US008340634B2

(12) **United States Patent**
Raleigh

(10) **Patent No.: US 8,340,634 B2**
(45) **Date of Patent: Dec. 25, 2012**

(54) **ENHANCED ROAMING SERVICES AND CONVERGED CARRIER NETWORKS WITH DEVICE ASSISTED SERVICES AND A PROXY**

(75) Inventor: **Gregory G. Raleigh**, Woodside, CA (US)

(73) Assignee: **Headwater Partners I, LLC**, Redwood Shores, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 209 days.

(21) Appl. No.: **12/695,980**

(22) Filed: **Jan. 28, 2010**

(65) **Prior Publication Data**

US 2010/0197268 A1 Aug. 5, 2010

Related U.S. Application Data

(63) Continuation-in-part of application No. 12/380,780, filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/695,019, filed on Jan. 27, 2010, and a continuation-in-part of application No. 12/695,021, filed on Jan. 27, 2010.

(60) Provisional application No. 61/206,354, filed on Jan. 28, 2009, provisional application No. 61/206,944, filed on Feb. 4, 2009, provisional application No. 61/207,393, filed on Feb. 10, 2009, provisional application No. 61/207,739, filed on Feb. 13, 2009, provisional application No. 61/270,353, filed on Jul. 6, 2009.

(51) **Int. Cl.**
H04M 11/00 (2006.01)

(52) **U.S. Cl.** **455/407**; 455/432.1; 709/224

(58) **Field of Classification Search** 705/30; 455/405–408, 411, 414.1, 432.1, 469; 709/203, 709/223, 224, 229; 715/736; 726/1
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,577,100	A	11/1996	McGregor et al.	
5,594,777	A *	1/1997	Makkonen et al.	455/406
5,794,142	A	8/1998	Vanttila et al.	
5,892,900	A	4/1999	Ginter et al.	
5,903,845	A	5/1999	Buhrmann et al.	

(Continued)

FOREIGN PATENT DOCUMENTS

EP	1463238	9/2004

(Continued)

OTHER PUBLICATIONS

Author Unknown, "Data Roaming Tariffs—Transparency Measures." EUROPA—Europe's Information Society Thematic Portal website, date unknown.

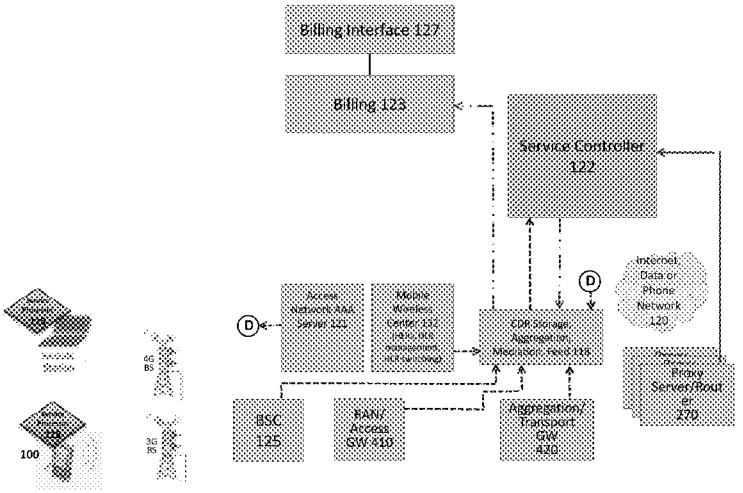
(Continued)

Primary Examiner — Andrew Joseph Rudy
(74) *Attorney, Agent, or Firm* — Krista S. Jacobsen; Sheppard, Mullin, Richter & Hampton LLP

(57) **ABSTRACT**

Enhanced roaming services and converged networks with device assisted services and a proxy is provided. In some embodiments, enhanced roaming services and converged networks with device assisted services and a proxy includes collecting device generated service usage information for one or more devices in wireless communication on the wireless network; and providing the device generated service usage information in a syntax and a communication protocol that can be used by other network devices to augment or replace network generated service usage information for the one or more devices in wireless communication on the wireless network.

57 Claims, 23 Drawing Sheets



U.S. PATENT DOCUMENTS

5,933,778	A	8/1999	Buhrmann et al.	
5,940,472	A	8/1999	Newman et al.	
6,038,452	A	3/2000	Strawczynski et al.	
6,047,268	A	4/2000	Bartoli et al.	
6,078,953	A	6/2000	Vaid et al.	
6,098,878	A	8/2000	Dent et al.	
6,141,686	A	10/2000	Jackowski et al.	
6,148,336	A	11/2000	Thomas et al.	
6,198,915	B1	3/2001	McGregor et al.	
6,226,277	B1	5/2001	Chuah	
6,263,055	B1	7/2001	Garland et al.	
6,317,584	B1	11/2001	Abu-Amara et al.	
6,418,147	B1	7/2002	Wiedeman	
6,449,479	B1	9/2002	Sanchez	
6,477,670	B1	11/2002	Ahmadvand	
6,502,131	B1	12/2002	Vaid et al.	
6,505,114	B2	1/2003	Luciani	
6,532,235	B1	3/2003	Benson et al.	
6,532,579	B2	3/2003	Sato et al.	
6,539,082	B1	3/2003	Lowe et al.	
6,563,806	B1	5/2003	Yano et al.	
6,574,321	B1	6/2003	Cox et al.	
6,574,465	B2	6/2003	Marsh et al.	
6,603,969	B1	8/2003	Vuoristo et al.	
6,606,744	B1	8/2003	Mikurak	
6,639,975	B1	10/2003	O'Neal et al.	
6,650,887	B2	11/2003	McGregor et al.	
6,651,101	B1	11/2003	Gai et al.	
6,658,254	B1	12/2003	Purdy et al.	
6,678,516	B2 *	1/2004	Nordman et al.	455/414.1
6,683,853	B1	1/2004	Carlsson et al.	
6,684,244	B1	1/2004	Goldman et al.	
6,725,031	B2	4/2004	Watler et al.	
6,763,000	B1	7/2004	Walsh	
6,765,864	B1	7/2004	Natarajan et al.	
6,785,889	B1	8/2004	Williams	
6,829,596	B1	12/2004	Frazee	
6,829,696	B1	12/2004	Balmer et al.	
6,839,340	B1	1/2005	Voit et al.	
6,920,455	B1	7/2005	Weschler	
6,922,562	B2	7/2005	Ward et al.	
6,952,428	B1	10/2005	Necka et al.	
6,965,667	B2	11/2005	Trabandt et al.	
6,967,958	B2	11/2005	Ono et al.	
6,996,076	B1	2/2006	Forbes et al.	
6,998,985	B2	2/2006	Reisman et al.	
7,002,920	B1	2/2006	Ayyagari et al.	
7,024,200	B2	4/2006	McKenna et al.	
7,027,408	B2	4/2006	Nabkel et al.	
7,042,988	B2	5/2006	Juitt et al.	
7,058,968	B2	6/2006	Rowland et al.	
7,069,248	B2	6/2006	Huber	
7,092,696	B1	8/2006	Hosain et al.	
7,113,997	B2 *	9/2006	Jayapalan et al.	709/229
7,142,876	B2	11/2006	Trossen et al.	
7,158,792	B1	1/2007	Cook et al.	
7,174,174	B2 *	2/2007	Boris et al.	455/461
7,180,855	B1	2/2007	Lin	
7,197,321	B2	3/2007	Erskine et al.	
7,212,491	B2	5/2007	Koga	
7,242,920	B2	7/2007	Morris	
7,245,901	B2	7/2007	McGregor et al.	
7,251,218	B2	7/2007	Jorgensen	
7,280,816	B2	10/2007	Fratti et al.	
7,280,818	B2	10/2007	Clayton	
7,283,561	B1	10/2007	Picher-Dempsey	
7,289,489	B1	10/2007	Kung et al.	
7,290,283	B2	10/2007	Copeland, III	
7,317,699	B2	1/2008	Godfrey et al.	
7,322,044	B2	1/2008	Hrastar	
7,324,447	B1	1/2008	Morford	
7,325,037	B2	1/2008	Lawson	
7,336,960	B2	2/2008	Zavalkovsky et al.	
7,349,695	B2	3/2008	Oommen et al.	
7,353,533	B2	4/2008	Wright et al.	
7,356,337	B2	4/2008	Florence	
7,366,497	B2	4/2008	Nagata	
7,373,136	B2	5/2008	Watler et al.	
7,388,950	B2	6/2008	Elsey et al.	
7,401,338	B1	7/2008	Bowen et al.	
7,403,763	B2	7/2008	Maes	
7,418,253	B2	8/2008	Kavanagh	
7,418,257	B2 *	8/2008	Kim	455/411
7,421,004	B2	9/2008	Feher	
7,450,591	B2	11/2008	Korling et al.	
7,450,927	B1	11/2008	Creswell et al.	
7,486,185	B2	2/2009	Culpepper et al.	
7,499,537	B2	3/2009	Elsey et al.	
7,515,608	B2	4/2009	Yuan et al.	
7,516,219	B2	4/2009	Moghaddam et al.	
7,574,731	B2	8/2009	Fascenda	
7,580,857	B2	8/2009	VanFleet et al.	
7,610,328	B2	10/2009	Haase et al.	
7,617,516	B2	11/2009	Huslak et al.	
7,620,041	B2	11/2009	Dunn et al.	
7,620,065	B2	11/2009	Falardeau	
7,620,162	B2	11/2009	Aaron et al.	
7,627,314	B2	12/2009	Carlson et al.	
7,636,574	B2 *	12/2009	Poosala	455/456.3
7,644,267	B2	1/2010	Ylikoski et al.	
7,647,047	B2	1/2010	Moghaddam et al.	
7,650,137	B2	1/2010	Jobs et al.	
7,668,176	B2	2/2010	Chuah	
7,668,903	B2	2/2010	Edwards et al.	
7,685,131	B2	3/2010	Batra et al.	
7,693,720	B2	4/2010	Kennewick et al.	
7,710,932	B2	5/2010	Muthuswamy et al.	
7,720,505	B2	5/2010	Gopi et al.	
7,734,784	B1	6/2010	Araujo et al.	
7,747,240	B1	6/2010	Briscoe et al.	
7,747,699	B2	6/2010	Prueitt et al.	
7,756,534	B2 *	7/2010	Anupam et al.	455/466
7,778,643	B2	8/2010	Laroia et al.	
7,792,538	B2	9/2010	Kozisek	
7,792,708	B2	9/2010	Alva	
7,797,204	B2 *	9/2010	Balent	705/28
7,797,401	B2	9/2010	Stewart et al.	
7,801,523	B1	9/2010	Kenderov	
7,822,837	B1	10/2010	Urban et al.	
7,848,768	B2	12/2010	Omori et al.	
7,868,778	B2	1/2011	Kenwright	
7,873,705	B2	1/2011	Kalish	
7,877,090	B2	1/2011	Maes	
7,881,199	B2	2/2011	Krstulich	
7,882,029	B2	2/2011	White	
7,886,047	B1	2/2011	Potluri	
7,890,084	B1	2/2011	Dudziak et al.	
7,890,111	B2	2/2011	Bugenhagen	
7,903,553	B2	3/2011	Liu	
7,911,975	B2	3/2011	Droz et al.	
7,912,025	B2	3/2011	Pattenden et al.	
7,929,960	B2	4/2011	Martin et al.	
7,930,553	B2 *	4/2011	Satarasinghe et al.	713/184
7,937,069	B2	5/2011	Rassam	
7,941,184	B2	5/2011	Prendergast et al.	
7,948,968	B2	5/2011	Voit et al.	
7,949,529	B2	5/2011	Weider et al.	
7,953,808	B2	5/2011	Sharp et al.	
7,957,511	B2 *	6/2011	Drudis et al.	379/201.01
7,970,426	B2	6/2011	Poe et al.	
7,975,184	B2	7/2011	Goff et al.	
7,984,130	B2	7/2011	Bogineni et al.	
7,986,935	B1	7/2011	D'Souza et al.	
8,005,459	B2	8/2011	Balsillie	
8,010,080	B1	8/2011	Thenthiruperai et al.	
8,010,081	B1	8/2011	Roskowski	
8,015,133	B1	9/2011	Wu et al.	
8,015,234	B2	9/2011	Lum et al.	
8,019,687	B2	9/2011	Wang et al.	
8,023,425	B2	9/2011	Raleigh	
8,050,275	B1	11/2011	Iyer	
8,064,896	B2	11/2011	Bell et al.	
8,095,666	B2	1/2012	Schmidt et al.	
8,099,077	B2	1/2012	Chowdhury et al.	
8,099,517	B2	1/2012	Jia et al.	
8,108,520	B2	1/2012	Ruutu et al.	
8,126,123	B2 *	2/2012	Cai et al.	379/114.03

8,135,392 B2 3/2012 Marcellino et al.
8,144,591 B2 3/2012 Ghai et al.
8,155,620 B2 * 4/2012 Wang et al. 455/405
8,160,015 B2 4/2012 Rashid et al.
8,170,553 B2 5/2012 Bennett
8,185,158 B2 5/2012 Tamura et al.
8,190,675 B2 5/2012 Tribbett
8,194,549 B2 6/2012 Huber et al.
8,194,553 B2 6/2012 Liang et al.
8,200,775 B2 6/2012 Moore
8,238,287 B1 * 8/2012 Gopi et al. 370/328
8,239,520 B2 8/2012 Grah et al.
8,244,241 B2 * 8/2012 Montemurro 455/434
8,254,915 B2 8/2012 Kozisek
8,275,830 B2 * 9/2012 Raleigh 709/203
2002/0022472 A1 2/2002 Watler et al.
2002/0120540 A1 8/2002 Kende et al.
2002/0131404 A1 9/2002 Mehta et al.
2002/0138601 A1 9/2002 Piponius et al.
2002/0176377 A1 11/2002 Hamilton
2002/0199001 A1 12/2002 Wenocur et al.
2003/0004937 A1 1/2003 Salmenkaita et al.
2003/0005112 A1 1/2003 Krautkremer
2003/0013434 A1 1/2003 Rosenberg et al.
2003/0018524 A1 1/2003 Fishman et al.
2003/0046396 A1 3/2003 Richter
2003/0050070 A1 3/2003 Mashinsky et al.
2003/0050837 A1 3/2003 Kim
2003/0088671 A1 5/2003 Klinker et al.
2003/0133408 A1 7/2003 Cheng et al.
2003/0161265 A1 8/2003 Cao et al.
2003/0182420 A1 9/2003 Jones et al.
2003/0182435 A1 9/2003 Redlich et al.
2003/0220984 A1 11/2003 Jones et al.
2003/0224781 A1 12/2003 Milford et al.
2003/0229900 A1 12/2003 Reisman
2003/0236745 A1 12/2003 Hartsell et al.
2004/0019539 A1 1/2004 Raman et al.
2004/0021697 A1 2/2004 Beaton et al.
2004/0030705 A1 2/2004 Bowman-Amuah et al.
2004/0044623 A1 3/2004 Wake et al.
2004/0047358 A1 3/2004 Chen et al.
2004/0073672 A1 4/2004 Fascenda
2004/0082346 A1 4/2004 Skytt et al.
2004/0098715 A1 5/2004 Aghera et al.
2004/0103193 A1 5/2004 Pandya et al.
2004/0107360 A1 6/2004 Herrmann et al.
2004/0127200 A1 7/2004 Shaw et al.
2004/0132427 A1 7/2004 Lee et al.
2004/0168052 A1 8/2004 Clisham et al.
2004/0198331 A1 10/2004 Coward et al.
2004/0236547 A1 11/2004 Rappaport et al.
2004/0249918 A1 12/2004 Sunshine
2005/0021995 A1 1/2005 Lal et al.
2005/0048950 A1 3/2005 Morper
2005/0055291 A1 3/2005 Bevente et al.
2005/0055309 A1 3/2005 Williams et al.
2005/0060266 A1 3/2005 DeMello et al.
2005/0097516 A1 5/2005 Donnelly et al.
2005/0107091 A1 5/2005 Vannithamby et al.
2005/0128967 A1 6/2005 Scobbie
2005/0166043 A1 7/2005 Zhang et al.
2005/0183143 A1 8/2005 Anderholm et al.
2005/0198377 A1 9/2005 Ferguson et al.
2005/0216421 A1 9/2005 Barry et al.
2005/0228985 A1 10/2005 Ylikoski et al.
2005/0238046 A1 10/2005 Hassan et al.
2005/0246282 A1 11/2005 Naslund et al.
2005/0250508 A1 11/2005 Guo et al.
2005/0254435 A1 11/2005 Moakley et al.
2005/0266825 A1 12/2005 Clayton
2005/0266880 A1 12/2005 Gupta
2006/0014519 A1 1/2006 Marsh et al.
2006/0019632 A1 1/2006 Cunningham et al.
2006/0026679 A1 2/2006 Zakas
2006/0034256 A1 2/2006 Addagatla et al.
2006/0040642 A1 2/2006 Boris et al.
2006/0045245 A1 3/2006 Aaron et al.
2006/0048223 A1 3/2006 Lee et al.
2006/0072646 A1 4/2006 Feher et al.
2006/0085543 A1 4/2006 Hrastar et al.
2006/0112016 A1 5/2006 Ishibashi
2006/0143098 A1 6/2006 Lazaridis
2006/0165060 A1 7/2006 Dua
2006/0178918 A1 8/2006 Mikurak
2006/0183462 A1 8/2006 Kolehmainen
2006/0190314 A1 8/2006 Hernandez
2006/0199608 A1 9/2006 Dunn et al.
2006/0206904 A1 9/2006 Watkins et al.
2006/0218395 A1 9/2006 Maes
2006/0233108 A1 10/2006 Krishnan
2006/0233166 A1 10/2006 Bou-Diab et al.
2006/0236095 A1 10/2006 Smith et al.
2006/0242685 A1 10/2006 Heard et al.
2006/0258341 A1 11/2006 Miller et al.
2006/0291477 A1 12/2006 Croak et al.
2007/0019670 A1 1/2007 Falardeau
2007/0022289 A1 1/2007 Alt et al.
2007/0036312 A1 2/2007 Cai et al.
2007/0055694 A1 3/2007 Ruge et al.
2007/0061243 A1 3/2007 Ramer et al.
2007/0076616 A1 4/2007 Ngo et al.
2007/0093243 A1 4/2007 Kapadekar et al.
2007/0100981 A1 5/2007 Adamczyk et al.
2007/0101426 A1 5/2007 Lee et al.
2007/0104126 A1 5/2007 Calhoun et al.
2007/0130315 A1 6/2007 Friend et al.
2007/0140113 A1 6/2007 Gemelos
2007/0140275 A1 6/2007 Bowman et al.
2007/0198656 A1 8/2007 Mazzaferri et al.
2007/0220251 A1 9/2007 Rosenberg et al.
2007/0226225 A1 9/2007 Yiu et al.
2007/0243862 A1 10/2007 Coskun et al.
2007/0248100 A1 10/2007 Zuberi et al.
2007/0254675 A1 11/2007 Zorlu Ozer et al.
2007/0255848 A1 11/2007 Sewall et al.
2007/0259673 A1 11/2007 Willars et al.
2007/0263558 A1 11/2007 Salomone
2007/0274327 A1 11/2007 Kaarela et al.
2007/0282896 A1 12/2007 Wydroug et al.
2007/0294395 A1 12/2007 Strub et al.
2007/0298764 A1 12/2007 Clayton
2008/0005285 A1 1/2008 Robinson et al.
2008/0005561 A1 1/2008 Brown et al.
2008/0010452 A1 1/2008 Holtzman et al.
2008/0039102 A1 2/2008 Sewall et al.
2008/0049630 A1 2/2008 Kozisek et al.
2008/0052387 A1 2/2008 Heinz et al.
2008/0059474 A1 3/2008 Lim
2008/0059743 A1 3/2008 Bychkov et al.
2008/0060066 A1 3/2008 Wynn et al.
2008/0062900 A1 3/2008 Rao
2008/0064367 A1 3/2008 Nath et al.
2008/0066149 A1 3/2008 Lim
2008/0066150 A1 3/2008 Lim
2008/0081606 A1 4/2008 Cole
2008/0082643 A1 4/2008 Storrie et al.
2008/0083013 A1 4/2008 Soliman et al.
2008/0095339 A1 4/2008 Elliott et al.
2008/0098062 A1 4/2008 Balia
2008/0109679 A1 5/2008 Wright et al.
2008/0120688 A1 5/2008 Qiu et al.
2008/0127304 A1 5/2008 Ginter et al.
2008/0130534 A1 6/2008 Tomioka
2008/0130656 A1 6/2008 Kim et al.
2008/0132201 A1 6/2008 Karlberg
2008/0132268 A1 6/2008 Choi-Grogan et al.
2008/0134330 A1 6/2008 Kapoor et al.
2008/0147454 A1 6/2008 Walker et al.
2008/0160958 A1 7/2008 Abichandani et al.
2008/0162637 A1 7/2008 Adamczyk et al.
2008/0162704 A1 7/2008 Poplett et al.
2008/0164304 A1 7/2008 Narasimhan et al.
2008/0167027 A1 7/2008 Gautier et al.
2008/0167033 A1 7/2008 Beckers
2008/0168523 A1 7/2008 Ansari et al.
2008/0177998 A1 7/2008 Apsangi et al.
2008/0183812 A1 7/2008 Paul et al.

2008/0184127	A1	7/2008	Rafey et al.
2008/0189760	A1	8/2008	Rosenberg et al.
2008/0207167	A1	8/2008	Bugenhagen
2008/0212470	A1	9/2008	Castaneda et al.
2008/0221951	A1	9/2008	Stanforth
2008/0222692	A1	9/2008	Andersson et al.
2008/0225748	A1	9/2008	Khemani et al.
2008/0229385	A1	9/2008	Feder et al.
2008/0229388	A1	9/2008	Maes
2008/0256593	A1	10/2008	Vinberg et al.
2008/0268813	A1	10/2008	Maes
2008/0298230	A1	12/2008	Luft et al.
2008/0305793	A1	12/2008	Gallagher et al.
2008/0311885	A1	12/2008	Dawson et al.
2008/0316923	A1	12/2008	Fedders et al.
2008/0318547	A1	12/2008	Ballou et al.
2008/0318550	A1	12/2008	Deatley
2008/0319879	A1	12/2008	Carroll et al.
2009/0005005	A1	1/2009	Forstall et al.
2009/0013157	A1	1/2009	Beaule
2009/0054030	A1	2/2009	Golds
2009/0068984	A1	3/2009	Burnett
2009/0077622	A1	3/2009	Baum et al.
2009/0079699	A1	3/2009	Sun
2009/0113514	A1	4/2009	Hu
2009/0125619	A1	5/2009	Antani
2009/0180391	A1	7/2009	Petersen et al.
2009/0197585	A1	8/2009	Aaron
2009/0248883	A1	10/2009	Suryanarayana et al.
2009/0257379	A1	10/2009	Robinson et al.
2009/0271514	A1	10/2009	Thomas et al.
2009/0286507	A1	11/2009	O'Neil et al.
2009/0287921	A1	11/2009	Zhu et al.
2009/0288140	A1	11/2009	Huber et al.
2010/0017506	A1	1/2010	Fadell
2010/0042675	A1	2/2010	Fujii
2010/0043068	A1	2/2010	Varadhan et al.
2010/0071053	A1	3/2010	Ansari et al.
2010/0082431	A1	4/2010	Ramer et al.
2010/0103820	A1	4/2010	Fuller et al.
2010/0144310	A1	6/2010	Bedingfield, Sr. et al.
2010/0188975	A1	7/2010	Raleigh
2010/0188990	A1	7/2010	Raleigh
2010/0188992	A1	7/2010	Raleigh
2010/0188994	A1	7/2010	Raleigh
2010/0191576	A1	7/2010	Raleigh
2010/0191612	A1	7/2010	Raleigh
2010/0191846	A1	7/2010	Raleigh
2010/0192170	A1	7/2010	Raleigh
2010/0192212	A1	7/2010	Raleigh
2010/0195503	A1	8/2010	Raleigh
2010/0197268	A1	8/2010	Raleigh et al.
2010/0198698	A1	8/2010	Raleigh et al.
2010/0198939	A1	8/2010	Raleigh et al.
2010/0325420	A1	12/2010	Kanekar
2011/0126141	A1	5/2011	King et al.

FOREIGN PATENT DOCUMENTS

EP	1739518		6/2005
EP	1772988	A1	4/2007
EP	1978772	A1	10/2008
WO	WO99/65185		12/1999
WO	WO 99/65185		12/1999
WO	WO 03/014891		2/2003
WO	WO 03/058880		4/2003
WO	WO 2004/028070		4/2004
WO	WO 2004/077797		9/2004
WO	WO 2004/095753		11/2004
WO	WO 2006/004467		1/2006
WO	WO 2006/050758		5/2006
WO	WO 2006/073837		7/2006
WO	WO 2006/077481		7/2006
WO	WO 2007/018363		8/2006
WO	WO 2006/130960		12/2006
WO	WO 2007/001833		1/2007
WO	WO 2007/014630		2/2007
WO	WO 2007/053848		5/2007
WO	WO 2007/069245		6/2007
WO	WO 2007/107701		9/2007
WO	WO 2008/017837		2/2008
WO	WO 2008/051379		5/2008
WO	WO 2008/066419		6/2008
WO	WO 2008/080139		7/2008
WO	WO 2008/080430		7/2008
WO	WO 2008/099802		8/2008
WO	2010088413		8/2010

OTHER PUBLICATIONS

Knight et al., Layer 2 and 3 Virtual Private Networks: Taxonomy, Technology, and Standardization Efforts, IEEE Communications Magazine, Jun. 2004.

Koutsopoulou et al., Middleware Platform for the Support of Charging Reconfiguration Actions, 2005.

Nilsson et al., A Novel MAC Scheme for Solving the QoS Parameter Adjustment Poblem in IEEE802.11e EDCA, Feb. 2006.

Author Unknown, Overview of GSM, GPRS, and UMTS, Chapter 2, Nov. 4, 2008.

Chaouchi et al., Policy Based Networking in the Integration Effort of 4G Networks and Services, 2004 IEEE.

Zhu et al., A Survey of Quality of Service in IEEE 802.11 Networks, IEEE Wireless Communications, Aug. 2004.

Kyriakakos et al., Ubiquitous Service Provision in Next Generation Mobile Networks, Proceedings of the 13th IST Mobile and Wireless Communications Summit, Lyon, France, Jun. 2004.

Farooq et al., An IEEE 802.16 WiMax Module for the NS-3 Simulator, Mar. 2-6, 2009.

Author Unknown, HP, IP Multimedia Services Charging, A White Paper from HP, Jan. 2006.

Author Unknown, Kindle™ User's Guide 3rd Edition, Copyright 2004-2009.

Hartmann et al., Agent-Based Banking Transactions & Information Retrieval-What about Performance Issues? 1999.

Van Eijk, et al., GigaMobile, Agent Technology for Designing Personalized Mobile Service Brokerage, Jul. 1, 2002.

Yu Li, Dedicated E-Reading Devices: The State of the Art and Challenges, Scroll, vol. 1, No. 1, 2008.

Dikaiakos et al., A Distributed Middleware Infrastructure for Personalized Services, Nov. 24, 2003.

Rao et al., Evolution of Mobile Location-Based Services, Communication of the ACM, Dec. 2003.

Chandrasekhar et al., Femtocell Networks: A Survey, Jun. 28, 2008.

Hossain et al., Gain-Based Selection of Ambient Media Services in Pervasive Environments, 2008.

Author Unknown, 3GPP TS 23.203, V8.4.0, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Policy and Charging Control Architecture (Release 8), Dec. 2008.

Author Unknown, 3GPP TS 23.401, V8.4.0, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packer Radio Service (GPRS) Enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) Access (Release 8), Dec. 2008.

Stephan Steglich, I-Centric User Interaction, Nov. 21, 2003.

Han et al., Information Collection Services for Qos-Aware Mobile Applications, 2005.

Alonistioti et al., Intelligent Architectures Enabling Flexible Service Provision and Adaptability, 2002.

Rolf Oppliger, Internet Security: Firewalls and Bey, Communications of the ACM, May 1997, vol. 40. No. 5.

International Search Report and Written Opinion mailed Mar. 31, 2010 from International Serial No. PCT/US2010/022438 filed Jan. 28, 2010.

* cited by examiner

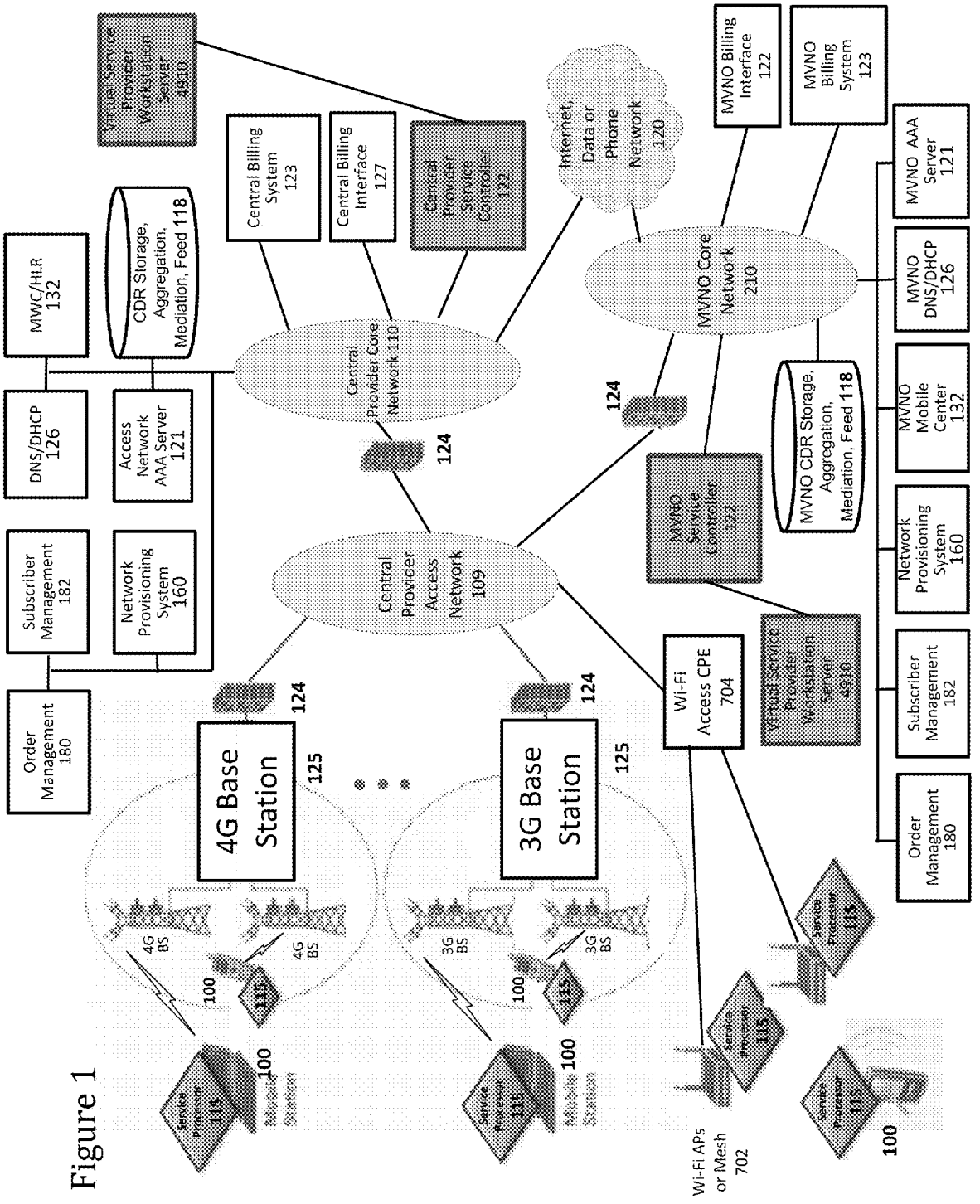

Virtual Service Provider Workstation Server 4910
Central Billing System 123
Central Billing Interface 127
Central Provider Service Controller 122
Internet, Data or Phone Network 120
MVNO Billing Interface 122
MVNO Billing System 123
MVNO AAA Server 121
MVNO DNS/DHCP 126
MVNO Mobile Center 132
Network Provisioning System 160
Subscriber Management 182
Order Management 180
MWC/HLR 132
CDR Storage, Aggregation, Mediation, Feed 118
DNS/DHCP 126
Access Network AAA Server 121
Subscriber Management 182
Network Provisioning System 160
Order Management 180
Central Provider Core Network 110
Central Provider Access Network 109
MVNO Core Network 210
MVNO Service Controller 122
MVNO CDR Storage, Aggregation, Mediation, Feed 118
Wi-Fi Access CPE 704
Virtual Service Provider Workstation Server 4910
124
4G Base Station
125
3G Base Station
4G BS
3G BS
100
115
Service Processor
Mobile Station
Wi-Fi APs or Mesh 702

Figure 1

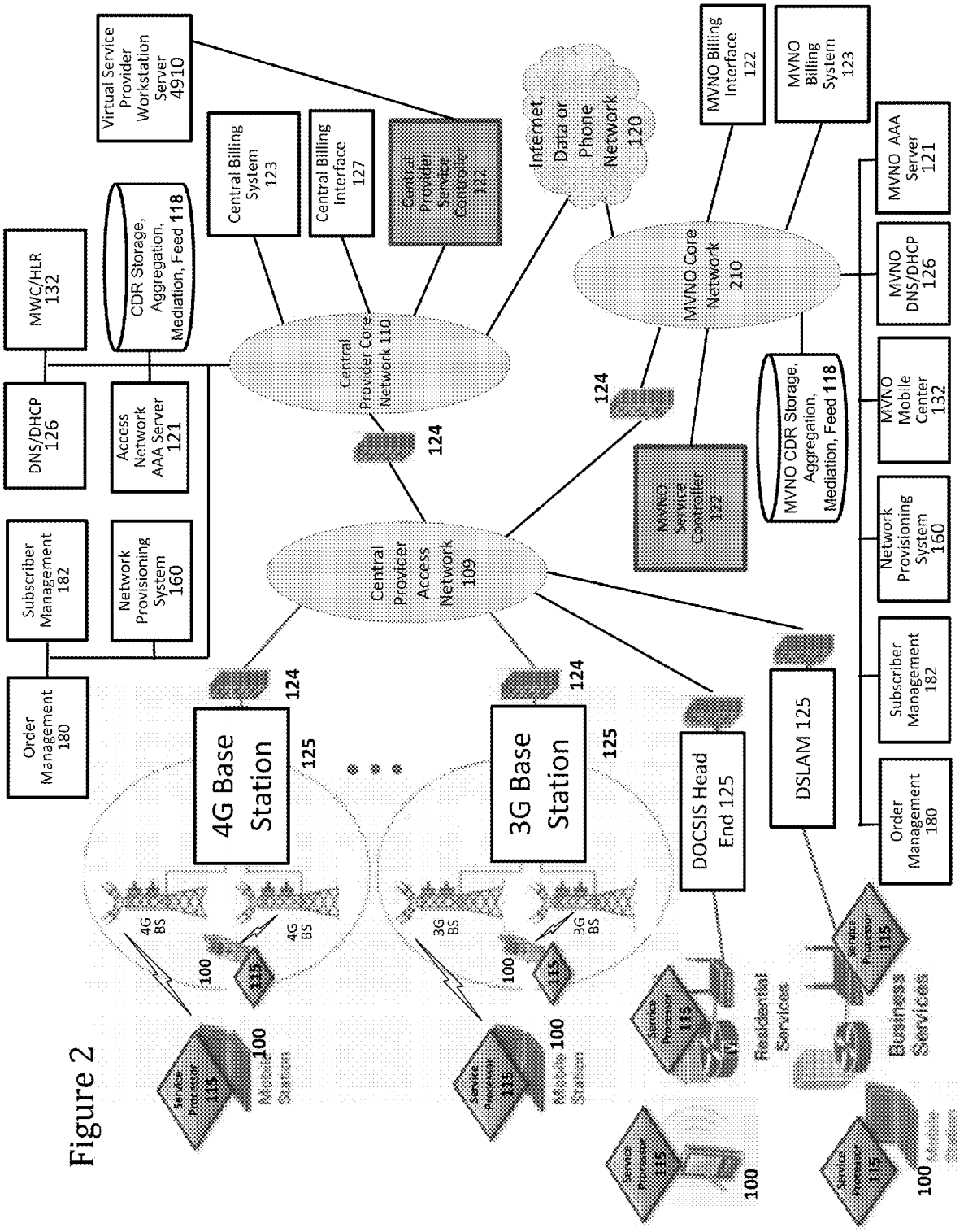

Virtual Service Provider Workstation Server 4910
Central Billing System 123
Central Billing Interface 127
Central Provider Service Controller 122
Internet, Data or Phone Network 120
MVNO Billing Interface 122
MVNO Billing System 123
MVNO AAA Server 121
MVNO DNS/DHCP 126
MVNO Mobile Center 132
Network Provisioning System 160
Subscriber Management 182
Order Management 180
MWC/HLR 132
CDR Storage, Aggregation, Mediation, Feed 118
DNS/DHCP 126
Access Network AAA Server 121
Subscriber Management 182
Network Provisioning System 160
Order Management 180
Central Provider Core Network 110
Central Provider Access Network 109
MVNO Core Network 210
MVNO Service Controller 122
MVNO CDR Storage, Aggregation, Mediation, Feed 118
124
4G Base Station
125
3G Base Station
DOCSIS Head End 125
DSLAM 125
4G BS
3G BS
100
115
Service Provider
Mobile Station
Residential Services
Business Services

Figure 2

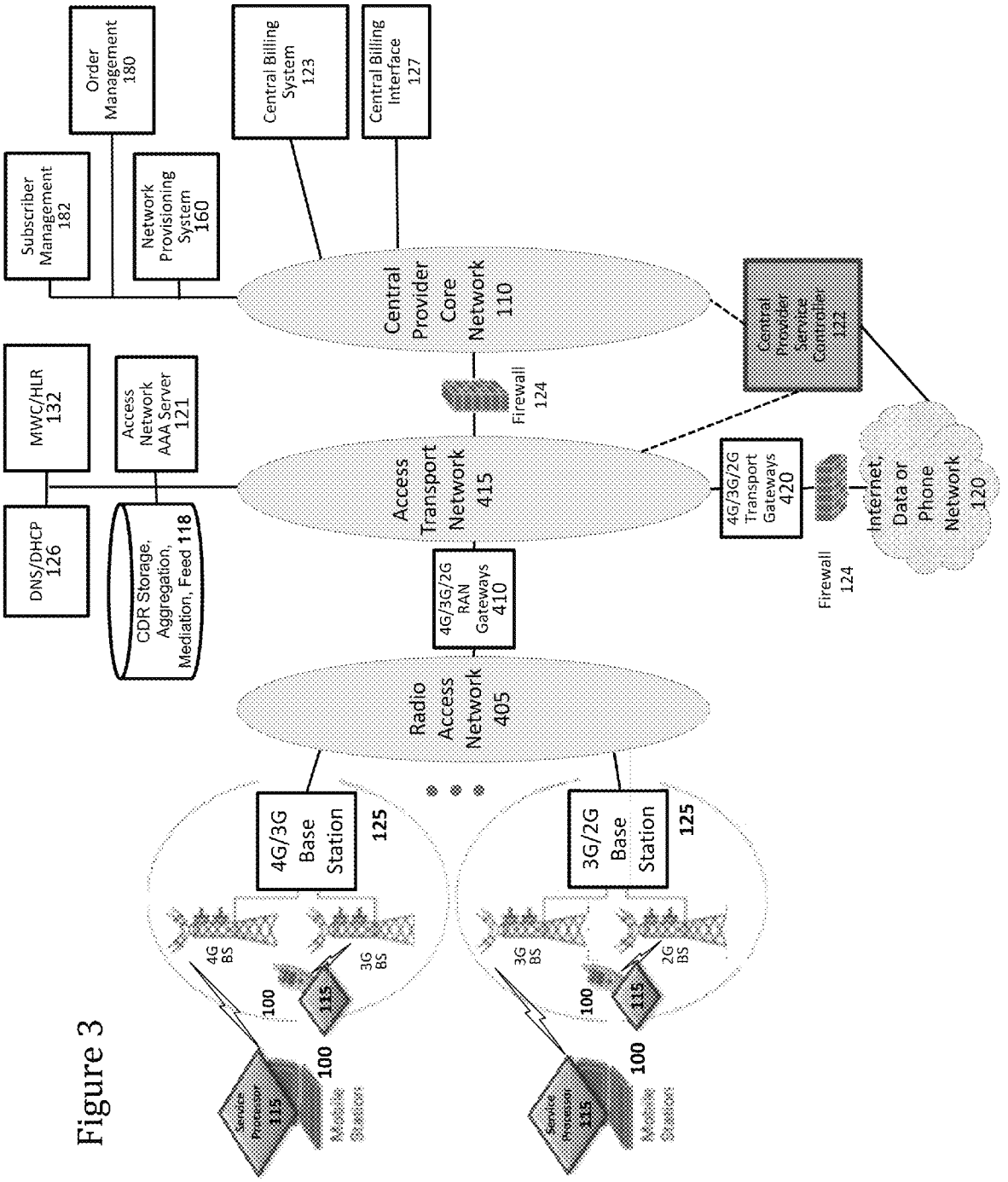
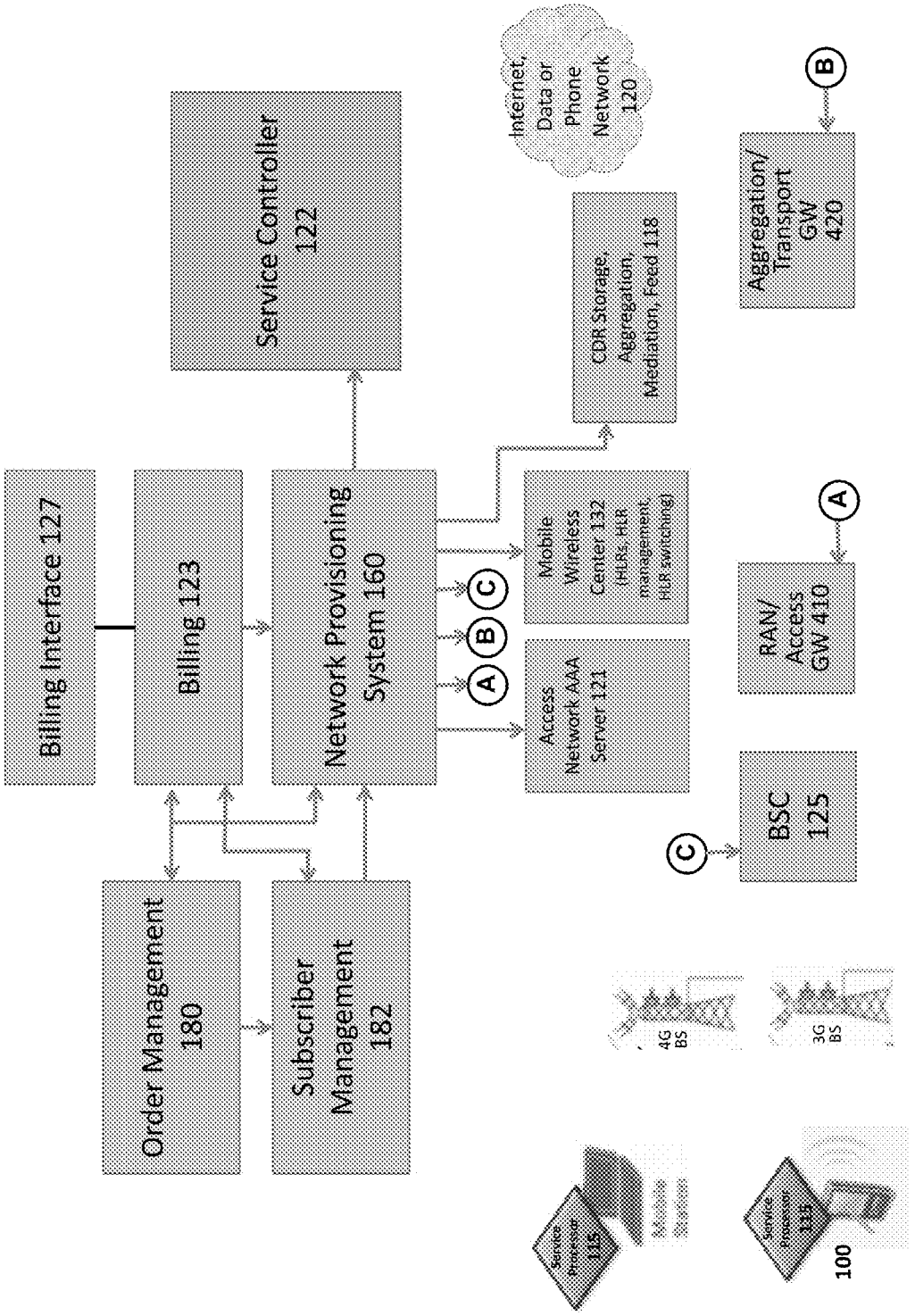

Order Management 180
Central Billing System 123
Central Billing Interface 127
Subscriber Management 182
Network Provisioning System 160
Central Provider Core Network 110
Central Provider Service Controller 122
MWC/HLR 132
Access Network AAA Server 121
Firewall 124
DNS/DHCP 126
CDR Storage, Aggregation, Mediation, Feed 118
Access Transport Network 415
4G/3G/2G Transport Gateways 420
Internet, Data or Phone Network 120
Firewall 124
4G/3G/2G RAN Gateways 410
Radio Access Network 405
4G/3G Base Station 125
3G/2G Base Station 125
4G BS
3G BS
3G BS
2G BS
100
115
Service Provider 115
Mobile Station 100

Figure 3

Figure 4


Billing Interface 127
Billing 123
Order Management 180
Subscriber Management 182
Network Provisioning System 160
Service Controller 122
Access Network AAA Server 121
Mobile Wireless Center 132 (HLRs, HLR management, HLR switching)
CDR Storage, Aggregation, Mediation, Feed 118
Internet, Data or Phone Network 120
BSC 125
RAN/ Access GW 410
Aggregation/ Transport GW 420
A
B
C
4G BS
3G BS
Service Provider 115
Service Provider 113
100

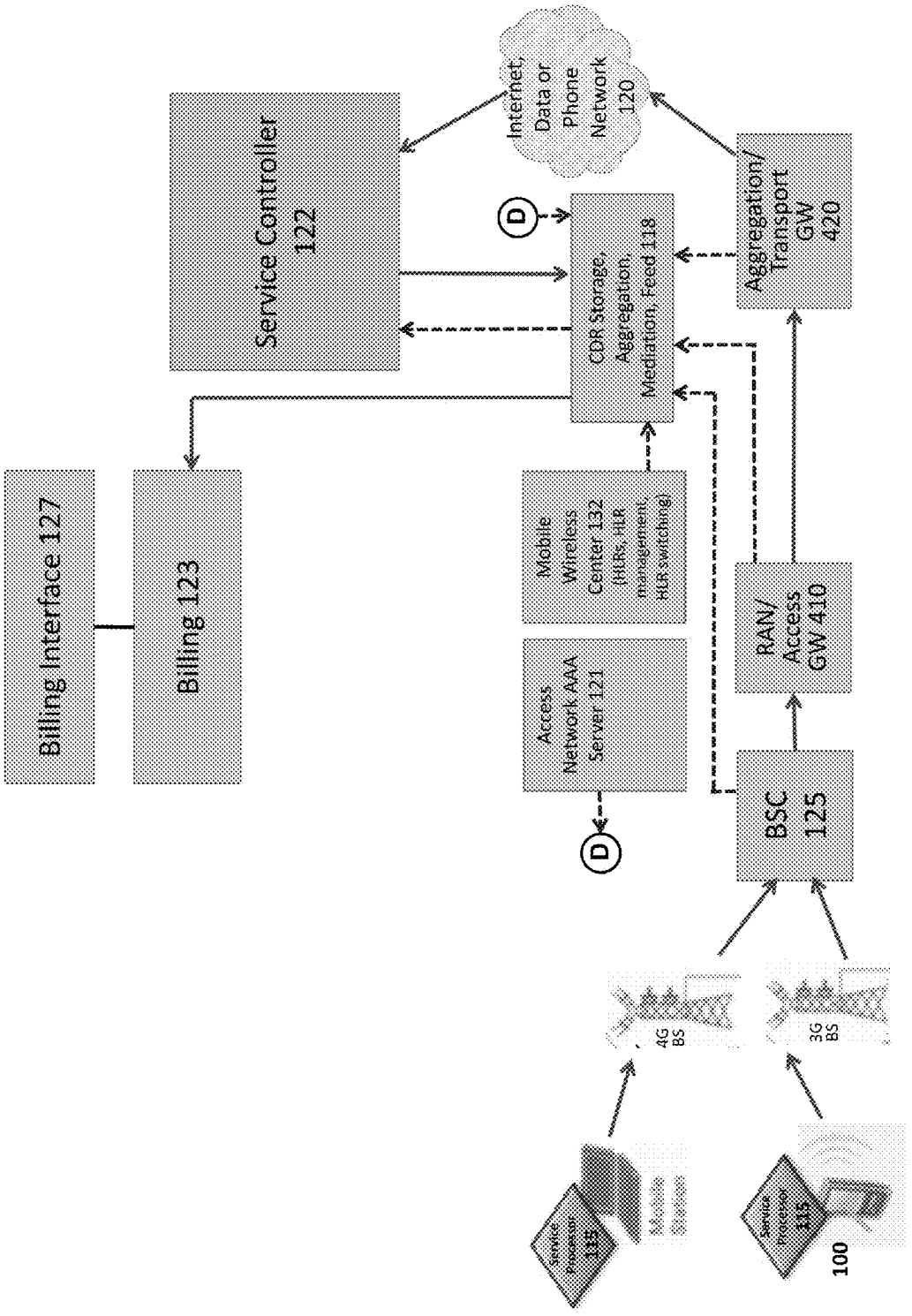

Service Controller 122
Internet, Data or Phone Network 120
D
CDR Storage, Aggregation, Mediation, Feed 118
Aggregation/ Transport GW 420
Billing Interface 127
Billing 123
Mobile Wireless Center 132 (HLRs, HLR management, HLR switching)
Access Network AAA Server 121
D
RAN/ Access GW 410
BSC 125
4G BS
3G BS
Service Processor 115
Service Processor 115
100

Figure 5

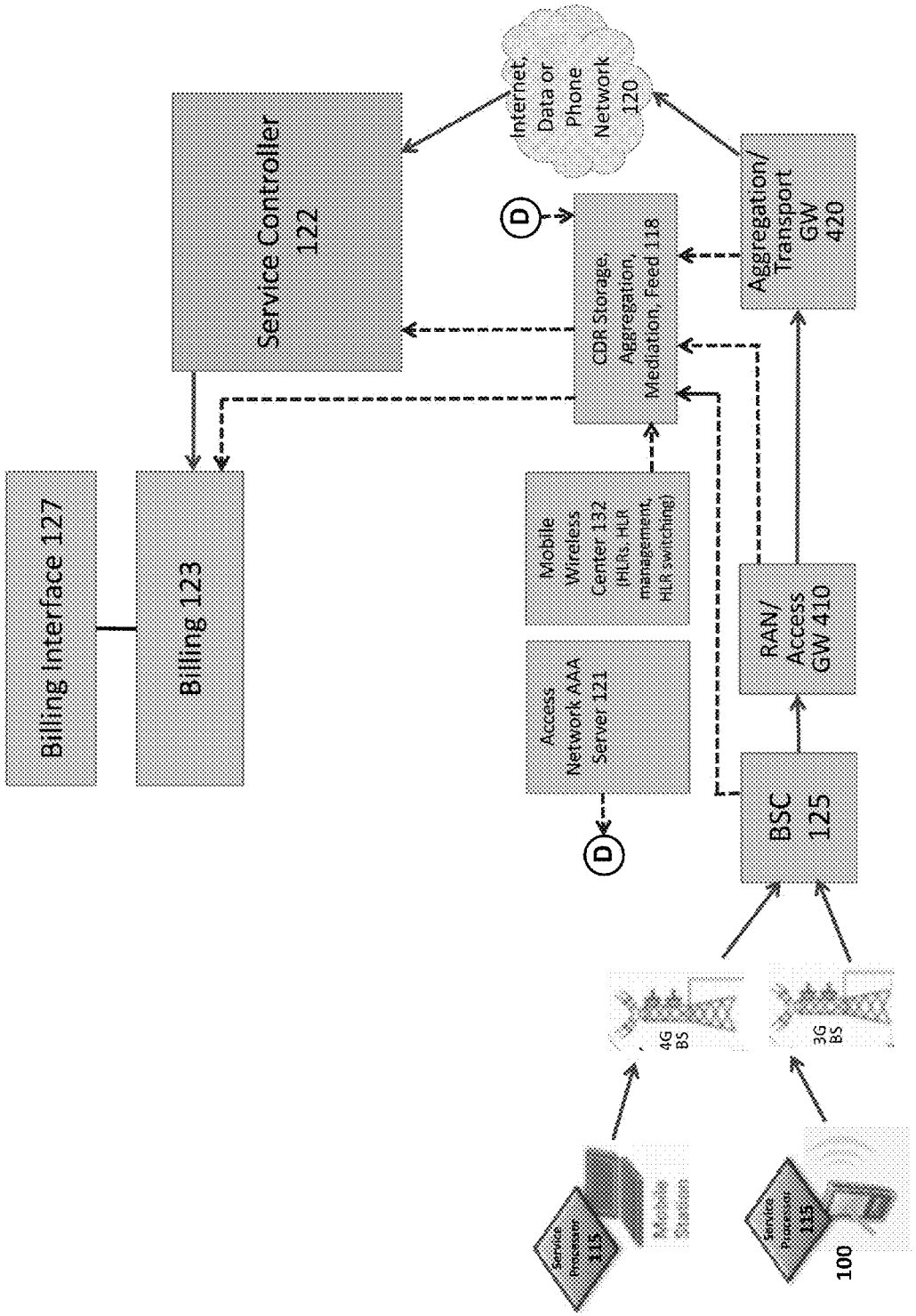

Billing Interface 127
Billing 123
Service Controller 122
Internet, Data or Phone Network 120
D
CDR Storage, Aggregation, Mediation, Feed 118
Aggregation/ Transport GW 420
Mobile Wireless Center 132 (HLRs, HLR management, HLR switching)
Access Network AAA Server 121
D
RAN/ Access GW 410
BSC 125
4G BS
3G BS
Service Processor 115
Service Processor 115
100

Figure 6

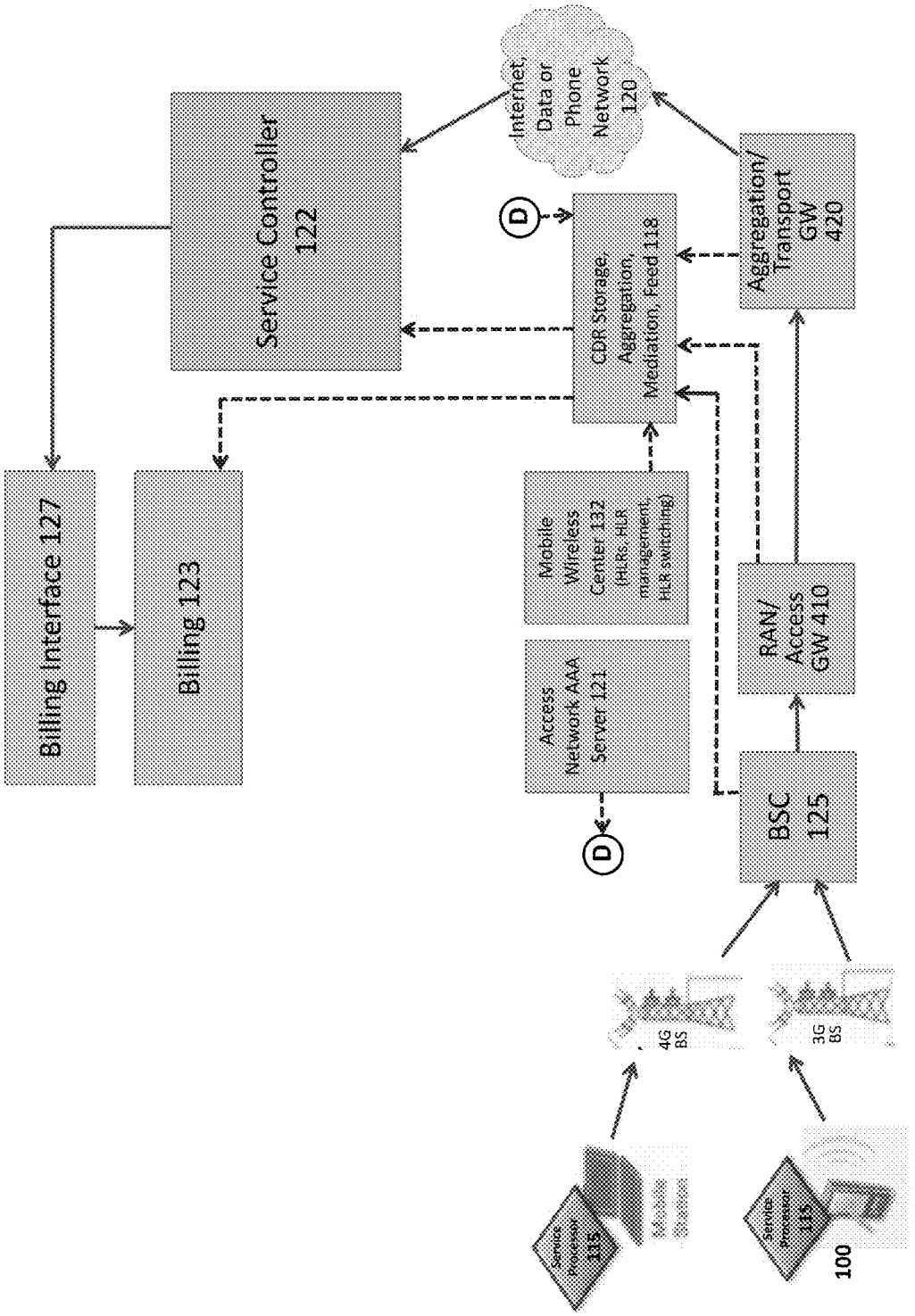

Service Controller 122
Internet, Data or Phone Network 120
Billing Interface 127
Billing 123
CDR Storage, Aggregation, Mediation, Feed 118
Aggregation/ Transport GW 420
Mobile Wireless Center 132 (HLRs, HLR management, HLR switching)
Access Network AAA Server 121
RAN/ Access GW 410
BSC 125
D
D
4G BS
3G BS
Service Processor 115
Service Processor 115
100

Figure 7

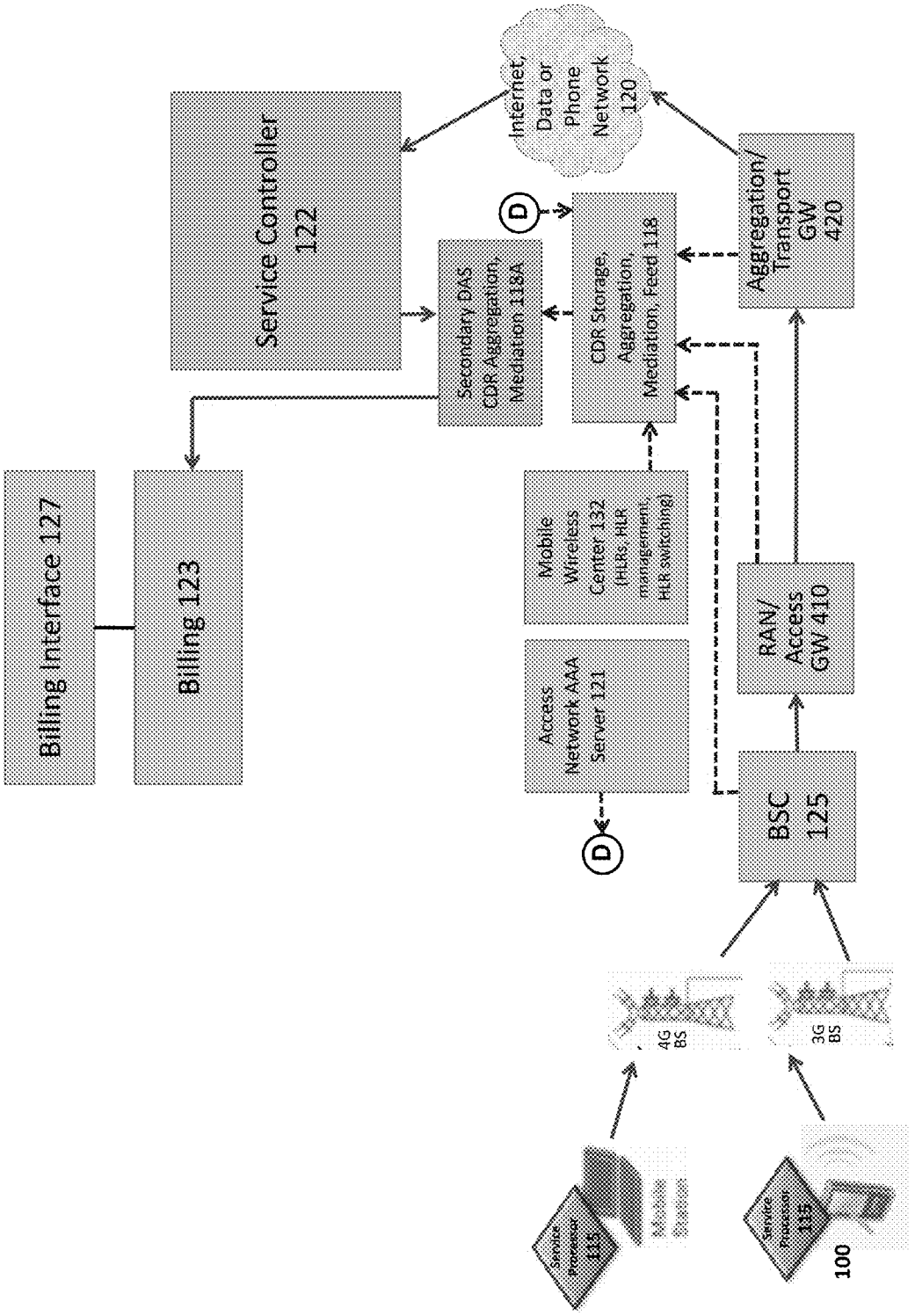

Billing Interface 127
Billing 123
Service Controller 122
Internet, Data or Phone Network 120
Secondary DAS CDR Aggregation, Mediation 118A
D
CDR Storage, Aggregation, Mediation, Feed 118
Aggregation/ Transport GW 420
Mobile Wireless Center 132 (HLRs, HLR management, HLR switching)
RAN/ Access GW 410
Access Network AAA Server 121
D
BSC 125
4G BS
3G BS
Service Provider 115
Service Provider 115
100

Figure 8

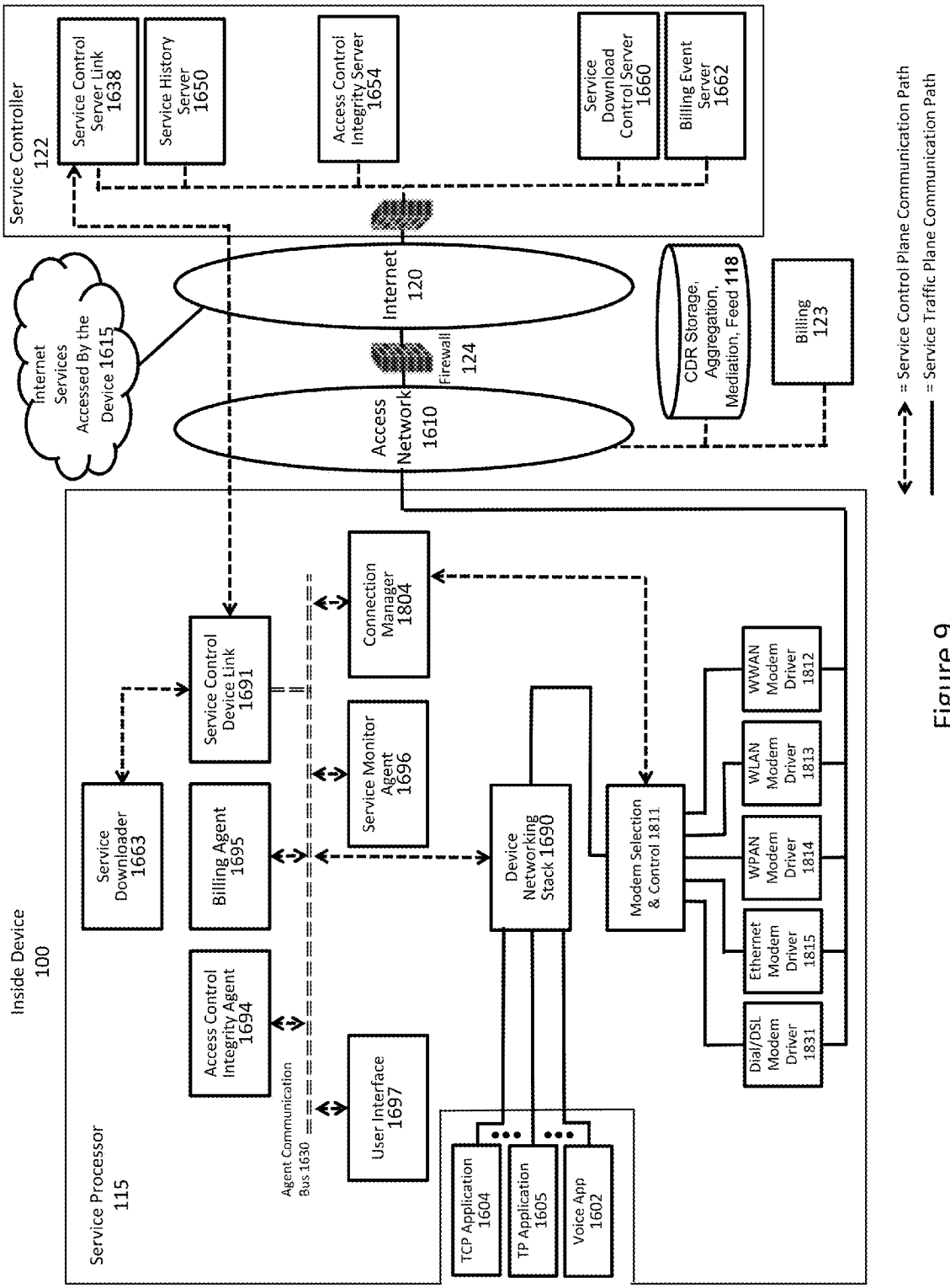

Service Controller 122
Service Control Server Link 1638
Service History Server 1650
Access Control Integrity Server 1654
Service Download Control Server 1660
Billing Event Server 1662
Internet Services Accessed By the Device 1615
Internet 120
Firewall 124
Access Network 1610
CDR Storage, Aggregation, Mediation, Feed 118
Billing 123
= Service Control Plane Communication Path
= Service Traffic Plane Communication Path
Inside Device 100
Service Processor 115
Service Downloader 1663
Billing Agent 1695
Access Control Integrity Agent 1694
Service Control Device Link 1691
Service Monitor Agent 1696
User Interface 1697
Connection Manager 1804
Agent Communication Bus 1630
Device Networking Stack 1690
Modem Selection & Control 1811
TCP Application 1604
TP Application 1605
Voice App 1602
WWAN Modem Driver 1812
WLAN Modem Driver 1813
WPAN Modem Driver 1814
Ethernet Modem Driver 1815
Dial/DSL Modem Driver 1831

Figure 9

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.
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.
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.
User Interface 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.

Figure 10

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.
Service History Server 118	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 123	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.
Service Download Control Server 1660	Provides a download function to install or update service software elements on the device.

Figure 11

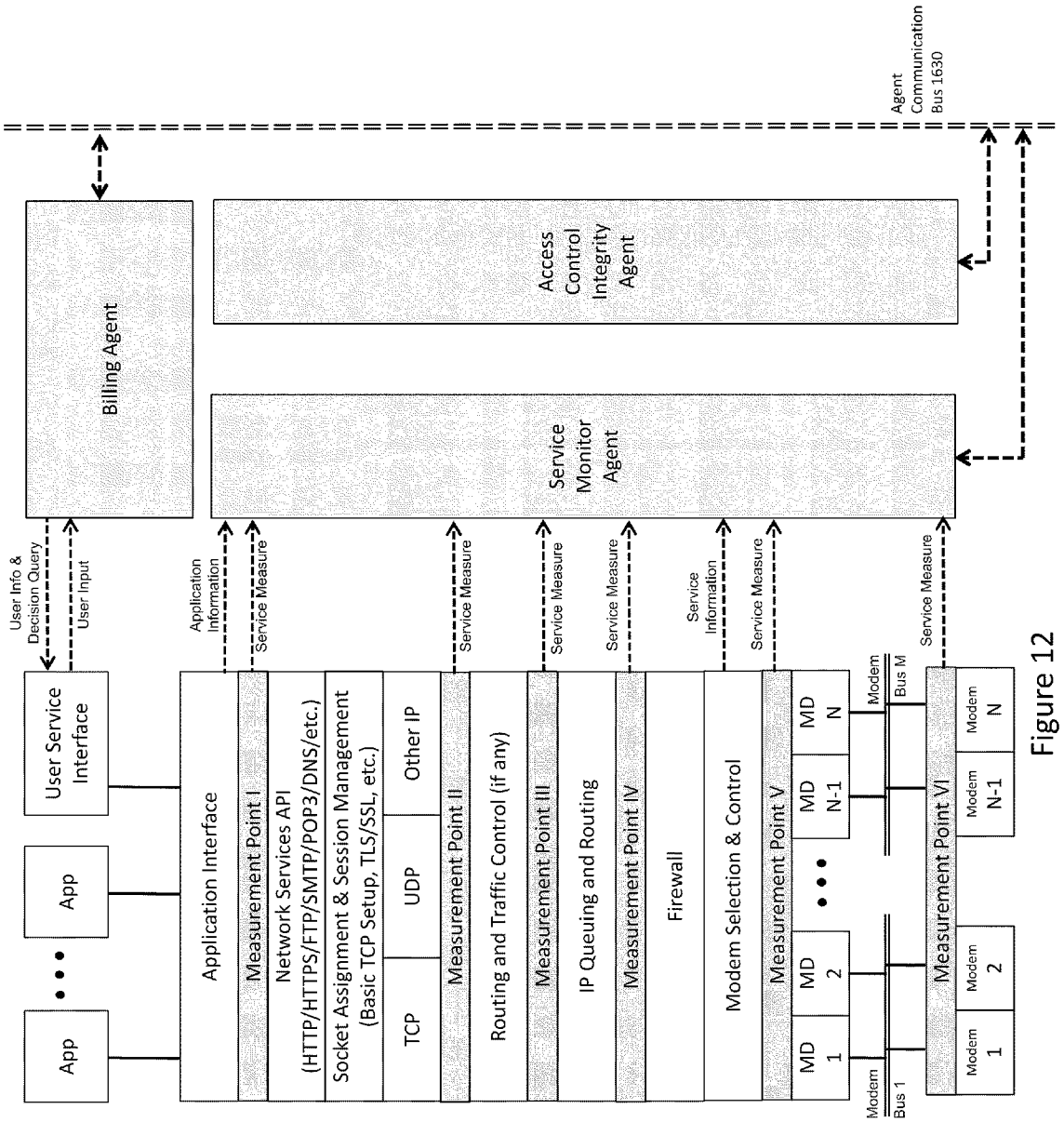

Agent Communication Bus 1630
Billing Agent
Access Control Integrity Agent
Service Monitor Agent
User Info & Decision Query
User Input
Application Information
Service Measure
Service Measure
Service Measure
Service Measure
Service Information
Service Measure
Service Measure
User Service Interface
App
App
Application Interface
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
Routing and Traffic Control (if any)
Measurement Point III
IP Queuing and Routing
Measurement Point IV
Firewall
Modem Selection & Control
Measurement Point V
MD 1
MD 2
MD N-1
MD N
Modem Bus 1
Modem Bus M
Measurement Point VI
Modem 1
Modem 2
Modem N-1
Modem N

Figure 12

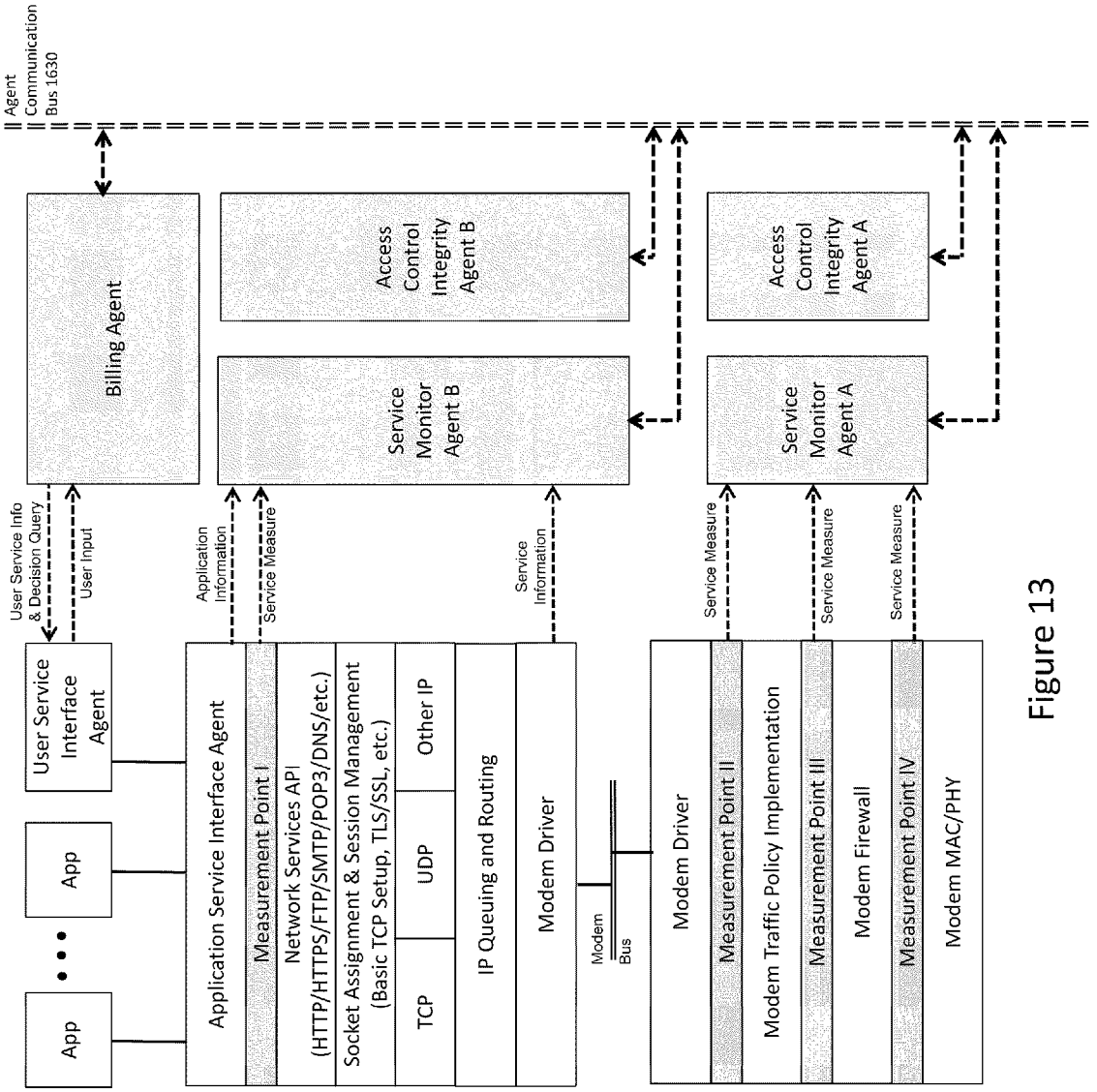

Agent Communication Bus 1630
Billing Agent
Access Control Integrity Agent B
Access Control Integrity Agent A
Service Monitor Agent B
Service Monitor Agent A
User Service Info & Decision Query
User Input
Application Information
Service Measure
Service Information
Service Measure
Service Measure
Service 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 Driver
Modem Bus
Modem Driver
Measurement Point II
Modem Traffic Policy Implementation
Measurement Point III
Modem Firewall
Measurement Point IV
Modem MAC/PHY

Figure 13

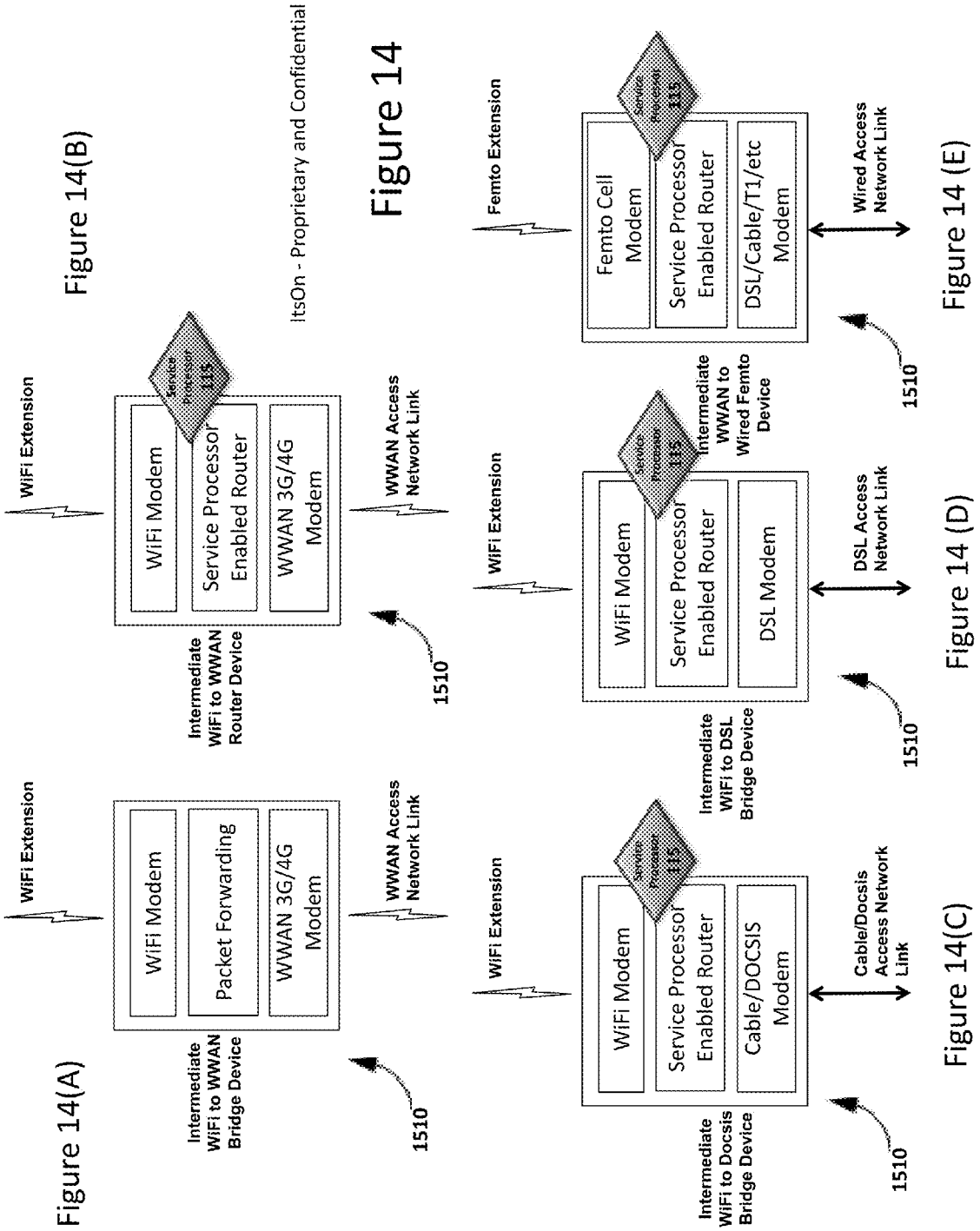


Figure 14

ItsOn - Proprietary and Confidential

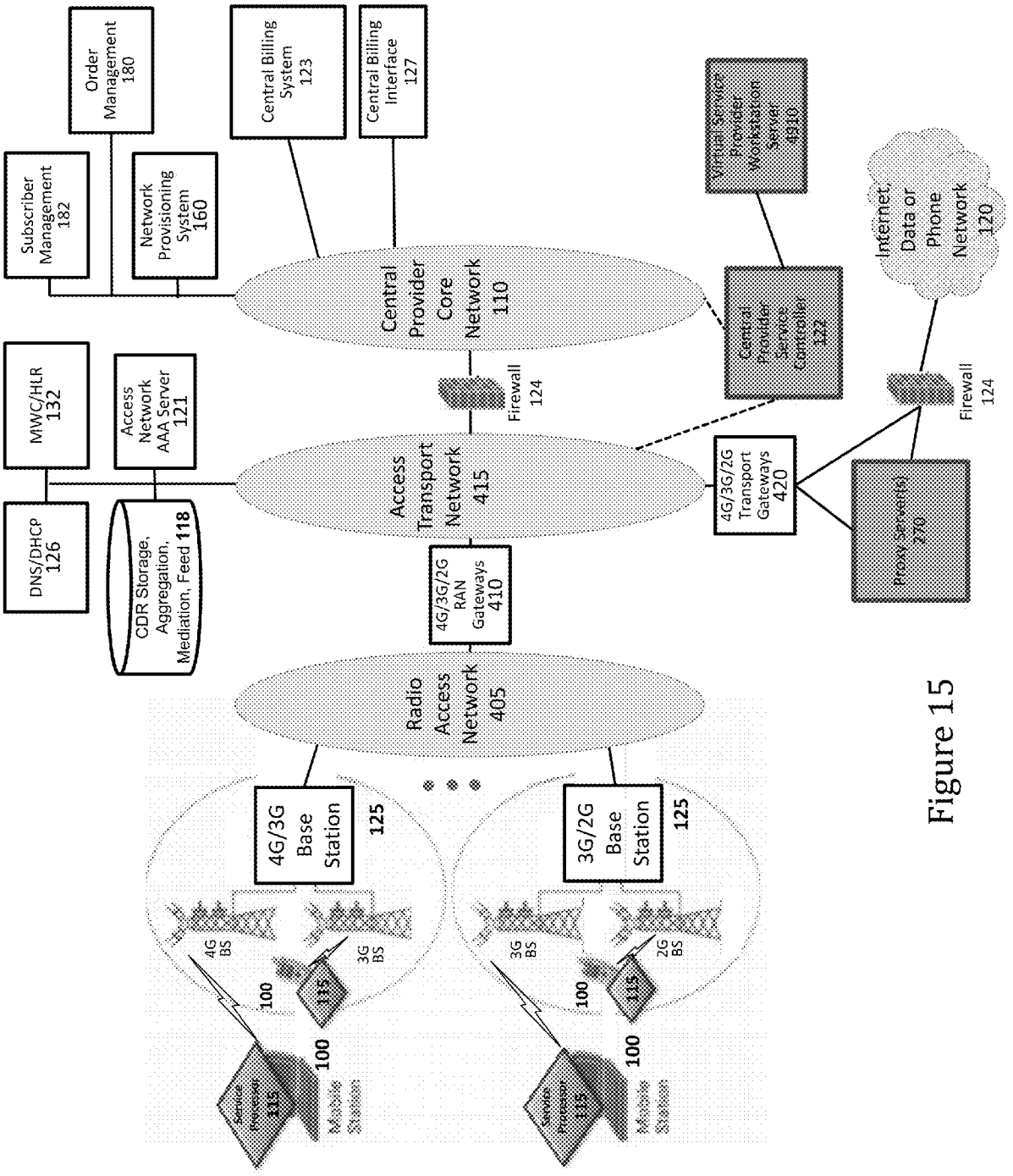

Order Management 180
Central Billing System 123
Central Billing Interface 127
Subscriber Management 182
Network Provisioning System 160
Virtual Service Provider Workstation Server 4910
Central Provider Core Network 110
Central Provider Service Controller 122
Internet, Data or Phone Network 120
MWC/HLR 132
Access Network AAA Server 121
Firewall 124
Firewall 124
Access Transport Network 415
4G/3G/2G Transport Gateways 420
DNS/DHCP 126
CDR Storage, Aggregation, Mediation, Feed 118
4G/3G/2G RAN Gateways 410
Proxy Server(s) 270
Radio Access Network 405
4G/3G Base Station 125
3G/2G Base Station 125
4G BS
3G BS
3G BS
2G BS
100
115
Service Provider 115
Mobile Station

Figure 15

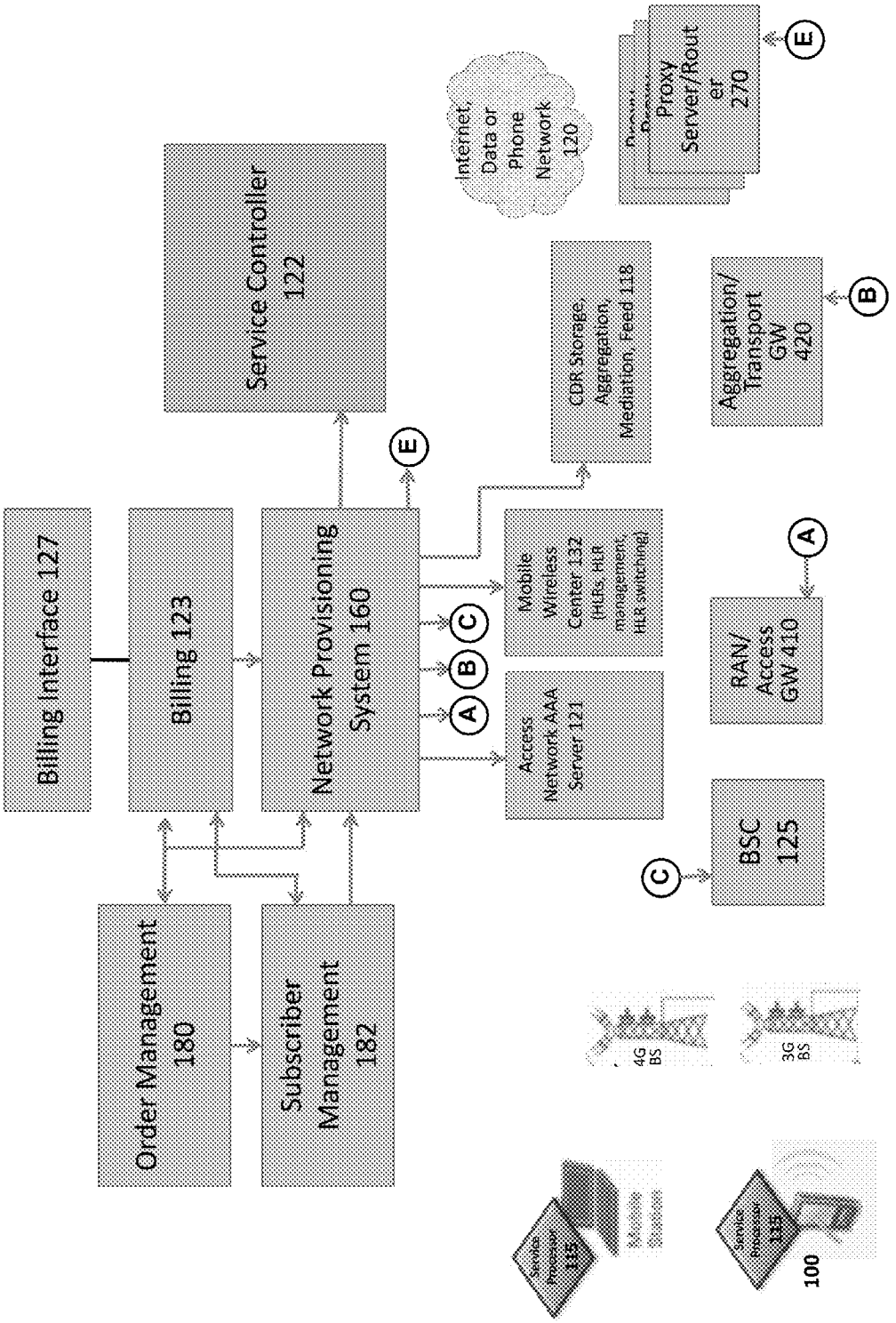

Billing Interface 127
Billing 123
Order Management 180
Subscriber Management 182
Network Provisioning System 160
Service Controller 122
Access Network AAA Server 121
Mobile Wireless Center 132 (HLRs, HLR management, HLR switching)
CDR Storage, Aggregation, Mediation, Feed 118
Internet, Data or Phone Network 120
Proxy Server/Router 270
Aggregation/ Transport GW 420
RAN/ Access GW 410
BSC 125
A
B
C
E
4G BS
3G BS
Service Processor 135
Service Processor 135
100

Figure 16

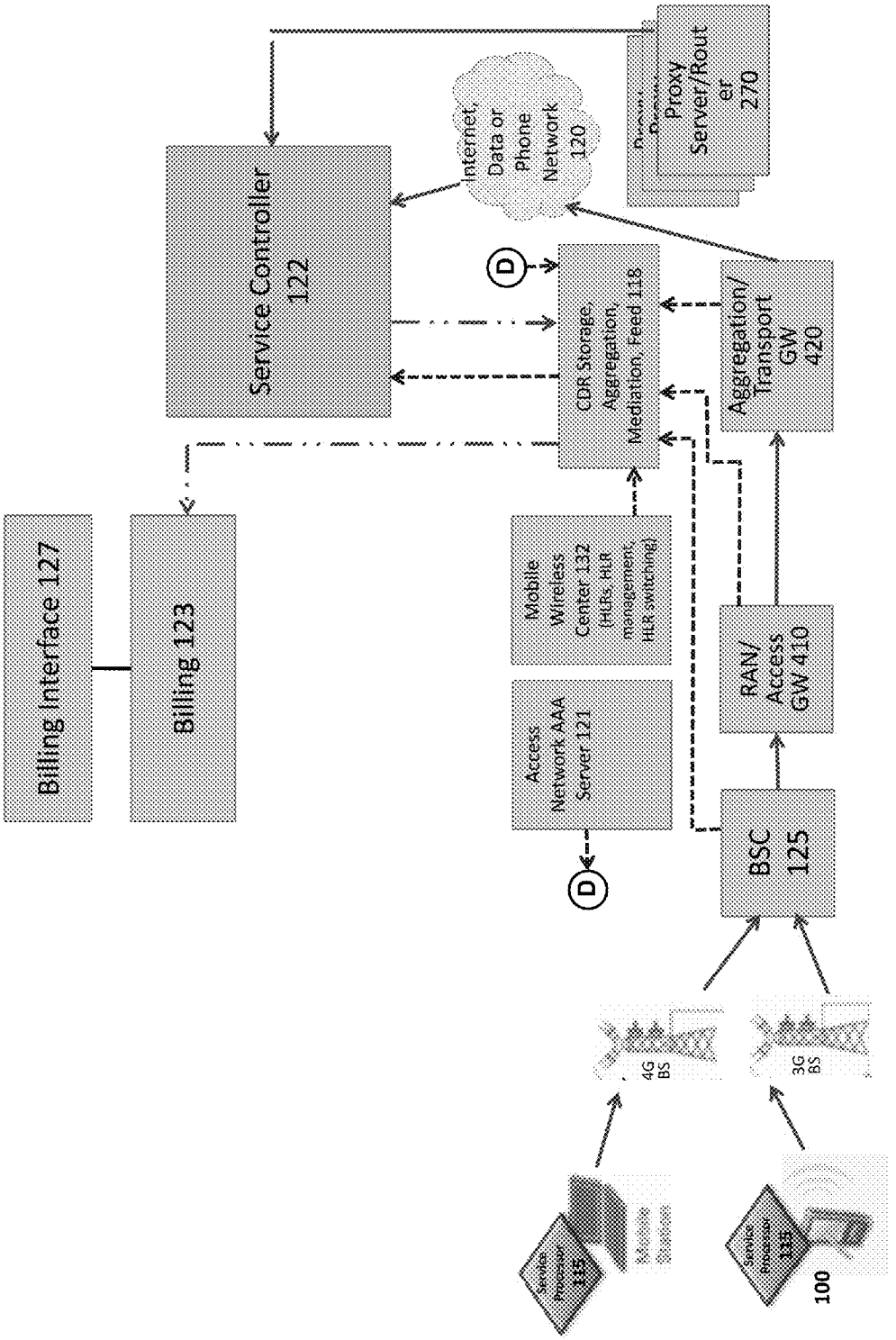

Billing Interface 127
Billing 123
Service Controller 122
Internet, Data or Phone Network 120
Proxy Server/Router 270
D
CDR Storage, Aggregation, Mediation, Feed 118
Aggregation/ Transport GW 420
Mobile Wireless Center 132 (HLRs, HLR management, HLR switching)
Access Network AAA Server 121
D
RAN/ Access GW 410
BSC 125
4G BS
3G BS
Service Processor 135
Service Processor 133
100

Figure 17

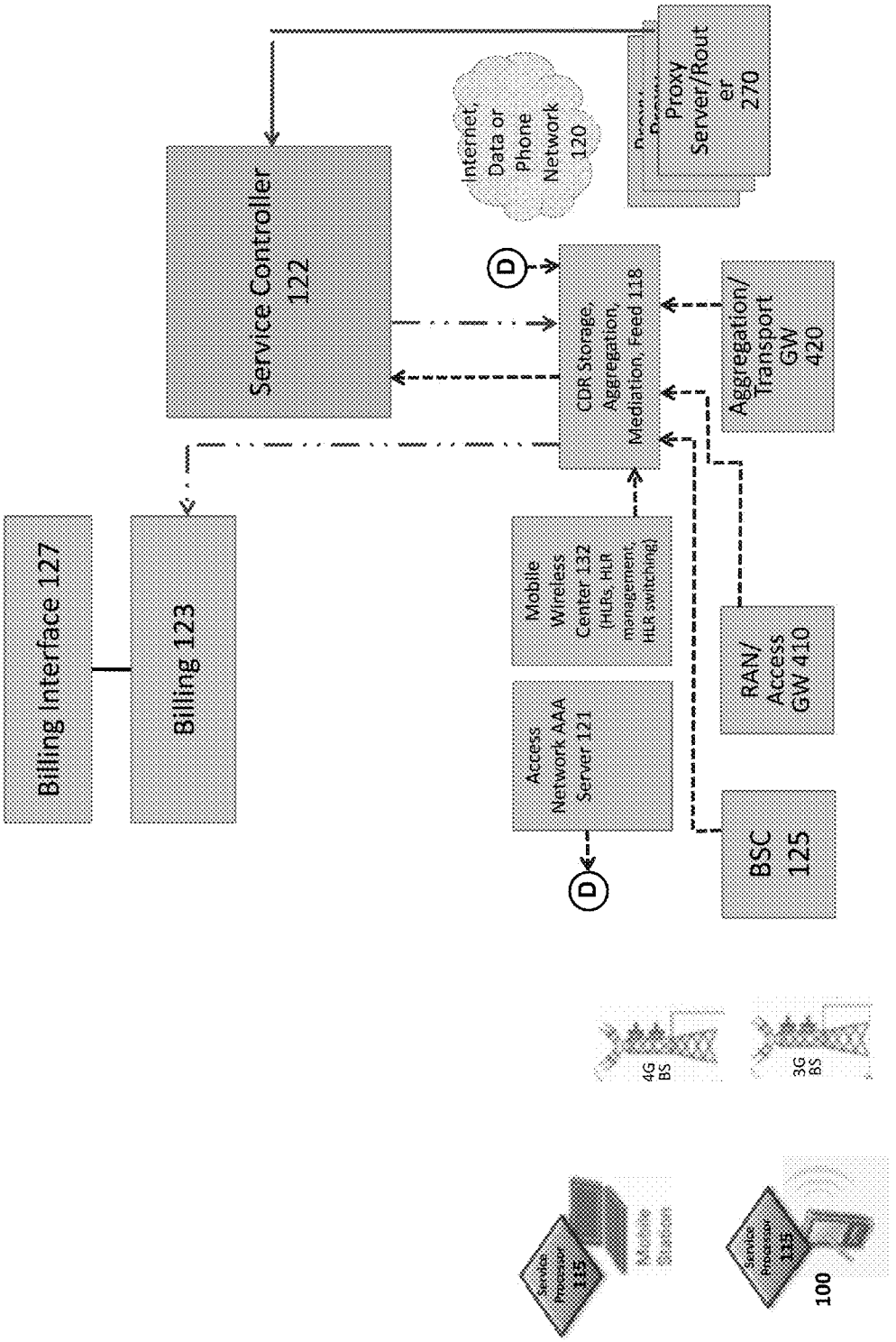

Billing Interface 127
Billing 123
Service Controller 122
Internet, Data or Phone Network 120
Proxy Server/Router 270
D
CDR Storage, Aggregation, Mediation, Feed 118
Aggregation/ Transport GW 420
Mobile Wireless Center 132 (HLRs, HLR management, HLR switching)
RAN/ Access GW 410
Access Network AAA Server 121
BSC 125
D
4G BS
3G BS
Service Processor 115
Service Processor 135
100

Figure 18

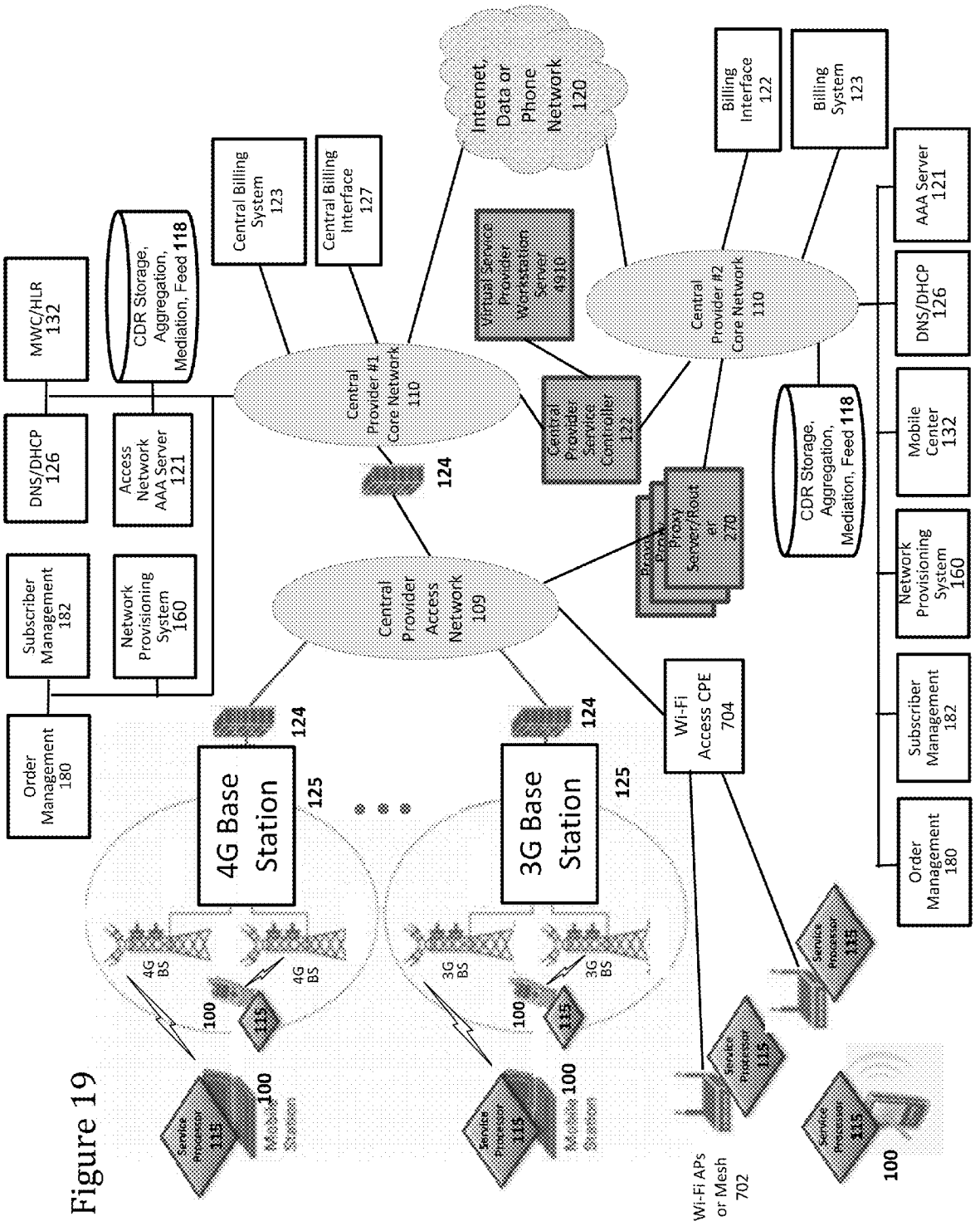

Order Management 180
Subscriber Management 182
DNS/DHCP 126
MWC/HLR 132
Network Provisioning System 160
Access Network AAA Server 121
CDR Storage, Aggregation, Mediation, Feed 118
Central Billing System 123
Central Billing Interface 127
Central Provider #1 Core Network 110
Central Provider Access Network 109
124
4G Base Station
125
3G Base Station
4G BS
3G BS
100
115
Service Processor
Mobile Station
Internet, Data or Phone Network 120
Virtual Service Provider Workstation Server 4910
Central Provider Service Controller 122
Proxy Server/Router 272
Central Provider #2 Core Network 110
Billing Interface 122
Billing System 123
Wi-Fi Access CPE 704
Wi-Fi APs or Mesh 702
AAA Server 121
DNS/DHCP 126
Mobile Center 132
Network Provisioning System 160
Subscriber Management 182
Order Management 180

Figure 19

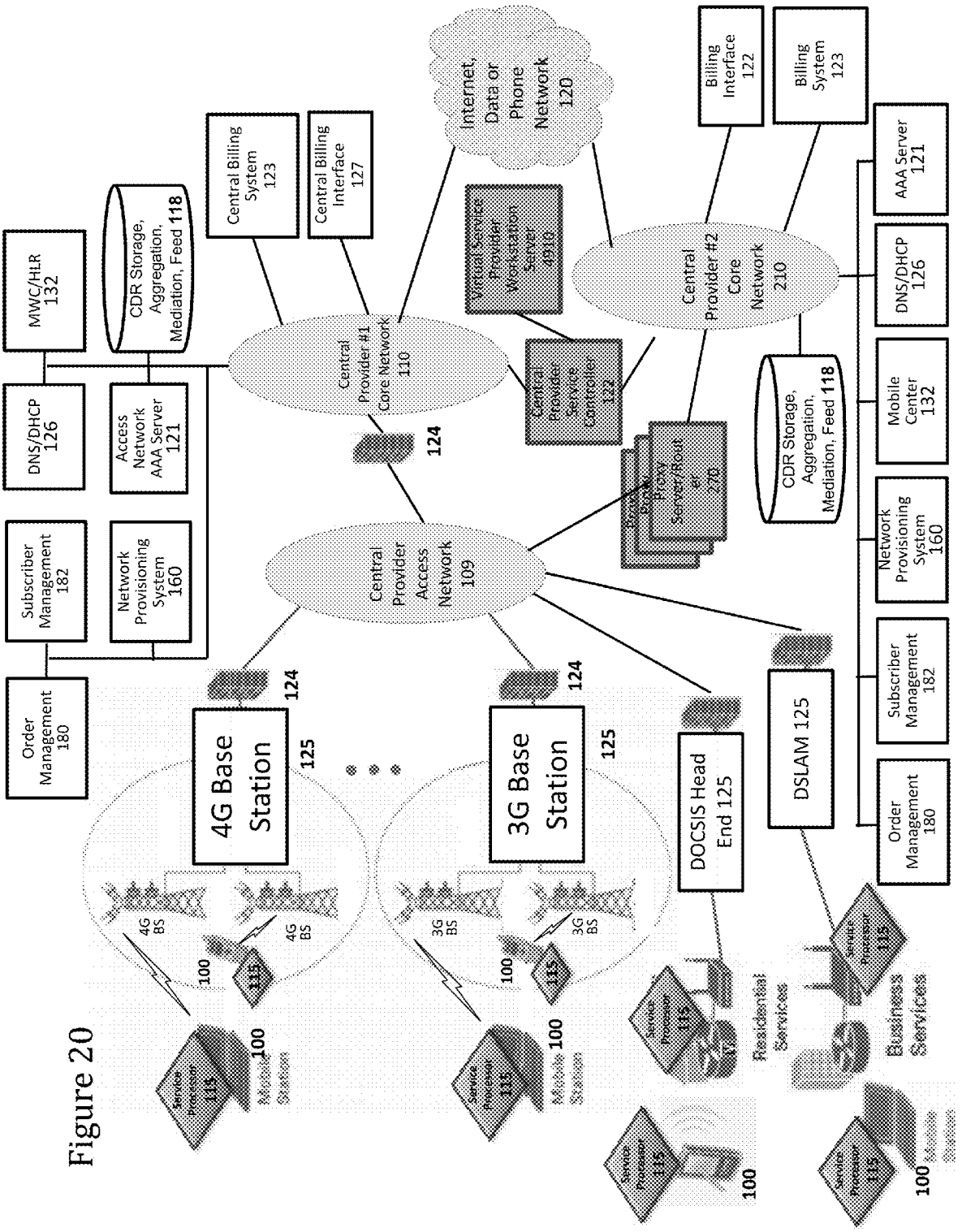
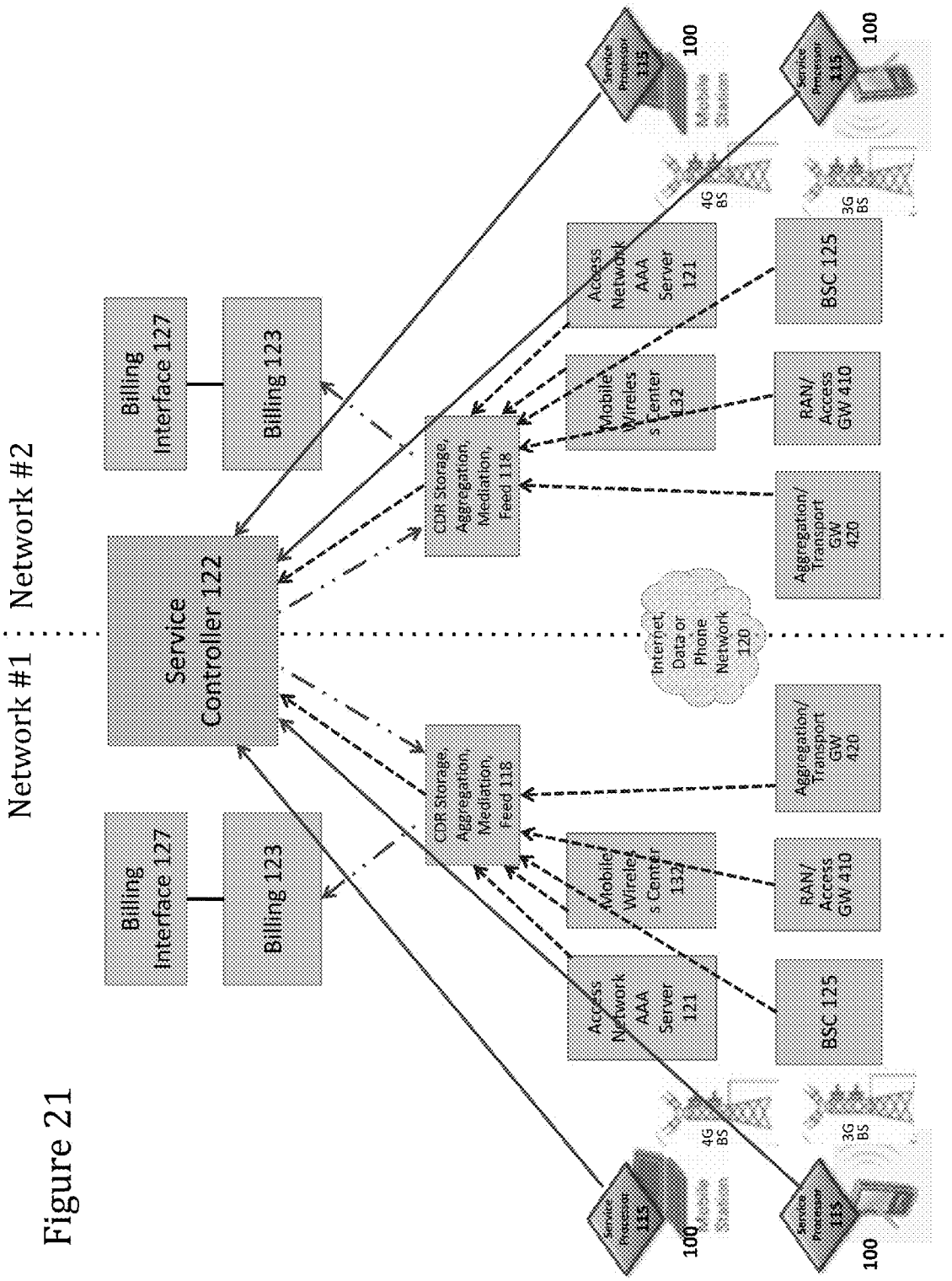

Order Management 180
Subscriber Management 182
Network Provisioning System 160
DNS/DHCP 126
MWC/HLR 132
Access Network AAA Server 121
CDR Storage, Aggregation, Mediation, Feed 118
Central Billing System 123
Central Billing Interface 127
Central Provider #1 Core Network 110
Central Provider Access Network 109
124
4G Base Station
125
3G Base Station
4G BS
3G BS
100
115
Mobile Station
Service Provider
Internet, Data or Phone Network 120
Virtual Service Provider Workstation Server 4910
Central Provider Service Controller 122
Proxy Server/Router 270
Central Provider #2 Core Network 210
Billing Interface 122
Billing System 123
CDR Storage, Aggregation, Mediation, Feed 118
DOCSIS Head End 125
DSLAM 125
Residential Services
Business Services
AAA Server 121
DNS/DHCP 126
Mobile Center 132
Network Provisioning System 160
Subscriber Management 182
Order Management 180

Figure 20

Figure 21


Network #1
Network #2
Billing Interface 127
Billing 123
Billing Interface 127
Billing 123
Service Controller 122
CDR Storage, Aggregation, Mediation, Feed 118
CDR Storage, Aggregation, Mediation, Feed 118
Access Network AAA Server 121
Mobile/ Wireless Center 132
Access Network AAA Server 121
Mobile/ Wireless Center 132
Internet, Data or Phone Network 120
Aggregation/ Transport GW 420
Aggregation/ Transport GW 420
RAN/ Access GW 410
RAN/ Access GW 410
BSC 125
BSC 125
4G BS
3G BS
4G BS
3G BS
Service Processor 115
Service Processor 115
Service Processor 115
Service Processor 115
100
100
100
100

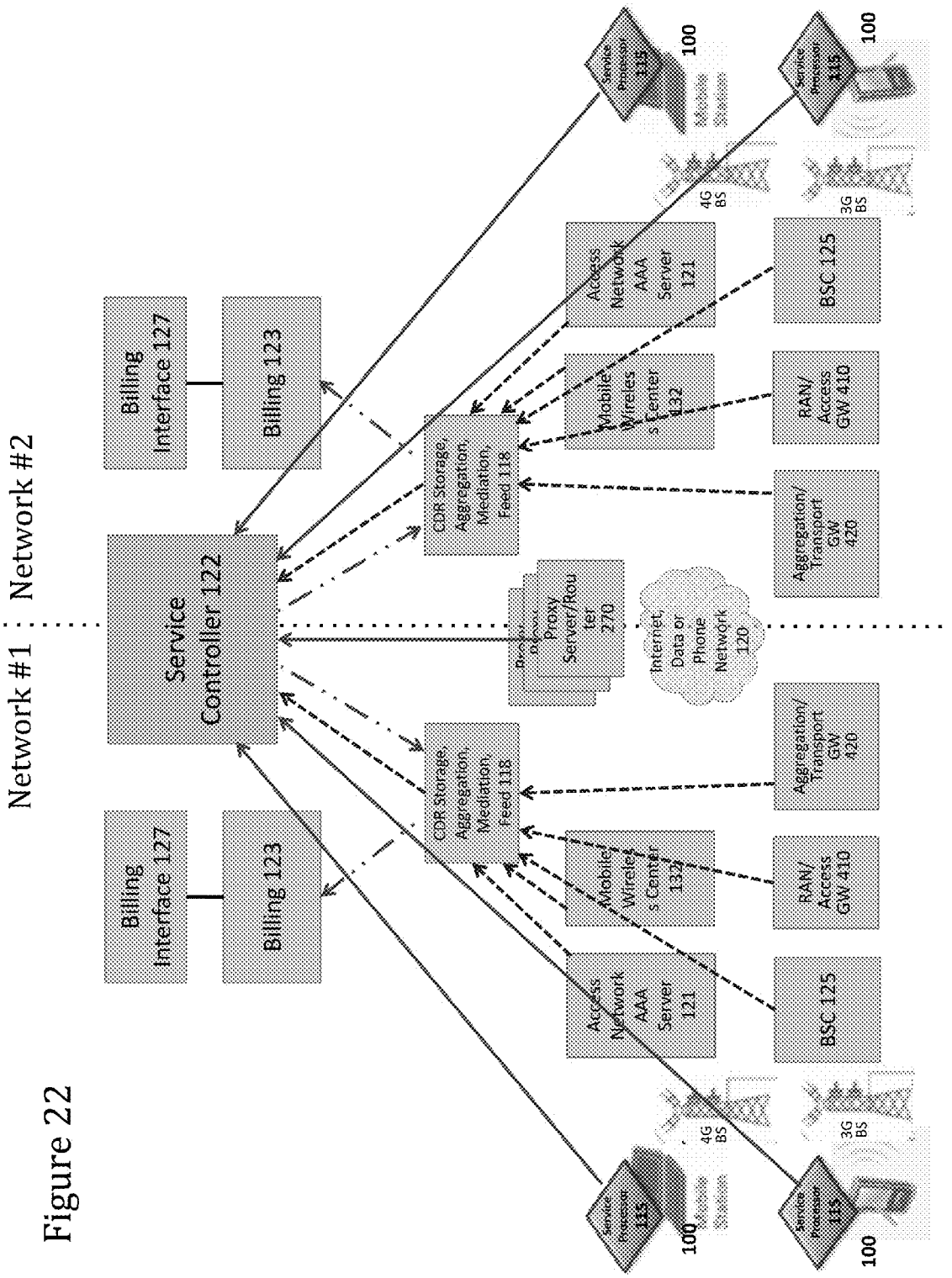

Network #1
Network #2
Billing Interface 127
Billing 123
Billing Interface 127
Billing 123
Service Controller 122
CDR Storage, Aggregation, Mediation, Feed 118
CDR Storage, Aggregation, Mediation, Feed 118
Proxy Server/Router 270
Internet, Data or Phone Network 120
Access Network AAA Server 121
Mobile Wireless Center 132
Access Network AAA Server 121
Mobile Wireless Center 132
Aggregation/ Transport GW 420
Aggregation/ Transport GW 420
RAN/ Access GW 410
RAN/ Access GW 410
BSC 125
BSC 125
4G BS
3G BS
4G BS
3G BS
Service Processor 115
Service Processor 115
Service Processor 115
Service Processor 115
100
100
100
100

Figure 22

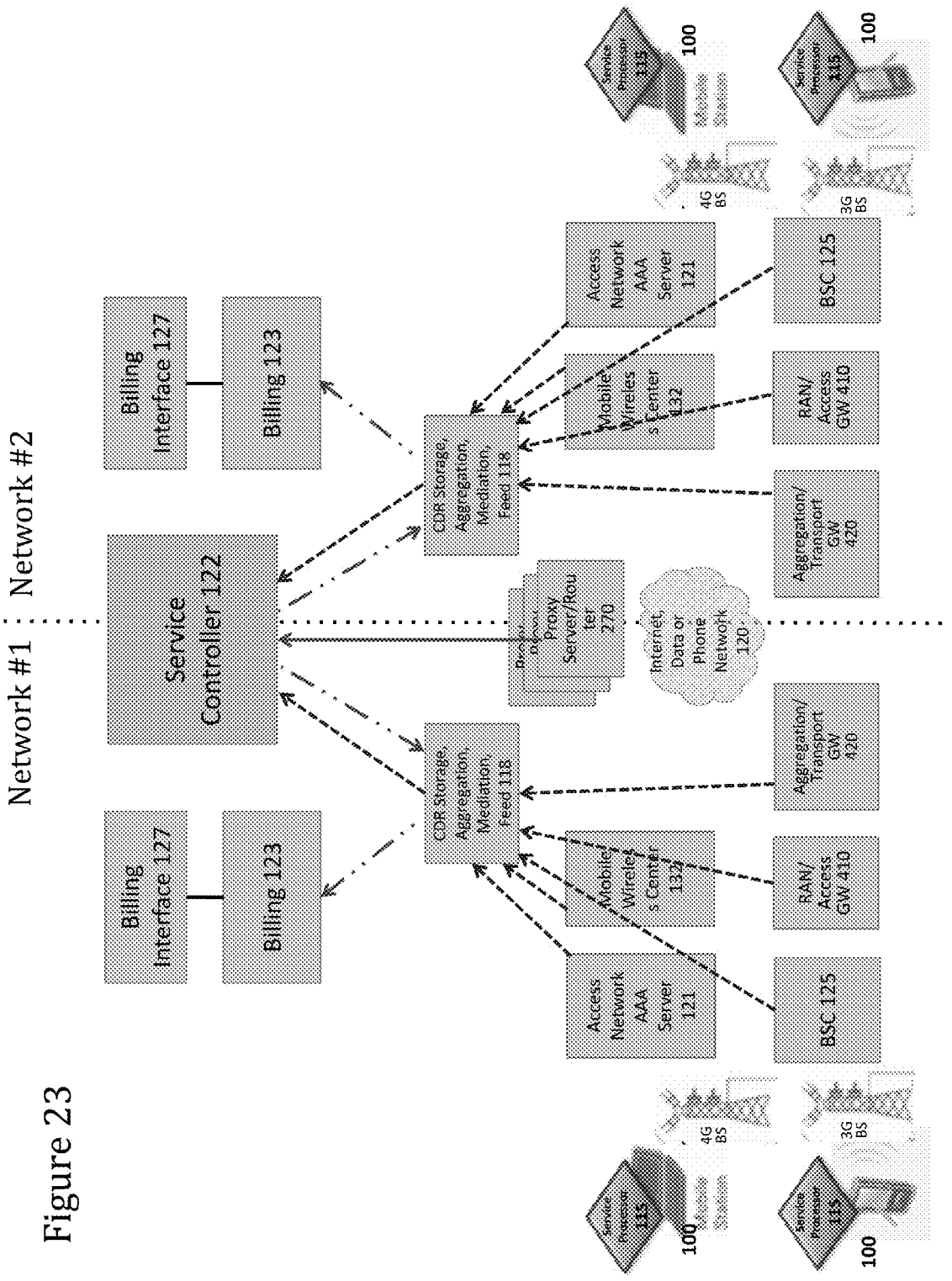

Network #1
Network #2
Billing Interface 127
Billing 123
Billing Interface 127
Billing 123
Service Controller 122
CDR Storage, Aggregation, Mediation, Feed 118
CDR Storage, Aggregation, Mediation, Feed 118
Proxy Server/Router 270
Internet, Data or Phone Network 120
Access Network AAA Server 121
Mobile Wireless Center 132
RAN/ Access GW 410
Aggregation/ Transport GW 420
Access Network AAA Server 121
Mobile Wireless Center 132
RAN/ Access GW 410
Aggregation/ Transport GW 420
BSC 125
BSC 125
4G BS
3G BS
4G BS
3G BS
Service Processor 115
Service Processor 115
Service Processor 115
Service Processor 115
100
100
100
100

Figure 23

ENHANCED ROAMING SERVICES AND CONVERGED CARRIER NETWORKS WITH DEVICE ASSISTED SERVICES AND A PROXY

CROSS REFERENCE TO OTHER APPLICATIONS

This application claims priority to U.S. Provisional Patent Application No. 61/206,354 entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD filed Jan. 28, 2009, U.S. Provisional Patent Application No. 61/206,944 entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD filed Feb. 4, 2009, U.S. Provisional Application No. 61/207,393 entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD filed Feb. 10, 2009, U.S. Provisional Patent Application No. 61/207,739 entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD filed on Feb. 13, 2009, U.S. Provisional Patent Application No. 61/270,353 entitled DEVICE ASSISTED CDR CREATION, AGGREGATION, MEDIATION AND BILLING filed on Jul. 6, 2009, which are incorporated herein by reference for all purposes.

This application is a continuation in part of co-pending U.S. patent application Ser. No. 12/380,780, entitled AUTOMATED DEVICE PROVISIONING AND ACTIVATION, filed on Mar. 2, 2009, which is incorporated herein by reference for all purposes, and which claims priority to U.S. Provisional Patent Application No. 61/206,354 entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD filed Jan. 28, 2009, U.S. Provisional Patent Application No. 61/206,944 entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD filed Feb. 4, 2009, U.S. Provisional Application No. 61/207,393 entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD filed Feb. 10, 2009, and U.S. Provisional Patent Application No. 61/207,739 entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD filed on Feb. 13, 2009, which are incorporated herein by reference for all purposes; U.S. patent application Ser. No. 12/695,019 entitled DEVICE ASSISTED CDR CREATION, AGGREGATION, MEDIATION AND BILLING filed on Jan. 27, 2010, which is incorporated herein by reference for all purposes, and U.S. Provisional Patent Application No. 61/206,354 entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD filed Jan. 28, 2009, U.S. Provisional Patent Application No. 61/206,944 entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD filed Feb. 4, 2009, U.S. Provisional Application No. 61/207,393 entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD filed Feb. 10, 2009, U.S. Provisional Patent Application No. 61/207,739 entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD filed on Feb. 13, 2009, U.S. Provisional Patent Application No. 61/270,353 entitled DEVICE ASSISTED CDR CREATION, AGGREGATION, MEDIATION AND BILLING filed on Jul. 6, 2009, and U.S. Provisional Patent Application No. 61/264,126 entitled DEVICE ASSISTED SERVICES ACTIVITY MAP filed on Nov. 24, 2009, which are incorporated herein by reference for all purposes; and U.S. patent application Ser. No. 12/695,021 entitled QUALITY OF SERVICE FOR DEVICE ASSISTED SERVICES filed on Jan. 27, 2010, which claims priority to U.S. Provisional Patent Application No. 61/206,354 entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD filed Jan. 28, 2009, U.S. Provisional Patent Application No. 61/206,944 entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD filed Feb. 4, 2009, U.S. Provisional Application No. 61/207,393 entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD filed Feb. 10, 2009, U.S. Provisional Patent Application No. 61/207,739 entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD filed on Feb. 13, 2009, U.S. Provisional Patent Application No. 61/252,151 entitled SECURITY TECHNIQUES FOR DEVICE ASSISTED SERVICES, filed on Oct. 15, 2009, and U.S. Provisional Patent Application No. 61/252,153 entitled DEVICE GROUP PARTITIONS AND SETTLEMENT PLATFORM filed on Oct. 15, 2009, which are incorporated herein by reference for all purposes.

BACKGROUND OF THE INVENTION

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.

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

BRIEF DESCRIPTION OF THE DRAWINGS

Various embodiments are disclosed in the following detailed description and the accompanying drawings.

FIG. **1** illustrates a wireless network architecture for providing device assisted CDR creation, aggregation, mediation and billing in accordance with some embodiments.

FIG. **2** illustrates another wireless network architecture for providing device assisted CDR creation, aggregation, mediation and billing in accordance with some embodiments.

FIG. **3** illustrates another wireless network architecture for providing device assisted CDR creation, aggregation, mediation and billing in accordance with some embodiments.

FIG. **4** illustrates provisioning of a wireless network for providing device assisted CDR creation, aggregation, mediation and billing in accordance with some embodiments.

FIG. **5** illustrates a network architecture for providing device assisted CDRs in accordance with some embodiments.

FIG. **6** illustrates another network architecture for providing device assisted CDRs in accordance with some embodiments.

FIG. **7** illustrates another network architecture for providing device assisted CDRs in accordance with some embodiments.

FIG. **8** illustrates another network architecture for providing device assisted CDRs in accordance with some embodiments.

FIG. **9** is a functional diagram illustrating a device based service processor and a service controller in accordance with some embodiments.

FIG. **10** provides a table summarizing various service processor functional elements in accordance with some embodiments.

FIG. **11** provides a table summarizing various service controller functional elements in accordance with some embodiments.

FIG. **12** illustrates a device stack providing various service usage measurement from various points in the networking stack for a service monitor agent, a billing agent, and an access control integrity agent to assist in verifying the service usage measures and billing reports in accordance with some embodiments.

FIG. **13** illustrates an embodiment similar to FIG. **12** in which some of the service processor is implemented on the modem and some of the service processor is implemented on the device application processor in accordance with some embodiments.

FIG. **14** illustrates various embodiments of intermediate networking devices that include a service processor for the purpose of verifiable service usage measurement, reporting, and billing reports in accordance with some embodiments.

FIG. **15** illustrates a wireless network architecture for providing device assisted CDR creation, aggregation, mediation and billing including a proxy server in accordance with some embodiments.

FIG. **16** illustrates a wireless network architecture for providing device assisted CDR creation, aggregation, mediation and billing including a service provider network in accordance with some embodiments, involving one or more of service controllers, service processors, and/or proxy server/routers.

FIG. **17** illustrates a wireless network architecture for providing device assisted CDR creation, aggregation, mediation and billing including a service provider network in accordance with some embodiments, involving one or more of service controllers, service processors, and/or proxy server/routers.

FIG. **18** illustrates a wireless network architecture for providing device assisted CDR creation, aggregation, mediation and billing including a service provider network in accordance with some embodiments, involving one or more of service controllers and/or proxy server/routers.

FIG. **19** illustrates a wireless network architecture for providing device assisted CDR creation, aggregation, mediation and billing including two service provider networks in accordance with some embodiments.

FIG. **20** illustrates a wireless network architecture for providing device assisted CDR creation, aggregation, mediation and billing including two service provider networks in accordance with some embodiments, involving one or more of service controllers and/or service processors.

FIG. **21** illustrates a wireless network architecture for providing device assisted CDR creation, aggregation, mediation and billing including two service provider networks in accordance with some embodiments.

FIG. **22** illustrates a wireless network architecture for providing device assisted CDR creation, aggregation, mediation and billing including two service provider networks in accordance with some embodiments, involving one or more of service controllers, service processors, and/or proxy server/routers.

FIG. **23** illustrates a wireless network architecture for providing device assisted CDR creation, aggregation, mediation and billing including two service provider networks in accordance with some embodiments, involving one or more of service controllers and/or proxy server/routers.

DETAILED DESCRIPTION

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.

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.

There are many new types of digital devices where it is becoming desirable, for example, to connect these devices to wireless networks including wireless wide area networks (WWAN, such as 3G and 4G) and/or wireless local area (WLAN) networks. These devices include, for example, consumer electronics devices, business user devices, and machine to machine devices that benefit from flexible wide area data connections and the Internet. Example devices include netbooks, notebooks, mobile Internet devices, personal navigation (e.g., GPS enabled) devices, music and multimedia players, eReaders, industrial telemetry, automotive emergency response and diagnostics, 2-way home and industrial power metering and control, vending machines, parking meters, and many other devices. For example, it is highly advantageous to offer service usage and service billing plans for such devices that are more optimal for each type of device and each type of desired user experience. To accomplish this, more sophisticated service usage measuring and service usage billing systems are needed as compared to the conventional network based techniques in existence today. By providing more flexibility in service measurement and billing, more advantageous and cost effective service plans can be created for, for example, the new WWAN connected devices cited above for all three markets (e.g., consumer, business and machine to machine) that still maintain the necessary profit margins for the WWAN carriers to be successful with these various service businesses.

Accordingly, various embodiments disclosed herein provide for a new and flexible augmentation or replacement for existing carrier network service usage measurement, service usage accounting, and service usage billing systems and techniques.

A charging data record (CDR) is a term that as used herein defines a formatted measure of device service usage information, typically generated by one or more network functions or device functions that supervise, monitor, control, account for, charge for, report, synchronize usage accounting or records and/or bill for network access or other service or purchase transactions for the device. To simplify the discussion, the term charging data record or CDR is often used interchangeably herein to refer to several different types of service usage records. For example, the term CDR is used herein interchangeably with one or more of other industry terms or record types including, for example, CDRs, flow data records (FDRs), start/stop records, interim accounting records, IP data records (IPDRs), call data records, micro-CDRs, service charging bucket accounting records, record types that include usage information identifying QoS level, QoS class, and/or other QoS classifier, records that include usage information identifying traffic type or class or other traffic identifier, records that identify traffic protocol, records that identify usage or purchase transactions, records that report a purchase transaction, etc. One of ordinary skill in the art will appreciate that in many of the embodiments the term CDR and/or many other terms can be interchanged for a given application or purpose. Any of these terms can refer in various embodiments to the lowest level of usage accounting records or can refer to various levels of charging record aggregation that may occur in the various network or device elements described herein.

CDRs typically form the basis for recording device network service usage, and often form the basis for billing for such usage. Various embodiments are provided herein for device assisted CDR creation, mediation, and billing. There are many limitations to the capabilities of service usage recording, aggregation and/or billing when CDRs are generated exclusively by network based functions or equipment. Accordingly, by either augmenting network based service usage measures with device based service usage measures, or by replacing network based service usage measures with device based service usage measures, it is possible to create a CDR generation, aggregation, mediation and/or billing solution that has superior or more desirable capabilities/features. While in theory, many of the service usage measures that can be evaluated on a device can also be evaluated in the network data path using various network equipment technologies including, for example, deep packet inspection (DPI), there are many examples where measuring service usage at the device is either more desirable or more practical, or in some cases it is the only way to obtain the desired measure. Such examples include but are not limited to the following:

- Application layer service usage measures (e.g., traffic usage categorized by application or by combinations of application, destination, and/or content type);
- Usage measures that do not involve user traffic but instead involve network overhead traffic (e.g., basic connection maintenance traffic, signaling traffic, network logon/AAA/authentication/monitoring traffic, service software update traffic);
- Usage that is associated with services that are charged to another entity other than the end user (e.g., basic network connection service offer traffic, traffic associated with providing network access to or downloading service marketing information, traffic associated with advertiser sponsored services, traffic associated with content provider sponsored services, 911 service traffic);
- Usage measures involving encrypted traffic (e.g., traffic that is run over encrypted networking protocols or between secure end points);
- Implementing service usage measure collection and/or service usage billing across multiple networks that may have different and in some cases incompatible, inaccessible (to the CDR system of record) or incomplete service usage measurement capabilities;
- Service usage measurement and/or service usage billing capabilities that are not supported by the present network gateways, routers, MWC/HLRs, AAA, CDR aggregation, CDR mediation, billing and/or provisioning systems;
- New service usage measures and/or new service usage billing capabilities that are desirable to implement in a manner that does not require major changes or upgrades to the existing network gateways, routers, MWC/HLRs, AAA, CDR aggregation, CDR mediation, billing and/or provisioning systems;
- New service usage measures and/or new service usage billing capabilities that are desirable to implement in a manner that allows for rapid definition and implementation of new service measures and/or billing plans;
- New service usage measures and/or new service usage billing capabilities that are desirable to implement in a manner that may be implemented in a manner that enables multiple device group definitions in which each device group gets a customized programmable definition for service usage collection, accounting and/or billing;
- Multi device billing;
- Multi user billing;
- Intermediate device billing with single user and multi user with and without multi device;
- Content downloads from a specific source to a specific application with the content being of a specific type or even identified down to a particular content ID; and/or
- Various other single event transactions used for billing purposes.

For these and other reasons, it is desirable to provide a system/process that utilizes device assisted service usage measures that provides either an enhancement of existing network based service usage CDR system capabilities and techniques and/or a replacement for network based CDR system capabilities and techniques.

In some embodiments, techniques, such as a system and/or process, that utilize device assisted service usage measures include one or more of the following: (1) receiving a service usage measure from a device in communication with a wireless network, (2) verifying or protecting the validity of the service usage measure, (3) generating a CDR based on the service usage measure (e.g., device assisted CDR), (4) aggregating CDRs, and (5) mediating the CDR with network CDRs. In some embodiments, the techniques also include providing a design and provisioning of devices/network equipment to recognize the CDRs. In some embodiments, the techniques also include provisioning to recognize that the device belongs to a Device Assisted Services (DAS) device group and that corresponding CDRs should be accepted and mediated. In some embodiments, the device assisted CDRs are also generated using formats, network communications protocols, network device authentication and/or provisioning to allow device assisted CDRs into the network CDR system, encryption, and/or signatures as required by the network

(e.g., to comply with network generated CDR requirements or based on any other network and/or service provider requirements and/or standards).

In some embodiments, mediation rules include multi device, multi user, single user devices, and/or intermediate networking devices that can be single user or multi user, as described herein.

In some embodiments, a device assisted CDR generator collects device based service usage measures that are used as the basis for, or as an enhancement (e.g., as a supplement or in addition) to, one or more (e.g., network generated) CDRs that provide one or more networking functions with properly formatted service usage reports that the network function(s) accepts as being transmitted from an authorized source, read, and utilized for helping to determine the service usage of a device or group of devices. In some embodiments, the network functions that the device assisted CDR generator shares CDRs with typically include one or more of the following: service usage/CDR aggregation and/or mediation servers, gateways, routers, communication nodes, Mobile Wireless Centers (MWCs, including HLRs), databases, AAA systems, billing interfaces, and billing systems. For example, the process of CDR creation in the CDR generator typically includes either using one or more device based measures of service usage, or one or more device based measures of service usage in combination with one or more network based measures of service usage, possibly processing one or more of such service usage measures according to a set of CDR creation, CDR aggregation, and/or CDR mediation rules to arrive at a final device usage measure that is, for example, then formatted with the proper syntax, framed, possibly encrypted and/or signed, and encapsulated in a communication protocol or packet suitable for sharing with network functions. In some embodiments, the CDR generator resides in the device. In some embodiments, the CDR generator resides in a network server function that receives the device assisted service usage measures, along with possibly network based usage measures, and then creates a CDR (e.g., in the service controller **122**).

In some embodiments, the device assisted CDR generator can reside in the service processor (e.g., service processor **115**), for example, in the service usage history or billing server functions. In some embodiments, the device assisted CDR generator resides in the device itself, for example, within the service processor functions, such as the billing agent or the service monitor agent.

There are several factors that are considered in the various embodiments in order to create a useful, reliable, and secure device assisted CDR system, including, for example, but not limited to:

- Identification of each device based service usage measure with one or more usage transaction codes;
- Verification of the device based usage measure(s);
- Secure communication of the device based usage measures to the network;
- Efficient (e.g., low bandwidth) communication of the device based service usage measure;
- Coordination/comparison/aggregation of the device based service usage measure with network based service usage measure(s);
- Formatting the device based service usage measure into a CDR that can be properly communicated to the network functions and/or equipment that process service usage information;
- Causing the network based functions and/or equipment used for CDR collection, aggregation, mediation and/or billing to recognize, authorize, and accept communications and CDRs from the device assisted CDR generator, reading and properly implementing the correct network session context for the CDR so that the CDR is properly associated with the correct device/user/session;
- Implementing the CDR aggregation rules that determine how to collect and aggregate the device assisted CDRs as they are reported through the network CDR system hierarchy;
- Implementing the mediation rules that determine how the various device based service usage transaction code measures are combined and mediated with the other device based service usage transaction code measures to result in consistent service usage information for each of the transaction code categories maintained in the network;
- Implementing the mediation rules that determine how the device assisted CDRs are combined and mediated with network based CDRs to result in consistent service usage information for each of the transaction code categories maintained in the network;
- Implementing mediation rules to reconcile the variances between network based CDR usage measures and device assisted CDR usage measures;
- Classification of one or more device groups, with each group having the capability to uniquely define the service usage collection, accounting, and/or billing rules;
- Collecting CDRs generated on networks other than the home network so that service usage may be measured, accounted for, and/or billed for across multiple networks;
- Multi device billing;
- Multi user billing; and/or
- Intermediate device billing with single user and multi user with and without multi device.

In some embodiments, verification of the relative accuracy of the device assisted service usage measure is provided. Given that, for example, the service usage measure is often being generated on an end user device or a device that is readily physically accessed by the general public or other non-secure personnel from a network management viewpoint, in some embodiments, the device agents used in one or more of the service processor **115** agents are protected from hacking, spoofing, and/or other misuse. Various techniques are provided herein for protecting the integrity of the agents used for generating the device assisted service usage measures.

In some embodiments, the service usage measures are verified by network based cross checks using various techniques. For example, network based cross checks can provide valuable verification techniques, because, for example, it is generally not possible or at least very difficult to defeat well designed network based cross checks using various techniques, such as those described herein, even if, for example, the measures used to protect the device agents are defeated or if no device protection measures are employed. In some embodiments, network based cross checks used to verify the device assisted service usage measures include comparing network based service usage measures (e.g., CDRs generated by service usage measurement apparatus in the network equipment, such as the BTS/BSCs **125**, RAN Gateways **410**, Transport Gateways **420**, Mobile Wireless Center/HLRs **132**, AAA **121**, Service Usage History/CDR Aggregation, Mediation, Feed **118**, or other network equipment), sending secure query/response command sequences to the service processor **115** agent(s) involved in device assisted CDR service usage measurement or CDR creation, sending test service usage event sequences to the device and verifying that the device

properly reported the service usage, and using various other techniques, such as those described herein with respect to various embodiments.

In some embodiments, one or more of the following actions are taken if the device based service usage measure is found to be in error or inaccurate: bill the user for usage overage or an out of policy device, suspend the device, quarantine the device, SPAN the device, and/or report the device to a network administration function or person.

In some embodiments, the CDR syntax used to format the device assisted service usage information into a CDR and/or network communication protocols for transmitting CDRs are determined by industry standards (e.g., various versions of 3GPP TS 32.215 format and 3GPP2 TSG-X X.S0011 or TIA-835 format). In some embodiments, for a given network implementation the network designers will specify modifications of the standard syntax, formats and/or network communication/transmission protocols. In some embodiments, for a given network implementation the network designers will specify syntax, formats, and/or network communication/transmission protocols that are entirely different than the standards.

In some embodiments, within the syntax and formatting for the CDR the device assisted service usage is typically categorized by a transaction code. For example, the transaction code can be similar or identical to the codes in use by network equipment used to generate CDRs, or given that the device is capable of generating a much richer set of service usage measures, the transaction codes can be a superset of the codes used by network equipment used to generate CDRs (e.g., examples of the usage activities that can be labeled as transaction codes that are more readily supported by device assisted CDR systems as compared to purely network based CDR systems are provided herein).

In some embodiments, the device sends an identifier for a usage activity tag, an intermediate server determines how to aggregate into CDR transaction codes and which CDR transaction code to use.

In some embodiments, the device service processor **115** compartmentalizes usage by pre-assigned device activity transaction codes (e.g., these can be sub-transactions within the main account, transactions within a given bill-by-account transaction or sub-transactions within a bill-by-account transaction). The device implements bill-by-account rules to send different usage reports for each bill-by-account function. In some embodiments, the service controller **122** programs the device to instruct it on how to compartmentalize these bill-by-account service usage activities so that they can be mapped to a transaction code.

In some embodiments, the device reports less compartmentalized service usage information and the service controller **122** does the mapping of service usage activities to CDR transaction codes, including in some cases bill-by-account codes.

In some embodiments, the CDR sent to **118** or other network equipment, for example, can include various types of transaction codes including, for example, a raw device usage CDR, a bill-by-account (e.g., a sub-activity transaction code) CDR, a billing offset CDR, and/or a billing credit CDR. For example, the decision logic (also referred to as business rules or CDR aggregation and mediation rules) that determines how these various types of CDR transaction codes are to be aggregated and mediated by the core network and the billing system can be located in the network equipment (e.g., a network element, such as service usage **118**), in the service controller **122**, and/or in the billing system **123**.

In some embodiments, the device assisted CDR generator uses the device assisted service usage measures to generate a CDR that includes service usage information, service usage transaction code(s), and, in some embodiments, network information context. In some embodiments, the service usage information, transaction code, and/or network information context is formatted into communication framing, syntax, encryption/signature, security and/or networking protocols that are compatible with the formatting used by conventional networking equipment to generate CDRs. For example, this allows networking equipment used for CDR collection, recording, aggregation, mediation, and/or conversion to billing records to properly accept, read, and interpret the CDRs that are generated with the assistance of device based service usage measurement. In some embodiments, the device assisted service measures are provided to an intermediate network server referred to as a service controller (e.g., service controller **122**). In some embodiments, the service controller uses a CDR feed aggregator for a wireless network to collect device generated usage information for one or more devices on the wireless network; and provides the device generated usage information in a syntax (e.g., charging data record (CDR)), and a communication protocol (e.g., 3GPP or 3GPP2, or other communication protocol(s)) that can be used by the wireless network to augment or replace network generated usage information for the one or more devices on the wireless network.

In some embodiments, mediation rules include multi device, multi user, single user devices, intermediate networking devices that can be single user or multi user. For example, the device assisted CDRs can be formatted by the device assisted CDR generator to include a transaction code for one user account, even though the CDRs originate from multiple devices that all belong to the same user. This is an example for a multi-user device assisted CDR billing solution. In another example for a multi-user device assisted CDR billing solution, device assisted CDRs from multiple devices and multiple users can all be billed to the same account (e.g., a family plan or a corporate account), but the bill-by-account CDR transaction records can be maintained through the billing system so that sub-account visibility is provided so that the person or entity responsible for the main account can obtain visibility about which users and/or devices are creating most of the service usage billing. For example, this type of multi-user, multi-device device assisted CDR billing solution can also be used to track types of service usage and/or bill for types of service usage that are either impossible or at least very difficult to account and/or bill for with purely network based CDR systems. In some embodiments, bill-by-account CDR transaction records can be used to provide sponsored transaction services, account for network chatter, provide service selection interfaces, and other services for multi-user or multi-device service plans.

In addition to conventional single user devices (e.g., cell phones, smart phones, netbooks/notebooks, mobile internet devices, personal navigation devices, music players, electronic eReaders, and other single user devices) device assisted service usage measurement and CDRs are also useful for other types of network capable devices and/or networking devices, such as intermediate networking devices (e.g., 3G/4G WWAN to WLAN bridges/routers/gateways, femto cells, DOCSIS modems, DSL modems, remote access/backup routers, and other intermediate network devices). For example, in such devices, particularly with a secure manner to verify that the device assisted service usage measures are relatively accurate and/or the device service processor **115** software is not compromised or hacked, many new service

provider service delivery and billing models can be supported and implemented using the techniques described herein. For example, in a WiFi to WWAN bridge or router device multiple user devices can be supported with the same intermediate networking device in a manner that is consistent and compatible with the central provider's CDR aggregation and/or billing system by sending device assisted CDRs as described herein that have a service usage and/or billing code referenced to the end user and/or the particular intermediate device.

In some embodiments, the device assisted CDRs generated for the intermediate networking device are associated with a particular end user in which there can be several or many end users using the intermediate networking device for networking access, and in some embodiments, with each end user being required to enter a unique log-in to the intermediate networking device. For example, in this way, all devices that connect using WiFi to the intermediate networking device to get WWAN access generate CDRs can either get billed to a particular end user who is responsible for the master account for that device, or the CDRs can get billed in a secure manner, with verified relative usage measurement accuracy to multiple end users from the same intermediate networking device. In another example, an end user can have one account that allows access to a number of intermediate networking devices, and each intermediate networking device can generate consistent device assisted CDRs with transaction codes for that end user regardless of which intermediate networking device the end user logs in on.

In some embodiments, some of the services provided by the intermediate networking device are billed to a specific end user device assisted CDR transaction code, while other bill-by-account services are billed to other transaction code accounts, such as sponsored partner transaction service accounts, network chatter accounts, sponsored advertiser accounts, and/or service sign up accounts. For example, in this manner, various embodiments are provided in which intermediate networking devices (e.g., a WWAN to WiFi router/bridge) can sold to one user but can service and be used to bill other users (e.g., and this can be covered in the first purchasing user's service terms perhaps in exchange for a discount), or such intermediate networking devices can be located wherever access is desired without concern that the device will be hacked into so that services can be acquired without charge.

In some embodiments, various types of service usage transactions are billed for on the intermediate networking device, to any of one or more users, in which the information required to bill for such services is not available to the central provider or MVNO network equipment, just as is the case with, for example, conventional single user devices. In view of the various embodiments and techniques described herein, those skilled in the art will appreciate that similar service models are equally applicable not just to WWAN to WiFi intermediate networking devices, but also to the Femto Cell, remote access router, DOCSIS, DSL and other intermediate WWAN to WiFi networking devices.

FIG. **1** illustrates a wireless network architecture for providing device assisted CDR creation, aggregation, mediation and billing in accordance with some embodiments. As shown, FIG. **1** includes a 4G/3G/2G wireless network operated by, for example, a central provider. As shown, various wireless devices **100** are in communication with base stations **125** for wireless network communication with the wireless network, and other devices **100** are in communication with Wi-Fi Access Points (APs) or Mesh **702** for wireless communication to Wi-Fi Access CPE 704 in communication with central provider access network **109**. In some embodiments, each of the wireless devices **100** includes a service processor **115** (as shown), and each service processor connects through a secure control plane link to a service controller **122**. In some embodiments, the network based service usage information (e.g., CDRs) is obtained from one or more network elements. As shown, an MVNO core network **210** also includes a CDR storage, aggregation, mediation, feed **118**, a MVNO billing interface **122**, and a MVNO billing system **123** (and other network elements as shown in FIG. **1**). A Virtual Service Provider Work Station **4910** (also referred to herein as a service design interface) provides a user interface to central provider service designers, MVNO service designers or other service designers for the purpose of simplifying and organizing the process of service design as described herein.

As shown in FIG. **1**, a CDR storage, aggregation, mediation, feed **118** (e.g., service usage **118**, including a billing aggregation data store and rules engine) is a functional descriptor for, in some embodiments, a device/network level service usage information collection, aggregation, mediation, and reporting function located in one or more of the networking equipment components attached to one or more of the sub-networks shown in FIG. **1** (e.g., central provider access network **109** and/or central provider core network **110**), which is in communication with the service controller **122**, and a central billing interface **127**. As shown in FIG. **1**, service usage **118** is shown as a function in communication with the central provider core network **110**. In some embodiments, the CDR storage, aggregation, mediation, feed **118** function is located elsewhere in the network or partially located in elsewhere or integrated with as part of other network elements. In some embodiments, CDR storage, aggregation, mediation, feed **118** functionality is located or partially located in the AAA server **121** and/or the mobile wireless center/Home Location Register (HLR) **132** (as shown, in communication with a DNS/DHCP server **126**). 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. **1**. In some embodiments, CDR storage, aggregation, mediation, feed **118** functionality is located or partially located in a networking component in the central provider access network **109**, a networking component in the core network **110**, the central billing system **123**, the central billing interface **127**, and/or in another network component or function. This discussion on the possible locations for the network based and device based service usage information collection, aggregation, mediation, and reporting function (e.g., CDR storage, aggregation, mediation, feed **118**) can be easily generalized as described herein and as shown in the other figures described herein by one of ordinary skill in the art. Also as shown in FIG. **1**, the service controller **122** is in communication with the central billing interface **123** (also sometimes referred to as the external billing management interface or billing communication interface) **127**, which is in communication with the central billing system **123**. As shown, an order management **180** and subscriber management **182** are also in communication with the central provider core network **110** for facilitating order and subscriber management of services for the devices **100** in accordance with some embodiments.

In some embodiments, the CDR storage, aggregation, mediation, feed **118** (and/or other network elements or combinations of network elements) provides a device/network level service usage information collection, aggregation, mediation, and reporting function. In some embodiments, the CDR storage, aggregation, mediation, feed **118** (and/or other network elements or combinations of network elements) col-

lects device generated usage information for one or more devices on the wireless network (e.g., devices **100**); and provides the device generated usage information in a syntax and a communication protocol that can be used by the wireless network to augment or replace network generated usage information for the one or more devices on the wireless network. In some embodiments, the syntax is a charging data record (CDR), and the communication protocol is selected from one or more of the following: 3GPP, 3GPP2, or other communication protocols. In some embodiments, the CDR storage, aggregation, mediation, feed **118** (and/or other network elements or combinations of network elements) includes a service usage data store (e.g., a billing aggregator) and a rules engine for aggregating the collected device generated usage information. In some embodiments, the syntax is a charging data record (CDR), and the network device is a CDR feed aggregator, and the CDR storage, aggregation, mediation, feed **118** (and/or other network elements or combinations of network elements) also aggregates CDRs for the one or more devices on the wireless network; applies a set of rules to the aggregated CDRs using a rules engine (e.g., bill by account, transactional billing, and/or any other billing or other rules for service usage information collection, aggregation, mediation, and reporting), and communicates a new set of CDRs for the one or more devices on the wireless network to a billing interface or a billing system (e.g., providing a CDR with a billing offset by account/service). In some embodiments, the CDR storage, aggregation, mediation, feed **118** (and/or other network elements or combinations of network elements) communicates a new set of CDRs for the one or more devices on the wireless network to a billing interface or a billing system. In some embodiments, the CDR storage, aggregation, mediation, feed **118** (and/or other network elements or combinations of network elements) communicates with a service controller to collect the device generated usage information for the one or more devices on the wireless network. In some embodiments, the CDR storage, aggregation, mediation, feed **118** (and/or other network elements or combinations of network elements) communicates with a service controller, in which the service controller is in communication with a billing interface or a billing system. In some embodiments, the CDR storage, aggregation, mediation, feed **118** (and/or other network elements or combinations of network elements) communicates the device generated usage information to a billing interface or a billing system. In some embodiments, the CDR storage, aggregation, mediation, feed (and/or other network elements or combinations of network elements) communicates with a transport gateway and/or a Radio Access Network (RAN) gateway to collect the network generated usage information for the one or more devices on the wireless network. In some embodiments, the service controller **122** communicates the device generated service usage information to the CDR storage, aggregation, mediation, feed **118** (and/or other network elements or combinations of network elements).

In some embodiments, the CDR storage, aggregation, mediation, feed **118** (and/or other network elements or combinations of network elements) performs rules for performing a bill by account aggregation and mediation function. In some embodiments, the service controller **122** in communication with the CDR storage, aggregation, mediation, feed **118** (and/or other network elements or combinations of network elements) performs a rules engine for aggregating and mediating the device generated usage information. In some embodiments, a rules engine device in communication with the CDR storage, aggregation, mediation, feed **118** (and/or other network elements or combinations of network elements) performs a rules engine for aggregating and mediating the device generated usage information.

In some embodiments, the rules engine is included in (e.g., integrated with/part of) the CDR storage, aggregation, mediation, feed **118**. In some embodiments, the rules engine and associated functions, as described herein, is a separate function/device. In some embodiments, the service controller **122** performs some or all of these rules engine based functions, as described herein, and communicates with the central billing interface **127**. In some embodiments, the service controller **122** performs some or all of these rules engine based functions, as described herein, and communicates with the central billing system **123**.

In some embodiments, duplicate CDRs are sent from the network equipment to the billing system **123** that is used for generating service billing. In some embodiments, duplicate CDRs are filtered to send only those CDRs/records for devices controlled by the service controller and/or service processor (e.g., the managed devices). For example, this approach can provide for the same level of reporting, lower level of reporting, and/or higher level of reporting as compared to the reporting required by the central billing system **123**.

In some embodiments, a bill-by-account billing offset is provided. For example, bill-by-account billing offset information can be informed to the central billing system **123** by providing a CDR aggregator feed that aggregates the device based service usage data feed to provide a new set of CDRs for the managed devices to the central billing interface **127** and/or the central billing system **123**. In some embodiments, transaction billing is provided using similar techniques. For example, transaction billing log information can be provided to the central billing interface **127** and/or the central billing system **123**.

In some embodiments, the rules engine (e.g., performed by the service usage **118** or another network element, as described herein) provides a bill-by-account billing offset. For example, device generated usage information (e.g., charging data records (CDRs)) includes a transaction type field (e.g., indicating a type of service for the associated service usage information). The rules engine can apply a rule or a set of rules based on the identified service associated with the device generated usage information to determine a bill-by-account billing offset (e.g., a new CDR can be generated to provide the determined bill-by-account billing offset). In some examples, the determined bill-by-account billing offset can be provided as a credit to the user's service usage account (e.g., a new CDR can be generated with a negative offset for the user's service usage account, such as for network chatter service usage, or transactional service usage, or for any other purposes based on one or more rules performed by the rules engine).

As another example, for a transactional service, a first new CDR can be generated with a negative offset for the user's service usage account for that transactional service related usage, and a second new CDR can be generated with a positive service usage value to charge that same service usage to the transactional service provider (e.g., Amazon, eBay, or another transactional service provider). In some embodiments, the service controller **122** generates these two new CDRs, and the service usage **118** stores, aggregates, and communicates these two new CDRs to the central billing interface **127**. In some embodiments, the service controller **122** generates these two new CDRs, and the service usage **118** stores, aggregates, and communicates these two new CDRs to the central billing interface **127**, in which the central billing

interface **127** applies rules (e.g., performs the rules engine for determining the bill-by-account billing offset).

In some embodiments, the service controller **122** sends the device generated CDRs to the rules engine (e.g., service usage **118**), and the rules engine applies one or more rules, such as those described herein and/or any other billing/service usage related rules as would be apparent to one of ordinary skill in the art. In some embodiments, the service controller **122** generates CDRs similar to other network elements, and the rules (e.g., bill-by-account) are performed in the central billing interface **127**. For example, for the service controller **122** to generate CDRs similar to other network elements, in some embodiments, the service controller **122** is provisioned on the wireless network and behaves substantially similar to other CDR generators on the network) as would be apparent to one of ordinary skill in the art.

In some embodiments, the service controller **122** is provisioned as a new type of networking function that is recognized as a valid and secure source for CDRs by the other necessary elements in the network (e.g., the Service Usage History/CDR Aggregation and Mediation Server **118**). In some embodiments, in which the network apparatus typically only recognize CDRs from certain types of networking equipment (e.g., RAN Gateway **410** or Transport Gateway **420** (as shown in FIG. **3**)), then the Service Controller **122** can provide authentication credentials to the other networking equipment that indicate it is one of the approved types of equipment (e.g., for purposes of generating/providing CDRs). In some embodiments, the link between the Service Controller **122** and the necessary CDR aggregation and mediation equipment is secured, authenticated, encrypted and/or signed.

In some embodiments, the CDR storage, aggregation, mediation, feed **118** discards the network based service usage information (e.g., network based CDRs) received from one or more network elements. In these embodiments, the service controller **122** can provide the device based service usage information (e.g., device based CDRs) to the CDR storage, aggregation, mediation, feed **118** (e.g., the CDR storage, aggregation, mediation, feed **118** can just provide a store, aggregate, and communication function(s)), and the device based service usage information is provided to the central billing interface **127** or the central billing system **123**.

In some embodiments, the device based CDRs and/or new CDRs generated based on execution of a rules engine as described herein is provided only for devices that are managed and/or based on device group, service plan, or any other criteria, categorization, and/or grouping.

FIG. **2** illustrates another wireless network architecture for providing device assisted CDR creation, aggregation, mediation and billing in accordance with some embodiments. As shown in FIG. **2**, some devices **100** are in communication with DOCSIS Head End **125** and some devices **100** are in communication with DSLAM **125**, which are in communication with the central provider access network **109**.

FIG. **3** illustrates another wireless network architecture for providing device assisted CDR creation, aggregation, mediation and billing in accordance with some embodiments. Referring now to the 4G/3G/2G access network as shown in FIG. **3**, the 4G/3G and 3G/2G base stations/nodes **125** are in communication with a 4G/3G/2G Radio Access Network (RAN) gateway **410** via a radio access network **405**, which are in communication with a 4G/3G/2G transport gateway **420** via an access transport network **415**. The central provider core network **110** is in network communication with the access transport network **415** (e.g., via a dedicated/leased line, and as shown, via a firewall **124**). The Internet, data, and/or phone network **120** is available via a firewall **124** and the transport gateway(s) **420**, as shown. Also, as shown, a network apparatus provisioning system **160**, order management **180**, and subscriber management **182** are in communication with the central provider core network **110**. As shown, a AAA server **121**, a mobile wireless center/Home Location Register (HLR) **132**, a DNS/DHCP **126**, and CDR storage, aggregation, mediation, feed **118** are also in communication with the access transport network **415**. The central billing system **123** and the central billing interface **127** are shown in communication with the central provider core network **110**.

As shown, FIG. **3** includes a 4G/3G/2G wireless network operated by, for example, a central provider. In some embodiments, each of the wireless devices **100** includes a service processor **115** (as shown), and each service processor connects through a secure control plane link to a service controller **122**. In some embodiments, the network based service usage information (e.g., network generated CDRs) is obtained from Radio Access Network (RAN) gateway(s) **410** and/or transport gateway(s) **420**. In some embodiments, device based service usage information (e.g., device assisted CDRs) are generated by the service processor **115** and/or service controller **122** for some or all of the wireless devices **100** using similar techniques as described herein, and in some embodiments, such device based service usage information (e.g., device assisted CDRs) is sent to the CDR storage, aggregation, mediation, feed **118** (e.g., the CDR storage, aggregation, mediation, feed **118** can just provide a store, aggregate, and communication function(s)), and/or to the central billing interface **127** or the central billing system **123**, as similarly described herein with respect to various embodiments.

FIG. **4** illustrates provisioning of a wireless network for providing device assisted CDR creation, aggregation, mediation and billing in accordance with some embodiments. As shown in FIG. **4**, the provisioning of various network equipment is provided as shown to recognize each other as an authorized source of CDRs (e.g., this can be done manually or in an automated manner). For example, order management **180**, subscriber management, billing interface **127**, billing system **123**, network provisioning system **160**, service controller **122**, access network AAA server **121**, mobile wireless center **132**, and CDR storage, aggregation, mediation feed **118** communicate with each other for such provisioning, which can be implemented using various techniques. In some embodiments, the various network elements are provisioned to recognize device assisted CDRs being generated by the service controller **122**, which, for example, can be provided to the billing interface **127** and/or the billing system **123**. In some embodiments, network generated CDRs are provided by RAN/Access gateway **410**, aggregation/transport gateway **425**, and/or base station controller **125**. In some embodiments, other network elements generate/receive/store device assisted CDRs.

In some embodiments, provisioning of various network equipment is provided to recognize a given device as belonging to a device group that supports a service usage and/or billing plan that relies upon and/or utilizes device assisted CDRs.

In some embodiments, the CDR formats, transaction codes, and CDR transmission destinations are programmed for each device that generates CDRs, including the service controller **122** (e.g., in some embodiments, the service controller **122** is the intermediary for CDRs) and/or service processor **115** (e.g., in some embodiments, the device sends CDRs to network CDR aggregation or billing interface **127**/billing system **123** with no intermediate server function).

While FIGS. **4** through **8** provide various embodiments in the context of wireless 3G/4G networks, it will be apparent to one of ordinary skill in the art that these techniques can similarly be applied to other types of access networks including, for example, WiFi, cable, DSL, fiber, satellite, and/or other networks.

FIG. **5** illustrates a network architecture for providing device assisted CDRs in accordance with some embodiments. As shown, network generated CDRs are sent from various network elements to the CDR storage, aggregation, mediation, feed **118** and the service controller **122**, as shown in dashed lines with arrows in FIG. **5**. In some embodiments, the network generated CDRs are used for verification of device assisted service (DAS) usage and/or billing information. In some embodiments, the network generated CDRs are provided to the service controller **122**, and the service controller **122** implements aggregation and/or mediation rules to examine and, in some cases, aggregate and/or mediate network generated/based CDRs with device assisted/based CDRs.

In some embodiments, device assisted CDRs are sent from the service controller **122** to CDR storage, aggregation, mediation, feed **118** and communicated to the billing system **123**, as shown in solid lines with arrows in FIG. **5**. In some embodiments, CDR storage, aggregation, mediation, feed **118** uses DAS service usage CDRs to augment network generated/based CDRs with bill-by-account transaction codes (e.g., as similarly described herein). In some embodiments, CDR storage, aggregation, mediation, feed **118** implements aggregation and/or mediation rules to account for DAS CDR usage amount in a new bill-by-account transaction code and removes the same service usage amount from the bulk device account transaction code. In some embodiments, a first DAS CDR is sent for the new bill by account transaction code, and a second DAS CDR is sent to be used as a correction (credit) to the main device usage account transaction code, and CDR storage, aggregation, mediation, feed **118** implements the rules to perform this mediation. In some embodiments, a first DAS CDR is used for a given bill-by-account transaction code, and a second DAS CDR is used as the main device account transaction code, in which the service controller **122** (or device) has already implemented the mediation rules so that CDR storage, aggregation, mediation, feed **118** simply passes such DAS CDRs to billing after aggregating them.

FIG. **6** illustrates another network architecture for providing device assisted CDRs in accordance with some embodiments. FIG. **6** also shows the communication of device assisted CDRs and network generated CDRs using solid and dashed lines with arrows, respectively. As shown, in some embodiments, CDR storage, aggregation, mediation, feed **118** sends network based CDRs to service controller **122** for various purposes, such as those previously described herein.

In some embodiments, service controller **122** sends DAS CDRs to billing for various uses by the billing system **123**. In some embodiments, the billing system **123** uses DAS service usage CDRs to augment network based CDRs with bill-by-account transaction codes. In some embodiments, the billing system **123** implements aggregation and/or mediation rules to account for DAS CDR usage amount in a new bill-by-account transaction code and removes the same service usage amount from the bulk device account transaction code. In some embodiments, a first DAS CDR is sent for the new bill by account transaction code, and a second DAS CDR is sent to be used as a correction (credit) to the main device usage account transaction code, and the billing system **123** implements the rules to perform this mediation. In some embodiments, a first DAS CDR is used for a given bill-by-account transaction code, and a second is used as the main device account transaction code, in which the service controller **122** (or device) has already implemented the mediation rules so that the billing system **123** simply passes such DAS CDRs after aggregating them.

FIG. **7** illustrates another network architecture for providing device assisted CDRs in accordance with some embodiments. FIG. **7** also shows the communication of device assisted CDRs and network generated CDRs using solid and dashed lines with arrows, respectively. FIG. **7** is similar to FIG. **6**, except as shown in FIG. **7**, service usage information is passed through the billing interface **127** instead of the billing CDR aggregation interface. For example, the service usage detailed bill-by-account information and offset (credit) information can be formatted as a CDR or can be formatted in a higher level syntax as required by the billing interface **127**.

FIG. **8** illustrates another network architecture for providing device assisted CDRs in accordance with some embodiments. FIG. **8** also shows the communication of device assisted CDRs and network generated CDRs using solid and dashed lines with arrows, respectively. In some embodiments, as shown in FIG. **8**, the central provider need not modify the existing CDR storage, aggregation, mediation, feed **118**, so the additional aggregation and mediation rules discussed above with respect to FIG. **5** are implemented as a new layer of rules in a new network function, shown as secondary DAS CDR aggregation mediation **118**A, that is located between the billing system and the CDR storage, aggregation, mediation, feed **118**. For example, this new network function (e.g., secondary DAS CDR aggregation mediation **118**A) can reside in the network (as shown) or in the service processor **115**, in the service controller **122**, or elsewhere in the network or on the device. In some embodiments, the CDRs described herein include QoS tagging information specifying the QoS level for the service usage. In these embodiments, a service controller (e.g., or other network element providing similar functions for this purpose) is used to provide a centralized function to collect and organize QoS tagged charging records and aggregate, format and/or mediate those records into a format that is compatible with and can be processed by a billing system. In some embodiments, a service controller is used for collection, mediation, and/or transmission to billing of device assisted charging records that include charging level.

In some embodiments, charging records that include QoS tags are used to verify QoS policy adherence in the device. In some embodiments, charging records that include QoS tags are used to verify QoS policy adherence in other network elements (e.g., proxy router or server, other network elements that reserve, establish, provision or control QoS channels). In some embodiments, the QoS policies being verified are one or more of QoS level authorization policy, QoS request policy, QoS reservation policy, QoS provisioning policy, QoS control policy, QoS charging or accounting policy, QoS billing policy, QoS roaming policy, and/or QoS notification policy.

In some embodiments, a service controller (e.g., or other network element providing similar functions for this purpose) is used for collection, aggregation and/or transmission of QoS tagged usage records for the purpose of displaying to a user interface to inform a user of status of QoS related charging, accounting, service plan and/or billing. In some embodiments, the user interface is a device user interface. In some embodiments, the user interface is an web site user interface.

In some embodiments, a service controller (e.g., or other network element providing similar functions for this purpose) is used for collection, aggregation, and/or transmission of QoS tagged usage records for the purpose of synchronizing a

user interface to inform a user of status of QoS related charging, accounting, service plan, and/or billing.

FIG. **9** 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, data, and/or phone network **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 will be apparent, 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, the functional elements shown in FIG. **9** are described below with respect to FIGS. **10** and **11**.

As shown in FIG. **9**, service processor **115** includes a service control device link **1691**. For example, as device based service control techniques involving supervision across a network become more sophisticated, it becomes increasingly important to have an efficient and flexible control plane communication link between the device agents and the network elements communicating with, controlling, monitoring, or verifying service policy. In some embodiments, the service control device link **1691** provides the device side of a system for transmission and reception of service agent to/from network element functions. In some embodiments, the traffic efficiency of this link is enhanced by buffering and framing multiple agent messages in the transmissions. In some embodiments, the traffic efficiency is further improved by controlling the transmission frequency or linking the transmission frequency to the rate of service usage or traffic usage. In some embodiments, one or more levels of security or encryption are used to make the link robust to discovery, eavesdropping or compromise. In some embodiments, the service control device link **1691** also provides the communications link and heartbeat timing for the agent heartbeat function. As discussed below, various embodiments disclosed herein for the service control device link **1691** provide an efficient and secure solution for transmitting and receiving service policy implementation, control, monitoring and verification information with other network elements.

As shown in FIG. **9**, 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. **9**, and, in some embodiments, this control plane communication link provides for a secure (e.g., encrypted) communications link for providing secure, bidirectional communications between the service processor **115** and the service controller **122**. In some embodiments, the service control server link **1638** provides the network side of a system for transmission and reception of service agent to/from network element functions. In some embodiments, the traffic efficiency of this link is enhanced by buffering and framing multiple agent messages in the transmissions (e.g., thereby reducing network chatter). In some embodiments, the traffic efficiency is further improved by controlling the transmission frequency and/or linking the transmission frequency to the rate of service usage or traffic usage. In some embodiments, one or more levels of security and/or encryption are used to secure the link against potential discovery, eavesdropping or compromise of communications on the link. In some embodiments, the service control server link **1638** also provides the communications link and heartbeat timing for the agent heartbeat function.

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 SSH version 1 or 2 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.

As shown in FIG. **9**, 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.

In some embodiments, the access control integrity server **1654** (and/or some other agent of service controller **122**) acts on access control integrity agent **1694** reports and error conditions. Many of the access control integrity agent **1654** checks can be accomplished by the server. For example, the access control integrity agent **1654** checks include one or more of the following: service usage measure against usage range consistent with policies (e.g., usage measure from the network and/or from the device); configuration of agents; operation of the agents; and/or dynamic agent download.

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 or CDRs, 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.

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. 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.

As shown in FIG. **9**, service controller **122** includes a service history server **1650**. In some embodiments, the service history server **1650** collects and records service usage or service activity reports from the Access Network AAA Server **1621** and the Service Monitor Agent **1696**. For example, although service usage history from the network elements can in certain embodiments be less detailed than service history from the device, the service history from the network can provide a valuable source for verification of device service policy implementation, because, for example, it is extremely difficult for a device error or compromise event on the device to compromise the network based equipment and software. For example, service history reports from the device can include various service tracking information, as similarly described above. In some embodiments, the service history server **1650** provides the service history on request to other servers and/or one or more agents. In some embodiments, the service history server **1650** provides the service usage history to the device service history **1618**. In some embodiments, for purposes of facilitating the activation tracking service functions (described below), the service history server **1650** maintains a history of which networks the device has connected to. For example, this network activity summary can include a summary of the networks accessed, activity versus time per connection, and/or traffic versus time per connection. As another example, this activity summary can further be analyzed or reported to estimate the type of service plan associated with the traffic activity for the purpose of bill sharing reconciliation.

As shown in FIG. **9**, 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.

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.

As shown in FIG. **9**, 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.

As shown in FIG. **9**, 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.

As shown in FIG. **9**, service controller **122** includes a service download control server **1660**. In some embodiments, the service download control server **1660** provides a down-

load 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.

As shown in FIG. **9** 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.

As shown in FIG. **9**, 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**).

As shown in FIG. **9**, 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.

As shown in FIG. **9**, 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**.

As shown in FIG. **9**, in some embodiments, modem selection and control **1811** selects the access network connection and is in communication with the modem firewall **1655**, and modem drivers **1831**, **1815**, **1814**, **1813**, **1812** convert data traffic into modem bus traffic for one or more modems and are in communication with the modem selection and control **1811**. 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 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.

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 from the device **100**). In some embodiments, the bill by account service can also track the transactions and, in some embodiments, advertisements for the purpose of revenue sharing, all using the service monitoring capabilities disclosed herein. After initiating services with the free ambient service discussed above, the user may later choose a post-pay monthly Internet, email and SMS service. In this case, the service controller **122** would obtain from the billing system **123** in the case of network based billing (or in some embodiments, the service controller **122** billing event server **1622** in the case of device based billing) the billing plan code for the new Internet, email and SMS service. In some embodiments, this code is cross referenced in a database (e.g., the policy management server **1652**) to find the appropriate service profile for the new service in combination with the initial ambient service. The new superset service profile is then applied so that the user maintains free access to the ambient services, and the billing partners continue to subsidize those services, the user also gets access to Internet services and may choose the service control profile (e.g., from one of the embodiments disclosed herein). The superset profile is the profile that provides the combined capabilities of two or more service profiles when the profiles are applied to the same device **100** service processor. In some embodiments, the device **100** (service processor **115**) can determine the superset profile rather than the service controller **122** when more than one "stackable" service is selected by the user or otherwise applied to the device. The flexibility of the service processor **115** and service controller **122** embodiments described herein allow for a large variety of service

profiles to be defined and applied individually or as a superset to achieve the desired device **100** service features.

As shown in FIG. **9**, 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. **9**, 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. In some embodiments, an application interface agent (not shown) 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. In some embodiments, an application interface agent (not shown) is in communication with various applications, including a TCP application **1604**, an IP application **1605**, and a voice application **1602**.

In some embodiments, device assisted services (DAS) techniques for providing an activity map for classifying or categorizing service usage activities to associate various monitored activities (e.g., by URL, by network domain, by website, by network traffic type, by application or application type, and/or any other service usage activity categorization/classification) with associated IP addresses are provided. In some embodiments, a policy control agent (not shown), service monitor agent **1696**, or another agent or function (or combinations thereof) of the service processor **115** provides a DAS activity map. In some embodiments, a policy control agent, service monitor agent, or another agent or function (or combinations thereof) of the service processor provides an activity map for classifying or categorizing service usage activities to associate various monitored activities (e.g., by Uniform Resource Locator (URL), by network domain, by website, by network traffic type, by application or application type, and/or any other service usage activity classification/categorization) with associated IP addresses. In some embodiments, a policy control agent, service monitor agent, or another agent or function (or combinations thereof) of the service processor determines the associated IP addresses for monitored service usage activities using various techniques to snoop the DNS request(s) (e.g., by performing such snooping techniques on the device **100** the associated IP addresses can be determined without the need for a network request for a reverse DNS lookup). In some embodiments, a policy control agent, service monitor agent, or another agent or function (or combinations thereof) of the service processor records and reports IP addresses or includes a DNS lookup function to report IP addresses or IP addresses and associated URLs for monitored service usage activities. For example, a policy control agent, service monitor agent, or another agent or function (or combinations thereof) of the service processor can determine the associated IP addresses for monitored service usage activities using various techniques to perform a DNS lookup function (e.g., using a local DNS cache on the monitored device **100**). In some embodiments, one or more of these techniques are used to dynamically build and maintain a DAS activity map that maps, for example, URLs to IP addresses, applications to IP addresses, content types to IP addresses, and/or any other categorization/classification to IP addresses as applicable. In some embodiments, the DAS activity map is used for various DAS traffic control and/or throttling techniques as described herein with respect to various embodiments. In some embodiments, the DAS activity map is used to provide the user various UI related information and notification techniques related to service usage as described herein with respect to various embodiments. In some embodiments, the DAS activity map is used to provide service usage monitoring, prediction/estimation of future service usage, service usage billing (e.g., bill by account and/or any other service usage/billing categorization techniques), DAS techniques for ambient services usage monitoring, DAS techniques for generating micro-CDRs (e.g., also referred to as service usage partition, service usage recording partition, service charging bucket, device generated CDRs, such as in the case where the device and not a network component are generating the usage records, ambient usage records, specialized service usage records, or other terms to indicate a service usage data record generated to provide a more refined or detailed breakdown of service usage for the device), and/or any of the various other DAS related techniques as described herein with respect to various embodiments.

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**. 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 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. 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.

FIG. **10** provides a table summarizing various service processor **115** functional elements in accordance with some embodiments. Many of these agents are similarly described above, and the table shown in FIG. **10** is 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 FIG. **10** is provided as a summary aid in understanding the basic functions of each agent in accordance with some embodiments, and how the agents interact with one another, with the service controller server elements, and/or with other network functions in certain embodiments to form a reliable device based service delivery solution and/or platform.

FIG. **11** provides a table summarizing various service controller **122** functional elements in accordance with some

embodiments. Many of these agents/elements are similarly described above, and the table shown in FIG. **11** 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. **11** 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.

FIG. **12** illustrates a device stack providing various service usage measurement from various points in the networking stack for a service monitor agent, a billing agent, and an access control integrity agent to assist in verifying the service usage measures and billing reports in accordance with some embodiments. As shown in FIG. **12**, 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, 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. 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.

In some embodiments, the service monitor agent and/or other agents implement virtual traffic tagging by tracking or tracing packet flows through the various communication stack formatting, processing and encryption steps, and providing the virtual tag information to the various agents that monitor, control, shape, throttle or otherwise observe, manipulate or modify the traffic. This tagging approach is referred to herein as virtual tagging, because there is not a literal data flow, traffic flow or packet tag that is attached to flows or packets, and the book-keeping to tag the packet is done through tracking or tracing the flow or packet through the stack instead. In some embodiments, the application interface and/or other agents identify a traffic flow, associate it with a service usage activity and cause a literal tag to be attached to the traffic or packets associated with the activity. This tagging approach is referred to herein as literal tagging. There are various advantages with both the virtual tagging and the literal tagging approaches. For example, it can be preferable in some embodiments, to reduce the inter-agent communication required to track or trace a packet through the stack processing by assigning a literal tag so that each flow or packet has its own activity association embedded in the data. As another example, it can be preferable in some embodiments, to re-use portions of standard communication stack software or components, enhancing the verifiable traffic control or service control capabilities of the standard stack by inserting additional processing steps associated with the various service agents and monitoring points rather than re-writing the entire stack to correctly process literal tagging information, and in such cases, a virtual tagging scheme may be desired. As yet another example, some standard communication stacks provide for unused, unspecified or otherwise available bit fields in a packet frame or flow, and these unused, unspecified or otherwise available bit fields can be used to literally tag traffic without the need to re-write all of the standard communication stack software, with only the portions of the stack that are added to enhance the verifiable traffic control or service control capabilities of the standard stack needing to decode and use the literal tagging information encapsulated in the available bit fields. In the case of literal tagging, in some embodiments, the tags are removed prior to passing the packets or flows to the network or to the applications utilizing the stack. In some embodiments, the manner in which the virtual or literal tagging is implemented can be developed into a communication standard specification so that various device or service product developers can independently develop the communication stack and/or service processor hardware and/or software in a manner that is compatible with the service controller specifications and the products of other device or service product developers.

It will be appreciated that although the implementation/use of any or all of the measurement points illustrated in FIG. **12** is not required to have an effective implementation, such as was similarly shown with respect to various embodiments described herein, 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 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).

Referring to FIG. **12**, describing the device communications stack from the bottom to the top of the stack as shown, the device communications stack provides a communication layer for each of the modems of the device at the bottom of the device communications stack. Example measurement point VI resides within or just above the modem driver layer. For example, the modem driver performs modem bus communications, data protocol translations, modem control and configuration to interface the networking stack traffic to the modem. As shown, measurement point VI is common to all modem drivers and modems, and it is advantageous for cer-

tain embodiments to differentiate the traffic or service activity taking place through one modem from that of one or more of the other modems. In some embodiments, measurement point VI, or another measurement point, is located over, within or below one or more of the individual modem drivers. The respective modem buses for each modem reside between example measurement points V and VI. In the next higher layer, a modem selection & control layer for multimode device based communication is provided. In some embodiments, this layer is controlled by a network decision policy that selects the most desirable network modem for some or all of the data traffic, and when the most desirable network is not available the policy reverts to the next most desirable network until a connection is established provided that one of the networks is available. In some embodiments, certain network traffic, such as verification, control, redundant or secure traffic, is routed to one of the networks even when some or all of the data traffic is routed to another network. This dual routing capability provides for a variety of enhanced security, enhanced reliability or enhanced manageability devices, services or applications. In the next higher layer, a modem firewall is provided. For example, the modem firewall provides for traditional firewall functions, but unlike traditional firewalls, in order to rely on the firewall for verifiable service usage control, such as access control and security protection from unwanted networking traffic or applications, the various service verification techniques and agents described herein are added to the firewall function to verify compliance with service policy and prevent tampering of the service controls. In some embodiments, the modem firewall is implemented farther up the stack, possibly in combination with other layers as indicated in other Figures. In some embodiments, a dedicated firewall function or layer is provided that is independent of the other processing layers, such as the policy implementation layer, the packet forwarding layer and/or the application layer. In some embodiments, the modem firewall is implemented farther down the stack, such as within the modem drivers, below the modem drivers, or in the modem itself. Example measurement point IV resides between the modem firewall layer and an IP queuing and routing layer. As shown, an IP queuing and routing layer is separate from the policy implementation layer where the policy implementation agent implements a portion of the traffic control and/or service usage control policies. As described herein, in some embodiments, these functions are separated so that a standard network stack function can be used for IP queuing and routing, and the modifications necessary to implement the policy implementation agent functions can be provided in a new layer inserted into the standard stack. In some embodiments, the IP queuing and routing layer is combined with the traffic or service usage control layer. For example, a combined routing and policy implementation layer embodiment can also be used with the other embodiments, such as shown in FIG. **12**. 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. **12**.

As shown in FIG. **12**, the application service interface layer is above the standard networking stack API and, in some embodiments, its function is to monitor and in some cases intercept and process the traffic between the applications and the standard networking stack API. In some embodiments, the application service interface layer identifies application traffic flows before the application traffic flows are more difficult or practically impossible to identify farther down in the stack. In some embodiments, the application service interface layer in this way assists application layer tagging in both the virtual and literal tagging cases. In the case of upstream traffic, the application layer tagging is straight forward, because the traffic originates at the application layer. In some downstream embodiments, where the traffic or service activity classification relies on traffic attributes that are readily obtainable, such as source address or URL, application socket address, IP destination address, time of day or any other readily obtained parameter, the traffic type can be identified and tagged for processing by the firewall agent or another agent as it initially arrives. In other embodiments, as described herein, in the downstream case, the solution is generally more sophisticated when a traffic parameter that is needed to classify the manner in which the traffic flow is to be controlled or throttled is not readily available at the lower levels of the stack, such as association with an aspect of an application, type of content, something contained within TLS, IPSEC or other secure format, or other information associated with the traffic. Accordingly, in some embodiments, the networking stack identifies the traffic flow before it is fully characterized, categorized or associated with a service activity, and then passes the traffic through to the application interface layer where the final classification is completed. In such embodiments, the application interface layer then communicates the traffic flow ID with the proper classification so that after an initial short traffic burst or time period the policy implementation agents can properly control the traffic. In some embodiments, there is also a policy for tagging and setting service control policies for traffic that cannot be fully identified with all sources of tagging including application layer tagging.

As shown in FIG. **12**, a service monitor agent, which is also in communication with the agent communication bus **1630**, communicates with various layers of the device communications stack. For example, the service monitor agent, performs monitoring at each of measurement points I through VI, receiving information including application information, service usage and other service related information, and assignment information. An access control integrity agent is in communication with the service monitor agent via the agent communications bus **1630**, as also shown.

FIG. **13** illustrates an embodiment similar to FIG. **12** in which some of the service processor is implemented on the modem and some of the service processor is implemented on the device application processor 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. **13** 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. **13** can be motivated by the advantages of including some or all of the service processor network communication stack processing and/or some or all of the other service agent func-

tions 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.

Referring to FIG. **13**, describing the device communications stack from the bottom to the top of the stack as shown, the device communications stack provides a communication layer for modem MAC/PHY layer at the bottom of the device communications stack. Measurement point IV resides above the modem MAC/PHY layer. The modem firewall layer resides between measurement points IV and III. In the next higher layer, the policy implementation agent is provided, in which the policy implementation agent is implemented on the modem (e.g., on modem hardware). Measurement point II resides between the policy implementation agent and the modem driver layer, which is then shown below a modem bus layer. The next higher layer is shown as the IP queuing and routing layer, followed by the transport layer, including TCP, UDP, and other IP as shown. The session layer resides above the transport layer, which is shown as a socket assignment and session management (e.g., basic TCP setup, TLS/SSL) layer. The network services API (e.g., HTTP, HTTPS, FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), POP3, DNS) resides above the session layer. Measurement point I resides between the network services API layer and an application layer, shown as application service interface agent in the device communications stack of FIG. **13**.

FIG. **14** illustrates various embodiments of intermediate networking devices that include a service processor for the purpose of verifiable service usage measurement, reporting, and billing reports in accordance with some embodiments. For example, FIGS. **14**(A) through **14**(E) 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**.

In some embodiments, device **100** includes a 3G and/or 4G network access connection in combination with the Wi-Fi LAN connection to the device **100**. For example, the intermediate device or networking device combination can be a device that simply translates the Wi-Fi data to the WWAN access network without implementing any portion of the service processor **115** as shown in FIG. **14**(A). 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.

Referring now to FIGS. **14**(B)-(D), in some embodiments, the service processors **115** are implemented in part or in whole on the intermediate modem or networking device combination. In the case where the service processor **115** is implemented in part or in whole on the intermediate modem or networking device combination, the service processor **115** can be implemented for each device or each user in the network so that there are multiple managed service provider accounts all gaining access through the same intermediate modem or networking device combination. In some embodiments, the functions of service processor **115** are implemented on an aggregate account that includes the WWAN access network traffic for all of the users or devices connected to the Wi-Fi LAN serviced by the intermediate modem or networking device combination. In some embodiments, the central provider can also provide an aggregated account service plan, such as a family plan, a corporate user group plan and/or an instant hotspot plan. In the case where there is one account for the intermediate modem or networking device combination, the intermediate modem or networking device combination can implement a local division of services to one or more devices **100** or users in which the services are controlled or managed by the intermediate modem or networking device combination or the device **100**, but the management is not subject to service provider control and is auxiliary to the service management or service policy implementation performed by service processors **115**. In some embodiments, another service model can also be supported in which there is an aggregate service provider plan associated with one intermediate modem or networking device combination, or a group of intermediate modems or networking device combinations but where each user or device still has its own service plan that is a sub-plan under the aggregate plan so that each user or device has independent service policy implementation with a unique instantiation of service processor **115** rather than aggregate service policy implementation across multiple users in the group with a single instantiation of service processor **115**.

As shown in FIG. **14**(B), in some embodiments, device **100** includes a Wi-Fi modem, a Wi-Fi modem combined with a 3G and/or 4G WWAN modem 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. Similarly, as shown in FIG. **14**(C), 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 FIG. **14**(D), USB, Ethernet, Bluetooth, or another LAN or point to point connection from device **100** to the intermediate modem or networking device combination **1510**, or a femto cell modem and DSL/cable/T1/other combination as shown in FIG. **14**(E).

FIG. **15** illustrates a wireless network architecture for providing device assisted CDR creation, aggregation, mediation and billing including a proxy server(s) **270** in accordance with some embodiments. As shown, FIG. **2** includes a proxy server(s) **270** in communication with a 4G/3G/2G wireless network operated by, for example, a central provider. For example, the

proxy server(s) **270** can be used to implement and/or assist in providing various techniques described herein, such as service usage measurement and/or other techniques as described herein.

FIG. **16** illustrates a wireless network architecture for providing device assisted CDR creation, aggregation, mediation and billing including a service provider network in accordance with some embodiments, involving one or more of service controllers, service processors and/or proxy server/routers. This diagram illustrates the connections and flows for the provisioning system, new subscriber activation system and order system with the equipment functions having similar or identical embodiments as described in the context of FIG. **4** except in this case one or more proxy server/routers **270** are included for embodiments as described herein.

While the specific illustrations in FIGS. **16** through **18** and associated descriptions refer to a the wireless 3G/4G network, it will be apparent to one of ordinary skill in the art that these techniques can similarly be applied to other types of access networks including, for example, WiFi, cable, DSL, fiber, satellite, and/or other networks. It will also now be apparent to one of ordinary skill in the art that in the context of the proxy server/router embodiments illustrated in FIGS. **16** through **18** that many other embodiments are possible for the CDR (or FDR, start/stop records, interim accounting records, IPDRs, micro-CDR or service charging bucket accounting) recording, reporting, aggregating, mediating and/or synchronizing usage records within the various network elements and/or device elements.

FIG. **17** illustrates a wireless network architecture for providing device assisted CDR creation, aggregation, mediation and billing including a service provider network in accordance with some embodiments, involving one or more of service controllers, service processors and/or proxy server/routers. This diagram illustrates the connections and flows for the charging system with the equipment functions having similar or identical embodiments as described in the context of FIGS. **4** through **8** except in this case one or more proxy server/routers **270** are included for embodiments as described herein. The charging flows are illustrated by three line types: solid lines for device generated CDRs and proxy server/router generated CDRs, dashed lines for network equipment generated CDRs, and double dot-dash line types for CDRs that have been mediated by a service controller **120** and/or mediation system **118**.

FIG. **18** illustrates a wireless network architecture for providing device assisted CDR creation, aggregation, mediation and billing including a service provider network in accordance with some embodiments, involving one or more of service controllers and/or proxy server/routers. This diagram illustrates the connections and flows for the charging system with the equipment functions having similar or identical embodiments as described in the context of FIG. **17** except in this case there is no service processor CDR feed and only CDR feeds from the network equipment and the proxy server/routers. The charging flows are illustrated by three line types: solid lines for proxy server/router generated CDRs, dashed lines for network equipment generated CDRs, and double dot-dash line types for CDRs that have been mediated by a service controller **120** and/or mediation system **118**.

In some embodiments, the proxy server is used for one or more of the functions of: generating, collecting, aggregating, mediating and/or reporting service usage charging information. In some embodiments, the proxy server/router is used for one or more of collecting, aggregating, mediating and/or reporting service usage charging information in which a client device service processor assists in routing traffic to and/or from the proxy server. In some embodiments, the proxy server is used for one or more of the functions of: generating, collecting, aggregating, mediating and/or reporting service usage charging information and the policies controlling the device service processor and the proxy servers are coordinated and distributed by a service controller. In some embodiments, the proxy server/router is used for one or more of: collecting, aggregating, mediating and/or reporting service usage charging information where a client device service processor assists in routing traffic to and/or from the proxy servers and the service processors are coordinated and distributed by a service controller. In some embodiments, in which the proxy server is used in conjunction with a device service processor (e.g., or other client function), the service processor detects one or more types of ambient service activity or other special service activity and routes the traffic to the appropriate proxy server destination for that activity.

In some embodiments, one or more proxy servers or routers are used for one or more of: generating, collecting, aggregating, mediating and/or reporting service usage charging information in which the proxy server communicates with a client device UI for the purpose of informing the user of service status and/or receiving user feedback on service status.

In some embodiments, one or more proxy servers or routers are used for controlling service usage in accordance with a set of policies for specialized services that are programmed by a service design UI (VSP Interface **4910**). In some embodiments, one or more proxy servers or routers are used for controlling service usage in accordance with a set of policies for specialized services that are programmed by a network element with a service design UI, and the policies controlling the device service processor and the proxy server are coordinated and distributed by a service controller.

In some embodiments, one or more proxy servers or routers are used for one or more of generating, collecting, aggregating, mediating and/or reporting service usage charging information in which a client device service processor assists in routing traffic to and/or from the proxy server and the policies controlling the device service processor and the proxy server are coordinated and distributed by a service controller.

In some embodiments, the proxy servers can be distributed and managed across diverse geographical separations so that the device traffic to the proxy server/routers does not need to traverse long distances before being connected through the proxy server/routers to the Internet, data, or phone network **120**. For example, this geographic diversity or redundancy can be accomplished in a number of ways including using a redundant server or router architecture with a load balancer to determine the best hop to the nearest equipment location, coupled with a distributed data base to persist the device service state so that if a proxy server/router element goes down the device service may be effectively resumed by a different proxy server/router in the same data center or in a geographically diverse data center. In some embodiments, the device service state is persisted in this way by a distributed or redundant diversity data base. In some embodiments, the device service state is held by the service controller network, which in some embodiments, are also distributed and/or redundant. In some embodiments, the device service state is persisted by other network equipment elements. In some embodiments, the device service state is persisted by the device client software (e.g., service processor).

In some embodiments, it may not be possible to accurately identify every network service access attempt or service usage (e.g., or traffic access) as belonging to a given service

usage partition (e.g., a given ambient service usage, background network chatter usage, user service plan usage, emergency service usage, and/or other type of service usage). As used herein, the terms service usage partition, service usage recording partition, service charging bucket, and micro-CDRs are used interchangeably. Accordingly, it is desirable to provide a service charging bucket for traffic that is allowed and not definitively identified as belonging to a known service charging bucket. This allows for techniques to employ an "allow but verify" approach to traffic that is likely to be legitimately associated with an ambient service or a user service or a network service that is intended to be allowed, but is not definitively identified as being associated with an allowed service.

As an example, there may be a web site access associated with an ambient service that does not have a reference identifier or other traffic parameter that allows the service processor to associate it with the correct ambient service. In this case, a set of rules can be applied to determine if it is likely that the web site access is a legitimate access given the access control policies that are in place, and if it is the access can be allowed and the traffic usage either recorded in the ambient service charging bucket that it is suspected to be associated with, or the traffic usage can be charged to a network chatter service usage bucket, or the traffic usage can be charged to the user service usage bucket, or the traffic usage may be recorded in a "not classified but allowed" service charging bucket. In some embodiments, in which such traffic is charged to the "not classified but allowed" service usage charging bucket, additional verification measures are employed to ensure that the amount of traffic that is not classified but allowed does not grow too large or become a back-door for service usage errors. For example, the access control policy rules for allowing unclassified traffic can be relatively loose as long as the amount of service usage charges accumulating in the not classified charging bucket remains within certain bounds, and/or the rate of service usage charged to the not classified bucket remains within certain bounds, but if the not classified traffic becomes large or the rate of not classified traffic growth becomes large then the rules governing when to allow not classified traffic can be tightened.

As another example, a browser application can access a web site that is known to be an ambient service website, and that web site might serve back a series of traffic flows, some of which are associated with the ambient service website through URL identifiers that are known to be part of the website, and other traffic can be associated with the ambient service website by virtue of a referring website tag or header, and some traffic can be returned to the same application with a relatively close time proximity to the other traffic as being identified as ambient traffic. In this example, as long as the not classified traffic service charging bucket does not exceed a given pre-set policy limit on its size, and/or does not grow faster than a given pre-set policy rate, and/or is received within a certain pre-set policy period of time difference from the time that other ambient service charging bucket traffic is received, then the not classified traffic is continued to be allowed. However, if the not classified traffic amount or rate of growth exceeds the pre-set policy limits, or if the period of time between when verified ambient service traffic is received and the not classified traffic is received exceeds policy limits, then the not classified traffic can be blocked or other action can be taken to further analyze the not classified traffic.

In some embodiments, it is important to provide a hierarchy of service usage charging rules for the various service usage partitions on a device. As an example, for a given service plan there can be two ambient service charging buckets, a network chatter (e.g., or network overhead) service charging bucket, and a user service plan service charging bucket and it is desirable to make sure that no ambient services or network overhead service or unclassified service is charged to the user service plan, and it is also desirable to ensure that all known ambient service traffic is charged to the appropriate ambient service partner, and it is desirable to ensure that no network overhead service or unclassified service is charged to ambient service partners. In such situations, a service charging bucket hierarchy can be provided as follows: determine if a traffic flow (e.g., or socket) is associated with network overhead, and if so allow it and charge that service bucket, then determine if a traffic flow (or socket) is associated with ambient service #1, and if so allow it and charge that service bucket, then determine if a traffic flow (or socket) is associated with ambient service #2, and if so allow it and charge that service bucket, then determine if a traffic flow (or socket) is associated with not classified traffic, and if so allow it and charge that service bucket, then if the traffic is not associated with any of the above service charging buckets allow it and charge it to the user service plan charging bucket. In another example, if the user has not yet chosen to pay for a user service plan, then the same hierarchical access control and service charging policy can be used except the final step would be: then if the traffic is not associated with any of the above service charging buckets block the traffic. Hierarchical service charging bucket identification such as depicted in these examples can be a crucial aspect of a robust access control policy and/or service charging policy system. Many other access control policy hierarchies and service charging bucket policy hierarchies will now be apparent to one of ordinary skill in the art.

In some embodiments, the not classified traffic is charged according to service charging rules that rely on the most likely candidate service charging bucket for the traffic. As another example, if the not classified traffic is being delivered to the same application as other known ambient service traffic and the time difference between delivery of the known ambient service traffic and the not classified traffic is small, then the not classified traffic can be charged to the ambient service in accordance with a pre-set charging policy rule specifying these conditions. Other embodiments that will now be apparent to one of ordinary skill in the art. For example, another charging rule for not classified traffic could be to perform a pro-rata allocation of the not classified traffic to all of the other service charging buckets with the pro-rata allocation being based on the percentage of the total traffic used by the device for each service charging bucket. As another example, the not classified traffic can be charged to a subset of the service charging buckets for the device (e.g., all ambient services plus the network overhead service) in accordance with the pro-rata share for each service included in the pro-rata split.

In some embodiments, the user service plan agreement is structured so that the user acknowledges that ambient services in which the access connection to the service is sponsored, paid for, and/or partially subsidized by an entity other than the user are a benefit to the user, and/or the user acknowledges that there is no inherent right to free ambient services, and that the service usage accounting system may not always properly characterize usage for a sponsored or subsidized ambient service (e.g., or some other specialized service) in the correct accounting service charging bucket, and, thus, the user service plan account can be charged and/or billed with some of this traffic. By having the user acknowledge a service use agreement of this form then some ambient traffic can be

charged to the user service plan account, including, for example, allowed but not classified traffic, excess ambient service usage beyond pre-set policy limits, ambient service usage during busy network periods or on congested network resources, and/or other criteria/measures. In some embodiments, the user might be notified that they are being charged for service activities that are sometimes subsidized or free to the user. As discussed above, it is important to ensure that a not classified service charging bucket does not become a back door for service charging errors or hacking. It will now be apparent to one of ordinary skill in the art that the not classified service usage charges can be verified in a variety of manners, including, for example, observing the size of the not classified service charging bucket as compared to other service usage charges on the device (e.g., total device service usage, ambient service usage, user bucket service usage, and/or other criteria/measures), capping the not classified bucket, and/or capping the rate of growth of the not classified bucket.

In some embodiments, it is important to verify not only that the total device service usage amount is correct, but that the service usage is being reported in the proper service charging buckets. For example, if the service processor software can be hacked so that it correctly reports the total service usage, but reports user service plan traffic under one or more ambient service buckets, then simply verifying that the total amount of service usage is correct will not be sufficient to prevent the device from obtaining free user service that can be charged to ambient service partners. There are a variety of direct and indirect embodiments to accomplish this verification of service charging bucket divisions. For example, in direct verification embodiments, one or more alternative measures of service usage are employed to cross-check the accuracy of the service charging bucket divisions. In indirect embodiments one of two classes of verification are employed: the size and rate of growth for service charging buckets is analyzed and compared to a pre-set group of policies to detect and/or modify service charging bucket growth that is out of policy; and/or the proper operation of the service processor elements involved in service charging bucket partitioning is verified.

Various embodiments involving direct verification of service charging bucket usage and/or accounting include the use of network based service usage measures such as CDRs, IPDRs, flow data records (e.g., FDRs—detailed reports of service usage for each service flow, such as network socket connection, opened and used to transmit data to or from the device), accounting records, interim accounting records or other similar usage records to verify that the device is within service policy and/or the device based service usage reports are accurate. Use of such network generated service usage records to directly verify service charging and/or proper service usage policy adherence are described herein. When network address destination and/or source information is available in these records, as described herein, this can be used in some embodiments, to verify the service charging bucket accounting provided by the device service processor. In some embodiments, some types of service usage records include real-time data but not necessarily all of the useful information needed to help verify service charging bucket accounting, while other types of service usage records provide more detail (e.g., IP address for destination and source) but do not always arrive in real-time. For example, in some embodiments, FDRs are created each time a new service flow (e.g., network socket connection) is opened and then closed. At the time the service flow is closed, a (e.g., possibly time stamped) data usage record indicating source address, destination address and amount of data transmitted is created and sent to a charging aggregation function in the network. The charging aggregation function can then forward the FDRs to the service controller for verification or direct accounting of service charging bucket accounting. By comparing the FDR addresses with known ambient service traffic address associations, the partitioning of service charging buckets between one or more ambient services and other services such as a user service plan service charging bucket may be verified. However, in some cases it can be a long period of time for an FDR to be generated when a device service flow (e.g., socket) remains open for a long period of time, as in the case for example with a long file download, a peer to peer connection with a socket keep alive, or a proxy server service with a socket keep alive. In such cases, it can be disadvantageous to have large amounts of data to be transferred without an FDR to confirm device service processor based reports, and in some cases this can provide an opportunity for service processor service reporting hacks. This can be remedied in a variety of ways by using other network reported service usage information to augment the FDR information. For example, start and stop accounting records can sometimes be obtained in some embodiments, from a network element such as a service gateway or the AAA servers (e.g., or other network equipment elements depending on the network architecture). Although start and stop records do not possess the detail of service usage information that FDRs, CDRs, IPDRs, interim accounting records or other service usage records posses, they do inform the service controller that a device is either connected to the network or has stopped connecting. If a device is connected to the network and is not transmitting device usage reports or heartbeats, then the service controller is alerted that an error or hacking condition is likely. As another example of how two or more types of network reported service usage information may be used to create a better real time or near real-time check on device service usage, if both FDRs and start/stop accounting records are available, the service controller can send a stop-then-resume service command to the device (e.g., or alternatively send a stop then resume service command to a network equipment element), which will cause the device to terminate all open service flows before re-initiating them, and once the service flows are stopped then the FDR flow records will be completed and transmitted for any service flows that were in process but unreported when the stop service command was issued. This will cause any long term open socket file transfers to be reported in the FDR flow records thus plugging the potential back door hole in the FDR service usage accounting verification method.

As another example showing how multiple types of network generated service usage accounting records may be used to complement each other and strengthen the verification of service charging bucket accounting partitions, interim data records can be used with FDRs. Interim data records are available in accordance with some embodiments, n which the interim data records are generated on a regularly scheduled basis by a network element (e.g., gateway, base station, HLR, AAA, and/or other network element/function). Interim data records are typically near real time records that report the aggregate traffic usage for the device as of a point in time, but often do not include traffic address information or other traffic details. In embodiments in which both interim accounting records and FDRs are available, when the interim accounting records are indicating service usage that is not being reported in the FDR stream this is evidence that a device has one or more long term socket connections that are open and are not terminating. In this case, the service controller can verify that the device based usage reports are properly accounting for the total amount of service usage reported by the interim accounting records, and/or the service controller can force an FDR

report for the open sockets by issuing a stop-resume service command as similarly discussed above.

As described herein, other embodiments involving direct verification of service charging bucket accounting can be provided. One example is to route ambient service traffic to a proxy server or router programmed to support only the network access allowed for the ambient service and to account for the ambient service usage. Additional proxy servers or routers can be similarly programmed for each ambient service that is part of the device service plan, and in some embodiments, another proxy server or router is programmed to support traffic control and account for the user service plan service access. By comparing the service usage accounting for each of these proxy servers or routers, the device generated service charging bucket accounting can be directly verified. In some embodiments, the usage accounting provided by the proxy servers or routers is used directly for service usage accounting.

In some embodiments, ambient service partner feedback is used to verify service charging bucket accounting. For example, web servers used by ambient service partners to provide ambient services can identify a user device based on header information embedded in the HTML traffic, and then account for either the service used by the device during the ambient service sessions or account for the number of transactions the user completes. If service usage is recorded, then it can be reported to the service controller and be used directly to verify ambient service charging bucket accounting. If transactions are all that are recorded, then this can be reported to the service controller and the amount of ambient service used by the device can be compared with the number of transactions completed to determine if the ambient service usage is reasonable or should be throttled or blocked. It will now be apparent to one of ordinary skill in the art that other embodiments can be provided that employ more than one type of network generated service usage records to verify service usage accounting and/or verify service charging bucket accounting.

Other embodiments involving indirect methods for verifying or controlling service charging bucket accounting include monitoring the size and/or growth rate of ambient service usage. In some embodiments, the access control policy rules call for restricting a given ambient service access when the amount of service usage charges accumulating in the ambient service charging bucket exceed a pre-set policy limit, and/or when the rate of service usage for the ambient service exceeds a pre-set policy limit. For example, once these limits are reached, the ambient service can be throttled back for a period of time, blocked for a period of time, or charged to the user service plan charging bucket. In some embodiments, before these actions are taken the user UI can be used to notify the user of the service policy enforcement action. In some embodiments, indirect verification of service charging bucket accounting includes the various techniques described herein for verifying proper operation of the service processor agent software and/or protecting the service processor agent software from errors, manipulation, or hacking.

In some embodiments, the device service processor directs traffic destined for a given ambient service to a proxy server or router programmed to support that ambient service, and any traffic control policies and/or access control policies for the ambient service are implemented in the proxy server or router. For example, in such embodiments the proxy server or router can be programmed to only allow access to one or more ambient services that are authorized by the device service plan, with the proxy server or router controlling device access so that other network destinations cannot be reached. Continuing this example embodiment, the proxy server or router can account for the ambient service usage in an ambient service charging bucket as discussed elsewhere. In such proxy server or router ambient service control embodiments, the same traffic association techniques described elsewhere that allow incoming traffic associated with an ambient service website or other service to be identified, allowed or blocked, potentially throttled, and accounted for in a service charging bucket can be implemented in the proxy server or router programming. Such proxy server or router embodiments can also implement user service plan service charging buckets, user service plan traffic controls, and user service plan access control as discussed herein. In some embodiments, the proxy server or router analyzes the HTML traffic content of the traffic flows as described herein to perform such associations, traffic control and/or service usage accounting. Similarly, in some embodiments, a proxy server or router can provide the "surf-out" capabilities described herein by performing the same surf-out traffic associations (e.g., HTML branch reference associations and/or other branch associations) described herein. It will now be apparent to one of ordinary skill in the art that many of the adaptive ambient service control and service usage charging functions described herein for a service processor can be readily implemented with a proxy server or router that is appropriately programmed.

In some embodiments, routing of device traffic for one or more ambient services and/or user service plan services to a proxy server or router is accomplished by the device service processor using the device service processor traffic control embodiments described herein. In some embodiments, routing of device traffic for one or more ambient services and/or user service plan services to a proxy server or router is accomplished by dedicated network equipment such as the gateways (e.g., SGSN, GGSN, PDSN, or PDN), home agents, HLRs or base stations, with the network equipment being provisioned by a service controller (e.g., or other interchangeable network element with similar functions for this purpose) to direct the device traffic to the proxy server or router. In some embodiments, the ambient service traffic or the user service plan traffic is controlled by the proxy server according to a service plan policy set supplied by the service controller (e.g., or equivalent network function for this purpose). The traffic control service policy thus implemented by the proxy server can control traffic based on one or more of the following: period of time, network address, service type, content type, application type, QoS class, time of day, network busy state, bandwidth, and data usage.

In some embodiments, a proxy server or router is used to verify accounting for a given service, for example, an ambient service. In some embodiments, this is accomplished by the device service processor directing the desired service flows to a proxy server or router programmed to handle the desired service flows, with the proxy server or router being programmed to only allow access to valid network destinations allowed by the access control policies for the desired service, and the proxy server or router also being programmed to account for the traffic usage for the desired services. In some embodiments, the proxy service usage accounting may then be used to verify device based service usage accounting reported by the service processor. In some embodiments, the accounting thus reported by the proxy server or router can be used directly to account for service usage, such as ambient service usage or user service plan service usage.

In some embodiments, in which a proxy server is used for device service usage accounting, the proxy server maintains a link to the device service notification UI via a secure communication link, such as the heartbeat device link described

herein. For example, the proxy server or router can keep track of device service usage versus service plan usage caps/limits and notify the user device UI through the device communication link (e.g., heartbeat link) between the service controller and the device. In some embodiments, the proxy server/router communicates with a device UI in a variety of ways, such as follows: UI connection through a device link (e.g., heartbeat link), through a device link connected to a service controller (e.g., or other network element with similar function for this purpose), presenting a proxy web page to the device, providing a pop-up page to the device, and/or installing a special portal mini-browser on the device that communicates with the proxy server/router. In some embodiments, the UI connection to the proxy server/router is used as a user notification channel to communicate usage notification information, service plan choices, or any of the multiple services UI embodiments described herein.

In some embodiments, for the proxy server/router techniques for implementing service traffic/access controls and/or service charting bucket accounting, it is desirable to have the same information that is available to the service processor on the device, including, for example, application associated with the traffic, network busy state, QoS level, or other information about the service activity that is available at the device. For example, such information can be used to help determine traffic control rules and/or special services credit is due (e.g., ambient services credit). In some embodiments, information available on the device can be communicated to the proxy server/router and associated with traffic flows or service usage activities in a variety of ways. For example, side information can be transmitted to the proxy server/router that associates a traffic flow or service activity flow with information available on the device but not readily available in the traffic flow or service activity flow itself. In some embodiments, such side information may be communicated over a dedicated control channel (e.g., the device control link or heartbeat link), or in a standard network connection that in some embodiments, can be secure (e.g., TLS/SSL, or a secure tunnel). In some embodiments, the side information available on the device can be communicated to the proxy server/router via embedded information in data (e.g., header and/or stuffing special fields in the communications packets). In some embodiments, the side information available on the device can be communicated to the proxy server/router by associating a given secure link or tunnel with the side information. In some embodiments, the side information is collected in a device agent or device API agent that monitors traffic flows, collects the side information for those traffic flows, and transmits the information associated with a given flow to a proxy server/router. It will now be apparent to one of ordinary skill in the art that other techniques can be used to communicate side information available on the device to a proxy server/router.

For example, just as the hierarchy of charging rules can be important for implementations in which the service processor is creating the service charging bucket accounting, it can also important in implementations that use a proxy server or router for service charging bucket accounting. Accordingly, various embodiments described herein for creating a hierarchy of service usage charging rules can be applied to proxy server or proxy router embodiments. It will be apparent to one of ordinary skill in the art that the service charging bucket embodiments and traffic control and access control embodiments described herein for allowed but not classified buckets apply equally to the proxy server/router embodiments. For example, pre-defined service policy rules can be programmed into the proxy server/router to control the traffic flows and/or place usage limits or access limits on an ambient service, or a user service plan service. It will also now be apparent to one of ordinary skill in the art that the embodiments described herein disclosing an initial allowed service access list, temporarily allowing additional service activities until they are determined to be allowed or not allowed, expanding the allowed service activity list, maintaining a not allowed service activity list and expanding the not allowed service activity list also apply equally to proxy server/router embodiments. Similarly, it will now be apparent to one of ordinary skill in the art that the proxy/server router embodiments can be employed to directly generate the service charging bucket (or micro-CDR) usage reports used to provide further detail and/or billing capabilities for service usage. In some embodiments, in which the device service processor directs traffic to a proxy server/router, there are advantageous design feature embodiments available that can reduce the need to provision network to detect and force specialized device service traffic to the appropriate proxy server/router. For example, this can be done by creating a "usage credit" system for the services supported by the proxy server/outer. Total service usage is counted on the one hand by the device service processor, or by other network equipment, or by both. Credit on the other hand for ambient service or other specialized access service usage that is not charged to the user is then provided for services that the device directs through the proxy server/router destination (e.g., URL or route hop) supporting the particular ambient service or other specialized access service. If the device correctly directs traffic to the proxy server/router, then the counting and/or access rules are correctly implemented by the proxy server/router. The service can be thus controlled and/or accounted for. When the service is accounted for, the proxy server/router reports the service charging bucket accounting back to the service controller (e.g., or other network equipment responsible for service charging bucket/micro CDR mediation) and the user service plan service charging bucket account can be credited for the services. Traffic that reaches the proxy server/router is controlled by the access rules and/or traffic control rules and/or QoS control rules of the proxy server/router programming, so there is no question regarding the type of service that is supported with the service charging buckets that are reported to mediation functions (e.g., mediation functions can be performed by one or more of service controller, usage mediation, billing, AAA, and/or HLR/home agent). As the proxy server/router is in the network and can be physically secured and protected from hacking, there is high confidence that the service control and/or charging rules intended for ambient services or some other specialized service are properly implemented and that the proxy server/router connection is being used for the intended service and not some other unintended hacked service. If the device is somehow hacked or otherwise in error so that the traffic is not directed through the appropriate proxy server/router, then the proxy server/router does not log the traffic in micro CDRs/buckets and no specialized service usage credit is sent to the mediation functions, so there is no usage credit deducted from the device user service plan service usage totals. Thus, the user pays for the services when the device is hacked to avoid the proxy server/router. The user account service agreement can specify that if the user tampers with software and traffic is not routed to servers then credit will not be provided and user plan will be charged.

In some proxy server/router embodiments, the usage credit is sometimes recorded by the proxy server/router detecting which device is performing the access. Device identification can be accomplished in a variety of ways including a header/tag inserted into the traffic by the device, a route in the

network specified for that device, a secure link (e.g., TLS/SSL, IP Sec, or other secure tunnel), a unique device IP address or other credential (e.g., where proxy server/router has access to an active IP address look up function), a unique proxy server/router address and/or socket for the device.

In some embodiments, the coordination of the device service controller traffic control elements with a proxy server/outer can make it simpler to locate, install, provision and operate the proxy servers. The proxy server/routers do not need to be located "in line" with the access network because it is the device's responsibility to make sure the traffic is routed to the servers/routers or else there is not credit and the user account is charged. In some embodiments, this makes it unnecessary or reduces the need to force device traffic routes in carrier network. In some embodiments, the proxy server/routers can be located in carrier network or on the Internet. If the proxy server/routers are on Internet, then traffic can be authenticated in a firewall before being passed to server/routers to enhance security to attack.

In some embodiments, the service charging bucket recording software in the proxy server/router can be programmed into an ambient service partners network equipment directly thus eliminating the need for special apparatus. The ambient service partner's equipment (e.g., a web server, load balancer or router) can recognize the device using one of the techniques described above, aggregate the device service charging bucket accounting, and periodically send the usage accounting to the service controller or other network service usage mediation function.

Programming and/or provisioning the types of ambient services, user service plan services and/or specialized services disclosed in various embodiments described herein can be a complex process. In some embodiments, a simplified central network user or MVNO user programming interface, also referred to herein as a Virtual Service Provider Work Station **4910** or interchangeably as a service design interface or VSP Interface, is used to program the necessary policy settings for such services is desirable. For example, a service design interface (VSP Interface **4910**) is provided that organizes and/or categorizes the various policy settings that are required to set up an ambient service (e.g., or other service) including one or more of the following: a policy list of service activities that are allowed under the ambient service (e.g., or other service), access control policies, rules for implementing and/or adapting an allowed list of network destinations, rules for implementing and/or adapting a blocked list of network destinations, service charging bucket policies, user notification policies, service control, and/or service charging bucket verification policies, actions to be taken upon verification errors. In some embodiments, the required information for one or more of these policy sets is formatted into a UI that organizes and simplifies the programming of the policies. In some embodiments, the UI is partly graphical to help the user understand the information and what settings need to be defined in order to define the service. In some embodiments, the UI is created with an XML interface. In some embodiments, the UI is offered via a secure web connection. In some embodiments, a basic service policy for an ambient service (e.g., or another service) is created that includes one or more of the above service policy settings, and then this service policy set becomes a list or an object that can be replicated and used in multiple service plan policy set definitions (e.g., "dragged and dropped" in a graphical UI). In some embodiments, the resulting set of policies created in this service design interface (VSP Interface **4910**) are then distributed to the necessary policy control elements in the network and/or on the device that act in coordination to implement the service policy set for a given device group. For example, if a service processor is used in conjunction with a service controller, then the service design (VSP Interface **4910**) interface can load the service policy settings subsets that need to be programmed on the service controller and the device service processor into the service controller, and the service controller loads the service controller policy settings subset into the service controller components that control the policies and loads the device policy settings subset to the devices that belong to that device group. In embodiments in which a proxy server/router is used to help control and account for services, in some embodiments, the service design interface (VSP Interface **4910**) loads the service policy settings subsets that need to be programmed on the proxy server/router into the proxy server/router. In embodiments where other network equipment (e.g., gateways, base stations, service usage recording/aggregation/feed equipment, AAA, home agent/HLR, mediation system, and/or billing system) need to be provisioned or programmed, in some embodiments, the service design interface (VSP Interface **4910**) also loads the appropriate device group policy subsets to each of the equipment elements. Accordingly, various techniques can be used as described herein to greatly simplify the complex task of translating a service policy set or service plan into all the myriad equipment and/or device settings, programming, and/or provisioning commands required to correctly implement the service. It will now be apparent to one of ordinary skill in the art that several of these techniques can similarly be used for the VSP service design interface (VSP Interface **4910**). In some embodiments, a service processor is used in conjunction with one or more proxy servers or routers for one or more of QoS charging, QoS provisioning and/or QoS control. In some embodiments, one or more proxy servers or routers are used in conjunction with a service controller (e.g., or other network function with similar functions for this purpose) for one or more of QoS charging, QoS provisioning, and/or QoS control. In some embodiments, a service processor is used in conjunction with one or more proxy servers or routers and a service controller (e.g., or other network function with similar functions for this purpose) for one or more of QoS charging, QoS provisioning, and/or QoS control. In some embodiments, one or more proxy servers or routers are used in conjunction with a service controller (e.g., or other network function with similar functions for this purpose) for one or more of QoS charging, QoS provisioning, and/or QoS control, in which the proxy server or router policies for this QoS service implementation are programmed by a service design UI (VSP Interface **4910**).

FIG. **19** illustrates a wireless network architecture for providing device assisted CDR creation, aggregation, mediation and billing including two service provider networks in accordance with some embodiments. The description of the network equipment element functions is generally identical to the embodiments depicted in other figures, except that one or more service controllers **120** and/or proxy servers/routers **270** and/or service design interfaces (VSP Interface **4910**) are shared between the two networks as described herein. For example, the network equipment, charging record formats, provisioning systems can be similar in the two networks, or may be completely different since in the various embodiments the service controller **120**, service processor **115**, and/or proxy sever router **270** are used to provide unified roaming services, or in some embodiments, to provide common network service features across the different networks.

FIG. **20** illustrates a wireless network architecture for providing device assisted CDR creation, aggregation, mediation and billing including two service provider networks in accor-

dance with some embodiments, involving one or more of service controllers and/or service processors. FIG. **20** is similar to FIG. **19** except that FIG. **20** illustrates that various types of access network technology and equipment can be used on any number of the central provider networks (e.g., 2G/3G/4G cellular wireless plus WiFi is the example in FIG. **19** while 2G/3G/4G cellular wireless plus DSL and cable is the example in FIG. **20**). FIGS. **19** and **20** do not show the access network connections to the central provider #2 core network, but that the second central provider network can have all of or some of the access equipment elements that the first central provider network possesses, or the second central provider network can posses different access network technology and equipment as described herein would be apparent to one of ordinary skill in the art. For example, if any aspect of the 2G/3G/4G technology is different for the two networks, then multi-mode wireless modules can be used in the device modems to allow for access connection using one technology on the first central provider network, and access connection using a second technology on the second central provider network. As many of the techniques and embodiments described herein allow for network service policy implementation at layers above the modem physical layer, modem MAC layer and the access network access control and authorization layers, then any number of multi-mode modem technologies can be employed to bridge connect to either of the two networks while enhancing roaming services or providing unified network services in one or more of the areas of service traffic control, user notification interfaces, charging policies and/or systems, QoS services, instant activation services and/or billing services. It will be apparent to one of ordinary skill in the art that while the discussion herein is for service provider (e.g., central provider, MVNO, VSP, etc) networks, many of the embodiments can similarly be applied to private networks such as, for example, enterprise networks, enterprise WAN solutions and/or remote office solutions, government networks, emergency networks, and/or networks involving intermediate networking devices.

FIG. **21** illustrates a wireless network architecture for providing device assisted CDR creation, aggregation, mediation and billing including two service provider networks in accordance with some embodiments. For example, FIG. **21** includes elements that can be identical or very similar to those described in the context of FIGS. **5** through **8**, except that in FIG. **21** there are two central provider networks in which the CDR reporting and service controls are unified through one or more common service controllers **120** and/or service processors **115**. As shown in FIG. **21**, the charging flows are illustrated by three line types: solid lines for device generated CDRs, dashed lines for network equipment generated CDRs, and double dot-dash line types for CDRs that have been mediated by a service controller **120** and/or mediation system **118**.

In the context of the multiple service provider network embodiments illustrated in FIGS. **19** through **23**, many of the device assisted service techniques disclosed herein that involve a service processor and/or a service controller, including, for example, service usage charging, QoS enabled service usage charging, service usage notification, service usage control, and service usage user feedback UI that apply to the case of improving roaming services or unifying different service provider networks with a common service may be employed. In addition, in some embodiments, the application of verifiable device assisted services (e.g., verifiable service processor service policy adherence) can be accomplished both on the first service provider network and the second service provider network by virtue of the fact that both networks are supplying network generated service usage information to the one or more service controllers and/or proxy servers or routers.

Accordingly, this allows a number of embodiments for one or not of the service providers, including, for example: common service usage and/or recording platform that can provide unified service usage reporting and/or billing across multiple networks, common network service controls and/or traffic controls across multiple networks, common user information sharing across multiple networks, and common QoS controls across multiple networks, common service design services across multiple networks. It is also possible to unify networks with different access technologies into a common network service. For example, by creating different network interface "shim" software layers, it is possible to interface a common set of service controller capabilities, service processor capabilities, proxy server and/or router capabilities and/or service design interface capabilities into different networks that have different equipment and even different communication protocols for provisioning equipment, CDR collection and aggregation equipment, traffic control equipment, AAA, home agent/HLR, billing systems, QoS reservation and control equipment, and/or other capabilities/protocols. The equipment software shims translate the different equipment communication protocols for each network into the common protocols supported in the service controller, service processor, proxy server and/or router, and/or service design center apparatus.

In some embodiments, the techniques described herein to unify network services across multiple networks can be used to provide consistent service control, notification, billing across networks locally or globally without the need to backhaul the data traffic through wholesale pipes from one network to another as is the case with conventional network technologies. For example, a subscriber can be acquired and/or billed for by network #1 and then be serviced with a uniform service experience and deep service notification, control, charging capabilities on both network #1 and network #2. In some embodiments, a subscriber can be acquired and billed for by network #2 and then be serviced with a uniform service experience and deep service notification, control, charging capabilities on both network #1 and network #2. Service plans, settings, notification, carrier branding, etc. can all be the same or different for subscribers originated on one network versus the other. Additionally, in some embodiments, one or more of the service controller, proxy servers or routers and/or other apparatus that handles traffic including the mediation systems can be distributed and/or redundant with diversity as discussed elsewhere to reduce the need to back haul device service traffic or service control traffic. In some embodiments, it is possible for both carrier networks to posses a common service design network element and UI despite the fact that the different networks can have very different provisioning, AAA, traffic handling, charging, billing, etc equipment.

FIG. **22** illustrates a wireless network architecture for providing device assisted CDR creation, aggregation, mediation and billing including two service provider networks in accordance with some embodiments, involving one or more of service controllers, service processors and/or proxy server/routers. FIG. **22** includes elements that can be identical or very similar to those described in the context of FIGS. **5** through **8**, **16** through **18**, and **21** except that in FIG. **21** there are two central provider networks where the CDR reporting and service controls are unified through one or more common service controllers **120**, service processors **115** and/or proxy server/routers **270**. As shown in FIG. **22**: the charging flows

are illustrated using the following three line types: solid lines for device generated CDRs and/or proxy server/router generated CDRs, dashed lines for network equipment generated CDRs, and double dot-dash line types for CDRs that have been mediated by a service controller **120** and/or mediation system **118**.

FIG. **23** illustrates a wireless network architecture for providing device assisted CDR creation, aggregation, mediation and billing including two service provider networks in accordance with some embodiments, involving one or more of service controllers and/or proxy server/routers. FIG. **23** includes elements that may be identical or very similar to those described in the context of FIG. **22**, except in this case there is no service processor CDR feed and only CDR feeds from the network equipment and the proxy server/routers. As shown in FIG. **23**, the charging flows are illustrated using the following three line types: solid lines for device generated CDRs and/or proxy server/router generated CDRs, dashed lines for network equipment generated CDRs, and double dot-dash line types for CDRs that have been mediated by a service controller **120** and/or mediation system **118**.

In some embodiments, one or more proxy servers or routers are used to create a common network service between two or more different networks. In some embodiments, one or more proxy servers or routers are used in conjunction with device client (DAS service processor) used to create a common network service between two or more different networks. In some embodiments, one or more proxy servers or routers are used to create a common network service between two or more different networks in which the proxy server is programmed with a centralized service design interface. In some embodiments, one or more proxy servers or routers are used to create a common service usage recording and/or accounting system across different networks. In some embodiments, one or more proxy servers or routers are used in conjunction with device client (e.g., DAS service processor) used to create a common network service between two or more different networks, in which the proxy server and the device client have coordinated policy settings and/or are both controlled by a service controller element in a network.

In some embodiments, one or more proxy servers or routers are used in conjunction with a device client (e.g., DAS service processor) to create a common network service between two or more different networks in which the proxy router and the device client have coordinated policy settings and/or are both controlled by a service controller element in a network.

In some embodiments, one or more proxy servers or routers are used to create a common network service between two or more different networks in which the proxy server is programmed with a centralized service design interface and the is controlled by a service controller element in a network.

In some embodiments, one or more proxy servers or routers are used to create a common network service between two or more different networks in which the proxy server is programmed with a centralized service design interface and one or more of the service policies are is controlled by a service controller element in a network. In some embodiments, one or more proxy servers or routers are used to create a coordinated QoS signaling, reservation, provisioning, control, charging, and/or user interface across different service provider networks.

Those of ordinary skill in the art will appreciate that various other rules can be provided for the rules engine as described herein. Those of ordinary skill in the art will also appreciate that the functions described herein can be implemented using various other network architectures and network implementations (e.g., using various other networking protocols and corresponding network equipment and techniques).

Although the foregoing embodiments have been described in some detail for purposes of clarity of understanding, the invention is not limited to the details provided. There are many alternative ways of implementing the invention. The disclosed embodiments are illustrative and not restrictive.

What is claimed is:

1. A system, comprising:

one or more processors, including a processor of a proxy network device in communication with a device through a particular logical channel over a wireless network, the particular logical channel configured to support less than all data traffic associated with the device, the less than all data traffic including traffic associated with a particular service activity of a plurality of service activities available to the device, the one or more processors configured to:

obtain service usage information for the device, the service usage information associated with the particular service activity;

format the service usage information into a syntax that can be used by a network accounting system; and

provide the formatted service usage information to the network accounting system; and

memory coupled to the one or more processors and configured to provide the one or more processors with instructions.

2. The system recited in claim **1**, wherein the proxy network device includes a proxy server.

3. The system recited in claim **1**, wherein the proxy network device includes a proxy router.

4. The system recited in claim **1**, wherein the wireless network is a first wireless network, and wherein the proxy network device is configured to support the particular service activity over a second wireless access network.

5. The system recited in claim **1**, further comprising service design interface configured to assist in programming more processors to implement a service policy.

6. The system recited in claim **1**, wherein the one or more processors are configured to obtain the service usage information by generating the service usage information.

7. The system recited in claim **1**, wherein the syntax is a charging data record (CDR).

8. The system recited in claim **1**, wherein the one or more processors are configured to obtain the service usage information from the device.

9. The system recited in claim **1**, wherein the proxy network device includes a service usage data store.

10. The system recited in claim **1**, wherein the proxy network device includes a service usage data store and a rules engine for aggregating the service usage information.

11. The system recited in claim **1**, wherein the one or more processors are configured to format the service usage information into a syntax that can be used by a network accounting system by:

aggregating the service usage information; and

applying a set of rules to the aggregated service usage information.

12. The system recited in claim **1**, wherein the syntax is a charging data record (CDR), and wherein the one or more processors are configured to format the service usage information into a syntax that can be used by a network accounting system by:

aggregating the service usage information; and

applying a set of rules to the aggregated service usage information;

and wherein the one or more processors are configured to provide the formatted service usage information to the network accounting system by communicating a set of one or more CDRs to the network accounting billing system.

13. The system recited in claim **1**, wherein the syntax is a charging data record (CDR), and wherein the one or more processors are configured to format the service usage information into a syntax that can be used by a network accounting system by:

aggregating the service usage information; and

verifying the aggregated service usage information;

and wherein the one or more processors are configured to provide the formatted service usage information to the network accounting system by communicating a set of one or more CDRs to the network accounting system.

14. The system recited in claim **1**, wherein the syntax is a charging data record (CDR), and wherein the one or more processors are configured to format the service usage information into a syntax that can be used by a network accounting system by:

aggregating the service usage information; and

verifying the aggregated service usage information by comparing at least a subset of the aggregated service usage information to at least one network generated CDR;

and wherein the one or more processors are configured to provide the formatted service usage information to the network accounting system by communicating a set of one or more CDRs associated with service usage for the device to the network accounting system.

15. The system recited in claim **1**, wherein the syntax is a charging data record (CDR), and wherein the one or more processors are configured to format the service usage information into a syntax that can be used by a network accounting system by:

aggregating the service usage information device; and

applying a set of at least one ruleto the aggregated service usage information, wherein the set of at least one rule includes a bill by account rule;

and wherein the one or more processors are configured to provide the formatted service usage information to the network accounting system by communicating a set of one or more CDRs to a billing interface or a billing system.

16. The system recited in claim **1**, wherein the syntax is a charging data record (CDR), and wherein the one or more processors are configured to format the service usage information into a syntax that can be used by a network accounting system by:

aggregating the service usage information; and

applying a set of at least one ruleto the aggregated service usage information, wherein the set of at least one rule includes a bill by account rule;

and wherein the one or more processors are configured to provide the formatted service usage information to the network accounting system by communicating a set of one or more CDRs to a billing interface or a billing system, wherein at least one of the one or more CDRs includes a billing offset.

17. The system recited in claim **1**, wherein the syntax is a charging data record (CDR), and wherein the one or more processors are configured to format the service usage information into a syntax that can be used by a network accounting system by:

communicating a set of one or more CDRs to the network accounting system, and wherein the network accounting system comprises a billing system.

18. The system recited in claim **1**, wherein the one or more processors are further configured to provide a service controller function, and wherein the one or more processors are configured to obtain service usage information for the device by collecting the service usage information with assistance from the service controller function.

19. The system recited in claim **1**, wherein the network accounting system comprises:

a service controller.

20. The system recited in claim **1**, wherein the network accounting system comprises:

a billing interface or a billing system.

21. The system recited in claim **1**, wherein the particular service activity is an activity associated with a particular application on the device.

22. The system recited in claim **1**, wherein the particular service activity is an activity associated with a source address or a destination address.

23. The system recited in claim **1**, wherein the particular service activity is an activity associated with a particular content type.

24. The system recited in claim **1**, wherein the particular service activity is an activity associated with a data socket, a communication end point, or a communication source.

25. The system recited in claim **1**, wherein the particular service activity is an activity that takes place at a particular time of day.

26. The system recited in claim **1**, wherein the particular service activity is an activity associated with a particular quality-of-service (QoS) parameter.

27. The system recited in claim **1**, wherein the particular service activity is an activity associated with a network busy state.

28. The system recited in claim **1**, wherein the particular service activity is an ambient service activity.

29. They system recited in claim **1**, further comprising the network accounting system, and wherein the network accounting system is configured to assist in allocating at least a portion of the formatted service usage information to an account associated with a sponsor entity, the sponsor entity being an entity other than a user of the device.

30. The system recited in claim **29**, wherein the network accounting system is further configured to assist in billing the sponsor entity.

31. The system recited in claim **1**, wherein the one or more processors are further configured to assist in controlling the traffic associated with the particular service activity.

32. The system recited in claim **31**, wherein the particular service activity is a roaming service activity.

33. The system recited in claim **1**, wherein the one or more processors are further configured to assist in controlling the traffic associated with the particular service activity by allowing the traffic associated with the particular service activity.

34. The system recited in claim **1**, wherein the one or more processors are further configured to assist in controlling the traffic associated with the particular service activity by blocking or limiting the traffic associated with the particular service activity.

35. The system recited in claim **1**, wherein the one or more processors are further configured to assist in controlling the traffic associated with the particular service activity based on a set of one or more rules.

36. The system recited in claim **1**, wherein the particular service activity is an ambient service activity, and wherein the one or more processors are further configured to impose a limit on the traffic associated with the ambient service activity.

37. The system recited in claim **1**, wherein the proxy network device resides in the wireless network.

38. The system recited in claim **1**, wherein the proxy network device resides in a partner server or a partner network.

39. The system recited in claim **1**, wherein the particular service activity is a roaming service activity, and wherein the one or more processors are further configured to assist in implementing a policy associated with the roaming service activity.

40. The system recited in claim **1**, wherein the proxy network device resides in a home wireless network, and wherein the particular service activity comprises a roaming service activity.

41. The system recited in claim **1**, further comprising the network accounting system, and wherein the network accounting system is configured to assist in allocating at least a portion of the service usage information to a user of the device.

42. The system recited in claim **41**, wherein the network accounting system is further configured to assist in billing the user.

43. The system recited in claim **1**, further comprising the network accounting system, and wherein the network accounting system is configured to assist in allocating a credit based at least in part on the service usage information.

44. The system recited in claim **1**, further comprising the network accounting system, and wherein the network accounting system is configured to reduce a service usage or service cost allocated to a user account based on a credit or an offset.

45. The system recited in claim **1**, wherein the particular logical channel comprises a tunnel or a secure link.

46. The system recited in claim **1**, wherein the particular logical channel is associated with side information.

47. The system recited in claim **1**, wherein at least one of the one or more processors is configured to assist in establishing the particular logical channel.

48. The system recited in claim **1**, wherein the particular logical channel comprises a secure channel between an agent or software on the device and the proxy network device.

49. The system recited in claim **1**, wherein at least one of the one or more processors is configured to assist in implementing an accounting policy to account for the particular service activity.

50. The system recited in claim **1**, wherein at least one of the one or more processors is configured to assist in implementing a traffic control policy.

51. The system recited in claim **1**, wherein at least one of the one or more processors is configured to assist in identifying the traffic associated with the particular service activity.

52. The system recited in claim **1**, wherein at least one of the one or more processors is configured to assist in identifying traffic that is not associated with the particular service activity.

53. The system recited in claim **1**, wherein at least one of the one or more processors is configured to assist in routing or directing traffic associated with the particular service activity to the particular logical channel.

54. The system recited in claim **1**, wherein the processor of the proxy network device is configured to generate the service usage information.

55. The system recited in claim **7**, wherein the CDR includes information about an amount of usage.

56. The system recited in claim **7**, wherein the CDR includes information about one or more of: an application, an application type, a domain, a website, a traffic type, a traffic class, a communication end point, a source or destination, a socket, an address, a quality of service (QoS), a protocol, a transaction, and a uniform resource locator (URL).

57. The system recited in claim **1**, wherein the one or more processors are configured to format the service usage information into a syntax that can be used by a network accounting system for service usage accounting by:

aggregating the service usage information, and verifying the aggregated service usage information by comparing the service usage information to a limit,

and wherein the one or more processors are configured to provide the formatted service usage information to the network accounting system by communicating a set of one or more CDRs to the network accounting system.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 8,340,634 B2
APPLICATION NO. : 12/695980
DATED : December 25, 2012
INVENTOR(S) : Gregory G. Raleigh

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

In the Claims

In column 48, lines 40-41 (the first and second lines of claim 5), the phrase "further comprising service design interface" should be changed to --further comprising a service design interface--.

In column 48, lines 41-42 (the second and third lines of claim 5), the phrase "programming more processors to implement a service policy" should be changed to --programming the one or more processors to implement a service policy--.

In column 49, lines 7-8 (the twelfth and thirteenth lines of claim 12), the phrase "the network accounting billing system" should be changed to --the network accounting system--.

In column 49, line 42 (the sixth line of claim 15), the word "device" should be deleted.

In column 49, line 43 (the seventh line of claim 15), the word "ruleto" should be changed to --rule to--.

In column 49, line 57 (the seventh line of claim 16), the word "ruleto" should be changed to --rule to--.

In column 50, line 44 (the first line of claim 29), the word "They" should be changed to --The--.

Signed and Sealed this
Thirteenth Day of May, 2014

Michelle K. Lee

Michelle K. Lee
Deputy Director of the United States Patent and Trademark Office