifier, such as a password, a shared secret, key, a digital certificate, etc., associated with each service provider, such as one or more of service providers 322, 324, subscribed to by MS 302. In addition, memory devices 406 store instructions for assembling messages that are exchanged by the MS with WLAN 304.

Preferably, communication system 300 operates in accordance with the Institute for Electrical and Electronic Engineers (IEEE) 802.11 standards for WLAN communication systems, and in particular the IEEE P802.1X/D11 and 802.11i/D2 standards, which standards are hereby incorporated herein in their entirety and are available from the IEEE administrative offices in Piscataway, NJ, or on-line at standards.ieee.org. In addition, communication system 300 preferably further operates in accordance with the Third Generation Partnership Project (3GPP) requirements for WLAN-Cellular Interworking standards (TR 22.934 and TR 23.934), which standards are available from the 3GPP at ETSI, Mobile Competence Centre, 650, route des Lucioles, 06921 Sophia-Antipolis Cedex, France, or on-line at 3gpp.org, the Internet Engineering Task Force (IETF) RFC (Request For Comments) 2284, which is available from the IETF offices in Reston, VA, or on-line at ietf.org/rfc and describes a medium access control (MAC) layer Extensible Authentication Protocol (EAP) that provides for MAC layer negotiation of an Authentication Protocol for authenticating a peer before allowing Network Layer protocols to transmit over a link, which standards and protocols are hereby incorporated herein in their entirety, and the IETF memoranda "EAP AKA Authentication," by H. Haverinen, dated February 2002, and "EAP SIM Authentication," by H. Haverinen, dated June 2002.

In order for MS 302 to obtain access to WLAN 304, the MS first establishes a communication link with the WLAN in accordance with well known link establishment

and configuration techniques. Upon establishing the link, communication system 300 authenticates MS 302 before authorizing the MS to transmit data traffic. In the prior art, in order to subscribe to the services of a WLAN, the authentication process merely allowed a user of an MS to make a subscription decision on a basis of an SSID of an associated service provider. Unlike the prior art, communication system 300 provides an authentication process whereby a user of MS 302 may select a WLAN service provider from among one or more WLAN service providers and/or one or more 3GPP service providers before being authenticated and further to make a decision to subscribe to the services of the selected service provider based on network service information, other than or in addition to an Service Set Identifier (SSID), associated with the selected service provider.

FIG. 5 is a signal flow diagram 500 of an authentication process executed by communication system 300 in accordance with an embodiment of the present invention. The authentication process begins when the MS transmits an authentication procedure start message 502, preferably an EAPOL (Extensible Application Protocol Over LAN)-Start message, to WLAN 304, and in particular to AP 308. Upon receiving authentication procedure start message 502, AP 308, an in particular processor 310 of the AP, retrieves from memory 312 network identification and service information concerning each service provider associated with the AP, such as service providers 322 and 324. AP 308 then conveys the retrieved network identification and service information to MS 302 in a network identification and services information message 504, preferably an EAPOL-EAP-Request/Information message.

Upon receiving network identification and services information message 504, MS 302 displays 508, in the display screen of user interface 402, at least a portion of the received network identification and service information in association with the corresponding service provider 322, 324. By displaying the network identification and services information, MS 302 permits a user of the MS to make an informed selection of the service provider subscribed to for a particular communication session instead of being limited to making a selection merely based on SSIDs. Furthermore, by providing MS 302 with network identification and service information corresponding to each service provider 322, 324 associated with AP 308 at the outset of the authentication process,

system 300 reduces the need for MS 302 to individually solicit the network service information of each service provider associated with a BSS by providing an AP with a single SSID and receiving, in return, the network service information corresponding to the provided SSID.

Based on the information displayed on user interface 402 of MS 302, a user of the MS is then able to decide whether to access WLAN 304. Upon determining to access the WLAN, the user inputs to MS 302, and the MS receives 508 from the user, a selection of a service provider. For example, the user may input his or her selection by selecting a softkey or a text message displayed on the display screen of the user interface or by depressing a key in a keypad of the user interface. In another embodiment of the present invention, wherein AP 308 provides wireless communication services on behalf of only a single service provider, the user of MS 302 may not need to input a selection of a service provider and may instead input an indication of a desire to access WLAN 304. In yet another embodiment of the present invention, the user or a vendor of the MS may store service preferences in memory devices 406 of MS 302. The stored preferences may then be used by MS 302 to automatically select a service provider or determine whether to access WLAN 304 based on the network and services information received by the MS from AP 308.

Upon receiving network services information message 504, MS 302 acknowledges receipt of the message by conveying an acknowledgment 510, preferably an EAPOL-EAP-Response/Information/ACK message, back to AP 308. Upon receiving acknowledgment 510, AP 308 conveys a message 512 to MS 302 requesting authentication information from the MS, such as an identifier uniquely associated with the MS, an SSID associated with a selected service provider, and a password. Preferably the message 512 requesting authentication information is an EAPOL-EAP-Request/Identity message. Upon receiving message 512 requesting authentication information and upon receiving a selection of a service provider from a user of the MS, receiving an indication of the user's desire to access WLAN 304, or automatically selecting a service provider or determining to access WLAN 304, MS 102 transmits a message 514 providing the requested authentication information, preferably an EAPOL-EAP-Response/Identity message that includes the identifier of the selected network, that

is, the SSID, and at least a portion of the received network identification and services information. By providing the SSID and the at least a portion of the received network identification and services information, MS 302 provides WLAN 304, and in particular AP 308, with the selected service provider. Based on the SSID and information received from the MS, the WLAN is able to determine an appropriate AAA server 314, 318 for authenticating the MS.

Upon receiving the requested authentication information, AP 308 is able to determine an appropriate AAA server 314, 318 for performing authentication. AP 308 then forwards the identifier and password provided by MS 302 to the AAA server associated with the selected service provider, such as AAA server 314, in an authentication information message 516, preferably a RADIUS-EAP-Response/Identity message. Similar to communication system 100, upon receiving authentication information message 516, AAA server 314 then chooses an EAP authentication method by which the AAA server authenticates MS 302. The EAP authentication method involves one or more rounds of EAP authentication request messages 518, 520 that are respectively conveyed from AAA server 314 to AP 308 and from AP 308 to MS 302 and, in response, EAP authentication response messages 522, 524 that are respectively conveyed from the MS to the AP and from the AP to the AAA server. In one embodiment of the present invention, the EAP messages are MAC layer messages or data link layer messages that are carried in RADIUS protocol messages between AAA server 314 and AP 308 and in EAPOL messages between AP 308 and MS 302. In another embodiment of the present invention, the EAP messages exchanged between AAA server 314 and AP 308 are MAC layer messages or data link layer messages that are carried in Diameter protocol messages.

At the end of the final exchange of authentication requests and authentication responses, AAA server 314 authenticates MS 302 based on one or more well known authentication identifiers, such as a password, a shared secret, a public key, or a digital certificate, that is stored in the AAA's database 316. If AAA server 314 can successfully authenticate MS 302, then AAA server 314 conveys an authorization message 526, preferably RADIUS-EAP-Success message, to AP 308 authorizing the AP to unblock access to MS 302. Upon receiving authorization message 526, AP 308 conveys an

authorization message 528, preferably an EAPOL-EAP-Success message, to MS 302 authorizing the MS to access WLAN 304 and unblocks 530 access to MS 302. If AAA server 314 cannot successfully authenticate MS 302, then the AAA server conveys an authorization failure message 532, preferably a RADIUS-EAP-Failure message, to the AP 308. In this case, AP 308 continues to block 534 access to MS 302.

In summary, WLAN communication system 300 provides an authentication process whereby a user of MS 302 may select a WLAN service provider from among one or more WLAN service providers and/or one or more 3GPP service providers 322, 324 sharing the WLAN before being authenticated and further to make a decision to subscribe to the services of the selected service provider based on network service information, other than or in addition to an Service Set Identifier (SSID), associated with the selected service provider. As part of the authentication process, WLAN 304 provides to the MS network identification and services information concerning the one or more service providers, such as services supported by each service provider, service costs, methods of billing, and a relationship between the visited network provider and the user's home network, thereby allowing the user of the MS to make an informed selection of a WLAN service provider. The MS may then select a service provider from among the one or more service provider and inform the WLAN of the selected service provider by conveying to the WLAN an associated SSID and at least a portion of the received network identification and services information. Based on the SSID and information received from the MS, the WLAN is able to determine an appropriate AAA server 314, 318 for authenticating the MS.

While the present invention has been particularly shown and described with reference to particular embodiments thereof, it will be understood by those skilled in the art that various changes may be made and equivalents substituted for elements thereof without departing from the scope of the invention as set forth in the claims below. Accordingly, the specification and figures are to be regarded in an illustrative rather then a restrictive sense, and all such changes and substitutions are intended to be included within the scope of the present invention.

Benefits, other advantages, and solutions to problems have been described above with regard to specific embodiments. However, the benefits, advantages, solutions to problems, and any element(s) that may cause any benefit, advantage, or solution to occur or become more pronounced are not to be construed as a critical, required, or essential feature or element of any or all the claims. As used herein, the terms "comprises," "comprising," or any variation thereof, are intended to cover a non-exclusive inclusion, such that a process, method, article, or apparatus that comprises a list of elements does not include only those elements but may include other elements not expressly listed or inherent to such process, method, article, or apparatus. It is further understood that the use of relational terms, if any, such as first and second, top and bottom, and the like are used solely to distinguish one entity or action from another entity or action without necessarily requiring or implying any actual such relationship or order between such entities or actions.

What is claimed is:

1. A method for providing network service information to a user of a mobile station accessing a wireless local area network comprising:

receiving a request to authenticate the mobile station; and

in response to receiving the request, conveying network identification and service information with respect to each service provider of a plurality of service providers to the mobile station.

2. The method of claim 1, wherein the request to authenticate the mobile station and the network identification and service information are each conveyed in a medium access control layer message.

3. The method of claim 1, further comprising:

requesting authentication information; and

receiving authentication information comprising a selection of a service provider from among the plurality of service providers.

4. The method of claim 3, further comprising:

determining an Authentication, Authorization, and Accounting server based on the received authentication information; and

requesting authorization of the mobile station by the determined Authentication, Authorization, and Accounting server.

5. A method for accessing a wireless local area network comprising:

conveying a request to authenticate a mobile station;

receiving network identification and service information with respect to a service provider; and

determining whether to access the wireless local area network based on the received network identification and service information.

IPR2025-01571
Apple EX1002 Page 1028

6. The method of claim 5, wherein the request to authenticate the mobile station and the network identification and service information are each conveyed in a medium access control layer message.

7. The method of claim 5, wherein receiving network identification and service information with respect to a service provider comprises receiving network identification and service information with respect to each service provider of a plurality of service providers and wherein the method further comprises:

receiving a request for authentication information; and

conveying a selection of a service provider from among the plurality of service providers.

8. An Access Point in a wireless local area network comprising:

a memory that stores a service provider identifier and network service information in association with each service provider of a plurality of service providers; and

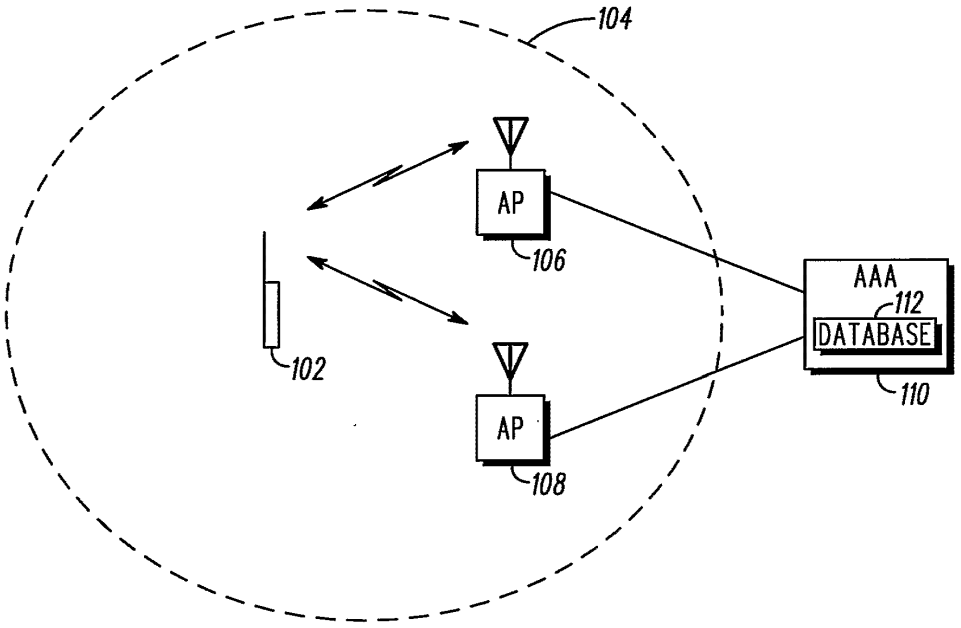
a processor coupled to the memory that assembles one or more messages comprising the service provider identifier and the network service information associated with each service provider of a plurality of service providers and conveys the one or more messages to a mobile station.

9. The Access Point of claim 8, wherein the first one or more messages comprises a first one or more messages and wherein the processor receives a request to authenticate the mobile station, in response to receiving the request, assembles the first one or more messages, and further assembles a second message comprising a request for authentication information and conveys the second message to the mobile station.

10. The Access Point of claim 9, wherein the processor further, in response to conveying the request for authentication information, receives the requested authentication information and, in response to receiving the requested authentication information, assembles a third message requesting authorization of the mobile station and conveys the third message to a server.

11. The Access Point of claim 10, wherein the memory stores, in association with the server, a service provider identifier, wherein the received authentication information comprises the service provider identifier, and wherein the processor determines the server based on the received service provider identifier.

5



100

FIG. 1
—PRIOR ART—

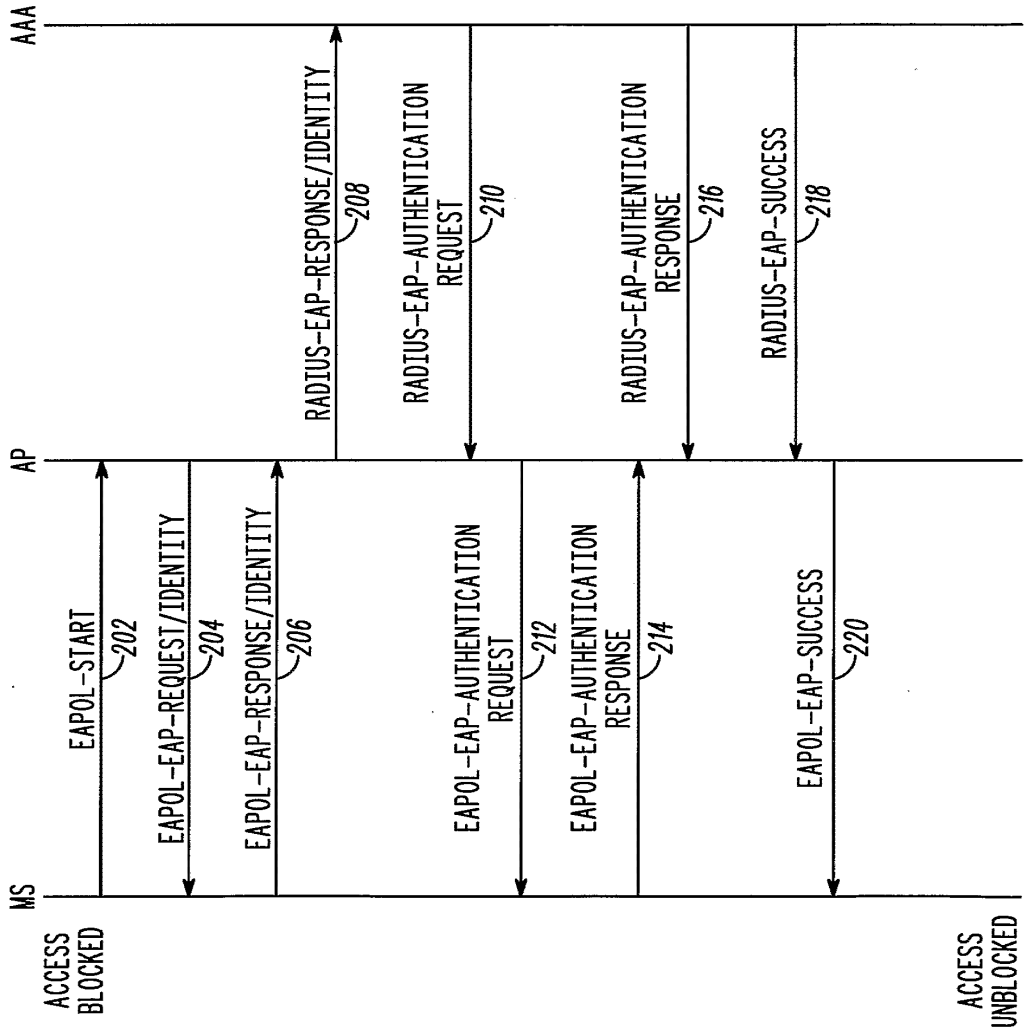


FIG. 2 200
—PRIOR ART—

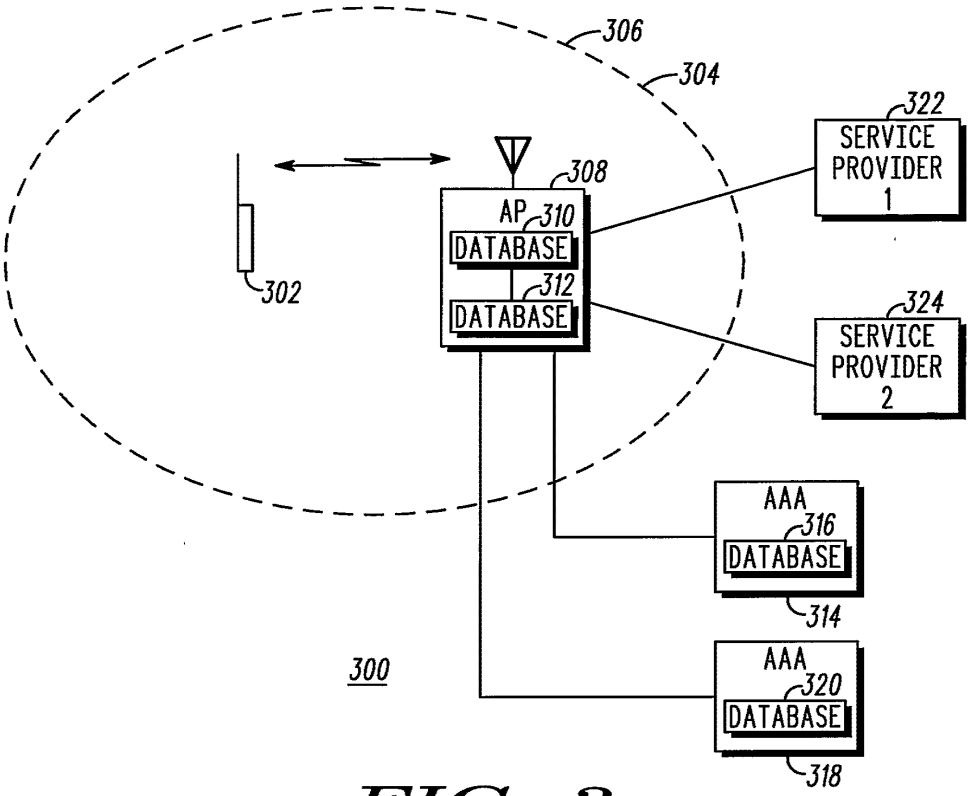

306
304
322
SERVICE PROVIDER 1
308
AP 310
DATABASE
312
DATABASE
302
324
SERVICE PROVIDER 2
AAA 316
DATABASE
314
300
AAA 320
DATABASE
318

FIG. 3

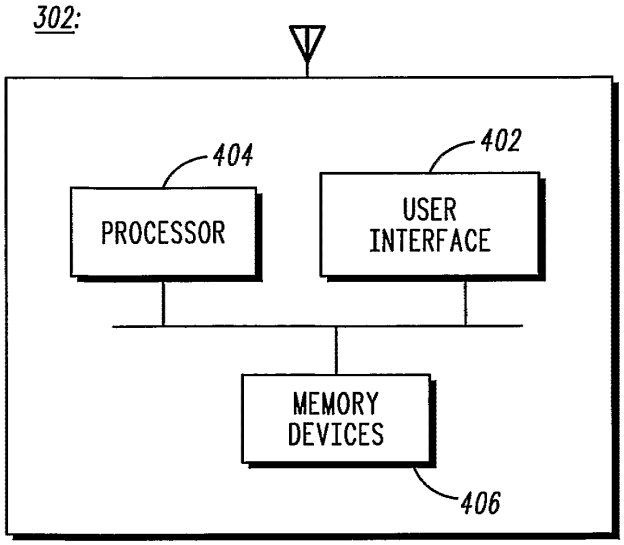
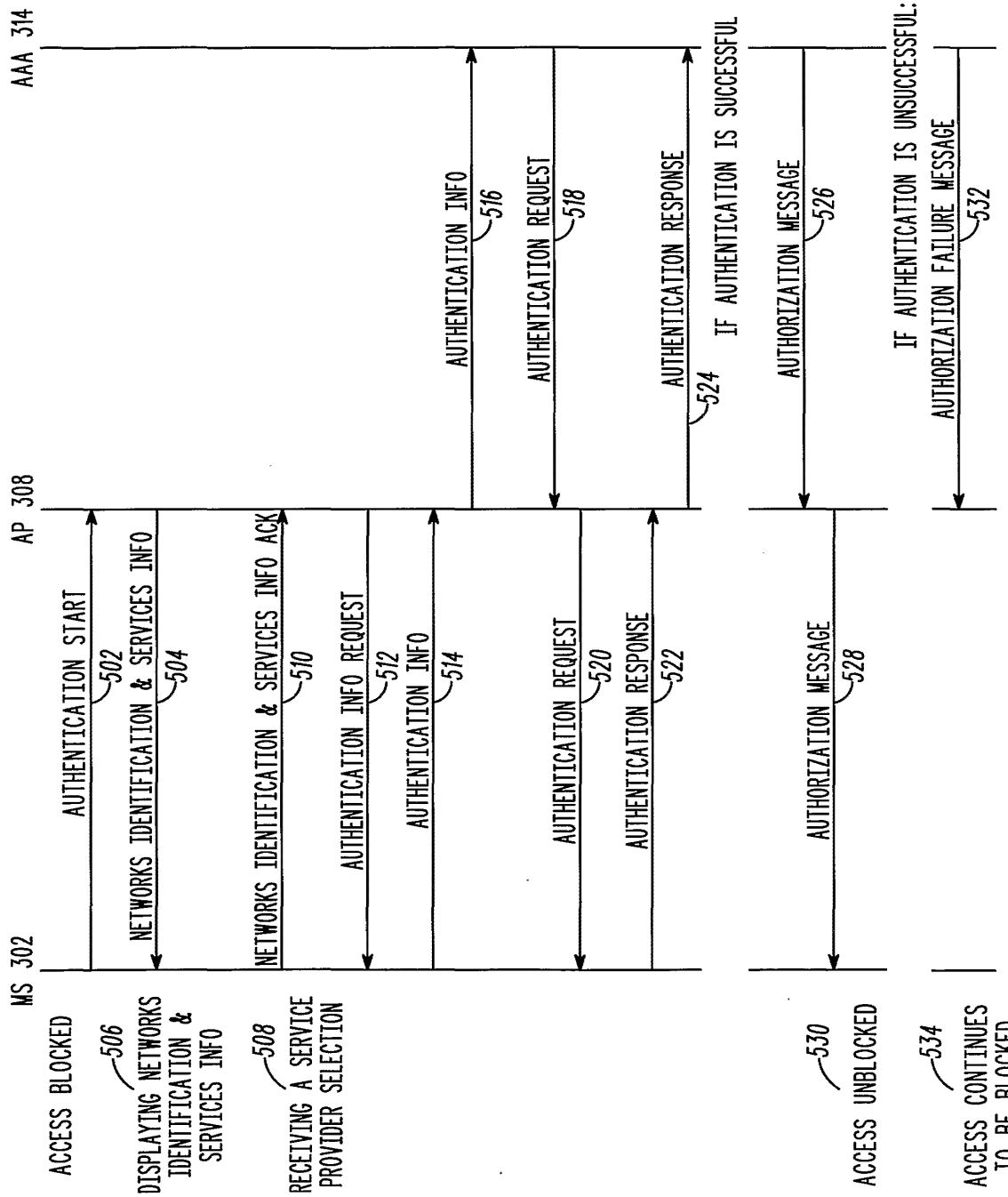

302:
404
PROCESSOR
402
USER INTERFACE
MEMORY DEVICES
406

FIG. 4


MS 302
AP 308
AAA 314
ACCESS BLOCKED
AUTHENTICATION START
502
NETWORKS IDENTIFICATION & SERVICES INFO
504
DISPLAYING NETWORKS IDENTIFICATION & SERVICES INFO
506
NETWORKS IDENTIFICATION & SERVICES INFO ACK
510
RECEIVING A SERVICE PROVIDER SELECTION
508
AUTHENTICATION INFO REQUEST
512
AUTHENTICATION INFO
514
AUTHENTICATION INFO
516
AUTHENTICATION REQUEST
518
AUTHENTICATION REQUEST
520
AUTHENTICATION RESPONSE
522
AUTHENTICATION RESPONSE
524
IF AUTHENTICATION IS SUCCESSFUL
AUTHORIZATION MESSAGE
528
ACCESS UNBLOCKED
530
AUTHORIZATION MESSAGE
526
IF AUTHENTICATION IS UNSUCCESSFUL:
AUTHORIZATION FAILURE MESSAGE
532
ACCESS CONTINUES TO BE BLOCKED
534

500 FIG. 5

Electronic Patent Application Fee Transmittal	
Application Number:	13705055
Filing Date:	04-Dec-2012
Title of Invention:	AUTOMATED DEVICE PROVISIONING AND ACTIVATION
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Filer:	Krista Susan Jacobsen/Ann Taylor
Attorney Docket Number:	RALEP007C03
Filed as Large Entity	

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
		Total in USD ($)		**180**

Electronic Acknowledgement Receipt	
EFS ID:	17502092
Application Number:	13705055
International Application Number:	
Confirmation Number:	3375
Title of Invention:	AUTOMATED DEVICE PROVISIONING AND ACTIVATION
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	Krista Susan Jacobsen/Ann Taylor
Filer Authorized By:	Krista Susan Jacobsen
Attorney Docket Number:	RALEP007C03
Receipt Date:	26-NOV-2013
Filing Date:	04-DEC-2012
Time Stamp:	01:06:39
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$180
RAM confirmation Number	13783
Deposit Account	505876
Authorized User	

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)	P007C03IDS1.pdf	373418 d2852d6de109124c92c0b3614c09d05126d793b6	no	10
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
2	Information Disclosure Statement (IDS) Form (SB08)	P007C03IDS2.pdf	347200 2c6c0bbd42dbdc01c8ab05a0d56ed372c010ae3f	no	4
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
3	Foreign Reference	2037_CN1538730A.pdf	550169 2e3e24baa9d5890cdf219fc4a3d0303062aeda8c	no	11
Warnings:					
Information:					
4	Foreign Reference	2038_CN101115248B.pdf	798834 75acfe730044fed57cd917c2eae4f33b5e7d5028	no	15
Warnings:					
Information:					
5	Foreign Reference	2039_CN101341764A.pdf	1138895 2e2dbcd7a125a434c6548925e43e263bfbdc4a20	no	25
Warnings:					
Information:					
6	Foreign Reference	2039_WO2007068288A1.pdf	216996 5471cebc5a9ee9308c5123883f1aef1064b81f4f	no	32
Warnings:					
Information:					
7	Foreign Reference	2040_CN1802839A.pdf	891159 52b2d7b964ee757bb22239fc56aa4b0e6b82ac84	no	18
Warnings:					
Information:					
8	Foreign Reference	2040_WO2004064306A2.pdf	510026 4efd4e07b8efec25946c766ec966cd4a4accab55	no	22
Warnings:					
Information:					

9	Non Patent Literature	3032_Verizon.pdf	80548 984c09646690e8def9b16a30b9eef2c953a6263d	no	2
Warnings:					
Information:					
10	Non Patent Literature	3033_ChineseLit.pdf	692944 27c80a849cc8dbc81b552f052687e58018a96512	no	2
Warnings:					
Information:					
11	Non Patent Literature	5115_P007CNOAx.pdf	325953 f778229c8658a44da3f2a4c82f999ccaadcdb961	no	11
Warnings:					
Information:					
12	Fee Worksheet (SB06)	fee-info.pdf	30272 a3358b504865a43409630da47dc1925eb63f2366	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	5956414		

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.

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 11/20/2013
Headwater Partners I LLC
350 Marine Parkway, Suite 300
Redwood Shores, CA 94065

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

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

Ann Taylor	(Depositor's name)
	(Signature)
November 26, 2013	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/705,055	12/04/2012	Gregory G. Raleigh	RALEP007C03	3375

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	$890	$0	$0	$890	02/20/2014

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

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 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 Krista S. Jacobsen
2
3

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

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

(A) NAME OF ASSIGNEE: Headwater Partners I LLC
(B) RESIDENCE: (CITY and STATE OR COUNTRY): Redwood Shores, CA

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

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

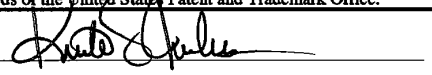
4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
☐ A check is enclosed.
☐ Payment by credit card. Form PTO-2038 is attached.
☒ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number 505876 (enclose an extra copy of this form).

IPR2025-01571
Apple EX1002 Page 1040

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

Authorized Signature  Date November 26, 2013

Typed or printed name Krista S. Jacobsen Registration No. 59374

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

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

IPR2025-01571
Apple EX1002 Page 1041

Electronic Patent Application Fee Transmittal

Application Number:	13705055
Filing Date:	04-Dec-2012
Title of Invention:	AUTOMATED DEVICE PROVISIONING AND ACTIVATION
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Filer:	Krista Susan Jacobsen/Ann Taylor
Attorney Docket Number:	RALEP007C03

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Utility Appl Issue Fee	2501	1	890	890
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
		Total in USD ($)		**890**

Electronic Acknowledgement Receipt	
EFS ID:	17516255
Application Number:	13705055
International Application Number:	
Confirmation Number:	3375
Title of Invention:	AUTOMATED DEVICE PROVISIONING AND ACTIVATION
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	Krista Susan Jacobsen/Ann Taylor
Filer Authorized By:	Krista Susan Jacobsen
Attorney Docket Number:	RALEP007C03
Receipt Date:	26-NOV-2013
Filing Date:	04-DEC-2012
Time Stamp:	21:27:55
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$890
RAM confirmation Number	11488
Deposit Account	505876
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

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

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

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

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	P007C03IssueFee.pdf	500214 e8e92e2776192e43ecfd7f58ffad51ac3a3755c1	no	2
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30433 02a063216fc6a69bcc5c617294076e82451a05aa	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	530647		

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.
13/705,055	12/04/2012	Gregory G. Raleigh	RALEP007C03	3375

106963 7590 12/13/2013

Headwater Partners I LLC
350 Marine Parkway, Suite 300
Redwood Shores, CA 94065

EXAMINER	
RUDY, ANDREW J	
ART UNIT	PAPER NUMBER
3687	

NOTIFICATION DATE	DELIVERY MODE
12/13/2013	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

IPR2025-01571
Apple EX1002 Page 1046

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.
13/705,055	04 December, 2012	RALEIGH, GREGORY G.	RALEP007C03

Headwater Partners I LLC
350 Marine Parkway, Suite 300
Redwood Shores, CA 94065

EXAMINER	
ANDREW JOSEPH RUDY	
ART UNIT	PAPER
3687	20131205

DATE MAILED:

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

Commissioner for Patents

Applicant's two Information Disclosure Statement (IDS's) submitted on November 26, 2013 have been reviewed. Note the attached IDS's.

/ANDREW JOSEPH RUDY/
Primary Examiner
Art Unit: 3687

PTO-90C (Rev.04-03)

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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Andrew J RUDY
	Attorney Docket Number	RALEP007C03

U.S.PATENTS						
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.						

U.S.PATENT APPLICATION PUBLICATIONS						
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.						

FOREIGN PATENT DOCUMENTS								
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	1802839A	CN		2006-07-12	Motorola Inc.		☐
	2	2004064306	WO		2004-07-29	Motorola Inc.		☐
If you wish to add additional Foreign Patent Document citation information please click the Add button								
NON-PATENT LITERATURE DOCUMENTS								

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Andrew J RUDY
	Attorney Docket Number	RALEP007C03

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	9/30/2013 First Office Action in Chinese Patent Application No. 201080013732.4	☐

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

EXAMINER SIGNATURE

Examiner Signature	/Andrew Joseph Rudy/	Date Considered	12/05/2013

*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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Andrew J RUDY
	Attorney Docket Number	RALEP007C03

U.S.PATENTS						
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	5983270	A	1999-11-09	Abraham et al.	
	2	6104700	A	2000-08-15	Haddock, Stephen R. et al.	
	3	6598034	B1	2003-07-22	Kloth, Axel K.	
	4	6748195	B1	2004-06-08	Phillips, W. Garland	
	5	7013469	B2	2006-03-14	Smith et al.	
	6	7032072	B1	2006-04-18	Quinn et al.	
	7	7043268	B2	2006-05-09	Yukie et al.	
	8	7113780	B2	2006-09-26	Mckenna Daniel 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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Andrew J RUDY
	Attorney Docket Number	RALEP007C03

	9	7203169	B1	2007-04-10	Okholm, Jon et al.	
	10	7286834	B2	2007-10-23	Walter	
	11	7460837	B2	2008-12-02	Diener, Neil R.	
	12	7540408	B2	2009-06-02	Levine, Judah et al.	
	13	7555757	B2	2009-06-30	Smith et al.	
	14	7580356	B1	2009-08-25	Mishra et al.	
	15	7596373	B2	2009-09-29	Mcgregor, Christopher et al.	
	16	7610396	B2	2009-10-27	Taglienti et al.	
	17	7616962	B2	2009-11-10	Oswal, Anand K. et al.	
	18	7653394	B2	2010-01-26	McMillin, Brian K.	
	19	7697540	B2	2010-04-13	Haddad et al.	

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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Andrew J RUDY
	Attorney Docket Number	RALEP007C03

	20	7742406	B1	2010-06-22	Muppala, Suresh	
	21	7774323	B2	2010-08-10	Helfman, Nadav	
	22	7826427	B2	2010-11-02	Sood et al.	
	23	7826607	B1	2010-11-02	De Carvalho Resende et al.	
	24	7953877	B2	2011-05-31	Vemula et al.	
	25	7957381	B2	2011-06-07	Clermidy et al.	
	26	7958029	B1	2011-06-07	Bobich et al.	
	27	7984511	B2	2011-07-19	Kocher Paul et al.	
	28	7987510	B2	2011-07-26	Kocher et al.	
	29	8031601	B2	2011-10-04	Feroz et al.	
	30	8130793	B2	2012-03-06	Edwards, Stephen K. 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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Andrew J RUDY
	Attorney Docket Number	RALEP007C03

	31	8166554	B2	2012-04-24	John, Pramod	
	32	8185093		2012-05-22	Jheng, Yu-Syuan et al.	
	33	8185127	B1	2012-05-22	Cai, Zheng et al.	
	34	8195163	B2	2012-06-05	Gisby, Doug et al.	
	35	8196199	B2	2012-06-05	Hrastar et al.	
	36	8204505	B2	2012-06-19	Jin et al.	
	37	8255534	B2	2012-08-28	Assadzadeh, Alireza	
	38	8296404		2012-10-23	McDysan, Dave et al.	
	39	8320244	B2	2012-11-27	Muqattash et al.	
	40	8351592	B2	2013-01-08	Freeny Jr et al.	
	41	8352360	B2	2013-01-08	De Judicibus 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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Andrew J RUDY
	Attorney Docket Number	RALEP007C03

	42	8411691	B2	2013-04-02	Aggarwal	
	43	8437734		2013-05-07	Ray, Amar N. et al.	
	44	8461958	B2	2013-06-11	Saenz et al.	
	45	8463232	B2	2013-06-11	Tuli et al.	
	46	8483694	B2	2013-07-09	Lewis et al.	
	47	8484327	B2	2013-07-09	Werner et al.	
	48	8489720	B1	2013-07-16	Morford, Michael et al.	
	49	8509082	B2	2013-08-13	Heinz, John M. et al.	
	50	8522039	B2	2013-08-27	Hyndman et al.	
	51	8526329	B2	2013-09-03	Mahany, Ronald L. et al.	
	52	8526350	B2	2013-09-03	Xue, Qi 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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Andrew J RUDY
	Attorney Docket Number	RALEP007C03

	53	8543265	B2	2013-09-24	Ekhaguere et al.	
	54	8544105	B2	2013-09-24	Mclean et al.	
	55	8561138	B2	2013-10-15	Rothman, Michael M. et al.	
	56	8571474	B2	2013-10-29	Chavez et al.	
	57	8571993	B2	2013-10-29	Kocher et al.	
	58	8583499		2013-11-12	De Judicibus, Dario et al.	

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

U.S.PATENT APPLICATION PUBLICATIONS

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	20060174035	A	2006-08-03	Tufail, Mudassir	
	2	20070025301	A	2007-02-01	Petersson et al.	
	3	20070140145	A	2007-06-21	Kumar 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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Andrew J RUDY
	Attorney Docket Number	RALEP007C03

	4	20070147324		2007-06-28	McGary, Faith	
	5	20070155365	A	2007-07-05	Kim, Sung-Jun et al.	
	6	20070168499	A	2007-07-19	Chu, Jing-Long	
	7	20080120129	A	2008-05-22	Seubert et al.	
	8	20100080202		2010-04-01	Hanson, Mark	
	9	20100131584		2010-05-27	Johnson, William J.	
	10	20110264923	A	2011-10-27	Kocher et al.	
	11	20130144789		2013-06-06	Aaltonen, Janne et al.	

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

FOREIGN PATENT DOCUMENTS

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	101115248A	CN		2008-01-30	Lenovo Beijing 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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Andrew J RUDY
	Attorney Docket Number	RALEP007C03

	2	101341764A	CN		2009-01-07	Telefonaktiebolaget LM Ericsson		☐
	3	1538730A	CN		2004-10-20	Zhongxing Communication Co., Ltd.		☐
	4	2007068288	WO		2007-06-21	Telefonaktiebolaget LM Ericsson		☐

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

NON-PATENT LITERATURE DOCUMENTS

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	"The Construction of Intelligent Residential District in Use of Cable Television Network," Shandong Science, Vol. 13, No. 2, June 2000	☐
	2	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	☐

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

EXAMINER SIGNATURE

Examiner Signature	/Andrew Joseph Rudy/	Date Considered	12/05/2013

*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./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Raleigh, Gregory G.
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP007C3

	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 ~~2012~~-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	

Change(s) applied to document,
/R.M.L./
12/4/2013

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

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/705,055	01/14/2014	8631479	RALEP007C03	3375

106963 7590 12/24/2013

Headwater Partners I LLC
350 Marine Parkway, Suite 300
Redwood Shores, CA 94065

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

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

The Patent Term Adjustment is 0 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Gregory G. Raleigh, Woodside, CA;
HEADWATER PARTNERS I LLC, Redwood Shores, CA

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

Doc code: RCEX
Doc description: Request for Continued Examination (RCE)

PTO/SB/30EFS (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL
(Submitted Only via EFS-Web)

Application Number	13705055	Filing Date	2012-12-04	Docket Number (if applicable)	RALEP007C03	Art Unit	3687
First Named Inventor	Gregory G. Raleigh			Examiner Name	Rudy, Andrew J.		

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV

SUBMISSION REQUIRED UNDER 37 CFR 1.114

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

☐ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

- ☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____
- ☐ Other _____

☒ Enclosed

- ☐ Amendment/Reply
- ☒ Information Disclosure Statement (IDS)
- ☐ Affidavit(s)/ Declaration(s)
- ☒ Other 1. Certification & Request for Consideration of an IDS Filed After Payment of the Issue Fee Under the QPIDS Program (2); 2. Petition to Withdraw an Application from Issue After Payment of Issue Fee Under 37 CFR 1.313(c)

MISCELLANEOUS

☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months _____ (Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

☐ Other _____

FEES

☒ **The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.**
The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to Deposit Account No 505876

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

☒ Patent Practitioner Signature

☐ Applicant Signature

IPR2025-01571
Apple EX1002 Page 1060

PTO/SB/30EFS (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Signature of Registered U.S. Patent Practitioner			
Signature	/Krista S. Jacobsen/	Date (YYYY-MM-DD)	2014-01-09
Name	Krista S. Jacobsen	Registration Number	59374

This collection of information is required by 37 CFR 1.114. 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.

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 the Freedom of Information Act requires disclosure of these records.

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

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

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

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

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

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

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

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

IPR2025-01571
Apple EX1002 Page 1062

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	13705055
Filing Date	2012-12-04
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Andrew J RUDY
Attorney Docket Number	RALEP007C03

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	5774532	A	1998-06-30	Gottlieb 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	20060156398	A	2006-07-13	Ross et al.	
	2	20060173959	A	2006-08-03	Mckelvie et al.	
	3	20070033194	A	2007-02-08	Srinivas et al.	
	4	20080201266	A	2008-08-21	Chua et al.	
	5	20100284327	A	2010-11-11	Miklos, Gyorgy	

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

FOREIGN PATENT DOCUMENTS Remove

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Andrew J RUDY
	Attorney Docket Number	RALEP007C03

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	"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	☐

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.

IPR2025-01571
Apple EX1002 Page 1064

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	13705055
	Filing Date	2012-12-04
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Andrew J RUDY
	Attorney Docket Number	RALEP007C03

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	/Krista S. Jacobsen/	Date (YYYY-MM-DD)	2014-01-09
Name/Print	Krista S. Jacobsen	Registration Number	59374

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.

IPR2025-01571
Apple EX1002 Page 1066

Doc Code: TRAN.LET

Document Description: Transmittal Letter

PTO/SB/21 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission

Application Number	13/705,055
Filing Date	December 4, 2012
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP007C03

ENCLOSURES *(Check all that apply)*

- ☑ Fee Transmittal Form
  - ☐ Fee Attached
- ☐ Amendment/Reply
  - ☐ After Final
  - ☐ Affidavits/declaration(s)
- ☐ Extension of Time Request
- ☐ Express Abandonment Request
- ☑ Information Disclosure Statement
- ☐ Certified Copy of Priority Document(s)
- ☐ Reply to Missing Parts/ Incomplete Application
  - ☐ Reply to Missing Parts under 37 CFR 1.52 or 1.53
- ☐ Drawing(s)
- ☐ Licensing-related Papers
- ☑ Petition
- ☐ Petition to Convert to a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s) _____
  - ☐ Landscape Table on CD
- ☐ After Allowance Communication to TC
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☐ Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- ☐ Proprietary Information
- ☐ Status Letter
- ☑ Other Enclosure(s) (please Identify below):
  1. Conditional Request for Continued Examination;
  2. Cert. & Req. for Consideration of an IDS Filed After Pymt. of the Issue Fee under QPIDS Program

Remarks

You are hereby authorized to charge any additional fee required or credit any overpayment to Deposit Account No. 50-5876.

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	Headwater Partners I LLC		
Signature	/Krista S. Jacobsen/		
Printed name	Krista S. Jacobsen		
Date	January 9, 2014	Reg. No.	59374

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature	/Ann Taylor/		
Typed or printed name	Ann Taylor	Date	January 9, 2014

This collection of information is required by 37 CFR 1.5. 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 and1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

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

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

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

Electronic Patent Application Fee Transmittal

Application Number:	13705055
Filing Date:	04-Dec-2012
Title of Invention:	AUTOMATED DEVICE PROVISIONING AND ACTIVATION
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Filer:	Krista Susan Jacobsen/Ann Taylor
Attorney Docket Number:	RALEP007C03

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Petition Fee-37CFR 1.17(h) (Group II)	2464	1	70	70
Request for Continued Examination	2801	1	600	600
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**670**

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

Decision Date : January 9, 2014

In re Application of :

Gregory Raleigh

DECISION ON PETITION

UNDER CFR 1.313(c)(2)

Application No : 13705055

Filed : 04-Dec-2012

Attorney Docket No : RALEP007C03

This is an electronic decision on the petition under 37 CFR 1.313(c)(2), filed January 9, 2014 , to withdraw the above-identified application from issue after payment of the issue fee.

The petition is **GRANTED.**

The above-identified application is withdrawn from issue for consideration of a submission under 37 CFR 1.114 (request for continued examination). See 37 CFR 1.313(c)(2).

Petitioner is advised that the issue fee paid in this application cannot be refunded. If, however, this application is again allowed, petitioner may request that it be applied towards the issue fee required by the new Notice of Allowance.

Telephone inquiries concerning this decision should be directed to the Patent Electronic Business Center (EBC) at 866-217-9197.

This application file is being referred to Technology Center AU 3687 for processing of the request for continuing examination under 37 CFR 1.114 .

Office of Petitions

Electronic Acknowledgement Receipt	
EFS ID:	17873791
Application Number:	13705055
International Application Number:	
Confirmation Number:	3375
Title of Invention:	AUTOMATED DEVICE PROVISIONING AND ACTIVATION
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	Krista Susan Jacobsen/Ann Taylor
Filer Authorized By:	Krista Susan Jacobsen
Attorney Docket Number:	RALEP007C03
Receipt Date:	09-JAN-2014
Filing Date:	04-DEC-2012
Time Stamp:	20:58:14
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$670
RAM confirmation Number	7900
Deposit Account	505876
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)	
Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)	
Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Petition automatically granted by EFS	petition-request.pdf	31611 eacf27be69f4ef4ff92a6c58f057d0e903cacecd	no	2
Warnings:					
Information:					
2	Request for Continued Examination (RCE)	P007C03CondRCE.pdf	697972 7109d30ece77f71938b7b8f17e5d50de9a204162	no	3
Warnings:					
Information:					
3	Quick Path Information Disclosure Statement	P007C03QPIDS.pdf	73120 68a72950c89a4b2463e730f42c917141a16db37c	no	2
Warnings:					
Information:					
4	Information Disclosure Statement (IDS) Form (SB08)	P007C03IDS.pdf	612311 042875a6bb1d1d554b2591bc1274ddbe9f7e832a	no	4
Warnings:					
Information:					
5	Transmittal Letter	P007C03Trans.pdf	265281 d92b2cbebb8435c29c7a7aef6c34aec6ad78f17a	no	2
Warnings:					
Information:					
6	Non Patent Literature	3034_Baumann.pdf	2145168 7dcd8af1ff9cab4f61cecb7522d5e0d9c220729a	no	13
Warnings:					
Information:					
7	Fee Worksheet (SB06)	fee-info.pdf	32132 8dd5cb665d3bab676681a73272463d8f4d33f908	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	3857595		

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.

Doc Code: PET.AUTO Document Description: Petition automatically granted by EFS-Web	PTO/SB/140 U.S. Patent and Trademark Office Department of Commerce

Electronic Petition Request	**PETITION TO WITHDRAW AN APPLICATION FROM ISSUE AFTER PAYMENT OF THE ISSUE FEE UNDER 37 CFR 1.313(c)**
Application Number	13705055
Filing Date	04-Dec-2012
First Named Inventor	Gregory Raleigh
Art Unit	3687
Examiner Name	ANDREW RUDY
Attorney Docket Number	RALEP007C03
Title	AUTOMATED DEVICE PROVISIONING AND ACTIVATION

An application may be withdrawn from issue for further action upon petition by the applicant. To request that the Office withdraw an application from issue, applicant must file a petition under this section including the fee set forth in § 1.17(h) and a showing of good and sufficient reasons why withdrawal of the application from issue is necessary.

APPLICANT HEREBY PETITIONS TO WITHDRAW THIS APPLICATION FROM ISSUE UNDER 37 CFR 1.313(c).

A grantable petition requires the following items:
(1) Petition fee; and
(2) One of the following reasons:
(a) Unpatentability of one or more claims, which must be accompanied by an unequivocal statement that one or more claims are unpatentable, an amendment to such claim or claims, and an explanation as to how the amendment causes such claim or claims to be patentable;
(b) Consideration of a request for continued examination in compliance with § 1.114 (for a utility or plant application only); or
(c) Express abandonment of the application. Such express abandonment may be in favor of a continuing application, but not a CPA under 37 CFR 1.53(d).

Petition Fee

◉	Small Entity
○	Micro Entity
○	Regular Undiscounted

Reason for withdrawal from issue

◯ One or more claims are unpatentable ◉ Consideration of a request for continued examination (RCE) (List of Required Documents and Fees) ◯ Applicant hereby expressly abandons the instant application (any attorney/agent signing for this reason must have power of attorney pursuant to 37 CFR 1.32(b)).
RCE request,submission, and fee. ☐ I certify, in accordance with 37 CFR 1.4(d)(4) that : The RCE request ,submission, and fee have already been filed in the above-identified application on ☒ Are attached.
THIS PORTION MUST BE COMPLETED BY THE SIGNATORY OR SIGNATORIES I certify, in accordance with 37 CFR 1.4(d)(4) that I am: ◉ An attorney or agent registered to practice before the Patent and Trademark Office who has been given power of attorney in this application. ◯ An attorney or agent registered to practice before the Patent and Trademark Office, acting in a representative capacity. ◯ A sole inventor ◯ A joint inventor; I certify that I am authorized to sign this submission on behalf of all of the inventors as evidenced by the power of attorney in the application ◯ A joint inventor; all of whom are signing this e-petition

Signature	/Krista S. Jacobsen/
Name	Krista S. Jacobsen
Registration Number	59374

Electronic Patent Application Fee Transmittal	
Application Number:	13705055
Filing Date:	04-Dec-2012
Title of Invention:	AUTOMATED DEVICE PROVISIONING AND ACTIVATION
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Filer:	Krista Susan Jacobsen/Ann Taylor
Attorney Docket Number:	RALEP007C03
Filed as Small Entity	

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
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:	17873839
Application Number:	13705055
International Application Number:	
Confirmation Number:	3375
Title of Invention:	AUTOMATED DEVICE PROVISIONING AND ACTIVATION
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	Krista Susan Jacobsen/Ann Taylor
Filer Authorized By:	Krista Susan Jacobsen
Attorney Docket Number:	RALEP007C03
Receipt Date:	09-JAN-2014
Filing Date:	04-DEC-2012
Time Stamp:	20:59:23
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	7906
Deposit Account	505876
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

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

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

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

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Fee Worksheet (SB06)	fee-info.pdf	30371 f6734ee4cf93a76175f69d8053e09731244e510e	no	2

Warnings:

Information:

Total Files Size (in bytes):	30371

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.

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE

PATENT WITHDRAWAL NOTICE

DATE WITHDRAWN	WITHDRAWAL NUMBER
1/14/2014	24037

The following application has been **WITHDRAWN** from the

1/14/2014 issue.

SERIAL NO.	PATENT NUMBER
13705055	8631479

TITLE

AUTOMATED DEVICE PROVISIONING AND ACTIVATION

NAME AND ADDRESS

GREGORY G. RALEIGH
WOODSIDE, CA

REASON FOR WITHDRAWAL

Auto-petition to withdraw - Granted.

APPROVED

/Kimberly Terrell/, Manager

Patent Publication Branch
Office of Data Management

FORM PTO-302 -- (REV. 05-2009)

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	13705055
Filing Date	2012-12-04
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Andrew J RUDY
Attorney Docket Number	RALEP007C03

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	5774532	A	1998-06-30	Gottlieb 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	20060156398	A	2006-07-13	Ross et al.	
	2	20060173959	A	2006-08-03	Mckelvie et al.	
	3	20070033194	A	2007-02-08	Srinivas et al.	
	4	20080201266	A	2008-08-21	Chua et al.	
	5	20100284327	A	2010-11-11	Miklos, Gyorgy	

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

FOREIGN PATENT 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	13705055
	Filing Date	2012-12-04
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Andrew J RUDY
	Attorney Docket Number	RALEP007C03

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	"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	☐

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	01/24/2014

*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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/705,055	12/04/2012	Gregory G. Raleigh	RALEP007C03	3375

106963 7590 01/31/2014

Headwater Partners I LLC
350 Marine Parkway, Suite 300
Redwood Shores, CA 94065

EXAMINER	
RUDY, ANDREW J	
ART UNIT	PAPER NUMBER
3687	

NOTIFICATION DATE	DELIVERY MODE
01/31/2014	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

IPR2025-01571
Apple EX1002 Page 1084

Corrected Notice of Allowability	**Application No.** 13/705,055	**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 *09 January 2014 IDS communication*.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on_____.
2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are *1-20,22,23,25-27 and 31-35*. 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 *See Continuation Sheet*.

/ANDREW JOSEPH RUDY/
Primary Examiner
Art Unit: 3687

IPR2025-01571
Apple EX1002 Page 1085

Continuation of Attachment(s) 7. Other: Applicant's Information Disclosure Statement submitted January 9, 2014 was reviewed and then forwarded to Applicant on 1/28/24 along with Office Communication associated therewith.

IPR2025-01571
Apple EX1002 Page 1086

Electronic Acknowledgement Receipt	
EFS ID:	17873791
Application Number:	13705055
International Application Number:	
Confirmation Number:	3375
Title of Invention:	AUTOMATED DEVICE PROVISIONING AND ACTIVATION
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	Krista Susan Jacobsen/Ann Taylor
Filer Authorized By:	Krista Susan Jacobsen
Attorney Docket Number:	RALEP007C03
Receipt Date:	09-JAN-2014
Filing Date:	04-DEC-2012
Time Stamp:	20:58:14
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$670
RAM confirmation Number	7900
Deposit Account	505876
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	
Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)	
Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Electronic Patent Application Fee Transmittal

Application Number:	13705055
Filing Date:	04-Dec-2012
Title of Invention:	AUTOMATED DEVICE PROVISIONING AND ACTIVATION
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Filer:	Krista Susan Jacobsen/Ann Taylor
Attorney Docket Number:	RALEP007C03

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Petition Fee-37CFR 1.17(h) (Group II)	2464	1	70	70
Request for Continued Examination	2801	1	600	600
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Adjustment date: 02/03/2014 SDIRETA1 13705055
01/10/2014 INTEFSW 00007900 505076
02 FC:2801 600.00 CR

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.
13/705,055	03/04/2014	8667571	RALEP007C03	3375

106963 7590 02/12/2014

Headwater Partners I LLC
350 Marine Parkway, Suite 300
Redwood Shores, CA 94065

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

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

The Patent Term Adjustment is 0 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Gregory G. Raleigh, Woodside, CA;
HEADWATER PARTNERS I LLC, Redwood Shores, CA

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