eNode B ID	Node B ID	GSM BS ID
1	0	1

Figure 7 is thus a flow chart, illustrating a method in accordance with the invention, whereby a congestion status flag is generated. In step 70 of the process, measurements are made, relating to the congestion status of the relevant radio base station. As mentioned above, these can include any relevant measurements relating to the downlink or uplink radio or fixed network resources. In step 72, measurements are made, relating to the performance of the base station. As described above, these can include any relevant measurements relating to the performance of the ongoing sessions in a cell. In step 74, a congestion status flag is generated. As described above, the flag can be generated by comparing the relevant measurements with respective thresholds, and then generating the flag to indicate the congestion status of the base station. In step 76, the radio base station transmits the generated congestion status flag to other network entities.

More specifically, regarding step 76, one possibility is that the congestion status flag can be used to prevent handover failures. Thus, each Node B sends the congestion flag to its neighbor Node Bs. The flag will indicate the overall resource situation in the transmitting Node B. This means that, when the transmitting Node B is a potential target Node B for a handover, the serving Node B can be prevented from sending handover requests to that target Node B when it is congested, i.e. when its flag = 1. On the one hand this will reduce the handover failure attempt, thereby minimizing handover latency and preventing unnecessary signaling exchange. On the other hand this will allow the

serving Node B to select the next possible Node B in terms of resource availability, thereby minimizing the call dropping probability. By using multi-RAT congestion status the handover failures due to congestion of base stations belonging to other access technologies can also be minimized.

The simplest way to send the flag is via the control plane, that is, via the respective Node B-Node B interface 18, 20, etc as shown in Figure 3, in E-UTRA. It is important to note that the congestion flag can either be sent as a separate message or it can be concatenated to other types of signaling messages. The main advantage of the former scheme is that some overheads such as base station identifier can be reduced. In any case the target base station receiving the congestion status flag should be able to uniquely identify and interpret the meaning of the congestion flag.

Another option is to send the flag by piggybacking it with the user data over the user plane and routing it to the destination Node Bs via the access gateway (aGW) 16. This approach is realizable since the flag comprises only one, or very few, bits. The control plane (Node B-Node B interface) is expected to have much lower capacity than the user plane. Thus, the second approach is also useful in situations where there is congestion on the Node B-Node B control plane.

Figure 8 is a flow chart, illustrating a process for initiating a handover, using the congestion status flag as described above. Thus, in step 90, the serving base station identifies another Node B as a potential target base station for a handover. In step 92, the serving base station reads the congestion status flag sent by that potential target base station and, in step 94, it determines whether that congestion status flag indicates that the potential target

base station is congested. If the flag indicates that the potential target base station is congested, the process returns to step 90, and the serving base station identifies an alternative potential target base station. If the flag indicates that the potential target base station is not congested, the process passes to step 96, and the serving base station proceeds with the handover to that target base station.

The indication of congestion status does not prevent any Node B from requesting measurement reports from neighbouring Node Bs, whose congestion status flags indicate that they are congested. However, a Node B can have an option not to request measurements reports from congested neighbour Node Bs. This will reduce unnecessary signalling overheads and processing at the Node B.

The congestion status flag can also be used for dynamic setting of neighbour cell lists. As shown in Figure 9, in step 100 of that process, a serving Node B can receive the congestion status information reported by one or more of the neighbour Node Bs, as described above. The serving Node B can then update its existing neighbour cell list at step 102 by excluding from that list any neighbouring Node B whose flag =1. The updated list can then be sent to the users in that cell by the serving Node B. This will prevent those users from doing measurements (for handover or cell change) on cells that are congested.

Thus, Figure 10 shows a system including a radio base station (RBS) 81, including a block 811 for generating a congestion status flag, operating as described above. Figure 10 also shows a user equipment (UE) 82, which may take the form of a mobile phone, or any type of portable wireless communications device, including a block 821 for

reading messages received from the RBS 81 and a processor 822.

In the process of Figure 9, the RBS 81 transmits the updated neighbour cell list to the UE 82, which is able to use that list for future handovers or cell changes.

The congestion status flag can also be used for prevention of admission failures. Thus, considering the system of Figure 10, the flag can also be broadcast to the users in its own cell using the same signalling mechanism as described above. Moreover, since the serving Node B 81 is also aware of the congestion status in the neighbour Node Bs, the serving Node B 81 can also broadcast the flag status of the neighbour Node Bs. This will prevent the UE 82 from listening to the neighbouring Node Bs for the purpose of inferring the congestion status.

In order to prioritize handover over new calls or vice verse, different measurement thresholds can be used to generate the flag for handovers and for admission control. The UE can then consider the overall resource situation by reading the broadcast flag before initiating a call (e.g. before sending random access request). For example, the UE can avoid access to a congested cell (e.g. whose flag =1) even though it is the best in terms of coverage or quality. Rather, the UE shall access the next best cell in terms of coverage or quality, which is not congested (e.g. flag = 0).

The multi-RAT flag can be used to steer the UE to access the best cell belonging to the best possible access technology in terms of available resources.

In the case of UE based handovers (e.g. in fully distributed systems), the broadcast information can also be used by the user equipment to perform handovers.

There is thus described a system for generating congestion status information, which can be used by network entities to operate efficiently.

CLAIMS

1. A method of indicating a status of a radio base station of a telecommunication network wherein said method comprises generating a congestion status flag based on a measured resource usage and based on a measured performance of said radio base station.

2. The method according to Claim 1 wherein the measured resource usage relates to usage of a set of any downlink or uplink radio or fixed network resources in the radio base station.

3. The method according to Claim 1 wherein the measured performance relates to performance of ongoing sessions in a cell.

4. The method according to Claim 1 wherein the congestion status flag is generated by comparing the measured resource usage and the measured performance with respective thresholds.

5. The method according to Claim 1 wherein the flag has two possible values, and wherein one value indicates full congestion whereas the other value indicates no congestion.

6. The method according to Claim 1 wherein the flag has more than two possible values, and wherein highest and lowest of said values indicate full congestion and no congestion, respectively, and intermediate values indicate respective different intermediate levels of congestion.

7. The method according to Claim 6 wherein a congestion status having more than two values is signalled by a single bit using state transitions.

8. The method according to Claim 7 wherein the congestion status of the radio base station belonging to multiple access technologies is signalled.

9. The method according to any preceding claim, comprising sending said congestion status flag to at least one other radio base station.

10. The method according to Claim 9, wherein the congestion status is signaled as a separate and independent message.

11. The method according to Claim 9, wherein the congestion status is sent by concatenating it with other signaling messages.

12. The method according to Claim 9, wherein the congestion status is sent by concatenating or piggybacking it with the user data.

13. The method according to any preceding claim, comprising sending said congestion status flag to users in its own cell.

14. The method according to claim 13, further comprising sending to users in its own cell said congestion status flag relating to at least one other radio base station.

15. A method of operation of a radio base station of a telecommunication network wherein said method comprises reading a congestion status flag generated in at least one other radio base station, said congestion status flag being based on a measured resource usage and based on a measured performance of said at least one other radio base station.

16. The method according to Claim 15, wherein said radio base station, acting as a serving radio base station, utilizes said congestion status flag to determine a target radio base station for the purpose of handovers.

17. The method according to Claim 15, wherein said radio base station, acting as a serving radio base station, utilizes said congestion status flag to dynamically update neighbour cell lists used by user equipment to perform downlink measurements for handovers and cell reselection.

18. A method of operation of a user equipment in a telecommunication network including one or more radio base stations, the method comprising reading a congestion status flag generated in a radio base station, said congestion status flag being based on a measured resource usage and based on a measured performance of said radio base station.

19. A method according to claim 19, comprising reading said congestion status flag of its own cell and at least one neighbouring cell, and utilizing this information to decide the best radio base station in terms of cell resources to establish a new call.

20. The method according to Claim 19, comprising utilizing said congestion status information to decide the best radio base station in terms of cell resources to perform handover.

21. A radio base station (81) for a telecommunication network (80) wherein said radio base station (81) comprises a means (811) for generating a congestion status flag based on the measured resource usage and measured performance.

22. A user equipment (82) for a telecommunication network (80) including one or more radio base stations, wherein the user equipment (82) comprises a means (821) for reading a congestion status message based on the measured resource usage and measured performance of its own cell and at least one neighbouring cell, and a means (822) for determining the best radio base station in terms of cell resources to establish a new call based on this information.

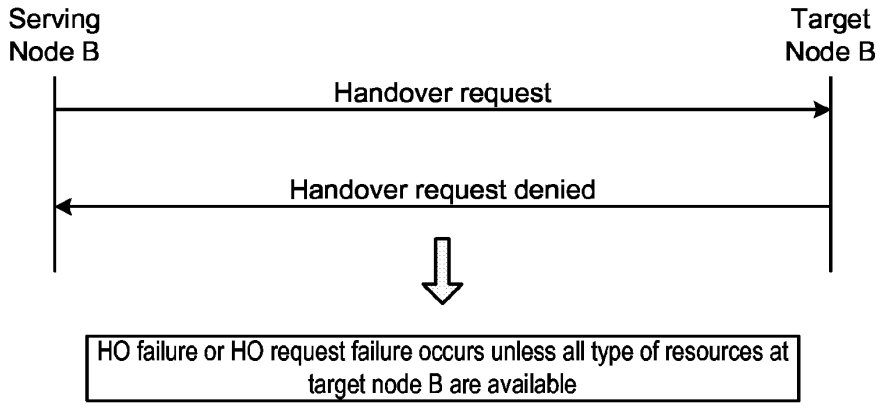


Figure 1

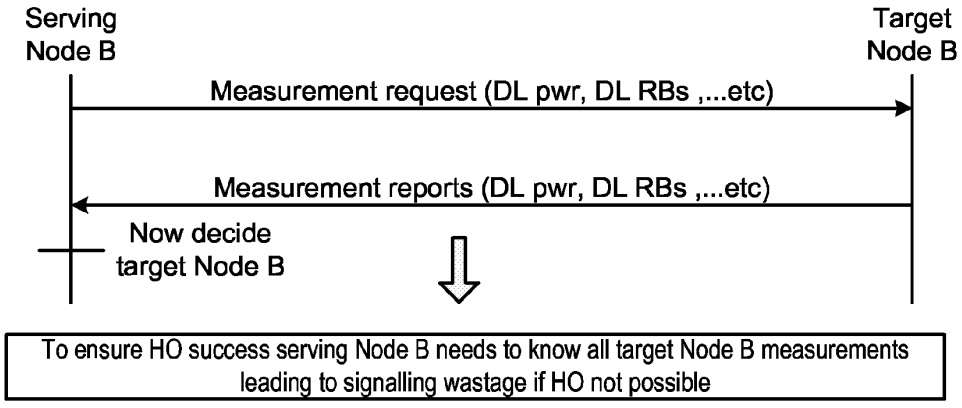


Figure 2

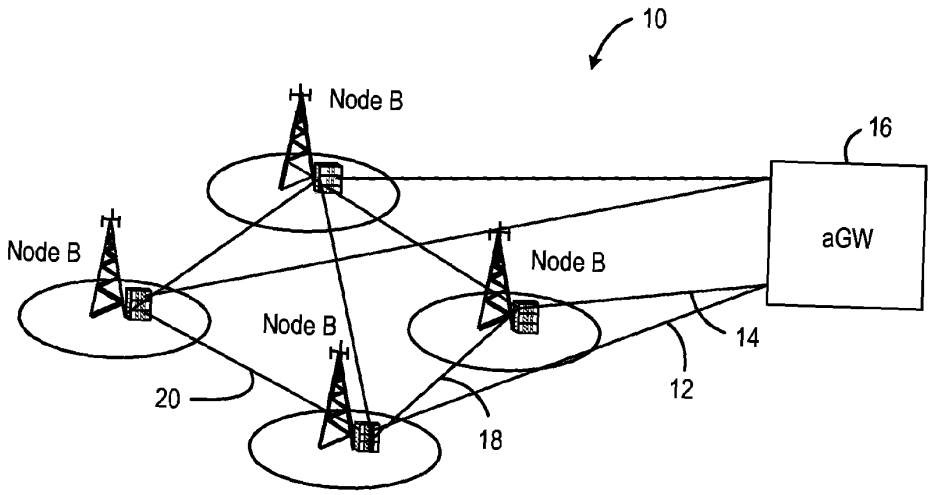


Figure 3

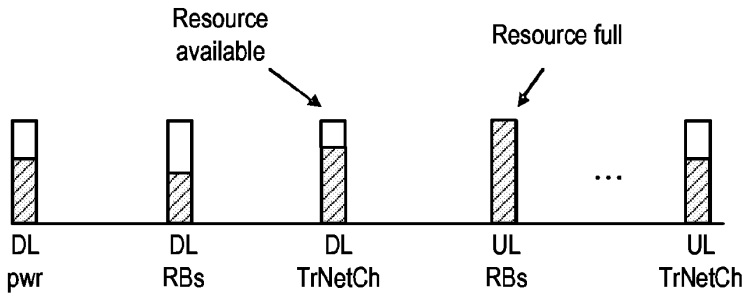

Resource available
Resource full
DL pwr
DL RBs
DL TrNetCh
UL RBs
UL TrNetCh

Figure 4

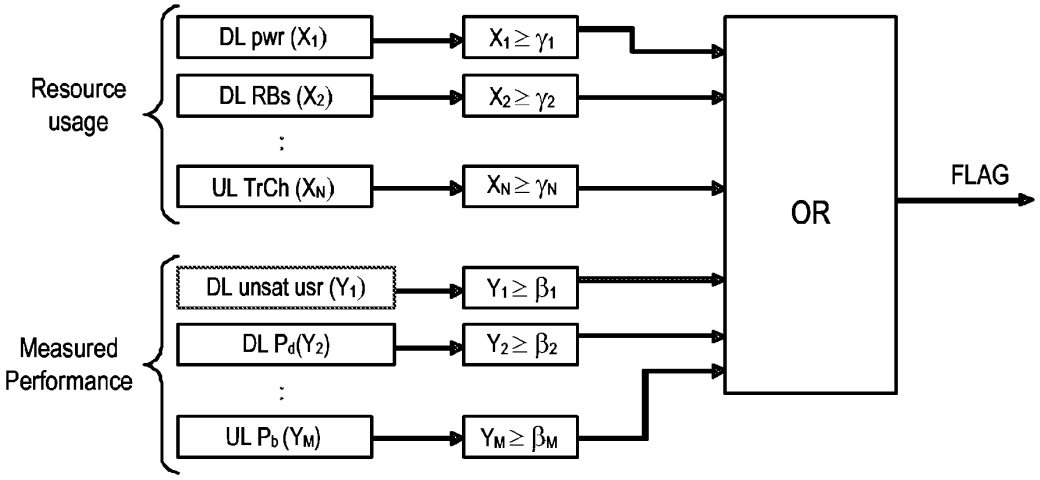

Resource usage
DL pwr (X_1)
DL RBs (X_2)
UL TrCh (X_N)
$X_1 \geq \gamma_1$
$X_2 \geq \gamma_2$
$X_N \geq \gamma_N$
Measured Performance
DL unsat usr (Y_1)
DL P_d(Y_2)
UL P_b (Y_M)
$Y_1 \geq \beta_1$
$Y_2 \geq \beta_2$
$Y_M \geq \beta_M$
OR
FLAG

Figure 5

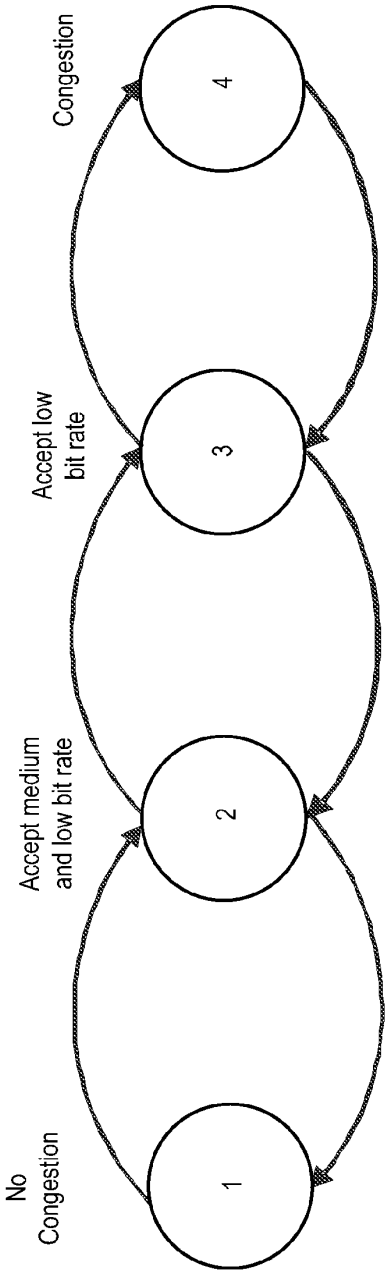

Congestion
4
Accept low
bit rate
3
Accept medium
and low bit rate
2
No
Congestion
1

Figure 6

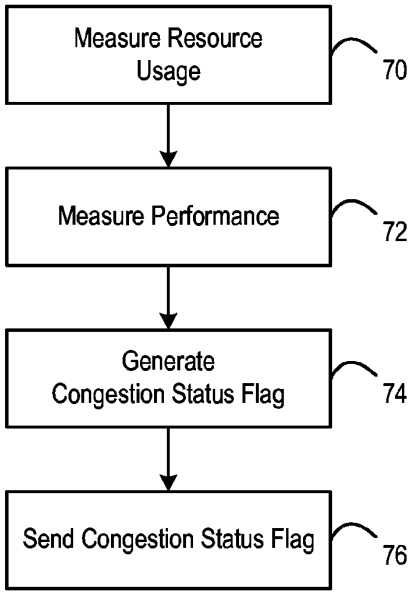

Measure Resource Usage
70
Measure Performance
72
Generate Congestion Status Flag
74
Send Congestion Status Flag
76

Figure 7

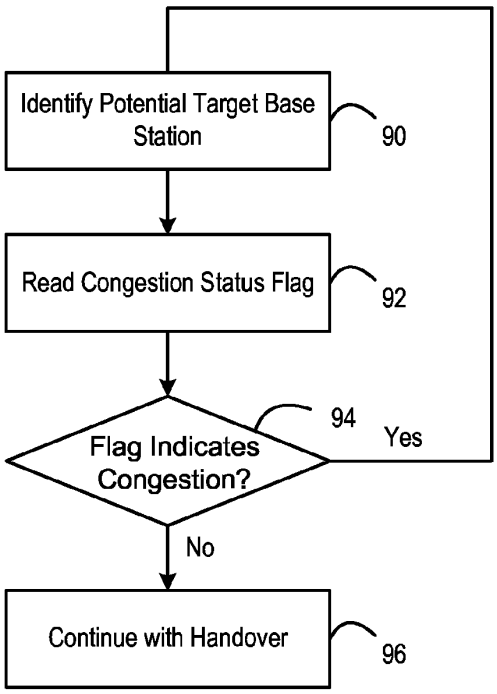


Figure 8

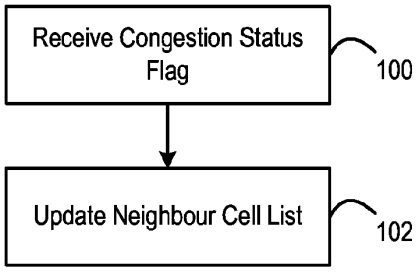


Figure 9

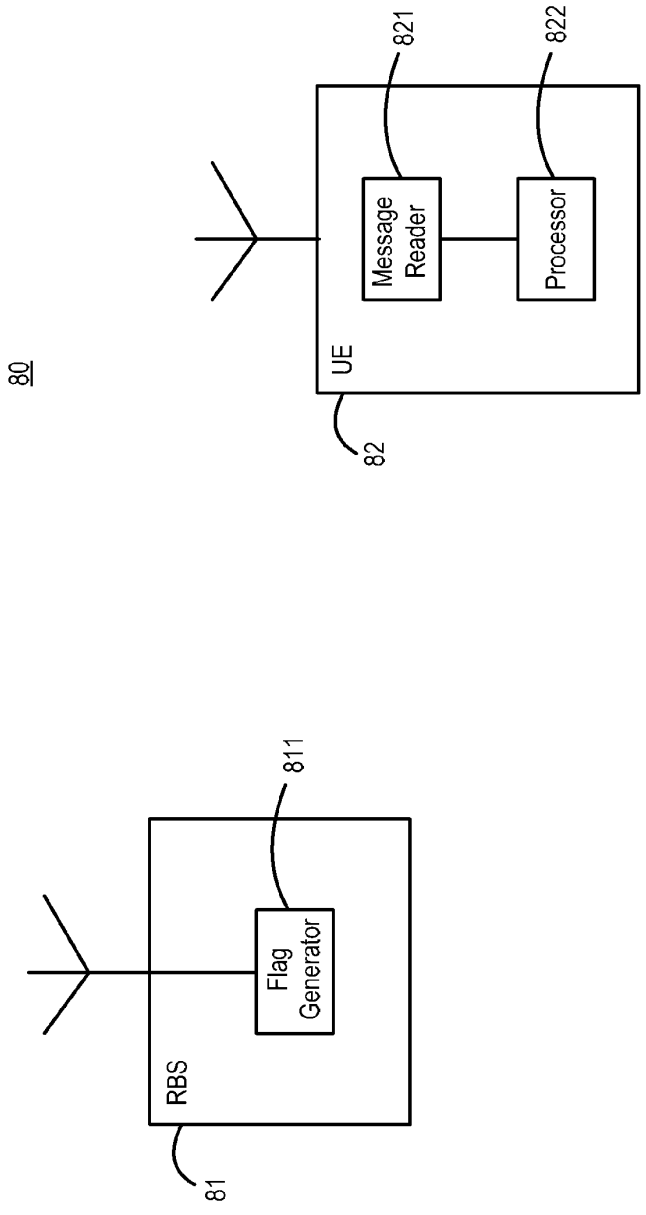

80
821
822
Message Reader
Processor
UE
82
811
Flag Generator
RBS
81

Figure 10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE2006/050538

A. CLASSIFICATION OF SUBJECT MATTER

IPC: see extra sheet
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04Q, H04L

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

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-INTERNAL, WPI DATA, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 20040160914 A1 (SANDIP SARKAR), 19 August 2004 (19.08.2004), figure 6, claims 1-9, abstract, paragraph 8-10, 25, 33, 41-43, 84, 125-130, 135-141, 147, 151-153 --	1-22
X	EP 1284583 A2 (FUJITSU LIMITED), 19 February 2003 (19.02.2003), claims 1-20, abstract, paragraph 7, 17-21, 24, 27, 30-32, 55-56, 59-60, 64, 70-73 --	1-22
A	US 6741555 B1 (XIANG LI ET AL), 25 May 2004 (25.05.2004), claim 1, abstract --	1-22

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 August 2007	28 -08- 2007
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Maziar Soltani/MN Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (April 2007)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE2006/050538

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6643318 B1 (KOUROSH PARSA ET AL), 4 November 2003 (04.11.2003), abstract -- --------	1-22

Form PCT/ISA/210 (continuation of second sheet) (April 2007)

International patent classification (IPC)

H04L 12/56 (2006.01)
H04Q 7/38 (2006.01)

Download your patent documents at www.prv.se
The cited patent documents can be downloaded at www.prv.se by following the links:

- In English/Searches and advisory services/Cited documents (service in English) or
- e-tjänster/anförda dokument (service in Swedish).

Use the application number as username.
The password is **SJKNYCJGUC**.

Paper copies can be ordered at a cost of 50 SEK per copy from PRV InterPat (telephone number 08-782 28 85).

Cited literature, if any, will be enclosed in paper form.

US	20040160914	A1	19/08/2004	AU	2004213980	A	02/09/2004
				AU	2004213981	A	02/09/2004
				AU	2004213994	A	02/09/2004
				AU	2004213995	A	02/09/2004
				AU	2004213996	A	02/09/2004
				AU	2004213998	A	02/09/2004
				AU	2004213999	A	02/09/2004
				AU	2004214794	A	10/09/2004
				BR	PI0407532	A	14/02/2006
				BR	PI0407545	A	14/02/2006
				BR	PI0407560	A	14/02/2006
				BR	PI0407562	A	14/02/2006
				BR	PI0407565	A	14/02/2006
				BR	PI0407567	A	14/02/2006
				BR	PI0407568	A	14/02/2006
				BR	PI0407571	A	01/03/2006
				CA	2516119	A	02/09/2004
				CA	2516176	A	02/09/2004
				CA	2516219	A	02/09/2004
				CA	2516227	A	02/09/2004
				CA	2516228	A	02/09/2004
				CA	2516231	A	10/09/2004
				CA	2516261	A	02/09/2004
				CA	2516296	A	02/09/2004
				CN	1751531	A	22/03/2006
				CN	1762119	A	19/04/2006
				CN	1762169	A	19/04/2006
				CN	1762174	A	19/04/2006
				CN	1768550	A	03/05/2006
				CN	1774885	A	17/05/2006
				CN	1774949	A	17/05/2006
				CN	1774950	A	17/05/2006
				EP	1595351	A	16/11/2005
				EP	1595355	A	16/11/2005
				EP	1595414	A	16/11/2005
				EP	1595419	A	16/11/2005
				EP	1595421	A	16/11/2005
				EP	1595422	A	16/11/2005
				EP	1595423	A	16/11/2005
				EP	1595424	A	16/11/2005
				JP	2006518161	T	03/08/2006
				JP	2006518171	T	03/08/2006
				JP	2006518172	T	03/08/2006
				JP	2006518173	T	03/08/2006
				JP	2006518174	T	03/08/2006
				JP	2006518175	T	03/08/2006
				JP	2006518176	T	03/08/2006
				JP	2006518577	T	10/08/2006
				KR	20050098942	A	12/10/2005
				KR	20050098943	A	12/10/2005
				KR	20050098944	A	12/10/2005
				KR	20050099627	A	14/10/2005
				KR	20050099629	A	14/10/2005
				KR	20050101218	A	20/10/2005
				KR	20050109497	A	21/11/2005

US	20040160914	A1	19/08/2004	KR	20060006772	A	19/01/2006
				MX	PA05008659	A	23/11/2005
				MX	PA05008660	A	23/11/2005
				MX	PA05008661	A	23/11/2005
				MX	PA05008662	A	07/04/2006
				MX	PA05008663	A	23/11/2005
				MX	PA05008767	A	20/09/2005
				MX	PA05008769	A	04/11/2005
				MX	PA05008771	A	20/09/2005
				RU	2005129076	A	20/03/2006
				RU	2005129077	A	27/07/2006
				RU	2005129079	A	10/02/2006
				RU	2005129080	A	27/01/2006
				RU	2005129081	A	10/02/2006
				RU	2005129095	A	10/03/2006
				RU	2005129097	A	20/03/2006
				RU	2005129104	A	20/02/2006
				US	7155236	B	26/12/2006
				US	20040160922	A	19/08/2004
				US	20040160933	A	19/08/2004
				US	20040162075	A	19/08/2004
				US	20040162083	A	19/08/2004
				US	20040162098	A	19/08/2004
				US	20040162099	A	19/08/2004
				US	20040240444	A	02/12/2004
				US	20050002444	A	06/01/2005
				US	20050003843	A	06/01/2005
				US	20050007986	A	13/01/2005
				US	20050176456	A	11/08/2005
				US	20060264220	A	23/11/2006
				WO	2004075448	A	02/09/2004
				WO	2004075468	A	02/09/2004
				WO	2004075496	A	02/09/2004
				WO	2004075593	A	02/09/2004
				WO	2004075595	A	02/09/2004
				WO	2004075596	A	02/09/2004
				WO	2004075597	A	02/09/2004
				WO	2004077726	A	10/09/2004
				AU	2004217283	A	16/09/2004
				AU	2004219053	A	23/09/2004
				BR	PI0408073	A	21/03/2006
				BR	PI0408075	A	21/03/2006
				CA	2518183	A	16/09/2004
				CA	2518252	A	23/09/2004
				CN	1784848	A	07/06/2006
				CN	1784921	A	07/06/2006
				EP	1599958	A	30/11/2005
				EP	1600027	A	30/11/2005
				JP	2006520160	T	31/08/2006
				JP	2006520174	T	31/08/2006
				KR	20050104421	A	02/11/2005
				KR	20050110659	A	23/11/2005
				MX	PA05009463	A	12/12/2005
				MX	PA05009465	A	12/12/2005
				RU	2005130980	A	10/05/2006

US	20040160914	A1	19/08/2004	RU	2005130981	A	10/05/2006
				US	7215930	B	08/05/2007
				US	20040228389	A	18/11/2004
				US	20050014470	A	20/01/2005
				US	20070111669	A	17/05/2007
				WO	2004080106	A	16/09/2004
				WO	2004082165	A	23/09/2004
EP	1284583	A2	19/02/2003	AT	349871	T	15/01/2007
				CN	1407822	A	02/04/2003
				DE	60217027	D	00/00/0000
				GB	0120033	D	00/00/0000
				JP	2003134550	A	09/05/2003
				KR	20030015859	A	25/02/2003
				US	20030083069	A	01/05/2003
US	6741555	B1	25/05/2004	AU	7436901	A	24/12/2001
				WO	0197446	A	20/12/2001
US	6643318	B1	04/11/2003	US	7075971	B	11/07/2006
				US	20040081115	A	29/04/2004

PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2009-212707**
(43)Date of publication of application : **17.09.2009**

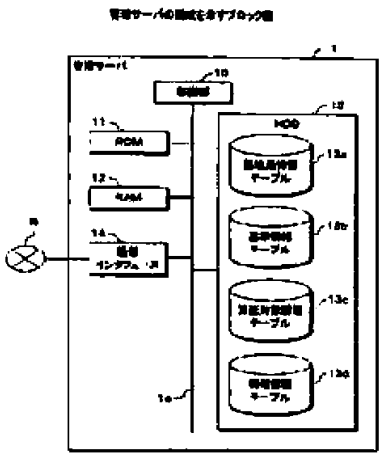
(51)Int.Cl. *H04W 24/02 (2009.01)*
H04L 12/56 (2006.01)

(21)Application number : **2008-052371**
(22)Date of filing : **03.03.2008**

(71)Applicant : **FUJITSU LTD**
(72)Inventor : **ASAI MASATO**
HOSHO YUMI
YOKOE MASANORI
ASAYAMA KOJI

(54) CONTROLLER, CONTROL METHOD AND COMPUTER PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a controller that estimates current congestion conditions in an area of a predetermined repeating installation on the basis of past communication condition in an area of other repeating installations that is set to the predetermined repeating installation.
SOLUTION: A control section 10 periodically generates an information accumulation table 13d listing the existence rate of base stations to be calculated at each time and the congestion rate of base stations to be monitored concerning each of the base stations to be monitored. The control section 10 also calculates a relative coefficient between the existence rate of the base stations to be calculated at current time and the existence rate thereof accumulated in the information accumulation table 13d. Furthermore, the control section 10 counts information of which calculated relative coefficient is a similar decision threshold or more among the information of the information accumulation table 13d, and it also counts the number of information of which congestion rate is a congestion decision threshold or more. The control section 10 calculates a ratio of the number of information having the congestion decision threshold or more in congestion rate to the number of information having the similar decision threshold or more in relative coefficient, resulting in the probability of congestion.



(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2009-212707
(P2009-212707A)
(43)公開日　平成21年9月17日(2009.9.17)

(51)Int.Cl.		F I			テーマコード（参考）
H04W 24/02	(2009.01)	H04Q	7/00	241	5K030
H04L 12/56	(2006.01)	H04L	12/56	200Z	5K067

審査請求 未請求　請求項の数 5　OL　（全 17 頁）

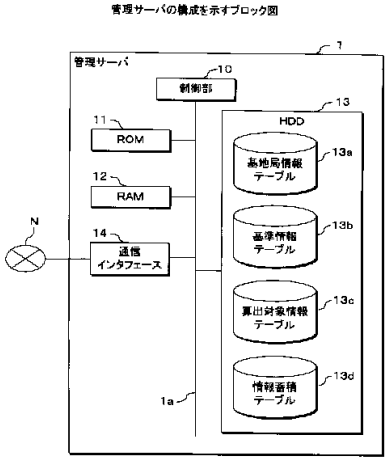
(21)出願番号　特願2008-52371 (P2008-52371)
(22)出願日　平成20年3月3日 (2008.3.3)

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100078868
弁理士　河野　登夫
(74)代理人　100114557
弁理士　河野　英仁
(72)発明者　浅居　正人
大阪府大阪市中央区城見二丁目２番５３号　富士通関西中部ネットテック株式会社内
(72)発明者　賀生　由美
大阪府大阪市中央区城見二丁目２番５３号　富士通関西中部ネットテック株式会社内

最終頁に続く

(54)【発明の名称】管理装置、管理方法及びコンピュータプログラム

(57)【要約】
【課題】所定の中継装置に対して予め設定された他の中継装置のエリアにおける過去の通信状態に基づいて、所定の中継装置のエリア内の現在の輻輳状態を予測する管理装置を提供する。
【解決手段】制御部１０は、定期的に、各監視対象基地局について、各日時における算出対象基地局の在圏率、監視対象基地局の輻輳率を登録した情報蓄積テーブル１３ｄを生成する。制御部１０は、現在日時における算出対象基地局の在圏率と、情報蓄積テーブル１３ｄに蓄積された算出対象基地局の在圏率との相関係数を算出する。制御部１０は、情報蓄積テーブル１３ｄの情報のうちで、算出した相関係数が類似判定閾値以上の情報の数と、さらにそのうちで、輻輳率が輻輳判定閾値以上の情報の数とを計数する。制御部１０は、相関係数が類似判定閾値以上の情報の数に対する、輻輳率が輻輳判定閾値以上の情報の数の割合を算出し、輻輳の発生確率とする。
【選択図】図２



$$r = \frac{\sum_{i=1}^{n}(x_i - \overline{x})(y_i - \overline{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \overline{x})^2}\sqrt{\sum_{i=1}^{n}(y_i - \overline{y})^2}} \quad \cdots(1)$$

r：相関係数　　n：自然数

$\overline{x}$：x_1，x_2，x_3 の平均値

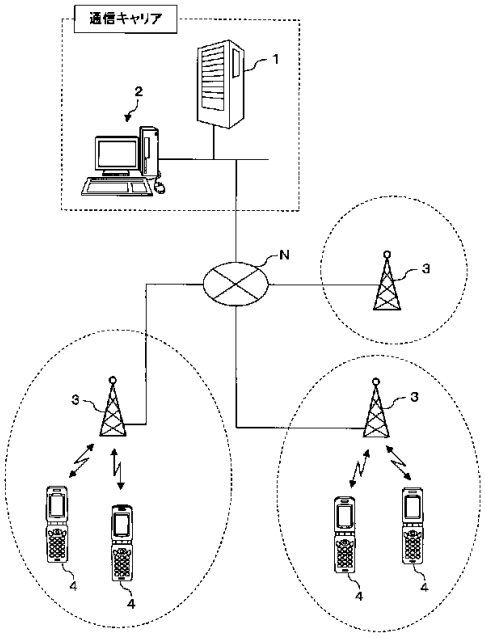
$\overline{y}$：y_1，y_2，y_3 の平均値

$$r = \frac{(x_1-\overline{x})(y_1-\overline{y}) + (x_2-\overline{x})(y_2-\overline{y}) + (x_3-\overline{x})(y_3-\overline{y})}{\sqrt{(x_1-\overline{x})^2+(x_2-\overline{x})^2+(x_3-\overline{x})^2}\sqrt{(y_1-\overline{y})^2+(y_2-\overline{y})^2+(y_3-\overline{y})^2}} \quad \cdots(2)$$

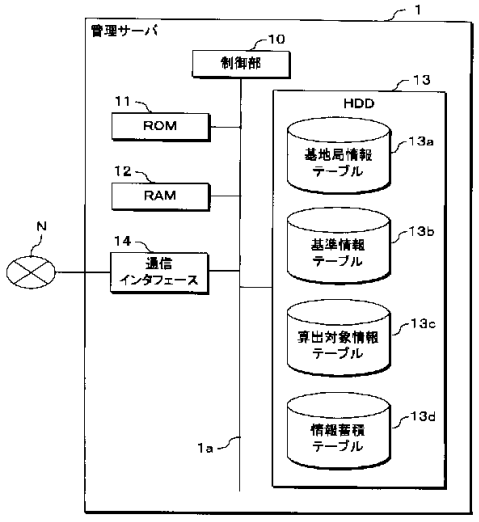
1 2 3

1 2 3

本実施形態に係る携帯端末管理システムの構成を示す模式図



管理サーバの構成を示すブロック図



基地局情報テーブルの登録内容を示す模式図

基地局番号	最大収容数（人）	日時	在圏者数（人）	輻輳率（%）
0001	2000	⋮	⋮	⋮
		2008/1/1 10:00	850	10
		2008/1/1 10:10	850	10
		2008/1/1 10:20	800	10
		⋮	⋮	⋮
0002	1500	⋮	⋮	⋮
		2008/1/1 10:00	500	12
		2008/1/1 10:10	450	12
		2008/1/1 10:20	450	12
		⋮	⋮	⋮
⋮	⋮	⋮	⋮	⋮

基準情報テーブル及び算出対象情報テーブルの登録内容を示す模式図

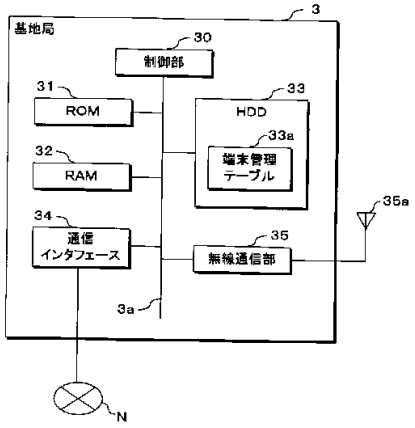
(a)

監視対象基地局番号	類似判定閾値	輻輳判定閾値	警告判定閾値
0001	0.5	60	0.7
0010	0.5	60	0.6
0100	0.5	50	0.8
⋮	⋮	⋮	⋮

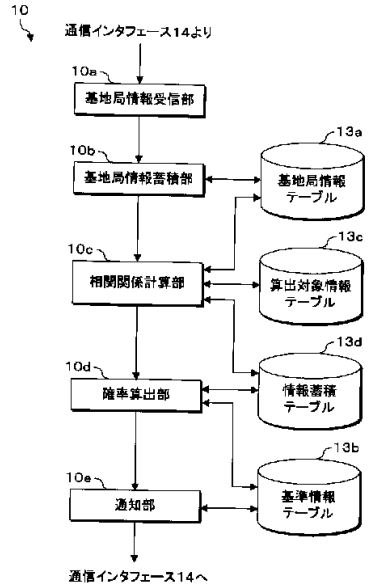
(b)

監視対象基地局番号	算出対象基地局番号	算出対象期間（時間）
0001	0002,0003	8760
0010	0008,0009,0011	1440
0100	0099,0101,0102,0103	8760
⋮	⋮	⋮

基地局の構成を示すブロック図



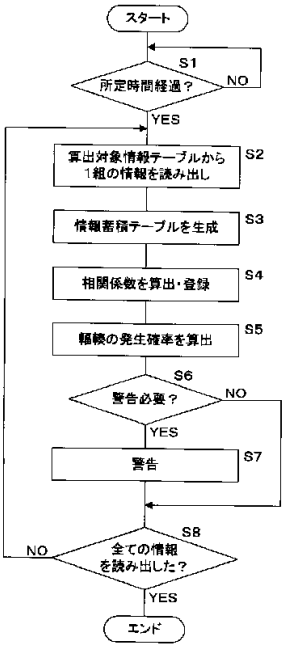
管理サーバの機能構成を示す機能ブロック図



情報蓄積テーブルの登録内容を示す模式図

日時	算出対象基地局の在圏率			輻輳率（%）	相関係数
	基地局「0008」	基地局「0009」	基地局「0011」		
⋮	⋮	⋮	⋮	⋮	⋮
2008/1/1 10:00	0.1	0.2	0.4	20	-0.5
2008/1/1 10:10	0.2	0.4	0.3	20	0.7
2008/1/1 10:20	0.3	0.6	0.1	60	1
2008/1/1 10:30	0.3	0.4	0.3	80	0.9
2008/1/1 10:40	0.2	0.4	0.4	80	0.2
⋮	⋮	⋮	⋮	⋮	⋮
2008/2/1 10:00	0.3	0.5	0.2		

輻輳の発生確率の算出処理の手順を示すフローチャート



フロントページの続き

(72)発明者　横江　政憲
大阪府大阪市中央区城見二丁目２番５３号　富士通関西中部ネットテック株式会社内
(72)発明者　朝山　幸二
大阪府大阪市中央区城見二丁目２番５３号　富士通関西中部ネットテック株式会社内

Ｆターム(参考) 5K030 GA14 HC09 HD05 JA10 LC11 MB02 MD07
5K067 AA21 EE02 EE10 EE16 HH22 HH23

PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2008-301121**
(43)Date of publication of application : **11.12.2008**

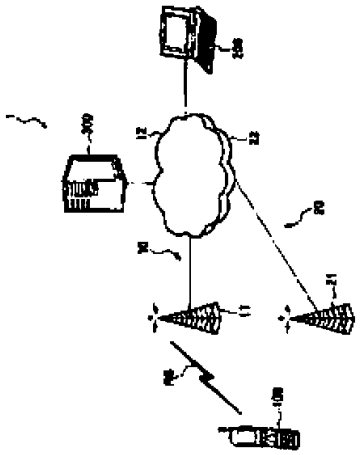
(51)Int.Cl. *H04Q 7/38 (2006.01)*
H04L 12/28 (2006.01)

(21)Application number : **2007-144176**
(22)Date of filing : **30.05.2007**

(71)Applicant : **KYOCERA CORP**
(72)Inventor : **KITACHI MITSUHIRO**

(54) COMMUNICATING SYSTEM, THRESHOLD MANAGEMENT SERVER, RADIO COMMUNICATION DEVICE, AND COMMUNICATING METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a communication system, a threshold management server, a radio communication device, and a communication method which can perform handover to other radio communication system at a timing suitable for each application when the quality deteriorates.
SOLUTION: A radio terminal 100 comprises: a radio condition information acquiring portion for acquiring radio condition information which indicates the state of a radio signal RS transmitted and received with a radio base station 11; and a handover executing portion for executing handover to a radio base station 21 based on a handover threshold value which is contained in a received session notification response and is in accordance with an application to be executed on the radio terminal 100 and the radio condition information acquired by the radio condition information acquiring portion.



(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2008-301121
(P2008-301121A)
(43)公開日　平成20年12月11日(2008.12.11)

(51)Int.Cl.			F I			テーマコード（参考）
H04Q	7/36	(2006.01)	H04B	7/26	109H	5K033
H04L	12/28	(2006.01)	H04L	12/28	310	5K067

審査請求 未請求　請求項の数 15　OL　（全 28 頁）

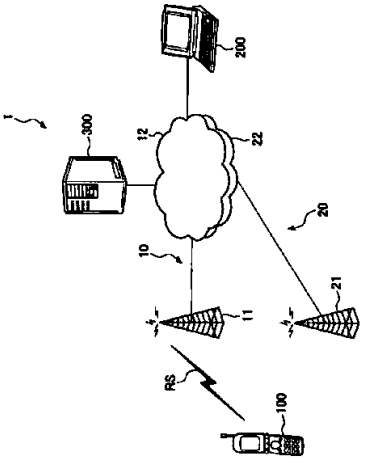
(21)出願番号　特願2007-144176 (P2007-144176)
(22)出願日　平成19年5月30日 (2007.5.30)

(71)出願人　000006633
京セラ株式会社
京都府京都市伏見区竹田鳥羽殿町６番地
(74)代理人　100149102
弁理士　松山　習
(72)発明者　北地　三浩
神奈川県横浜市都筑区加賀原２丁目１番１号　京セラ株式会社横浜事業所内

Ｆターム(参考)　5K033 DA01　DA19
5K067 AA23　BB04　BB21　DD45　EE04
EE10　GG11　HH22　HH23　JJ39

(54)【発明の名称】通信システム、閾値管理サーバ、無線通信装置及び通信方法

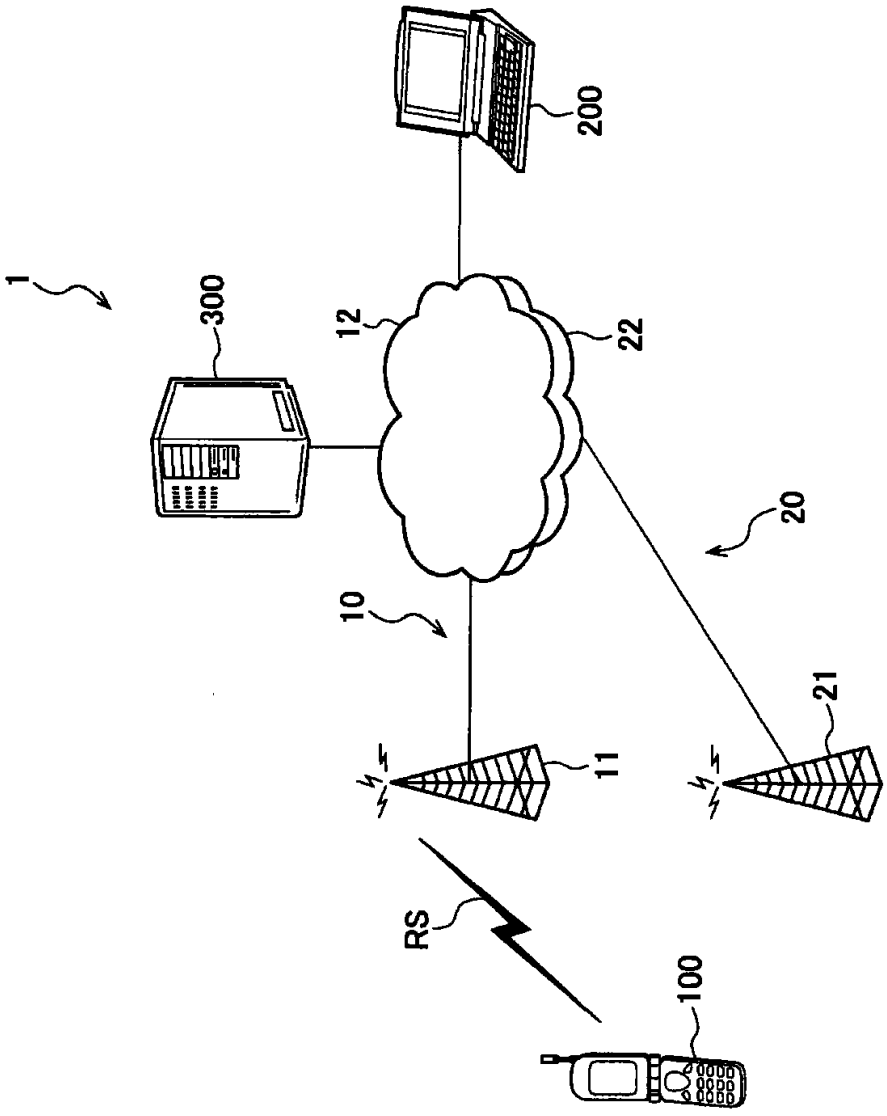
(57)【要約】
【課題】品質が劣化した場合に、アプリケーション毎に適切なタイミングで他の無線通信システムにハンドオーバを実行することができる通信システム、閾値管理サーバ、無線通信装置及び通信方法を提供する。
【解決手段】無線端末１００は、無線基地局１１と送受信される無線信号ＲＳの状態を示す無線状態情報を取得する無線状態情報取得部と、受信したセッション通知応答に含まれ、無線端末１００において実行されるアプリケーションに応じたハンドオーバ閾値と無線状態情報取得部によって取得された無線状態情報とに基づいて、無線基地局２１へのハンドオーバを実行するハンドオーバ実行部とを備える。
【選択図】図１

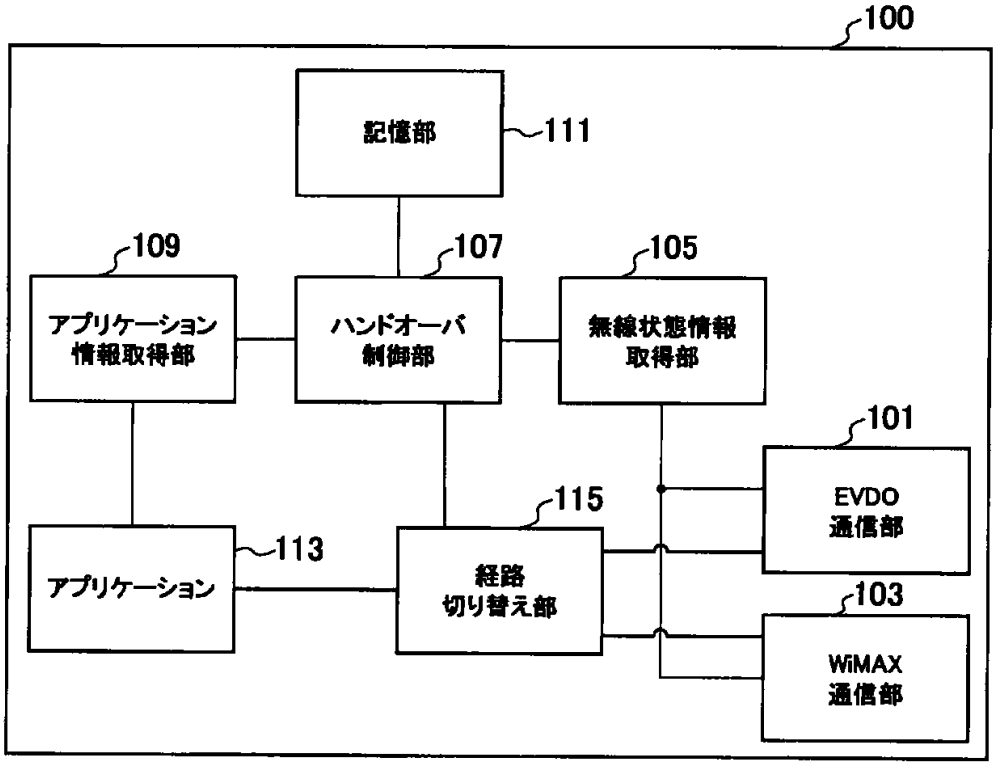


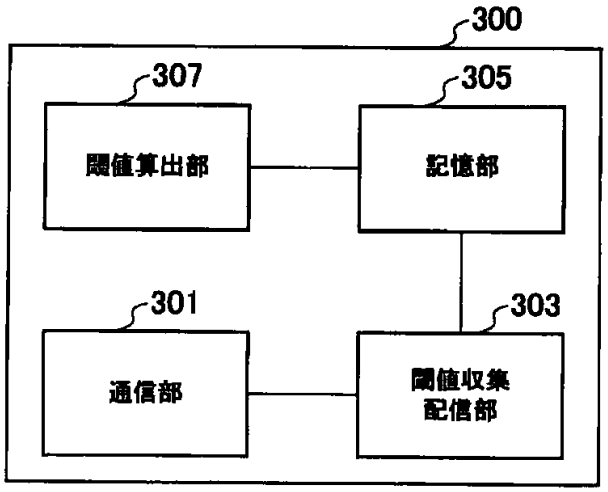
10

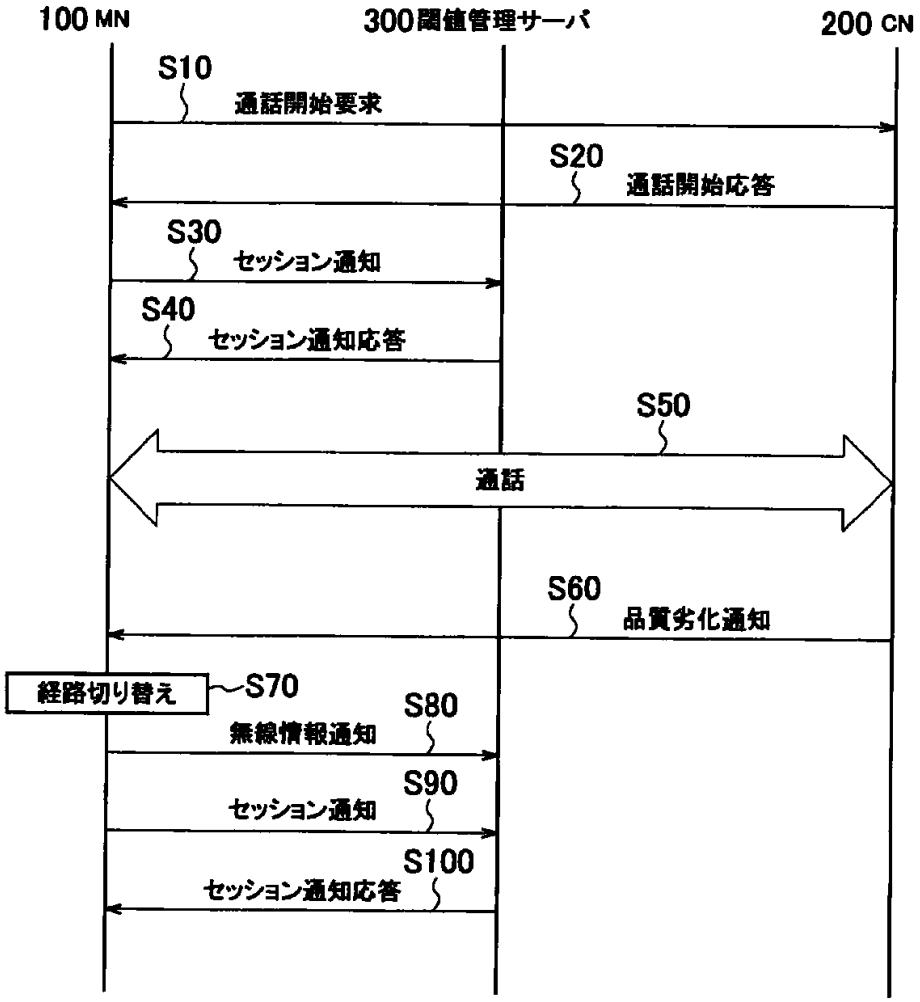
20

30


1
300
12
22
200
20
10
21
11
RS
100


100
記憶部
111
109
107
105
アプリケーション
情報取得部
ハンドオーバ
制御部
無線状態情報
取得部
101
EVDO
通信部
115
113
アプリケーション
経路
切り替え部
103
WiMAX
通信部


300
307
305
閾値算出部
記憶部
301
303
通信部
閾値収集
配信部


100 MN
300閾値管理サーバ
200 CN
S10
通話開始要求
S20
通話開始応答
S30
セッション通知
S40
セッション通知応答
S50
通話
S60
品質劣化通知
経路切り替え
S70
S80
無線情報通知
S90
セッション通知
S100
セッション通知応答

TB

TH

アプリケーション	通信システム	閾値パラメータ	閾値	トラフィック混雑度
G711	EVDO	C/I	−2	0 ～ 15
G711	EVDO	C/I	0	16 ～ 23
G711	EVDO	C/I	5	23 ～ 28
⋮	⋮	⋮	⋮	⋮
G729	WiMAX	RSSI	−92	0 ～ 20
G729	WiMAX	RSSI	−88	20 ～ 28
G729	WiMAX	RSSI	−75	29 ～ 35
⋮	⋮	⋮	⋮	⋮

N1

セッション通知

アプリケーション＝G711	通信システム＝EVDO

R1

セッション通知応答

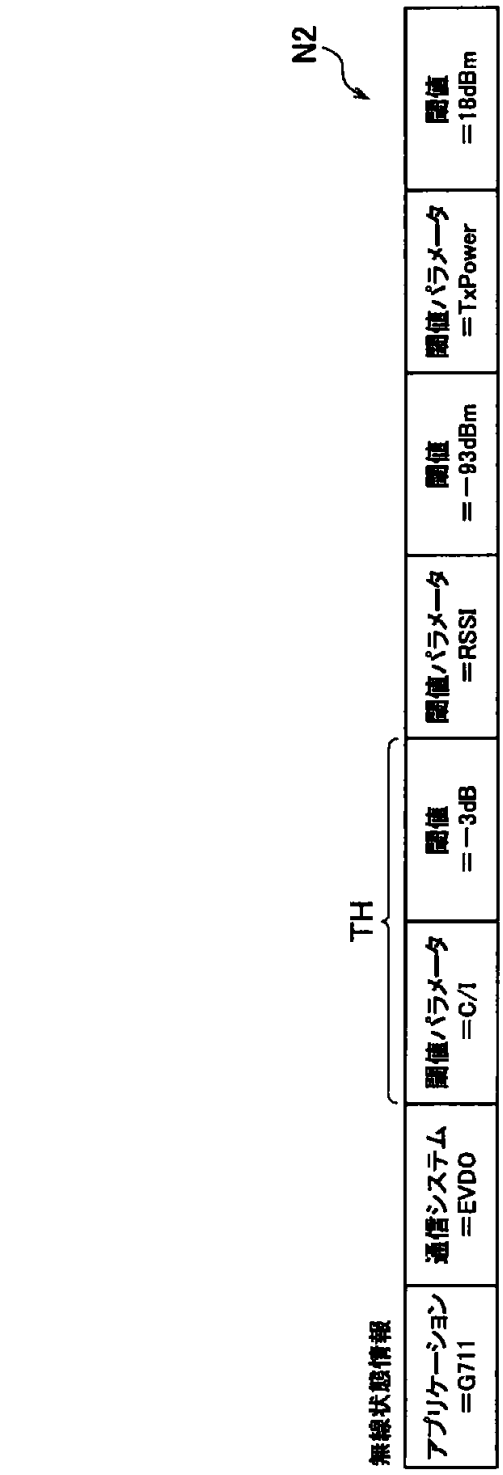
TH

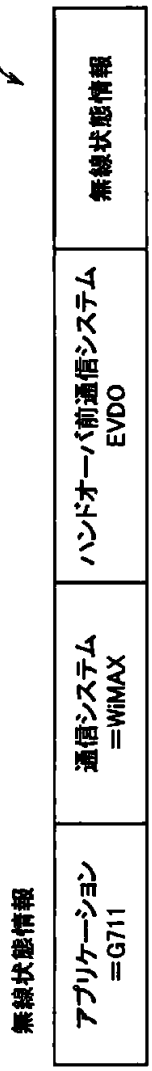
アプリケーション ＝G711	通信システム ＝EVDO	閾値パラメータ ＝C/I	閾値 ＝−3dB	閾値判定 Off

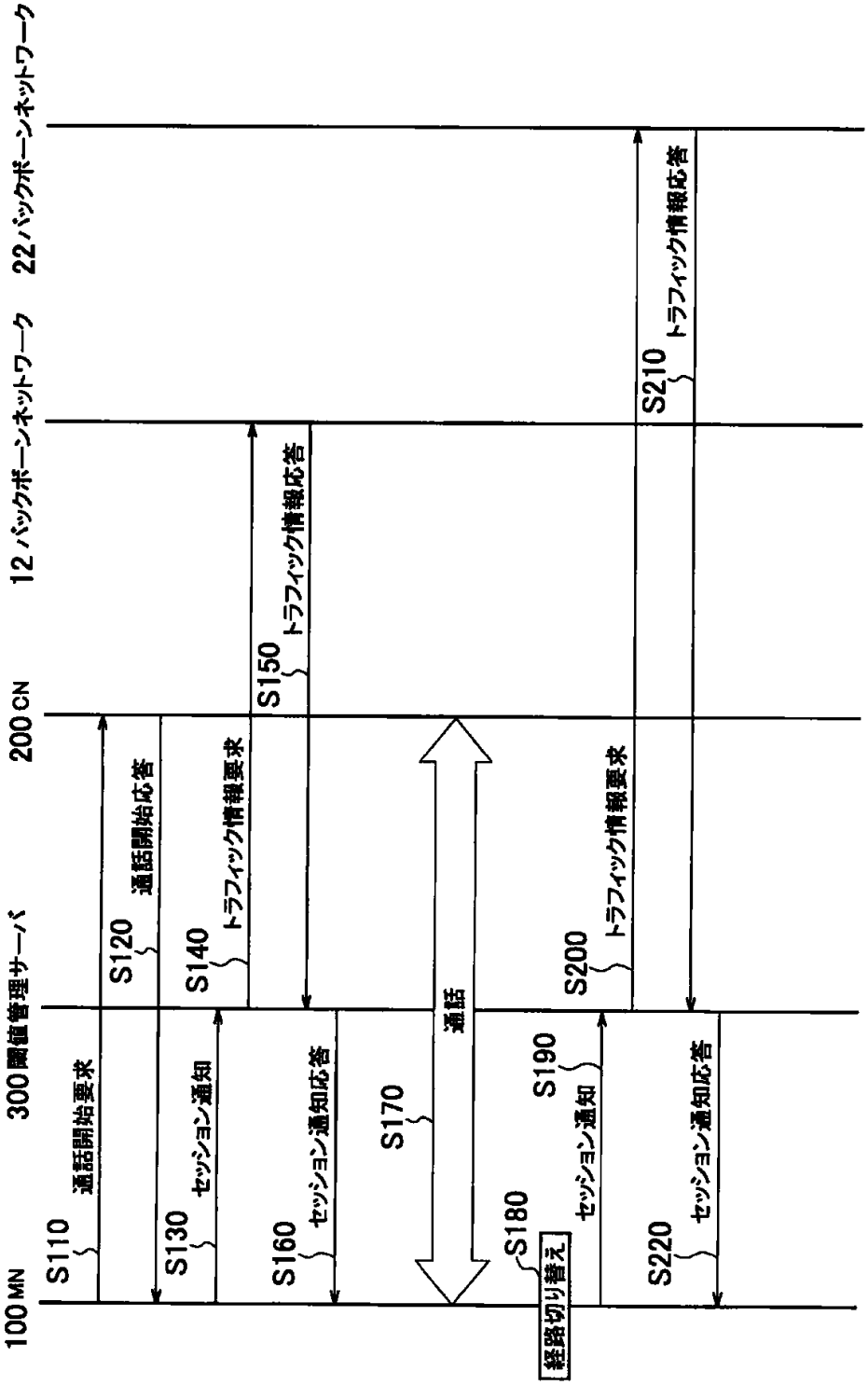
R2

セッション通知応答

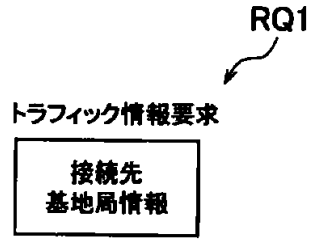
アプリケーション ＝G711	通信システム ＝EVDO	閾値パラメータ −	閾値 −	閾値判定 On

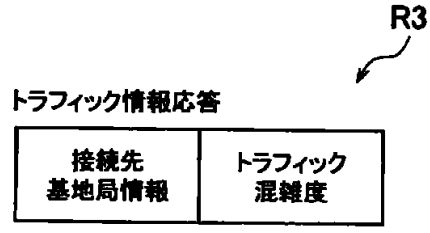

N2
無線状態情報
アプリケーション
=G711
通信システム
=EVDO
閾値パラメータ
=C/I
閾値
=−3dB
閾値パラメータ
=RSSI
閾値
=−93dBm
閾値パラメータ
=TxPower
閾値
=18dBm
TH


N3
無線状態情報
アプリケーション
=G711
通信システム
=WiMAX
ハンドオーバ前通信システム
EVDO
無線状態情報


100 MN
300 閾値管理サーバ
200 CN
12 バックボーンネットワーク
22 バックボーンネットワーク
S110
通話開始要求
S120
通話開始応答
S130
セッション通知
S140
トラフィック情報要求
S150
トラフィック情報応答
S160
セッション通知応答
S170
通話
S180
経路切り替え
S190
セッション通知
S200
トラフィック情報要求
S210
トラフィック情報応答
S220
セッション通知応答


N4
セッション通知
アプリケーション
＝G711
通信システム
＝EVDO
接続先
基地局情報


RQ1
トラフィック情報要求
接続先
基地局情報


R3
トラフィック情報応答
接続先
基地局情報
トラフィック
混雑度

TBa

アプリケーション	通信システム	閾値パラメータ	閾値
G711	EVDO	C/I	3
G711	WiMAX	RSSI	-85
G729	EVDO	C/I	-2
G729	WiMAX	RSSI	−92
G729	WiMAX	RSSI	−78
⋮	⋮	⋮	⋮

Electronic Acknowledgement Receipt

EFS ID:	20912082
Application Number:	14082040
International Application Number:	
Confirmation Number:	1015
Title of Invention:	Device-Assisted Services for Protecting Network Capacity
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	James E. Harris/Ann Taylor
Filer Authorized By:	James E. Harris
Attorney Docket Number:	RALEP032C1
Receipt Date:	09-DEC-2014
Filing Date:	15-NOV-2013
Time Stamp:	17:48:06
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	P032C1IDS.pdf	612584 c7d66dc553eaf4c8ebc16186d8de71b1097fc24c	no	6

Warnings:	
Information:	

2	Foreign Reference	2051.pdf	403577 d22e03358f57684914e973be2726a1020d61e766	no	20
Warnings:					
Information:					
3	Foreign Reference	2052.pdf	1089309 3986e176217ff4aabd958d4f301240ea4896296e	no	18
Warnings:					
Information:					
4	Foreign Reference	2053.pdf	513453 31e57d218f8274c4e588a81a345b9edf1e8d8125	no	16
Warnings:					
Information:					
5	Foreign Reference	2054.pdf	2451546 a2c79b6c1cd0073c23ae4a918ee197b9cb71a217	no	25
Warnings:					
Information:					
6	Foreign Reference	2055.pdf	362706 ade124f75667a4d2298f9390e64074e1a9570494	no	11
Warnings:					
Information:					
7	Foreign Reference	2056.pdf	2575701 24e70f7771bb68b3a29f93429c429d7c7fd9c846	no	34
Warnings:					
Information:					
8	Foreign Reference	2057.pdf	454629 1b7453dae97f43e4d44e293e6b2f7514f5bbcdd6	no	18
Warnings:					
Information:					
9	Foreign Reference	2058.pdf	1109411 4c2d545dca3e076795bb8a190443c7bf2fae96ad	no	29
Warnings:					
Information:					
		Total Files Size (in bytes):	9572916		

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

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

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

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

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

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

Application Number	14082040
Filing Date	2013-11-15
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP032C1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5131020	A	1992-07-14	Liebesny et al.	
	2	5325532	A	1994-06-28	Crosswy et al.	
	3	6640334	B	2003-10-28	Rasmussen, John H.	
	4	7409447	B	2008-08-05	Assadzadeh, Alireza	
	5	7614051	B	2009-11-03	Glaum et al.	
	6	7668612	B	2010-02-23	Okkonen, Harri	
	7	7756056	B2	2010-07-13	Kim et al.	
	8	8131281	B1	2012-03-06	Hildner et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	9	8160598	B2	2012-04-17	Savoor, Raghvendra	
	10	8223741	B	2012-07-17	Bartlett et al.	
	11	8370483	B	2013-02-05	Choong Jason et al.	
	12	8375136	B2	2013-02-12	Roman et al.	
	13	8396458	B	2013-03-12	Raleigh, Gregory G.	
	14	8645518	B	2014-02-04	David, Scott L.	
	15	8670334	B	2014-03-11	Keohane et al.	
	16	8676925	B	2014-03-18	Liu et al.	
	17	8693323		2014-04-08	McDysan, David E.	
	18	8725899	B	2014-05-13	Short et al.	
If you wish to add additional U.S. Patent citation information please click the Add button.						Add
U.S.PATENT APPLICATION PUBLICATIONS						Remove

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20040039792	A1	2004-02-26	Nakanishi, Tomoaki	
	2	20040137890	A1	2004-07-15	Kalke, Catherine	
	3	20040243992	A	2004-12-02	Gustafson et al.	
	4	20050075115	A1	2005-04-07	Corneille et al.	
	5	20050239447	A1	2005-10-27	Holzman et al.	
	6	20070143824	A1	2007-06-21	Shahbazi, Majid	
	7	20070213054	A1	2007-09-13	Han, Seung-Wook	
	8	20070226775	A	2007-09-27	Andreasen et al.	
	9	20070266422	A1	2007-11-15	Germano et al.	
	10	20080032715	A1	2008-02-07	Jia et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	11	20080139210	A	2008-06-12	Gisby et al.		
	12	20080166993	A1	2008-07-10	Gautier et al.		
	13	20080293395	A1	2008-11-27	Mathews et al.		
	14	20090044185	A1	2009-02-12	Krivopaltsev, Eugene		
	15	20090163173	A1	2009-06-25	Williams, Timothy D.		
	16	20090254857	A	2009-10-08	Romine et al.		
	17	20100075666	A1	2010-03-25	Garner, Neil Robert		
	18	20100235329	A	2010-09-16	Koren et al.		

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	101127988	CN	A	2008-02-20	ZTE Corporation		☐

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

NON-PATENT LITERATURE DOCUMENTS			Remove
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		☐

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

EXAMINER SIGNATURE			
Examiner Signature		Date Considered	

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

CERTIFICATION STATEMENT

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

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

OR

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

☐ See attached certification statement.

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

☒ None

SIGNATURE

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

Signature	/James E. Harris/	Date (YYYY-MM-DD)	2014-09-29
Name/Print	James E. Harris	Registration Number	40013

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04Q 7/32 (2006.01)
H04Q 7/34 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200710142965.4

[43] 公开日 2008 年 2 月 20 日

[11] 公开号 CN 101127988A

[22] 申请日 2007.8.13
[21] 申请号 200710142965.4
[71] 申请人 中兴通讯股份有限公司
地址 518057 广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦法务部
[72] 发明人 李 云 许军宁 吕 吉

[74] 专利代理机构 信息产业部电子专利中心
代理人 梁 军

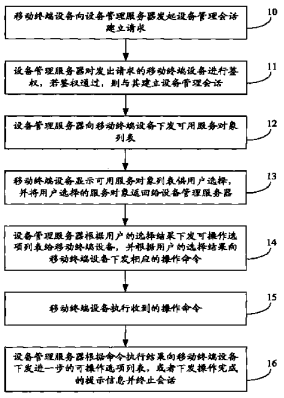
权利要求书 2 页 说明书 14 页 附图 7 页

[54] 发明名称

一种交互式设备管理的方法

[57] 摘要

本发明公开了一种交互式设备管理的方法，包括：移动终端设备向设备管理服务器发起设备管理会话建立请求，设备管理服务器与移动终端设备建立设备管理会话，并向其下发可用服务对象列表，移动终端设备显示可用服务对象列表供用户选择，设备管理服务器根据用户的选择结果下发可操作选项列表给移动终端设备，并根据用户的选择结果向移动终端设备下发相应的操作命令，移动终端设备执行收到的操作命令，设备管理服务器根据移动终端设备返回的命令执行的结果向移动终端设备下发进一步的可操作选项列表，或者向移动终端设备下发操作完成的提示信息并终止会话。 本发明极大的增强了系统和用户之间的交互能力，提高了运营商的服务质量。



1、一种交互式设备管理的方法，其特征在于，包括步骤：

A、移动终端设备向设备管理服务器发起设备管理会话建立请求，设备管理服务器与移动终端设备建立设备管理会话，并向其下发可用服务对象列表；

B、移动终端设备显示可用服务对象列表供用户选择，设备管理服务器根据用户的选择结果下发可操作选项列表给移动终端设备，并根据用户的选择结果向移动终端设备下发相应的操作命令；

C、设备管理服务器根据移动终端设备返回的命令执行的结果向移动终端设备下发进一步的可操作选项列表，或者向移动终端设备下发操作完成的提示信息并终止会话。

2、如权利要求 1 所述的方法，其特征在于，所述步骤 A 中，设备管理服务器收到设备管理会话建立请求后，对发出请求的移动终端设备进行鉴权，若鉴权通过，则设备管理服务器与移动终端设备建立设备管理会话。

3、如权利要求 1 所述的方法，其特征在于，所述步骤 B 中，可服务对象列表中包含以下服务对象中的至少一项：短消息、彩信、流媒体、接入点、电子邮箱、浏览器标签、设备管理帐户、数据同步帐户、软件管理和固件更新。

4、如权利要求 1 所述的方法，其特征在于，若移动终端设备为永久节点，所述步骤 B 中，设备管理服务器下发的可操作选项列表中针对用户选择的服务对象提供了查询、修改、默认设置、取消四种操作。

5、如权利要求 1 所述的方法，其特征在于，若移动终端设备为动态节点，所述步骤 B 中，设备管理服务器下发的可操作选项列表中针对用户选择的服务对象提供了查询、修改、默认设置、增加、删除、取消六种操作。

6、如权利要求 4 或 5 所述的方法，其特征在于，所述步骤 B 中，若用户选择的是修改或增加操作，则设备管理服务器向移动终端设备下发输入指令，以便用户输入一些关键参数，若用户选择的是默认设置，则设备管理服务器将默认参数下发给移动终端设备。

7、如权利要求 1 所述的方法，其特征在于，若用户从可用服务对象列表中选择了软件管理，则所述步骤 B 中，设备管理服务器向移动终端设备返回软件信息列表，其中提供了升级、卸载、激活、去激活当前已安装软件，取消本次操作及安装新软件的选项，若用户选择安装新软件，则设备管理服务器向移动终端设备返回可用软件列表供用户选择。

8、如权利要求 1 所述的方法，其特征在于，若用户从可用服务对象列表中选择了固件更新，则所述步骤 B 中，设备管理服务器根据移动终端设备的型号和版本向其返回升级包列表供用户选择。

9、如权利要求 1 所述的方法，其特征在于，所述步骤 C 中，设备管理服务器分析移动终端设备返回的命令执行结果，如果全部命令执行成功，则向移动终端设备下发操作成功的提示并终止会话；如果有执行失败的命令，则向移动终端设备下发失败原因提示并提供输入命令让用户重新输入参数，同时也提供放弃操作的选项。

10、如权利要求 9 所述的方法，其特征在于，如果用户选择重新输入参数，则流程返回步骤 C 的起始处。

一种交互式设备管理的方法

技术领域

本发明涉及移动通信技术领域，尤其涉及一种交互式设备管理的方法。

背景技术

移动终端设备是整个移动运营网络服务体系中最重要的组成部分，是和用户最密切相关的设备。根据开放移动联盟（OMA）的定义，设备管理是一个通用的术语，意指允许第三方为终端用户进行移动终端设备配置的技术。第三方包括运营商、服务提供商（SP）和信息管理部门。通过设备管理，一个外部实体可以远程为移动终端设备设置参数、引导移动终端设备进行故障检修、为移动终端设备安装或更新软件等等，同时还可以将运营商需要的业务信息和配置信息等从移动终端设备上采集到设备管理服务器中。因此设备管理系统可为用户提供免费或价廉的基本设备管理（DM）服务，如自动参数配置、故障诊断、固件更新、被盗手机锁定等，可为企业用户提供接入设置、应用设置、应用更新/升级、补丁下载、杀毒程序更新、故障诊断等，以及由网络侧向所有用户推送统企业标志（Logo）、电子邮件（Email）等与集团应用相关的客户化设置。

在目前的一些基于OMA DM协议的设备管理系统中，设备管理会话一般都是从服务端或者是服务端提供的门户上发起的，但是用户身边不可能随时随地带有接入网络的电脑，因而无法随时随地的连接设备管理的门户发起设备管理会话，这样就限制了业务的灵活性和便利性，影响了用户的体验。现有技术中一些设备管理管理系统也提供了从移动终端设备发起设备管理会话的功能，但是功能很简单，不支持用户的交互操作。

目前若干类似专利或专利申请也被相继提出来，专利号为

CN200510073504 的专利提出了一种在设备管理中处理交互超时的方法，但该专利仅仅说明了处理交互超时的方法而没有说明交互操作在设备管理过程中的详细应用。专利公开号为 US20050228847 的美国专利提出了一种使用 OMA DM 协议中的 alert 消息来进行交互的方法，该方法需要移动终端设备主动去请求可用服务列表，并且该发明不提供输入操作给用户，用户只能被动地去选择，极大的限制了用户的个性化设置内容。

发明内容

本发明提供一种交互式设备管理的方法，使得用户可直接通过移动终端设备发起设备管理会话，通过交互式命令完成该会话。

一种交互式设备管理的方法，包括步骤：

A、移动终端设备向设备管理服务器发起设备管理会话建立请求，设备管理服务器与移动终端设备建立设备管理会话，并向其下发可用服务对象列表；

B、移动终端设备显示可用服务对象列表供用户选择，设备管理服务器根据用户的选择结果下发可操作选项列表给移动终端设备，并根据用户的选择结果向移动终端设备下发相应的操作命令；

C、设备管理服务器根据移动终端设备返回的命令执行的结果向其下发进一步的可操作选项列表，或者向其下发操作完成的提示信息并终止会话。

所述步骤 A 中，设备管理服务器收到设备管理会话建立请求后，对发出请求的移动终端设备进行鉴权，若鉴权通过，则设备管理服务器与移动终端设备建立设备管理会话。

所述步骤 B 中，可服务对象列表中包含以下服务对象：短消息、彩信、流媒体、接入点、电子邮箱、浏览器标签、设备管理帐户、数据同步帐户、软件管理和固件更新。

若移动终端设备为永久节点，所述步骤 B 中，设备管理服务器下发的可操作选项列表中针对用户选择的服务对象提供了查询、修改、默认设置、取消四

种操作。

若移动终端设备为动态节点，所述步骤 B 中，设备管理服务器下发的可操作选项列表中针对用户选择的服务对象提供了查询、修改、默认设置、增加、删除、取消六种操作。

所述步骤 B 中，若用户选择的是修改或增加操作，则设备管理服务器向移动终端设备下发输入指令，以便用户输入一些关键参数，若用户选择的是默认设置，则设备管理服务器将默认参数下发给移动终端设备。

若用户从可用服务对象列表中选择了软件管理，则所述步骤 B 中，设备管理服务器向移动终端设备返回软件信息列表，其中提供了升级、卸载、激活、去激活当前已安装软件，取消本次操作及安装新软件的选项，若用户选择安装新软件，则设备管理服务器向移动终端设备返回可用软件列表供用户选择。

若用户从可用服务对象列表中选择了固件更新，则所述步骤 B 中，设备管理服务器根据移动终端设备的型号和版本向其返回升级包列表供用户选择。

所述步骤 C 中，设备管理服务器分析移动终端设备返回的命令执行结果，如果全部命令执行成功，则向移动终端设备下发操作成功的提示并终止会话；如果有执行失败的命令，则向移动终端设备下发失败原因提示并提供输入命令让用户重新输入参数，同时也提供放弃操作的选项。

如果用户选择重新输入参数，则流程返回步骤 C 的起始处。

采用本发明所述交互式设备管理的方法，用户可直接从移动终端设备发起设备管理会话，不再受电脑和网络的限制，同时本发明提供多种操作和菜单给用户进行选择，用户可实现个性化设置，而目前大多数方法仅提供统一设置。通过本发明，用户可以看到整个操作过程中的交互信息，能够及时了解发生了什么操作，可以选择是否进行下一步操作，从而极大的增强了系统和用户之间的交互能力，提高了运营商的服务质量。

附图说明

图 1 为本发明交互式设备管理的方法的实现原理流程图；

图 2 为本发明交互式设备管理的方法实施例一的流程图；

图 3 为本发明交互式设备管理的方法实施例二的流程图；

图 4 为本发明交互式设备管理的方法实施例三的流程图；

图 5 为本发明的交互式设备管理的方法中取消操作的流程图；

图 6 为本发明交互式设备管理的方法实施例四的流程图；

图 7 为本发明交互式设备管理的方法实施例五的流程图。

具体实施方式

下面将结合各个附图对本发明交互式设备管理的方法的具体实现过程进行进一步详细的阐述。

请参阅图 1，该图为本发明交互式设备管理的方法的实现原理流程图，其主要实现过程为：

步骤 10、移动终端设备向设备管理服务器发起设备管理会话建立请求，请求中携带有移动终端设备的基本信息和鉴权信息；

步骤 11、设备管理服务器收到设备管理会话建立请求后，对发出请求的移动终端设备进行鉴权，若鉴权通过，则设备管理服务器与移动终端设备建立设备管理会话；

步骤 12、设备管理服务器向移动终端设备下发可用服务对象列表；

步骤 13、移动终端设备显示可用服务对象列表供用户选择，用户从中指定服务对象，移动终端设备将用户选择的服务对象返回给设备管理服务器；

步骤 14、设备管理服务器根据用户的选择结果下发可操作选项列表给移动终端设备，并根据用户针对可操作选项列表的选择结果向移动终端设备下发相应的操作命令；

步骤 15、移动终端设备执行收到的操作命令；

步骤 16、设备管理服务器根据移动终端设备返回的命令执行的结果向移动

终端设备下发进一步的可操作选项列表，或者向移动终端设备下发操作完成的提示信息并终止会话。

请参阅图 2，该图为本发明交互式设备管理的方法实施例一的流程图，本实施例描述了采用本发明进行业务数据查询的过程，其主要实现流程如下：

步骤 101、移动终端设备向设备管理服务器发起建立 DM 会话请求，同时上报鉴权信息和移动终端设备的基本信息；

步骤 102、设备管理服务器接收到移动终端设备的请求后对终端设备进行鉴权，若鉴权通过则组装可服务对象列表；

步骤 103、设备管理服务器下发可服务对象列表给移动终端设备；

步骤 104、移动终端设备提示用户进行选择；

步骤 105、用户选择了菜单中的某项，如短消息、彩信、流媒体、接入点、电子邮箱等；

步骤 106、移动终端设备将选择结果返回给设备管理服务器；

步骤 107、设备管理服务器根据用户选择的服务对象生成可操作命令菜单；

步骤 108、设备管理服务器下发可操作命令菜单到移动终端设备；

步骤 109、移动终端设备提示用户进行选择；

步骤 110、用户选择命令菜单中的查询业务信息选项；

步骤 111、移动终端设备将用户选择的结果返回给设备管理服务器；

步骤 112、设备管理服务器收到返回后根据用户先前所选择的业务将对应的参数组装到查询命令当中；

步骤 113、设备管理服务器向移动终端设备下发采集命令；

步骤 114、移动终端设备将参数信息返回给设备管理服务器；

步骤 115、设备管理服务器收到采集的结果后将结果组装成合适的说明信息；

步骤 116、设备管理服务器将说明信息下发给移动终端设备，以便展示给用户；

步骤 117、移动终端设备将说明信息展现给用户；

步骤 118、用户确认该说明信息；

步骤 119、移动终端设备将用户的确认操作信息返回给设备管理服务器；

步骤 120、设备管理服务器终止本次会话。

请参阅图 3，该图为本发明交互式设备管理的方法实施例二的流程图，本实施例描述了采用本发明进行业务数据修改、增加或删除的过程，其主要实现流程如下：

步骤 201、移动终端设备向设备管理服务器发起建立 DM 会话请求，同时上报鉴权信息和移动终端设备的基本信息；

步骤 202、设备管理服务器接收到移动终端设备的请求后对移动终端设备进行鉴权，若鉴权通过则组装可服务对象列表；

步骤 203、设备管理服务器下发可服务对象列表给移动终端设备；

步骤 204、移动终端设备提示用户进行选择；

步骤 205、用户选择了菜单中的某项，如短消息，彩信，流媒体，接入点，电子邮箱等；

步骤 206、移动终端设备将选择结果返回给设备管理服务器；

步骤 207、设备管理服务器根据用户选择的服务对象生成相应命令，如果是永久节点，则生成命令菜单，菜单包含命令查询，修改，默认配置，取消，永久节点的定义是：移动终端设备上对于同一种应用只能有唯一一种配置；如果是动态节点，设备管理服务器生成采集该应用的参数的命令，动态节点的定义是：同一种应用可以有多种配置，例如同一个移动终端设备可以设置多个接入点，每个接入点的配置都不相同；

如果是永久节点，流程如下：

步骤 208、设备管理服务器下发可操作命令菜单到移动终端设备；

步骤 209、移动终端设备提示用户进行选择，流程跳转到步骤 224，后续继续说明。

如果是动态节点，流程如下：

步骤 210、设备管理服务器下发获取该业务的所有配置信息的命令；

步骤 211、移动终端设备将所有配置信息返回给设备管理服务器；

步骤 212、设备管理服务器将所述配置信息以列表形式下发给移动终端设备，此列表的最后一项为“增加”；

步骤 213、移动终端设备提示用户进行选择，若用户选择了增加，则流程跳转到步骤 224，后续继续说明。

步骤 214、用户选择了某个已存在的配置；

步骤 215、移动终端设备将用户的选择结果返回给设备管理服务器；

步骤 216、设备管理服务器组装命令菜单（修改、删除、取消）；

步骤 217、设备管理服务器向移动终端设备下发命令菜单；

步骤 218、移动终端设备提示用户进行选择，如果用户选择了修改，则流程跳转到步骤 224，后续继续说明。

步骤 219、用户选择了删除；

步骤 220、移动终端设备将结果返回给设备管理服务器；

步骤 221、设备管理服务器向移动终端设备下发删除命令；

步骤 222、移动终端设备将命令执行结果返回给设备管理服务器；

步骤 223、设备管理服务器向移动终端设备下发删除成功或失败的提示信息，并终止会话。

步骤 224、用户选择修改或增加业务信息；

步骤 225、移动终端设备将用户选择的结果返回给设备管理服务器；

步骤 226、设备管理服务器根据用户选择的业务将具体需要输入的关键参数组装成 DM 协议命令；

步骤 227、设备管理服务器将 DM 协议命令下发到移动终端设备；

步骤 228、移动终端设备提示用户输入业务参数；

步骤 229、用户输入业务参数；

步骤 230、移动终端设备将输入结果返回给设备管理服务器;

步骤 231、设备管理服务器收到用户的输入后将得到的参数组装成配置命令;

步骤 232、设备管理服务器将配置命令下发给移动终端设备;

步骤 233、移动终端设备根据配置命令进行相应的配置;

步骤 234、移动终端设备将配置操作的结果返回给设备管理服务器;

步骤 235、设备管理服务器分析返回的结果，若无出错信息，则执行步骤 236，若包含出错信息，则执行步骤 237;

步骤 236、设备管理服务器向移动终端设备返回配置成功的提示信息并终止会话;

步骤 237、设备管理服务器向移动终端设备返回操作选项，选项内容中包括继续输入或放弃;

步骤 238、移动终端设备提示用户进行选择;

步骤 239、用户选择输入或放弃;

步骤 240、移动终端设备将用户选择的结果返回给设备管理服务器;

步骤 241、设备管理服务器查看返回的结果，若用户选择的是输入，则流程返回步骤 226，若用户选择了放弃，则设备管理服务器终止会话，执行步骤 242;

步骤 242、设备管理服务器发送终止会话消息给移动终端设备。

请参阅图 4，该图为本发明交互式设备管理的方法实施例三的流程图，本实施例描述了采用本发明将某种业务数据的配置修改为默认设置的过程，其主要实现流程如下:

步骤 301、移动终端设备向设备管理服务器发起建立 DM 会话请求，同时上报鉴权信息和移动终端设备的基本信息;

步骤 302、设备管理服务器接收到移动终端设备的请求后对移动终端设备进行鉴权，若鉴权通过则组装可服务对象列表;

步骤 303、设备管理服务器下发可服务对象列表给移动终端设备;

步骤 304、移动终端设备提示用户进行选择;

步骤 305、用户选择了菜单中的某项，如短消息，彩信，流媒体，接入点，电子邮箱等;

步骤 306、移动终端设备将选择结果返回给设备管理服务器;

步骤 307、设备管理服务器根据用户选择的服务对象生成可操作命令菜单;

步骤 308，设备管理服务器下发可操作命令菜单到移动终端设备;

步骤 309、移动终端设备提示用户进行选择;

步骤 310、用户选择了默认配置选项;

步骤 311、移动终端设备将用户选择结果返回给设备管理服务器;

步骤 312、设备管理服务器按照默认参数来组装对应的配置命令;

步骤 313、设备管理服务器将配置命令下发给移动终端设备;

步骤 314、移动终端设备根据接收到的配置命令进行配置;

步骤 315、移动终端设备将配置操作的结果返回给设备管理服务器;

步骤 316、设备管理服务器分析返回的结果，若无出错信息，则执行步骤 317，若包含出错信息，则执行步骤 318;

步骤 317、设备管理服务器返回成功提示信息并终止会话.

步骤 318、设备管理服务器向移动终端设备返回继续输入或放弃的操作选项;

步骤 319、移动终端设备提示用户进行选择;

步骤 320、用户选择输入或放弃;

步骤 321、移动终端设备将用户的选择结果返回给设备管理服务器，若用户选择的是输入，则流程跳转到步骤 312，但此时是按照用户的输入来组装配置命令，若用户选择放弃，则执行步骤 322;

步骤 322、设备管理服务器终止会话;

步骤 323、设备管理服务器发送终止会话消息给移动终端设备。

请参阅图 5，该图为本发明的交互式设备管理的方法中取消操作的流程图，其主要实现过程如下：

步骤 401、移动终端设备向设备管理服务器发起建立 DM 会话请求，同时上报鉴权信息和移动终端设备的基本信息；

步骤 402、设备管理服务器接收到移动终端设备的请求后对移动终端设备进行鉴权，若鉴权通过则组装可服务对象列表；

步骤 403、设备管理服务器下发可服务对象列表给移动终端设备；

步骤 404、移动终端设备提示用户进行选择；

步骤 405、用户选择了菜单中的某项，如短消息，彩信，流媒体，接入点，电子邮箱等；

步骤 406、移动终端设备将选择结果返回给设备管理服务器；

步骤 407、设备管理服务器根据用户选择的服务对象生成可操作命令菜单；

步骤 408，设备管理服务器下发可操作命令菜单到移动终端设备；

步骤 409、移动终端设备提示用户进行选择；

步骤 410、用户选择了取消选项；

步骤 411、移动终端设备将用户选择的结果返回给设备管理服务器；

步骤 412、设备管理服务器终止本次会话。

请参阅图 6，该图为本发明交互式设备管理的方法实施例四的流程图，本实施例描述了采用本发明对移动终端设备进行软件管理的过程，其主要实现流程如下：

步骤 501、移动终端设备向设备管理服务器发起建立 DM 会话请求，同时上报鉴权信息和移动终端设备的基本信息；

步骤 502、设备管理服务器接收到移动终端设备的请求后对移动终端设备进行鉴权，若鉴权通过则组装可服务对象列表；

步骤 503、设备管理服务器下发可服务对象列表给移动终端设备；

步骤 504、移动终端设备提示用户进行选择；

步骤 505、用户选择了菜单中的软件管理;

步骤 506、移动终端设备将选择结果返回给设备管理服务器;

步骤 507、设备管理服务器组装获取该移动终端设备上所有软件信息的命令;

步骤 508、设备管理服务器下发获取命令到移动终端设备;

步骤 509、移动终端设备将软件信息返回给设备管理服务器;

步骤 510、设备管理服务器根据返回的结果组装生成软件信息列表，其中提供了升级、卸载、激活、去激活当前已安装软件，取消本次操作及安装新软件的选项;

步骤 511、设备管理服务器将软件信息列表下发到移动终端设备;

步骤 512、移动终端设备将软件信息列表展示给用户。

若此时用户想安装新软件，则流程如下:

步骤 513、用户选择安装新软件;

步骤 514、移动终端设备将用户选择结果返回给设备管理服务器;

步骤 515、设备管理服务器将可用软件列表下发给移动终端设备;

步骤 516、移动终端设备将软件信息列表展示给用户;

步骤 517、用户从软件信息列表选择某个软件进行安装;

步骤 518、移动终端设备将用户的选择结果返回给设备管理服务器;

步骤 519、设备管理服务器向移动终端设备下发该软件的安装包;

步骤 520、移动终端设备接收软件安装包并安装该软件;

步骤 521、移动终端设备将安装结果返回给设备管理服务器;

步骤 522、设备管理服务器向移动终端设备提示安装结果，成功或失败，并终止会话。

若此时用户想升级某个已经安装的软件，则流程如下:

步骤 523、用户选择某个已经安装的软件;

步骤 524、移动终端设备将用户选择结果返回给设备管理服务器;

步骤 525、设备管理服务器下发操作菜单给移动终端设备;

步骤 526、移动终端设备将操作列表展示给用户，此列表包含升级、激活、去激活和卸载;

步骤 527、用户选择升级;

步骤 528、移动终端设备将用户选择结果返回给设备管理服务器;

步骤 529、设备管理服务器根据先前用户选择的软件的名称和版本号选择升级包，若无可用更新则执行步骤 530，若有可用更新，则执行步骤 531;

步骤 530、设备管理服务器向移动终端设备下发无可用更新的提示信息并终止会话。

步骤 531、设备管理服务器向移动终端设备下发该软件的升级包;

步骤 532、移动终端设备接收升级包，并安装;

步骤 533、移动终端设备将升级结果返回给设备管理服务器;

步骤 534、设备管理服务器向移动终端设备下发成功或失败的升级结果提示信息，并终止会话。

若此用户希望对某个软件进行激活、去激活或卸载操作，则流程如下:

步骤 535、用户选择了某个已经安装的软件;

步骤 536、移动终端设备将用户选择结果返回给设备管理服务器;

步骤 537、设备管理服务器下发操作菜单给移动终端设备;

步骤 538、移动终端设备将操作列表展示给用户;

步骤 539、用户选择激活，去激活或卸载;

步骤 540、移动终端设备将用户选择结果返回给设备管理服务器;

步骤 541、设备管理服务器组装相应命令下发给移动终端设备;

步骤 542、移动终端设备执行相应命令;

步骤 543、移动终端设备将命令执行的结果返回给设备管理服务器;

步骤 544、设备管理服务器发送提示信息，提示用户成功或失败，并终止会话。

请参阅图 7，该图为本发明交互式设备管理的方法实施例五的流程图，本实施例描述了采用本发明对移动终端设备进行固件更新的过程，其主要实现流程如下：

步骤 601、移动终端设备向设备管理服务器发起建立 DM 会话请求，同时上报鉴权信息和移动终端设备的基本信息；

步骤 602、设备管理服务器接收到移动终端设备的请求后对移动终端设备进行鉴权，若鉴权通过则组装可服务对象列表；

步骤 603、设备管理服务器下发可服务对象列表给移动终端设备；

步骤 604、移动终端设备提示用户进行选择；

步骤 605、用户选择了菜单中的固件更新；

步骤 606、移动终端设备将用户选择结果返回给设备管理服务器；

步骤 607、设备管理服务器生成采集移动终端设备固件详细信息的命令；

步骤 608、设备管理服务器将该命令下发到移动终端设备；

步骤 609、移动终端设备将固件信息返回给设备管理服务器；

步骤 610、设备管理服务器根据固件信息查找可用的升级包并生成升级包列表；

步骤 611、设备管理服务器下发升级包列表到移动终端设备，此列表最后一项为默认；

步骤 612、设备管理服务器提示用户选择升级包；

步骤 613、用户选择某个升级包或选择默认；

步骤 614、移动终端设备将用户选择的结果返回给设备管理服务器；

步骤 615、设备管理服务器根据用户的选择获取相应的升级包数据，若选择的是默认，则获取最新的升级包数据；

步骤 616、设备管理服务器将用户选择的升级包下发到移动终端设备；

步骤 617、移动终端设备接收到升级包数据后执行升级操作；

步骤 618、移动终端设备将升级结果返回给设备管理服务器；

步骤619、设备管理服务器向移动终端设备下发固件更新成功或失败的提示信息，并终止会话。

显然，本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样，倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。

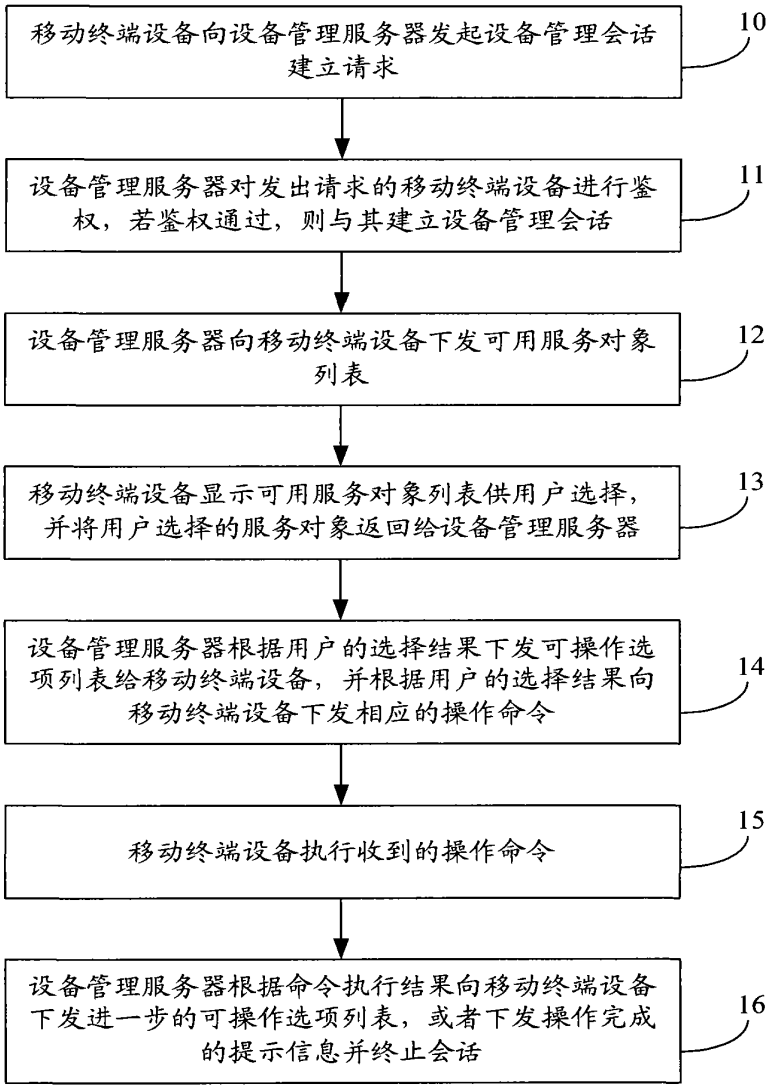

移动终端设备向设备管理服务器发起设备管理会话建立请求
10
设备管理服务器对发出请求的移动终端设备进行鉴权，若鉴权通过，则与其建立设备管理会话
11
设备管理服务器向移动终端设备下发可用服务对象列表
12
移动终端设备显示可用服务对象列表供用户选择，并将用户选择的服务对象返回给设备管理服务器
13
设备管理服务器根据用户的选择结果下发可操作选项列表给移动终端设备，并根据用户的选择结果向移动终端设备下发相应的操作命令
14
移动终端设备执行收到的操作命令
15
设备管理服务器根据命令执行结果向移动终端设备下发进一步的可操作选项列表，或者下发操作完成的提示信息并终止会话
16

图 1

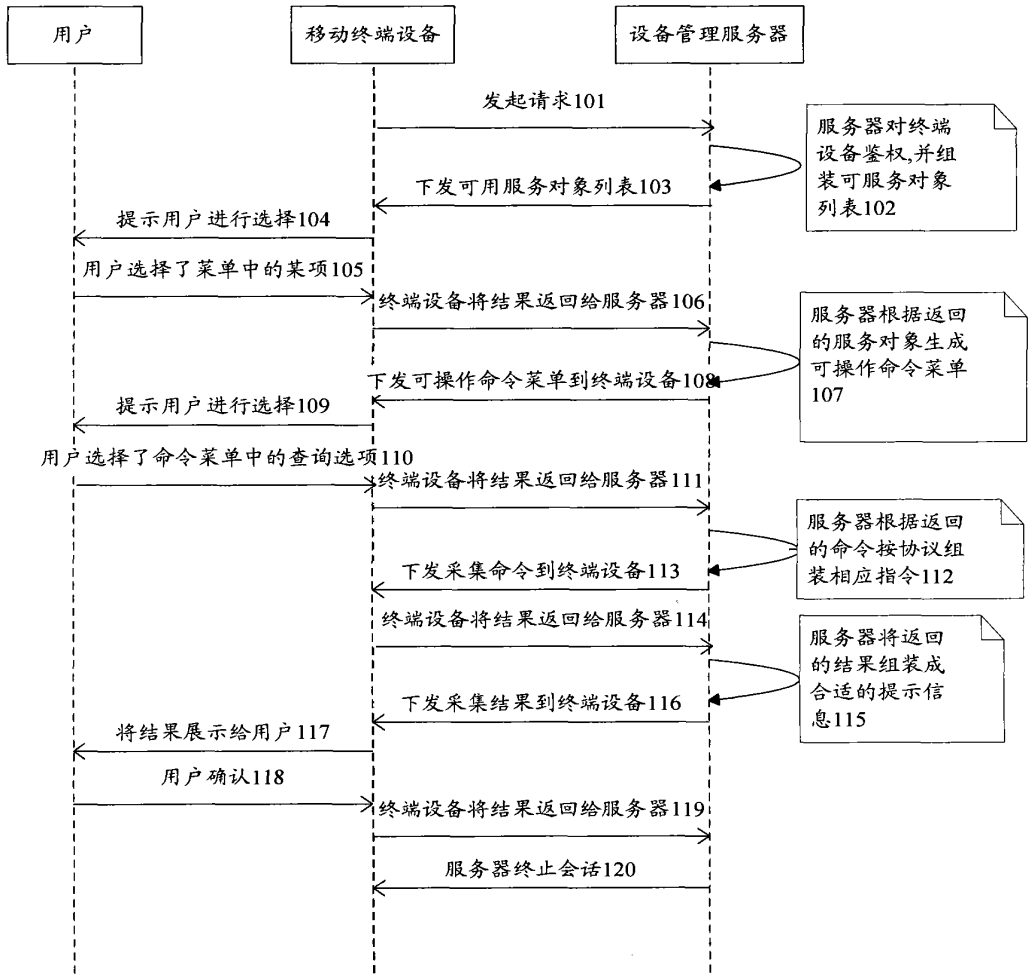

用户
移动终端设备
设备管理服务器
发起请求101
服务器对终端设备鉴权,并组装可服务对象列表102
下发可用服务对象列表103
提示用户进行选择104
用户选择了菜单中的某项105
终端设备将结果返回给服务器106
服务器根据返回的服务对象生成可操作命令菜单107
下发可操作命令菜单到终端设备108
提示用户进行选择109
用户选择了命令菜单中的查询选项110
终端设备将结果返回给服务器111
服务器根据返回的命令按协议组装相应指令112
下发采集命令到终端设备113
终端设备将结果返回给服务器114
服务器将返回的结果组装成合适的提示信息115
下发采集结果到终端设备116
将结果展示给用户117
用户确认118
终端设备将结果返回给服务器119
服务器终止会话120

图 2

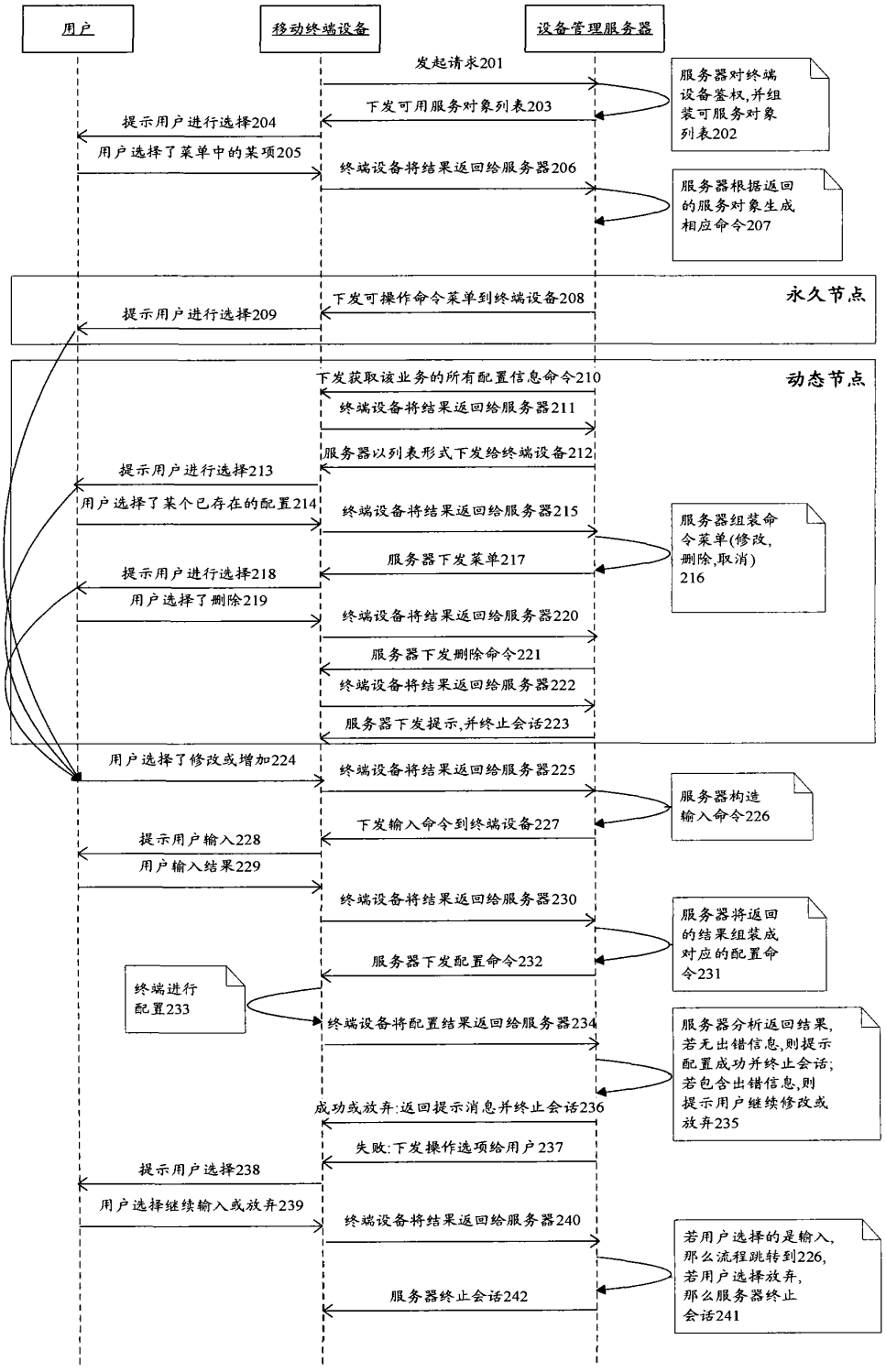

用户
移动终端设备
设备管理服务器
发起请求201
服务器对终端设备鉴权,并组装可服务对象列表202
下发可用服务对象列表203
提示用户进行选择204
用户选择了菜单中的某项205
终端设备将结果返回给服务器206
服务器根据返回的服务对象生成相应命令207
永久节点
下发可操作命令菜单到终端设备208
提示用户进行选择209
动态节点
下发获取该业务的所有配置信息命令210
终端设备将结果返回给服务器211
服务器以列表形式下发给终端设备212
提示用户进行选择213
用户选择了某个已存在的配置214
终端设备将结果返回给服务器215
服务器组装命令菜单(修改,删除,取消)216
服务器下发菜单217
提示用户进行选择218
用户选择了删除219
终端设备将结果返回给服务器220
服务器下发删除命令221
终端设备将结果返回给服务器222
服务器下发提示,并终止会话223
用户选择了修改或增加224
终端设备将结果返回给服务器225
服务器构造输入命令226
下发输入命令到终端设备227
提示用户输入228
用户输入结果229
终端设备将结果返回给服务器230
服务器将返回的结果组装成对应的配置命令231
服务器下发配置命令232
终端进行配置233
终端设备将配置结果返回给服务器234
服务器分析返回结果,若无出错信息,则提示配置成功并终止会话;若包含出错信息,则提示用户继续修改或放弃235
成功或放弃:返回提示消息并终止会话236
失败:下发操作选项给用户237
提示用户选择238
用户选择继续输入或放弃239
终端设备将结果返回给服务器240
若用户选择的是输入,那么流程跳转到226,若用户选择放弃,那么服务器终止会话241
服务器终止会话242

图 3

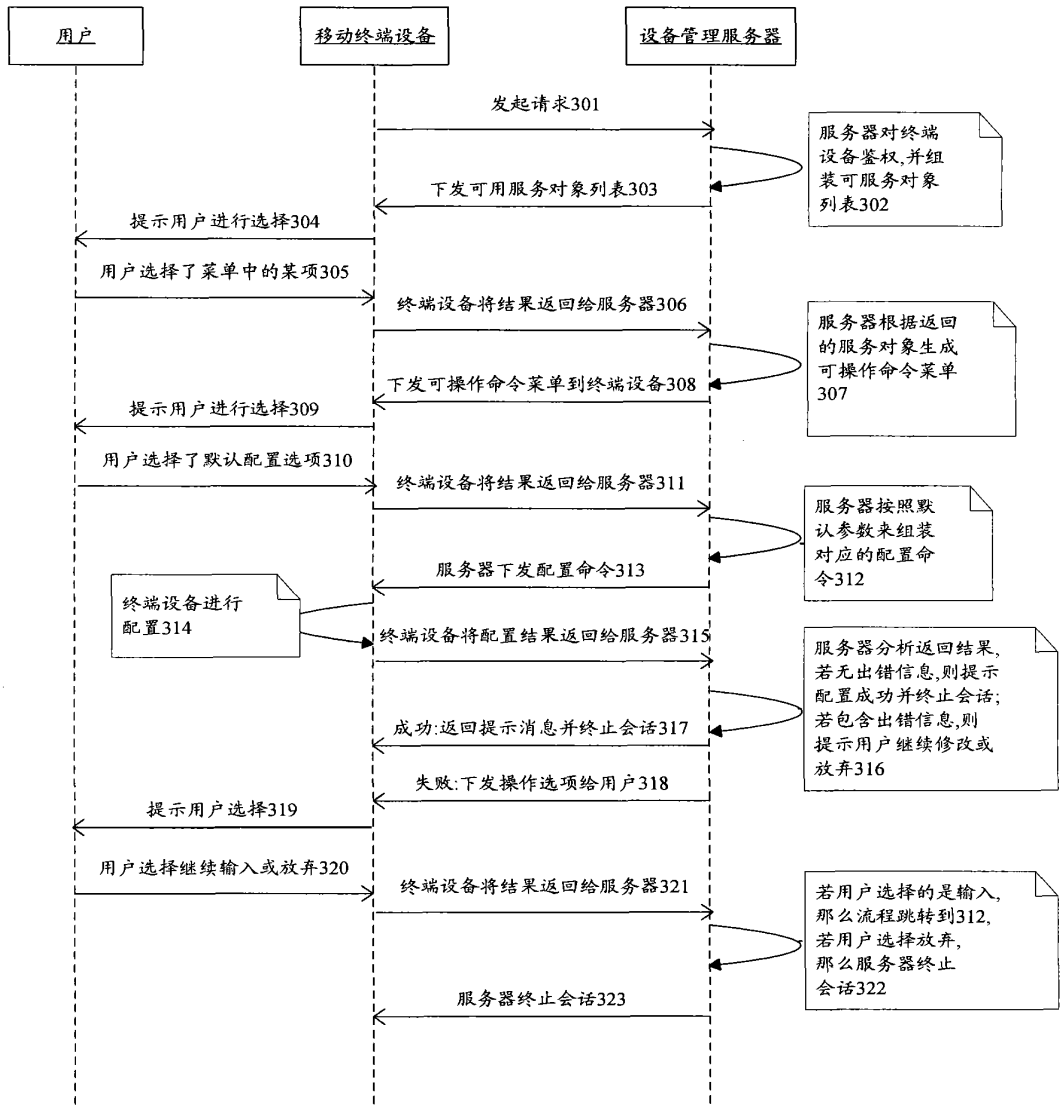

用户
移动终端设备
设备管理服务器
发起请求301
服务器对终端设备鉴权,并组装可服务对象列表302
下发可用服务对象列表303
提示用户进行选择304
用户选择了菜单中的某项305
终端设备将结果返回给服务器306
服务器根据返回的服务对象生成可操作命令菜单307
下发可操作命令菜单到终端设备308
提示用户进行选择309
用户选择了默认配置选项310
终端设备将结果返回给服务器311
服务器按照默认参数来组装对应的配置命令312
服务器下发配置命令313
终端设备进行配置314
终端设备将配置结果返回给服务器315
服务器分析返回结果,若无出错信息,则提示配置成功并终止会话;若包含出错信息,则提示用户继续修改或放弃316
成功:返回提示消息并终止会话317
失败:下发操作选项给用户318
提示用户选择319
用户选择继续输入或放弃320
终端设备将结果返回给服务器321
若用户选择的是输入,那么流程跳转到312,若用户选择放弃,那么服务器终止会话322
服务器终止会话323

图 4

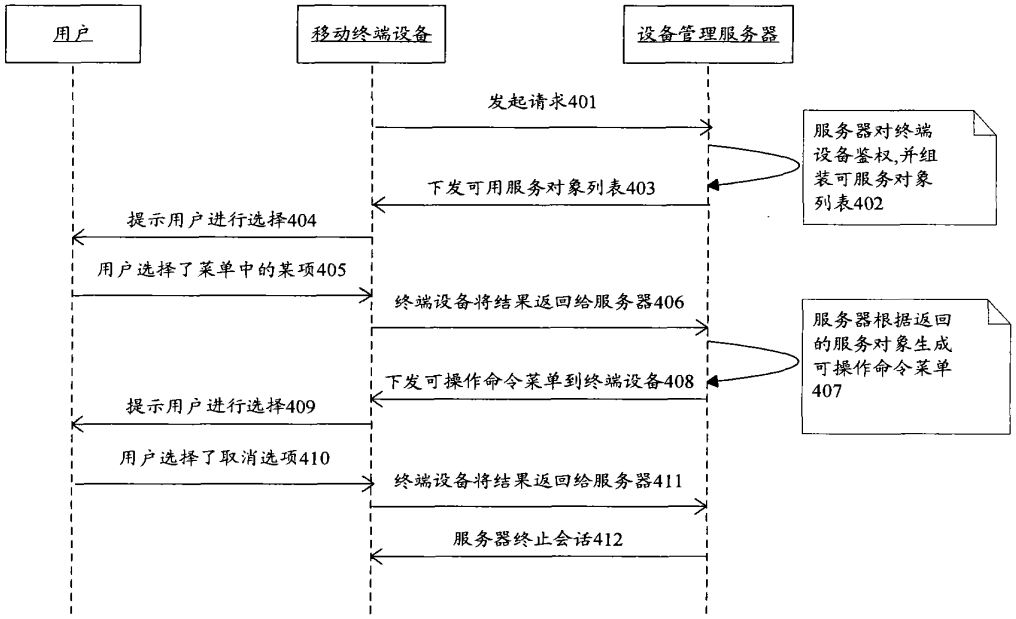

用户
移动终端设备
设备管理服务器
发起请求401
服务器对终端设备鉴权,并组装可服务对象列表402
下发可用服务对象列表403
提示用户进行选择404
用户选择了菜单中的某项405
终端设备将结果返回给服务器406
服务器根据返回的服务对象生成可操作命令菜单407
下发可操作命令菜单到终端设备408
提示用户进行选择409
用户选择了取消选项410
终端设备将结果返回给服务器411
服务器终止会话412

图 5

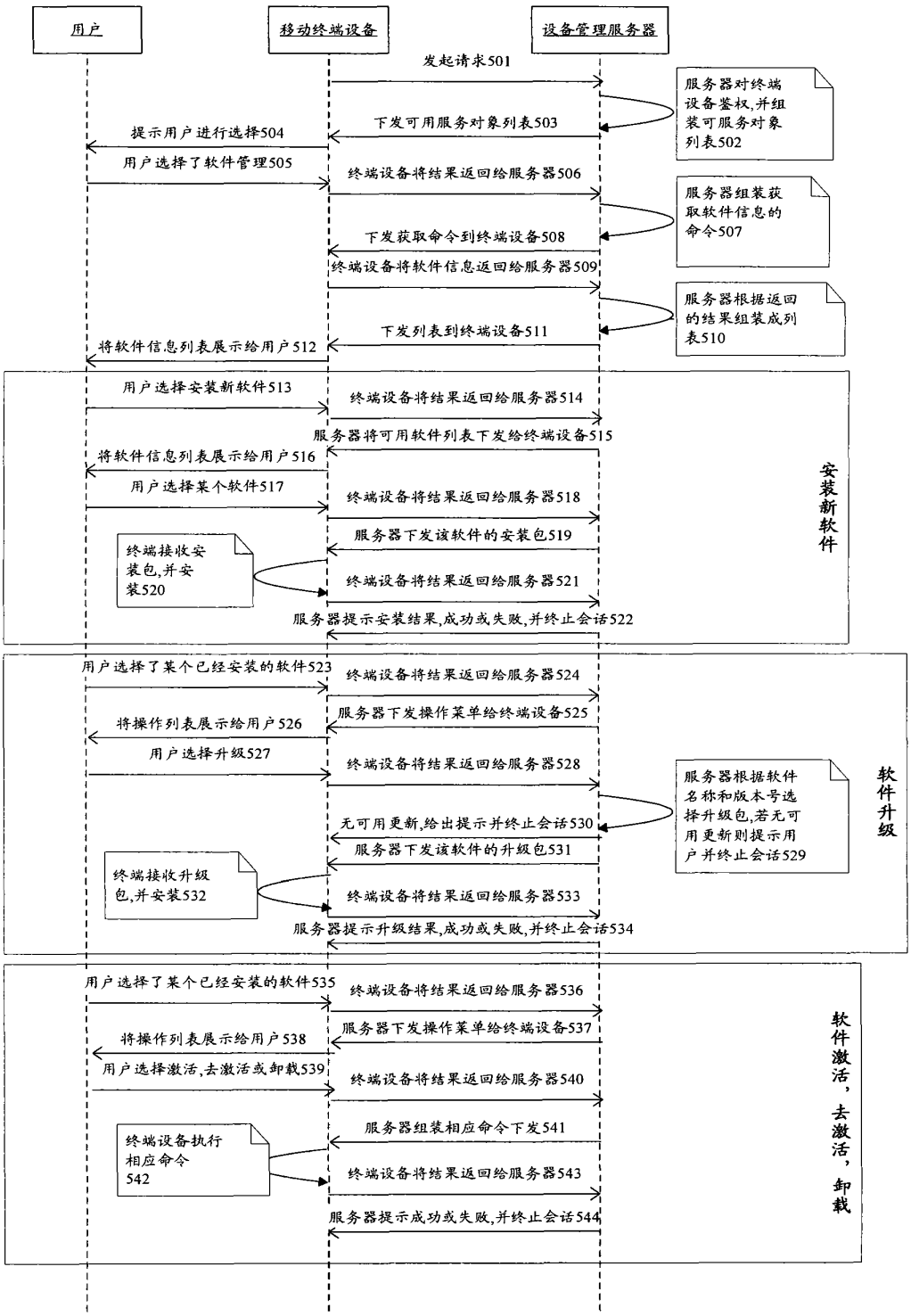

用户
移动终端设备
设备管理服务器
发起请求501
服务器对终端设备鉴权,并组装可服务对象列表502
下发可用服务对象列表503
提示用户进行选择504
用户选择了软件管理505
终端设备将结果返回给服务器506
服务器组装获取软件信息的命令507
下发获取命令到终端设备508
终端设备将软件信息返回给服务器509
服务器根据返回的结果组装成列表510
下发列表到终端设备511
将软件信息列表展示给用户512
用户选择安装新软件513
终端设备将结果返回给服务器514
服务器将可用软件列表下发给终端设备515
将软件信息列表展示给用户516
用户选择某个软件517
终端设备将结果返回给服务器518
服务器下发该软件的安装包519
终端接收安装包,并安装520
终端设备将结果返回给服务器521
服务器提示安装结果,成功或失败,并终止会话522
安装新软件
用户选择了某个已经安装的软件523
终端设备将结果返回给服务器524
服务器下发操作菜单给终端设备525
将操作列表展示给用户526
用户选择升级527
终端设备将结果返回给服务器528
服务器根据软件名称和版本号选择升级包,若无可用更新则提示用户并终止会话529
无可用更新,给出提示并终止会话530
服务器下发该软件的升级包531
终端接收升级包,并安装532
终端设备将结果返回给服务器533
服务器提示升级结果,成功或失败,并终止会话534
软件升级
用户选择了某个已经安装的软件535
终端设备将结果返回给服务器536
服务器下发操作菜单给终端设备537
将操作列表展示给用户538
用户选择激活,去激活或卸载539
终端设备将结果返回给服务器540
服务器组装相应命令下发541
终端设备执行相应命令542
终端设备将结果返回给服务器543
服务器提示成功或失败,并终止会话544
软件激活,去激活,卸载

图 6

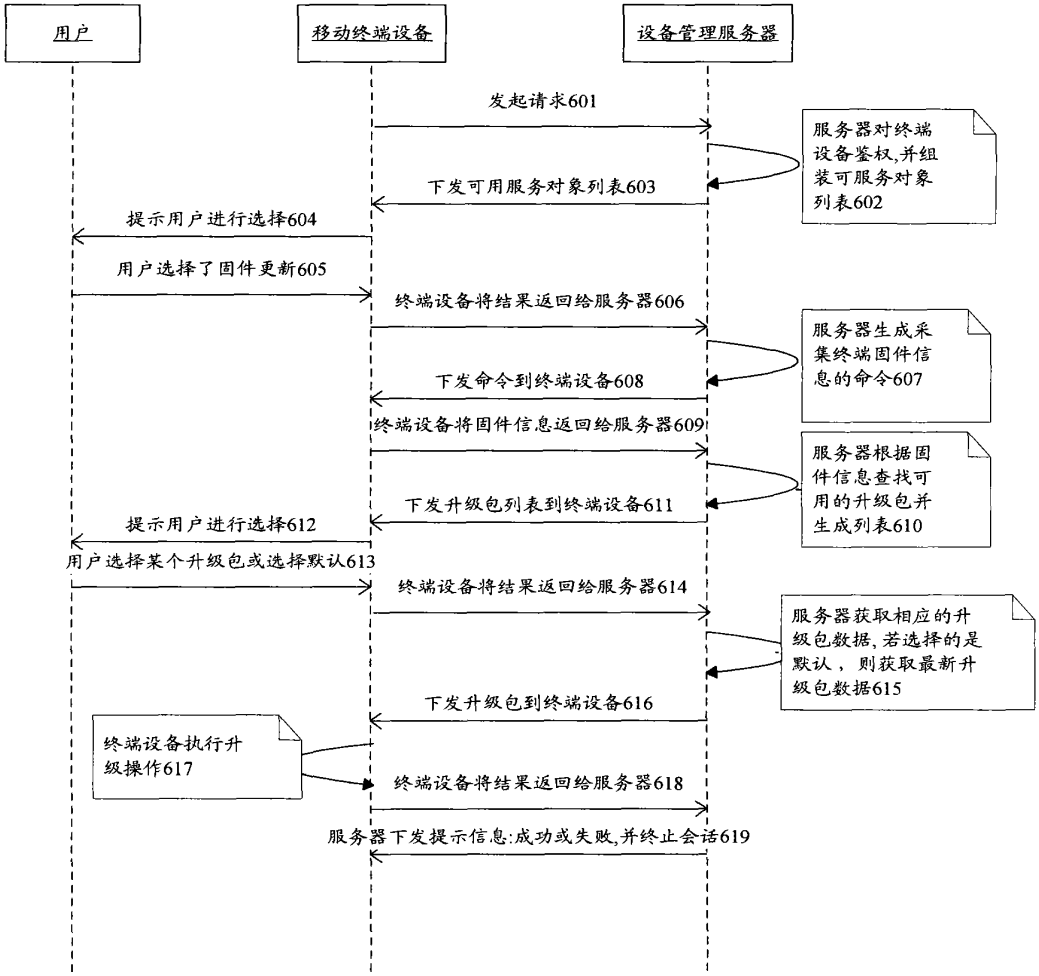

用户
移动终端设备
设备管理服务器
发起请求601
服务器对终端设备鉴权,并组装可服务对象列表602
下发可用服务对象列表603
提示用户进行选择604
用户选择了固件更新605
终端设备将结果返回给服务器606
服务器生成采集终端固件信息的命令607
下发命令到终端设备608
终端设备将固件信息返回给服务器609
服务器根据固件信息查找可用的升级包并生成列表610
下发升级包列表到终端设备611
提示用户进行选择612
用户选择某个升级包或选择默认613
终端设备将结果返回给服务器614
服务器获取相应的升级包数据,若选择的是默认，则获取最新升级包数据615
下发升级包到终端设备616
终端设备执行升级操作617
终端设备将结果返回给服务器618
服务器下发提示信息:成功或失败,并终止会话619

图 7

Electronic Acknowledgement Receipt

EFS ID:	20274891
Application Number:	14082040
International Application Number:	
Confirmation Number:	1015
Title of Invention:	Device-Assisted Services for Protecting Network Capacity
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	James E. Harris/Ann Taylor
Filer Authorized By:	James E. Harris
Attorney Docket Number:	RALEP032C1
Receipt Date:	29-SEP-2014
Filing Date:	15-NOV-2013
Time Stamp:	17:11:08
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	P032C1IDS.pdf	612972 228ce0c67cf313d9f95b147af71fc7a9a716ec45	no	7

Warnings:	
Information:	

2	Foreign Reference	2050.pdf	1136346 21c4e4c1c0f43b05ddbed691b4fd8f87df8a12e4	no	24

Warnings:	
Information:	
Total Files Size (in bytes):	1749318

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

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

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

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

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

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

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

Application Number	14082040
Filing Date	2013-11-15
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Gart, Matthew S.
Attorney Docket Number	RALEP032C1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	7805140	B2	2010-09-28	Friday et al.	
	2	8605691	B2	2013-12-10	Soomro et al.	
	3	8655357	B1	2014-02-18	Gazzard et al.	
	4	8706863		2014-04-22	Fadell, Anthony	

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20020188732	A1	2002-12-12	Buckman et al.	
	2	20080010379	A	2008-01-10	Zhao, Hang	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Gart, Matthew S.
	Attorney Docket Number	RALEP032C1

	3	20080034419	A	2008-02-07	Mullick et al.	

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	1878160	CN	A	2006-12-13	Jiang, Yong		☐
	2	2011149532	WO	A1	2011-12-01	Raleigh et al.		☐

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

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		☐

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

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Gart, Matthew S.
	Attorney Docket Number	RALEP032C1

CERTIFICATION STATEMENT

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

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

OR

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

☐ See attached certification statement.

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

☒ None

SIGNATURE

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

Signature	/Krista S. Jacobsen/	Date (YYYY-MM-DD)	2014-07-16
Name/Print	Krista S. Jacobsen	Registration Number	59374

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 29/00 (2006.01)
H04N 7/24 (2006.01)

[12] 发明专利申请公开说明书

[21] 申请号 200610099396.5

[43] 公开日 2006 年 12 月 13 日

[11] 公开号 CN 1878160A

[22] 申请日 2006.7.19
[21] 申请号 200610099396.5
[71] 申请人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼
[72] 发明人 蒋 勇

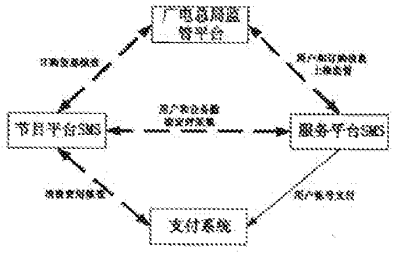
[74] 专利代理机构 北京凯特来知识产权代理有限公司
代理人 郑立明
权利要求书 4 页 说明书 27 页 附图 2 页

[54] 发明名称

一种节目交换系统

[57] 摘要

本发明提供一种节目交换系统，其核心为：服务平台将其存储的用户收视信息分别传输至监管平台和与其有节目交换的节目平台，节目平台将服务平台传输来的用户收视信息传输至监管平台，监管平台根据服务平台和节目平台分别传输来的用户收视信息对节目交换进行监管。本发明的节目交换系统和节目交换方法中的节目平台、服务平台和监管平台分工明确，且本发明对节目平台和服务平台以及传输网络都没有任何额外的要求，易于实施，降低了节目交换系统的建设成本及维护运营成本；本发明能够保证节目平台与服务平台分成结算的准确性和公证性；从而实现了提高节目交换系统可实用性的目的。



1、一种节目交换系统，包括：至少一个节目平台和至少一个服务平台，一个服务平台与至少一个节目平台进行节目交换，其特征在于，所述节目平台中设置有第一复用加扰设备，所述服务平台中设置有解扰设备和第二复用加扰设备；

第一复用加扰设备根据预定的服务平台授权信息为服务平台提供复用加扰节目流；

服务平台前端的解扰设备根据预定的服务平台授权信息对节目平台提供的节目流进行解扰，并将解扰后的节目流传输至第二复用加扰设备；

第二复用加扰设备根据其接收的节目流、预定的用户授权信息为用户提供复用加扰节目流。

2、如权利要求 1 所述的一种节目交换系统，其特征在于，所述解扰设备为：机顶盒和承载有服务平台授权信息的节目平台用户智能卡。

3、如权利要求 1 所述的一种节目交换系统，其特征在于，所述节目平台中还设置有节目服务控制模块；

节目服务控制模块：用于根据预定的服务平台授权信息对服务平台提供的节目服务进行开启/关停控制。

4、如权利要求 1 或 2 或 3 所述的一种节目交换系统，其特征在于，所述节目交换系统中还设置有监管平台；

服务平台将其存储的用户收视信息分别传输至监管平台和与其有节目交换的节目平台；

所述节目平台将所述服务平台传输来的用户收视信息传输至监管平台；

所述监管平台根据所述服务平台和所述节目平台分别传输来的用户收视

信息对节目交换进行监管。

5、如权利要求 4 所述的一种节目交换系统，其特征在于，监管平台为：对行业进行监管的节目监管平台、和/或处于第三方支付状态的支付监管平台。

6、如权利要求 5 所述的一种节目交换系统，其特征在于，所述监管平台为节目监管平台时，所述服务平台包括：第一收视信息传输模块和第二收视信息传输模块，且所述节目监管平台设置有第一一致性核查模块；

第一收视信息传输模块：用于采用服务平台与节目监管平台之间的节目监管接口将服务平台的用户管理系统和条件接收系统中的用户数据和用户订购数据传输至节目监管平台；

第二收视信息传输模块：用于采用服务平台与节目平台之间的节目监管接口将服务平台的用户管理系统中的与节目平台相关的用户数据和用户订购数据传输至节目平台；

第一一致性核查模块：用于对服务平台和节目平台分别传输来的用户数据和用户订购数据进行一致性核查。

7、如权利要求 6 所述的一种节目交换系统，其特征在于，所述服务平台与节目监管平台之间的节目监管接口为：基于广电总局的《有线数字电视节目平台与监管平台数据交换协议、内容与格式要求》的节目监管接口；所述服务平台与节目平台之间的节目监管接口为：周期性上报的服务平台销售明细、单用户的业务明细、指定日期的产品销售数量、业务发展报告。

8、如权利要求 6 所述的一种节目交换系统，其特征在于，所述节目监管平台与节目平台之间设置有节目监管接口，该接口为：基于广电总局的《用户管理系统与监管平台数据交换接口技术要求》的节目监管接口。

9、如权利要求 5 所述的一种节目交换系统，其特征在于，所述监管平台

为支付监管平台时，所述服务平台包括：第三收视信息传输模块和第四收视信息传输模块，且所述支付监管平台设置有第二一致性核查模块；

第三收视信息传输模块：用于采用服务平台与支付监管平台之间的支付接口将服务平台的用户管理系统中的用户节目支付费用数据传输至支付监管平台；

第四收视信息传输模块：用于采用服务平台与节目平台之间的节目监管接口将服务平台的用户管理系统中的与节目平台相关的节目销售收入数据传输至节目平台；

第二一致性核查模块：用于对服务平台传输来的用户节目支付费用数据和节目平台传输来的用户节目销售收入数据进行一致性核查。

10、如权利要求9所述的一种节目交换系统，其特征在于，所述服务平台与支付监管平台之间的支付接口包括下述接口中的一个或多个：建立支付关系的接口、解除支付关系的接口、支付费用接口、支付记录总额对帐接口、支付记录明细对帐接口、服务平台产品支付记录的交易总额对帐接口。

11、如权利要求9所述的一种节目交换系统，其特征在于，所述节目平台与支付监管平台之间设置有用户帐户支付核查接口，节目平台将所述服务平台传输来的节目销售收入数据通过所述用户帐户支付核查接口传输至支付监管平台；

所述用户帐户支付核查接口包括：服务平台产品支付记录明细对帐。

12、如权利要求1或2或3所述的一种节目交换系统，其特征在于，所述节目平台和/或服务平台中设置有分成结算模块；

当分成结算模块设置于节目平台时，节目平台通过节目交换接口从服务平台获取分成结算信息；

所述分成结算信息包括：节目销售收入数据，或者获取用户数据和节目销

售收入数据；

分成结算模块：用于根据预定结算分成协议、分成结算信息进行分成结算。

13、如权利要求12所述的一种节目交换系统，其特征在于，所述预定结算分成协议为下述一种或多种：基于固定时长统谈的分成协议、基于节目授权量的分成协议、基于节目授权时长的分成协议、基于节目销售收入的分成协议。

14、如权利要求12所述的一种节目交换系统，其特征在于，所述预定结算分成协议包括：节目平台与节目提供商之间的结算分成协议、和/或节目平台与服务平台之间的结算分成协议。

15、如权利要求14所述的一种节目交换系统，其特征在于，所述节目平台与服务平台之间的结算分成协议包括：分成策略协议、和/或累积奖励协议。

16、如权利要求12所述的一种节目交换系统，其特征在于，所述分成结算信息包括下述一种或多种：周期性的服务平台销售明细、单用户的业务明细、指定日期的产品销售数量、周期性的业务发展报告。

一种节目交换系统

技术领域

本发明涉及网络通讯技术领域，具体涉及一种节目交换系统。

背景技术

随着社会的进步，产业的分工越来越细化，就有线电视服务而言，已由模拟电视时期的内容制作与节目传输“一体化”模式，演进为内容制作与节目传输分离的“台网分离”模式。

在国内，典型的“台网分离”模式的应用场景为：广电网络公司提供数字电视网络，然后，广电网络公司从节目平台购买节目内容。数字电视用户通过向广电网络公司订购节目，即可收看丰富的数字电视节目。最后，节目平台与广电网络公司进行结算分成。在这个应用场景中广电网络公司做为服务平台向用户提供数字电视服务。

在这种“台网分离”模式下，节目平台与服务平台分工协作，向用户提供数字电视服务。节目平台提供丰富的数字电视节目，服务平台提供节目收视服务。目前，节目平台与服务平台之间的节目交换方法主要有如下两种：

方法一：完全开放方式，如附图1所示。

图1中，节目平台通过传输网络直接向服务平台提供清流或固定加扰的节目流，服务平台通过传输网络从节目平台获取节目流，对于固定加扰的节目流，服务平台则需要进行固定解扰，然后，服务平台通过数字电视前端系统对节目流进行复用加扰，并让调制后的节目流进入服务平台的有线网络。

服务平台可以通过SMS（用户管理系统）发展用户并进行节目销售授权。

节目平台和服务平台之间签订节目使用协议，并按照固定时长进行结算分成。

由于节目平台进入传输网络的节目流一般为清流或固定加扰的节目流，使节目流容易被破解，使该方法安全性低；由于节目平台和服务平台之间没有实际的节目控制通道，只能完全按照签订的节目通过人为方式来实现节目服务，无法灵活控制节目服务的开启和关停，使节目服务控制不灵活；在这种节目交换方法中，不存在监管关系，也没有良好的监控措施，节目平台和服务平台只能采用按固定时长的统谈方式，使结算分成方式单一。

方法二、两级加密，共同授权方式，实现了"用户透明，计费准确"，达到了对节目平台加扰传输的数字电视节目进行版权保护的目的。方法二具体如附图2所示。

图2中，节目平台加扰下传的数字付费电视节目，在服务平台前端不解扰，直接进入服务平台的有线网络，在服务平台运营范围内的数字电视用户收看节目平台数字付费电视节目时，必须同时获得节目平台和服务平台的授权。由于每次服务平台的用户授权都需要同时发送到节目平台，节目平台可以准确获知服务平台用户节目的收视情况，因此，节目平台和服务平台之间可以采用固定时长、节目授权量、节目授权时长等方式进行结算分成。

在方式二中，节目平台为实现对用户收视情况、服务平台实际收入等的监管，需要建设多家CAS（条件接收系统）、且CAS的数量与各服务平台的CAS厂家数量相当，使节目平台的CAS数量众多；服务平台的SMS需要通过IP网络提供的通道实时地将用户数据和节目销售授权信息传送给节目平台的SMS，该IP网络要求安全性高，双向具有足够大的带宽，且需要保持实时的连接，从而在IP网络通道的建设和运营上需要成本投入；由于服务平台的用户数据和授权信息都需要在节目平台上存储，随着服务平台数量的增多，服务平台用户数量的增多，节目平台系统需要不断升级扩容，节目平台升级扩容压力大使运营成本不断升高。上述原因使节目平台在CAS的建设和运营上成本高昂。

由于节目授权采用同密方式，要求节目平台的CAS和服务平台的CAS必须为同一厂家的CAS系统，而且，服务平台的CAS系统必须支持两级加密，使方法二对服务平台的CAS要求严格。

由于节目在节目平台和服务平台上两级加密，共同授权，因此，一次销售授权处理需要经过的设备和系统很多，不但增加了节目平台、服务平台的建设复杂度，而且，任何设备或系统的不稳定都会影响整个节目交换的处理过程，使系统稳定性差。

发明内容

本发明的目的在于，提供一种节目交换系统，通过预定的服务平台授权信息，使服务平台成为节目平台的用户，使节目平台能够方便的对其与服务平台之间的节目交换进行管理，避免了节目交换对节目平台、服务平台的CAS、SMS以及传输网络的额外要求，降低了节目交换系统的建设成本和运营成本。

为达到上述目的，本发明提供的一种节目交换系统，包括：至少一个节目平台和至少一个服务平台，一个服务平台与至少一个节目平台进行节目交换，所述节目平台中设置有第一复用加扰设备，所述服务平台中设置有解扰设备和第二复用加扰设备；

第一复用加扰设备根据预定的服务平台授权信息为服务平台提供复用加扰节目流；

服务平台前端的解扰设备根据预定的服务平台授权信息对节目平台提供的节目流进行解扰，并将解扰后的节目流传输至第二复用加扰设备；

第二复用加扰设备根据其接收的节目流、预定的用户授权信息为用户提供复用加扰节目流。

下述技术方案为可选技术方案。

所述解扰设备为：机顶盒和承载有服务平台授权信息的节目平台用户智能

卡。

所述节目平台中还设置有节目服务控制模块;

节目服务控制模块:用于根据预定的服务平台授权信息对服务平台提供的节目服务进行开启/关停控制。

所述节目交换系统中还设置有监管平台;

服务平台将其存储的用户收视信息分别传输至监管平台和与其有节目交换的节目平台;

所述节目平台将所述服务平台传输来的用户收视信息传输至监管平台;

所述监管平台根据所述服务平台和所述节目平台分别传输来的用户收视信息对节目交换进行监管。

监管平台为:对行业进行监管的节目监管平台、和/或处于第三方支付状态的支付监管平台。

所述监管平台为节目监管平台时,所述服务平台包括:第一收视信息传输模块和第二收视信息传输模块,且所述节目监管平台设置有第一一致性核查模块;

第一收视信息传输模块:用于采用服务平台与节目监管平台之间的节目监管接口将服务平台的用户管理系统和条件接收系统中的用户数据和用户订购数据传输至节目监管平台;

第二收视信息传输模块:用于采用服务平台与节目平台之间的节目监管接口将服务平台的用户管理系统中的与节目平台相关的用户数据和用户订购数据传输至节目平台;

第一一致性核查模块:用于对服务平台和节目平台分别传输来的用户数据和用户订购数据进行一致性核查。

所述服务平台与节目监管平台之间的节目监管接口为:基于广电总局的《有线数字电视节目平台与监管平台数据交换协议、内容与格式要求》的节目

监管接口；所述服务平台与节目平台之间的节目监管接口为：周期性上报的服务平台销售明细、单用户的业务明细、指定日期的产品销售数量、业务发展报告。

所述节目监管平台与节目平台之间设置有节目监管接口，该接口为：基于广电总局的《用户管理系统与监管平台数据交换接口技术要求》的节目监管接口。

所述监管平台为支付监管平台时，所述服务平台包括：第三收视信息传输模块和第四收视信息传输模块，且所述支付监管平台设置有第二一致性核查模块；

第三收视信息传输模块：用于采用服务平台与支付监管平台之间的支付接口将服务平台的用户管理系统中的用户节目支付费用数据传输至支付监管平台；

第四收视信息传输模块：用于采用服务平台与节目平台之间的节目监管接口将服务平台的用户管理系统中的与节目平台相关的节目销售收入数据传输至节目平台；

第二一致性核查模块：用于对服务平台传输来的用户节目支付费用数据和节目平台传输来的用户节目销售收入数据进行一致性核查。

所述服务平台与支付监管平台之间的支付接口包括下述接口中的一个或多个：建立支付关系的接口、解除支付关系的接口、支付费用接口、支付记录总额对帐接口、支付记录明细对帐接口、服务平台产品支付记录的交易总额对帐接口。

所述节目平台与支付监管平台之间设置有用户帐户支付核查接口，节目平台将所述服务平台传输来的节目销售收入数据通过所述用户帐户支付核查接口传输至支付监管平台；

所述用户帐户支付核查接口包括：服务平台产品支付记录明细对帐。

所述节目平台和/或服务平台中设置有分成结算模块；

当分成结算模块设置于节目平台时，节目平台通过节目交换接口从服务平台获取分成结算信息；

所述分成结算信息包括：节目销售收入数据，或者获取用户数据和节目销售收入数据；

分成结算模块：用于根据预定结算分成协议、分成结算信息进行分成结算。

所述预定结算分成协议为下述一种或多种：基于固定时长统谈的分成协议、基于节目授权量的分成协议、基于节目授权时长的分成协议、基于节目销售收入的分成协议。

所述预定结算分成协议包括：节目平台与节目提供商之间的结算分成协议、和/或节目平台与服务平台之间的结算分成协议。

所述节目平台与服务平台之间的结算分成协议包括：分成策略协议、和/或累积奖励协议。

所述分成结算信息包括下述一种或多种：周期性的服务平台销售明细、单用户的业务明细、指定日期的产品销售数量、周期性的业务发展报告。

通过上述技术方案的描述可知，本发明通过预定的服务平台授权信息，使服务平台成为节目平台的用户，使节目平台能够方便的对其与服务平台之间的节目交换进行管理；本发明中节目平台为服务平台提供节目的授权与服务平台为有线电视用户提供节目的授权完全独立，不但通过两级加密保证了节目交换的安全性，还避免了节目交换对节目平台、服务平台的CAS、SMS以及传输网络的额外要求，易于实施，且简化了节目交换的实现过程，提高了节目交换系统的稳定性，保证了节目交换运营的安全性，降低了节目交换维护的复杂度，从而降低了节目交换系统的建设成本和运营成本；本发明的节目平台能够按照预先签订的授权信息即节目使用协议灵活控制对服务平台提供节目服务的开启和关停，节目服务控制灵活，既提高了业务运营的灵活性，又达到了对节目

平台加扰传输的数字电视节目进行版权保护的目的；本发明通过在节目交换系统中设置监管平台，使节目平台、服务平台和监管平台分工明确，使节目平台能够专注于提供节目内容服务、服务平台能够专注于提供节目收视服务；本发明的监管平台可以为节目监管平台、支付监管平台，节目监管平台可以利用行业公用监管系统，如广电总局监管平台，支付监管平台可以利用第三方支付系统，如银行等，通过监管平台对服务平台上报至节目平台的运营数据进行核查，充分保证了节目平台与服务平台进行结算的基础数据的准确性，从而保证节目平台与服务平台分成结算的准确性和公证性；本发明的节目平台与服务平台之间的结算分成方式灵活多样；从而通过本发明提供的技术方案实现了提高节目交换系统实用性、可运营性的目的。

附图说明

图1是现有技术的节目交换方法的示意图一；

图2是现有技术的节目交换方法的示意图二；

图3是本发明实施例的节目交换系统示意图；

图4是本发明实施例的节目交换系统实现节目交换的示意图。

具体实施方式

本发明的节目交换系统的核心在于：节目平台中设置的第一复用加扰设备根据预定的服务平台授权信息为服务平台提供复用加扰节目流，服务平台前端的解扰设备根据预定的服务平台授权信息对节目平台提供的节目流进行解扰，并将解扰后的节目流传输至服务平台中设置的第二复用加扰设备，第二复用加扰设备根据其接收的节目流、预定的用户授权信息为用户提供复用加扰节目流。

下面基于本发明的核心思想、结合附图对本发明提供的节目交换系统进行详细描述。

为保证本发明节目交换系统中的节目平台能够方便的对其与服务平台之间的节目交换进行管理，同时，使服务平台能够安全、方便的为有线电视用户提供的有线电视节目，降低节目平台、服务平台的运营成本、降低有线电视用户收看电视节目的成本，本发明的节目交换系统中的节目平台、服务平台进行节目交换的过程如附图3所示。

图 3 中，节目平台将服务平台作为一个用户来管理，即在节目平台中对服务平台进行用户开户，节目平台将对该服务平台的授权信息承载于智能卡中，并向服务平台发放智能卡。这样，节目平台能够根据授权信息为服务平台提供相应的节目流，而且该节目流是加密的节目流，即节目平台根据预定的服务平台授权信息对相应的节目流进行复用加扰处理，然后，将复用加扰处理后的节目流传输至服务平台，节目平台对节目流的复用加扰处理过程由节目平台中的第一复用加扰设备来实现。

智能卡中的授权信息包括：一个或多个 PDK（个人密钥）、每个节目的 SK（加密密钥）等。服务平台使用 PDK 可以从节目平台传输来的加扰节目流中的 EMM（授权管理信息）中解出每个节目的 SK，SK 数量随着智能卡上授权的节目数而不同，SK 更新周期由 CA 系统（条件授权）确定，如 1 个月，服务平台可通过节目流中的 EMM 的版本号自动确定是否更新 SK。

节目平台可以根据预定的服务平台授权信息对其为服务平台提供的节目服务进行开启/关停控制，该控制功能由节目平台的节目服务控制模块来实现。

在服务平台前端，通过解扰设备如机顶盒和节目平台分配的智能卡，对节目平台传输来的节目流进行解扰，服务平台对节目流进行解扰的过程由服务平台的解扰设备来实现。服务平台前端重新对解扰后的节目流根据预定的用户授权信息进行复用加扰，复用加扰后的节目流进入服务平台的有线电视网络。服务平台对节目流进行复用加扰的过程由服务平台中设置的第二复用加扰设备来实现。

在服务平台运营范围内的有线电视用户收看节目平台的数字付费电视节目时，只需获得服务平台的授权即可。这样，服务平台的用户节目销售授权在服务平台前端系统中即可完成，无需实时请求节目平台的授权。

本发明为了使节目平台能够专注于提供节目内容服务、服务平台能够专注于提供节目收视服务、保证节目平台与服务平台进行结算的基础数据的准确性，本发明在图3的节目交换系统中设置了监管平台。

上述监管平台可以为对用户收视信息中的用户数据和用户订购数据进行监管的节目监管平台，也可以为对用户收视信息中的用户节目支付费用数据和节目销售收入数据进行监管的支付监管平台，由此，本发明的节目交换系统可以包括：至少一个节目平台、至少一个服务平台和节目监管平台，可以包括：至少一个节目平台、至少一个服务平台和支付监管平台，也可以同时包括：至少一个节目平台、至少一个服务平台、节目监管平台和支付监管平台。

当本发明的节目交换系统包括至少一个节目平台、至少一个服务平台、节目监管平台和支付监管平台时，节目交换系统实现节目交换方法的示意图如附图4所示。

图4中，本发明的节目交换系统包括：至少一个节目平台、至少一个服务平台、节目监管平台和支付监管平台。节目监管平台可以为公用的对行业进行监管的平台如广电总局监管平台，支付监管平台为处于第三方支付状态的平台，如银行、支付网关等支付系统。

服务平台需要将其存储的用户收视信息分别传输至节目监管平台、支付监管平台和节目平台。用户收视信息的具体传输过程为：服务平台和节目监管平台之间设置有节目监管接口，服务平台采用其与节目监管平台之间的节目监管接口将SMS和CAS中存储的用户数据和用户订购数据传输至节目监管平台。这部分功能由服务平台中的第一收视信息传输模块来实现。服务平台和节目平台之间设置有节目监管接口，服务平台采用其与节目平台之间的节目监管接口将

SMS中存储的与节目平台相关的用户数据和用户订购数据传输至节目平台，这部分功能由服务平台中的第二收视信息传输模块来实现。服务平台与支付监管平台之间设置有支付接口，服务平台采用其与支付监管平台之间的支付接口将SMS中存储的用户节目支付费用数据传输至支付监管平台，这部分功能由服务平台中的第三收视信息传输模块来实现；服务平台采用其与节目平台之间的节目监管接口将SMS中存储的与节目平台相关的节目销售收入数据传输至节目平台，这部分功能由服务平台中的第四收视信息传输模块来实现。

由于服务平台可以将用户数据、用户订购数据和节目销售收入数据一起传输至节目平台，所以，第三收视信息传输模块和第四收视信息传输模块可以将分别获取到的用户数据、用户订购数据和节目销售收入数据采用服务平台与节目平台之间的节目监管接口一起传输至节目平台。

服务平台可以采用主动定期上报的方式如日报、周报、月报等方式将上述信息分别上报至节目监管平台、支付监管平台和节目平台，服务平台也可以在接收到节目监管平台、支付监管平台或节目平台的请求时，根据请求中的信息上报上述信息。服务平台可以根据请求中包含的指定时间段，如指定的日期、指定的日期段等，上报指定时间段内的用户收视信息，服务平台也可以根据请求中包含的指定收视用户信息，上报指定收视用户的用户收视信息，还可以根据请求中包含的指定时间段、指定收视用户信息，上报指定收视用户在指定时间段内的用户收视信息。

节目平台在接收到服务平台传输来的用户数据和用户订购数据后，将其上报至节目监管平台，通过上述节目平台与节目监管平台之间的数据传输，使节目监管平台可以对服务平台上报的数据和节目平台上报的数据进行一致性核查，这部分功能由节目监管平台中的第一一致性核查模块实现。由于服务平台上报至节目监管平台如广电总局监管平台的数据具有较高的真实可靠性，所以，节目监管平台通过对服务平台上报至节目平台的数据进行一致性核查，能

够确定服务平台上报至节目平台的数据是否准确，从而，保证了节目平台能够从服务平台处获得真实、可信的数据，最终，保证了节目平台与服务平台进行结算的基础数据的准确性，使节目平台与服务平台的分成结算具有准确性和公证性。

服务平台需要将其用户管理系统中存储的用户节目支付费用数据传输至支付监管平台，这样，服务平台的收视用户即有线电视用户可以通过支付监管平台来完成节目订购费用的缴纳。节目平台在接收到服务平台上报的用户节目销售收入数据后，采用其与支付监管平台之间的用户帐户支付核查接口将用户节目销售收入数据上报至支付监管平台，使支付监管平台可以根据有线电视用户缴纳的节目订购费用对服务平台上报至节目平台的用户节目销售收入数据进行一致性核查，以证实节目平台从服务平台处获取的用户节目销售收入数据的正确性，最终，使节目平台与服务平台的分成结算具有准确性和公证性。这部分功能由支付监管平台中的第二一致性核查模块来实现。

节目平台还可以根据结算分成协议、预定的服务平台授权信息对其从服务平台获取的用户数据和节目销售授权数据进行多种形式的分成结算。这里的结算分成可以为：节目平台与服务平台之间的分成结算，还可以为节目平台与节目提供商之间的结算分成。这里的结算分成协议可以为基于固定时长统谈的结算分成协议、或基于节目授权量的结算分成协议、或基于节目授权时长的结算分成协议、或基于节目销售收入的结算分成协议中的一种或多种，如采用基于节目授权量＋节目授权时长的结算分成协议、再如采用基于节目授权量＋节目销售收入的结算分成协议等。上述结算分成过程由分成结算模块来实现，分成结算模块可设置于节目平台，也可以设置于服务平台，当然，节目平台和服务平台之间都可以设置分成结算模块。

从上述描述中可以看出，本发明中的节目平台不再需要对服务平台的收入情况及用户的收视情况进行监管，使节目平台能够专注于提供节目内容服务、

服务平台能够专注于提供节目收视服务，本发明对节目平台、服务平台的SMS和CAS、以及传输网络没有特殊的要求，使节目交换系统的建设成本、运营维护成本低、易于实施，且提高了节目平台与服务平台之间的运营灵活性。

本发明不限制服务平台、节目平台、支付监管平台、节目监管平台之间的接口形式，下面以提供一种具体的接口实现方式。

本发明中节目平台与服务平台之间的节目监管接口的通用属性如表1所示。也就是说，本发明中节目平台与服务平台之间交换的接口数据均包括表1中的内容。

表1

属性名称	说明
版本号	版本编号。
源系统标识	数据来源系统的标识号
目的系统标识	数据目标系统的标识号
交易流水号	一次操作的流水号
交易类型	交易分类
交易时间	若该值为空，默认为当前时刻。

表1中，版本号、源系统标识、目的系统标识、交易类型为消息校验信息，交易流水号和交易时间为消息标识信息。消息校验信息主要用于接收端判断其接收到的消息是否为合法的消息，消息标识信息主要用于表示该消息是针对哪个请求的应答消息。当节目平台与服务平台之间采用同步通讯方式时，接口数据可以不包括消息标识信息。

服务平台与节目平台之间的节目监管接口为：周期性上报的服务平台销售明细如服务平台月度销售明细、单用户的业务明细、指定日期的产品销售数量、业务发展报告如业务发展日报，业务发展周报等。

当节目平台向服务平台请求服务平台月度销售明细时，节目平台向服务平台发送的月度销售明细请求的接口数据如表2所示。

表2

属性名称	备注
月份	可以是自然月，也可以是双方约定的财政月，由于涉及到服务平台、节目交换平台、监管平台三方比对数据，简单起见，建议使用自然月。

服务平台在接收到指定月请求信息后，根据请求信息中的月份信息获取用户数据和用户订购数据，并发送至节目平台。服务平台发送至节目平台的接口数据中的用户数据和用户订购数据如表3所示。

表3

服务平台返回月度业务明细	
属性名称	备注
成功标志	成功返回码
智能卡卡号	发生订购的智能卡卡号
CAS的标识	条件授权系统的系统标识
订购类型	0000 － 个体订购；0001 － 大客户方式订购
大客户标识	大客户订购时的大客户标识
产品编号	订购的服务平台产品的编号，该产品中包含节目平台的节目
整月订购标志	是否整月订购
订购天数	订购服务的天数
销售金额	给用户实际月售价，单位为分
支付系统标识	本次消费费用支付的发生系统
支付帐号	本次消费的支付帐号
支付流水号	本次消费支付的交易流水号

表3中，智能卡卡号、订购类型、产品编号、订购天数、销售金额等属于用户订购数据；大客户标识、整月订购标志、支付系统标识、支付帐号、支付流水号等属于用户数据。

在上述例子中，服务平台也可以在预定的日期根据表3所示的格式主动向节目平台上报一个月的用户数据和用户订购数据。

当服务平台确定节目平台传输来的指定月的接口数据有误时，可以向节目平台返回如表4所示的信息。

表4

服务平台返回错误结果	
属性名称	备注
错误标志	错误码
错误描述	错误的详细信息

节目平台向服务平台发送请求某收视用户的用户数据和用户订购数据的请求信息如表5所示。

节目平台请求参数	
属性名称	备注
智能卡卡号	发生订购的智能卡卡号
CAS的标识	条件授权系统的系统标识

服务平台在接收到某收视用户请求信息后，根据请求信息中的智能卡号、CAS的标识获取用户数据和用户订购数据，并发送至节目平台。服务平台发送至节目平台的接口数据中的用户数据和用户订购数据如表6所示。

表6

服务平台返回用户业务明细		
属性名称		备注
成功标志		成功返回码
智能卡卡号		发生订购的智能卡卡号
CAS的标识		条件授权系统的系统标识
用户编号		服务平台用户编号
N个已订购产品信息	产品编号	服务平台定义的产品编号，该产品中包含节目平台的节目
	产品名称	服务平台的产品名称
	服务开始时间	若该值为空，默认为当前时刻。
	服务截止时间	若该值为空，默认为当前时刻。
	支付系统标识	支付系统的标识
	支付帐号	用户的支付帐号
	支付流水号	本次消费支付的交易流水号

当服务平台确定节目平台传输来的指定某收视用户收视信息的接口数据有误时，可以向节目平台返回如表4所示的错误信息。

节目平台向服务平台发送请求指定日期的用户订购数据的请求信息如表8所示。

表7

节目平台请求参数	
属性名称	备注
日期	表示获取从该日期到当前查询时间点的当天订购节目平台节目的数量(不需要扣除授权到期的用户)

服务平台在接收到指定日期的请求信息后，根据指定的日期获取用户订购数据，并发送至至节目平台。服务平台发送至节目平台的接口数据中的用户订购数据如表8所示。

表8

服务平台返回节目平台节目销售明细		
属性名称		备注
成功标志		成功返回码
日期		查询的日期
N个产品销售信息	产品编号	服务平台的产品编号，该产品中包含节目平台的节目
	产品名称	服务平台的产品名称
	销售数量	产品购买数量

当服务平台确定节目平台传输来的指定日期的接口数据有误时，可以向节目平台返回如表4所示的信息。

服务平台主动向节目平台上报日报的接口数据中的用户数据和用户订购数据如表9所示。

表9

服务平台请求参数		
属性名称		备注
日期		
产品用户发展情况	产品编号	服务平台的产品编号，该产品中包含节目平台的节目
	产品名称	服务平台的产品名称
	新增订购数	产品新购买数量
	取消订购数	产品退订的数量

节目平台在确定其接收到的服务平台上报日报的接口数据正确时，向服务平台返回的信息如表10所示。

表10

节目平台返回明细	
属性名称	备注
成功标志	成功返回码

节目平台在确定其接收到的服务平台上报日报的接口数据错误时，向服务平台返回的信息如表4所示。

节目平台向服务平台请求指定时间段内如一周内新增用户的用户数据和用户订购数据。节目平台通过该请求可以获得一周内各产品新增的收视用户数量、以及具体的新增收视用户信息。获取的数据主要用作产品销售情况统计分析使用。节目平台向服务平台发送请求指定一周内新增用户请求的接口数据中的用户数据和用户订购数据如表11所示。

表11

节目平台请求参数	
属性名称	备注
周日期	使用周一的日期表示一周

服务平台在接收到指定周请求信息后，根据请求信息中的周日期获取用户数据和用户订购数据、并发送至节目平台。服务平台发送的指定周的接口数据中的用户数据和用户订购数据如表12所示。

表12

服务平台返回周订购明细			
属性名称			备注
成功标志			成功返回码
周日期			查询的周日期
N条产品销售信息	产品编号		服务平台的产品编号，该产品中包含节目平台的节目
	产品名称		服务平台的产品名称
	新增订购用户总数		新购买产品的用户数量，具体明细信息在下面的“M个新增用户信息”
	M个新增用户信息	用户编号	服务平台新购买产品的用户编号
		CAS标识	用户对应的CAS标识
	取消订购用户总数		取消购买产品的用户数量，具体明细信息在下面的“K个取消订购用户信息”
	K个取消订购用户信息	用户编号	服务平台取消购买产品的用户编号
		CAS标识	用户对应的CAS标识

服务平台在确定其接收到的节目平台传输来的指定周请求信息的接口数据有误时，向节目平台返回的信息如表4所示。

服务平台与支付监管平台之间的支付接口包括：建立支付关系的接口、解除支付关系的接口、支付费用接口、支付记录总额对帐接口、支付记录明细对帐接口、服务平台产品支付记录的交易总额对帐接口中的一个或多个。

本发明中服务平台与支付监管平台之间的支付接口的通用属性如表13所示。也就是说，本发明中服务平台与支付监管平台之间交换的接口数据均包括表13中所示的内容。

表13

属性名称	说明
交易编码	交易编码，区别不同的业务
支付系统编号	支付系统编号，服务平台中对应支付系统的编号
交易流水号	流水号，为异步通讯的标识，客户端生成，服务端在应答包中原样返回。说明：如果服务端返回的报文大于一个包，则这一组包的流水号相同
是否存在后续包	是否还有后续包，'1'有，'0'无
包序号	包序号，从1开始
业务员编码	操作员或业务终端，只作为审计日志的信息
校验字	包体校验属性

表13中，支付系统编号、是否存在后续包、包序号、业务员编码和校验字为消息校验信息，交易编码和交易流水号为消息标识信息。消息校验信息主要用于接收端判断其接收到的消息是否为合法的消息，消息标识信息主要用于表示该消息是针对哪个请求的应答消息。当节目平台与支付监管平台之间采用同步通讯方式时，接口数据可以不包括消息标识信息。

服务平台与支付监管平台之间产生的请求信息和响应信息都使用表13所示的报文结构。

表13中的交易编码，客户端必须写入遵守系统提供的交易编码规则、服务端在应答报文中原样返回。上述客户端为发送请求信息的一方，上述服务端为发送响应信息的一方。

交易流水号为异步通讯的标识，由客户端生成，服务端在应答报文中原样返回。如果服务端返回的报文大于一个包，则这一组包的流水号相同。

是否存在后续包：当对应一个请求有多个应答报文时，必须通过该属性来说明是还有后续包，还是应答结束。如果有多个应答包，则只有最后一个应答包的多包标志为0，其它包的多包标志都为1。

包序号：对于每个请求，相应的一个或多个应答包都从1开始编号，逐次

连续加一。

校验字属性为报文的校验属性，使用MD5算法产生32位的字符串，取前4个和后4的字符，交叉后的字符串作为校验字，如果MD5串第一个字符为A0，第二个字符为A1，依次类推，那么最后产生的校验字为A0A28A1A29A2A30A3A31。正确报文：[5399990001 11 1 赵云625d1c2a 11]。MD5算法为输入记录信息字符串+双方约定的密钥，对输入信息使用MD5算法产生128比特数字摘要，128比特数字摘要转换为32字节16进制字符串。另外，计算校验字属性的值时，将校验字属性设置为空格。

下面对服务平台向支付监管平台发送用户节目支付费用数据的具体过程进行详细说明。

服务平台与支付监管平台之间需要建立支付关系。建立支付关系的具体过程为：支付监管平台向服务平台发送请求建立收视用户的支付关系的接口数据，接口数据中的请求信息如表14、表15所示。

表14

功能简述	支付系统向服务平台请求建立用户的支付关系
交易编码	0401
备注说明	支付系统 → 服务平台

表15

支付系统请求参数	
属性名称	备注
订户编码	用户证号
识别码	支付系统提供的用户标识码，当建立/解除支付关系时操作员要输入用户ID和识别码，用于防止操作员输入用户编号时敲错
支付帐号	支付帐号

表15中包含支付监管平台需要获取的用户节目支付费用数据具体包括的参数，如订户编码、识别码、支付帐号等。

服务平台在确定其接收的支付监管平台传输来的请求信息的接口数据正确时，根据支付监管平台需要获取的参数，将相应的数据发送至支付监管平台，

服务平台与支付监管平台建立支付关系。服务平台向支付监管平台发送的接口数据中的用户节目支付费用数据具体如表16所示。

表16

服务平台返回正确结果	
属性名称	备注
成功标志	成功返回码
订户编码	服务平台的用户编号
识别码	支付提供的用户标识码
支付帐号	支付帐号

支付监管平台在正确接收到服务平台传输来的用户节目支付费用数据时，支付监管平台与服务平台之间成功建立支付关系。

服务平台在确定其接收的支付监管平台传输来的请求信息的接口数据错误时，向支付监管平台返回的数据如表4所示。

服务平台与支付监管平台解除支付关系的具体过程为：支付监管平台向服务平台发送请求解除收视用户的支付关系的接口数据，接口数据中的请求信息如表17、表18所示。

表 17

功能简述	支付系统向服务平台请求解除用户的支付关系
交易编码	0402
备注说明	支付系统 → 服务平台

表 18

属性名称	备注
订户编码	服务平台的用户ID
识别码	支付系统提供的用户标识码

表18中包含支付监管平台需要解除支付关系的用户信息，如订户编码、识别码等。

服务平台在确定其接收的支付监管平台传输来的请求解除信息的接口数据正确时，根据请求解除信息中的用户信息进行解除操作，并向支付监管平台发送解除成功的信息，具体如表19所示。

表 19

服务平台返回正确结果	
属性名称	备注
成功标志	成功返回码

服务平台在确定其接收的支付监管平台传输来的请求解除信息的接口数据错误时，向支付监管平台发送解除失败的信息，具体如表 4 所示。

在服务平台与支付监管平台之间建立支付关系后，服务平台在需要收视用户进行费用支付时，向支付监管平台发送请求收视用户费用支付的接口数据，接口数据中的请求信息如表20、表21所示。

表20

功能简述	服务平台向支付系统发送为用户进行支付的请求
交易编码	0403
备注说明	服务平台 → 支付系统

表21

服务平台请求参数		
属性名称		备注
用户编号		用户的编号
结算月		结算的月份
总笔数		扣款的总笔数
总费用		扣款的总费用，单位分
N条产品明细费用	产品编号	服务平台的产品编号，该产品中包含节目平台的节目
	结算费用	产品的订购费用，单位分
	业务时长	产品的订购时长

表21中包含需要费用支付的收视用户信息和收视用户需要支付的费用信息。

支付监管平台在确定其接收的服务平台传输来的请求收视用户费用支付的接口数据正确、并在收视用户支付费用后，向服务平台发送费用支付成功的信息，具体如表22所示。

表22

支付系统返回正确结果	
属性名称	备注
成功标志	成功返回码
结算月	要支付的月份
总费用	支付的总费用，单位分

支付监管平台在确定其接收的服务平台传输来的请求收视用户费用支付的接口数据错误时，向服务平台发送错误信息，具体如表4所示。

支付监管平台还可以向服务平台发送对帐请求的接口数据，对帐请求可以分为总额对帐请求和明细对帐请求。接口数据中的总额对帐请求信息如表23、表24所示。

表 23

功能简述	支付系统向服务平台发送的对帐请求
交易编码	0404
备注说明	支付系统 → 服务平台

表 24

属性名称	备注
起始序列号	对帐的起始序列号，即支付流水号
截至序列号	对帐的截至序列号

服务平台在确定其接收的支付监管平台传输来的总额对帐请求信息的接口数据正确时，向服务平台发送总额对帐接口数据正确的信息，具体如表 25 所示。

表 25

服务平台返回正确结果	
属性名称	备注
成功标志	成功返回码
起始序列号	对帐的起始序列号，即支付流水号
截至序列号	对帐的截至序列号
总笔数	扣款的总笔数
总费用	扣款的总费用，单位分
总时长	产品的订购总时长，单位天

服务平台在确定其接收的支付监管平台传输来的总额对帐请求信息的接口数据错误时，向服务平台发送总额对帐接口数据错误的信息，具体如表 4 所

示。

接口数据中的明细对帐请求信息如表 26、表 27 所示。

表 26

功能简述	支付系统向服务平台发送的对帐请求
交易编码	0405
备注说明	支付系统 → 服务平台

表 27

支付系统请求参数	
属性名称	备注
起始序列号	对帐的起始序列号，即支付流水号
截至序列号	对帐的截至序列号

服务平台在确定其接收的支付监管平台传输来的明细对帐请求信息的接口数据正确时，向服务平台发送明细对帐接口数据正确的信息，具体如表 28 所示。

表 28

服务平台返回正确结果		
属性名称		备注
成功标志		成功返回码
起始序列号		对帐的起始序列号，即支付流水号
截至序列号		对帐的截至序列号
总笔数		扣款的总笔数
N条产品明细费用	产品编号	服务平台的产品编号，该产品中包含节目平台的节目
	结算费用	产品的订购费用，单位分
	业务时长	产品的订购时长

服务平台在确定其接收的支付监管平台传输来的明细对帐请求信息的接口数据错误时，向服务平台发送明细对帐接口数据错误的信息，具体如表 4 所示。

节目平台与支付监管平台之间的接口数据包括如下几种情况：

节目平台在需要与服务平台的产品支付记录的交易总额对帐时，向支付监管平台发送产品支付记录交易总额对帐请求信息，具体如表 29、30 所示。

表 29

功能简述	节目平台向支付系统发送的对服务平台交易总帐请求
交易编码	0501
备注说明	节目平台 → 支付系统

表 30

节目平台请求参数	
属性名称	备注
起始序列号	对帐的起始序列号，即支付流水号
截至序列号	对帐的截至序列号
产品编号	服务平台的产品编号，该产品中包含节目平台的节目
总笔数	扣款的总笔数
总费用	扣款的总费用，单位分

支付监管平台在确定其接收的服务平台传输来的产品支付记录交易总额对帐请求信息的接口数据正确时，向服务平台发送产品支付记录交易总额对帐接口数据正确的信息，具体如表 31 所示。

表 31

支付系统返回正确结果	
属性名称	备注
成功标志	成功返回码
起始序列号	对帐的起始序列号，即支付流水号
截至序列号	对帐的截至序列号
产品编号	服务平台的产品编号，该产品中包含节目平台的节目
总笔数误差	扣款的总笔数误差，如果为0则表示一致
总费用误差	扣款的总费用误差，单位分，如果为0则表示一致

支付监管平台在确定其接收的服务平台传输来的产品支付记录交易总额对帐请求信息的接口数据错误时，向服务平台发送产品支付记录交易总额对帐接口数据错误的信息，具体如表 4 所示。

本发明中节目平台与支付监管平台之间的用户帐户支付核查接口的通用属性如表 13 所示。也就是说，本发明中服务平台与支付监管平台之间交换的接口数据均包括表 13 中所示的内容。

节目平台在需要与服务平台的产品支付记录明细对帐时，向支付监管平台发送产品支付记录交易明细对帐请求信息，具体如表 32、表 33 所示。

表 32

功能简述	节目平台向支付系统发送的对服务平台交易明细帐请求
交易编码	0502
备注说明	节目平台 → 支付系统

表 33

节目平台请求参数		
属性名称		备注
起始序列号		对帐的起始序列号，即支付流水号
截至序列号		对帐的截至序列号
产品编号		服务平台的产品编号，该产品中包含节目平台的节目
N条支付明细	交易流水号	支付交易的流水号
	结算费用	产品的订购费用，单位分
	业务时长	产品的订购时长

支付监管平台在确定其接收的节目平台传输来的产品支付记录交易明细对帐请求信息的接口数据正确时，向服务平台发送产品支付记录交易明细对帐接口数据正确的信息，具体如表 34 所示。

表 34

支付系统返回正确结果		
属性名称		备注
成功标志		成功返回码
起始序列号		对帐的起始序列号，即支付流水号
截至序列号		对帐的截至序列号
产品编号		服务平台的产品编号，该产品中包含节目平台的节目
误差笔数		
N条误差支付明细	误差类型	
	交易流水号	误差的支付交易的流水号
	结算费用	误差的费用，单位分
	业务时长	误差的订购时长

支付监管平台在确定其接收的节目平台传输来的产品支付记录交易明细对帐请求信息的接口数据错误时，向服务平台发送产品支付记录交易明细对帐接口数据错误的信息，具体如表 4 所示。

服务平台与节目监管平台之间的节目监管接口参见广电总局发布的《有线数字电视节目平台与监管平台数据交换协议、内容与格式要求》，在本实施例

中不再详细描述。

节目平台与节目监管平台之间的节目监管接口参见广电总局发布的《用户管理系统与监管平台数据交换接口技术要求》，在本实施例中不再详细描述。

节目平台与节目提供商之间的节目结算分成协议如表35所示。

表35

项目名称	取值含义
策略编号	分成策略编号
策略描述	分成策略内容或用途的简述
策略有效时间	策略开始生效时间
策略失效时间	策略失效时间
节目平台编号	与节目商进行结算分成的节目平台的编号
节目标识	节目编号，节目是基本的分成实体单位
月份	对指定月份可以执行优惠定价，不指定则表示对所有月份都生效
分成方式	0 — 固定分成，统谈固定金额； 1 — 动态分成，节目平台节目销售收入的千分比；
具体数值	当分成方式为“0 — 固定分成，统谈固定金额”时指具体分成金额（分）； 当分成方式为“1 — 动态分成，节目平台产品销售收入的千分比”时指分成比例（千分比）；
月度参考价格	指整月最低价格（整月保底价格），当计算出通过分成方式计算出的整月价格低于该参考价格时，则采用该参考价格（分）
合同号	分成策略对应的合同号
备注信息	策略相关信息的说明

本发明的节目平台与服务平台之间的节目结算分成协议包括两部分的内容：一部分是分成策略协议；另一部分是为了鼓励服务平台的运营，在分成结算后对业务开展较好的服务平台进行累积奖励，即累积奖励协议；这两个部分共同组成了完整的结算分成协议。

节目平台与服务平台之间传输的分成策略协议的接口数据如表36所示。

表36

项目名称	取值含义
策略编号	分成策略编号
策略描述	分成策略内容或用途的简述
策略有效时间	策略开始生效时间
策略失效时间	策略失效时间
服务平台编号	与节目平台进行结算分成的服务平台的编号
节目标识	节目编号，节目是基本的分成实体单位
产品标识	服务平台定义的产品标识
大客户标识	服务平台定义的大客户标识，可对服务平台指定的大客户的消费分成进行特殊定价，可以不指定，不指定则表示对所有客户都生效
月份	对指定月份可以执行优惠定价，可以不指定，不指定则表示对所有月份都生效
分成方式	0 — 固定分成，统谈固定金额； 1 — 动态分成，服务平台产品销售收入的千分比； 2 — 动态分成，服务平台实际节目授权量的千分比进计算的费用；
具体数值	分成方式为“0 — 固定分成，统谈固定金额”时指具体分成金额(分)； 分成方式为“1 — 动态分成，服务平台产品销售收入的千分比”时指分成比例（千分比）； 分成方式为“2 — 动态分成，服务平台实际节目授权量的千分比进计算的费用”时指授权量分成比例（千分比）；
单次授权价格	分成方式为“2 — 动态分成，服务平台实际节目授权量的千分比进计算的费用”时单次授权的价格（分）
月度参考价格	指整月最低价格（整月保底价格），当计算出通过分成方式计算出的整月价格低于该参考价格时，则采用该参考价格（分）
合同号	分帐策略对应的合同号
备注信息	策略相关信息的说明

节目平台与服务平台之间传输的累积奖励协议的接口数据如表37所示。

表37

字段名称	取值含义
协议编号	累积奖励协议编号
协议有效时间	协议开始生效时间

协议失效时间	协议失效时间
服务平台编号	与节目平台进行结算分成的服务平台的编号
奖励周期	可以是月累积奖励、季累积奖励或年累积奖励
累积类别	0 — 用户数，在奖励周期内按服务平台中消费节目的用户数量进行累积； 1 — 销售收入，在奖励周期内按服务平台中节目的销售收入进行累积；
奖励阈值	能够进行奖励的最低值
奖励方式	0 — 奖励固定的金额； 1 — 按实际销售收入累积的千分比；
奖励值	分成方式为“固定分成，统谈固定金额”时指具体分成金额； 分成方式为“动态分成，服务平台产品销售收入的百分比”时指分成比例（百分比）
最高奖励金额	奖励的最高上限金额（分）
合同号	累积奖励协议对应的合同号
描述信息	策略相关信息的说明

虽然通过实施例描绘了本发明，本领域普通技术人员知道，本发明有许多变形和变化而不脱离本发明的精神，本发明的申请文件的权利要求包括这些变形和变化。

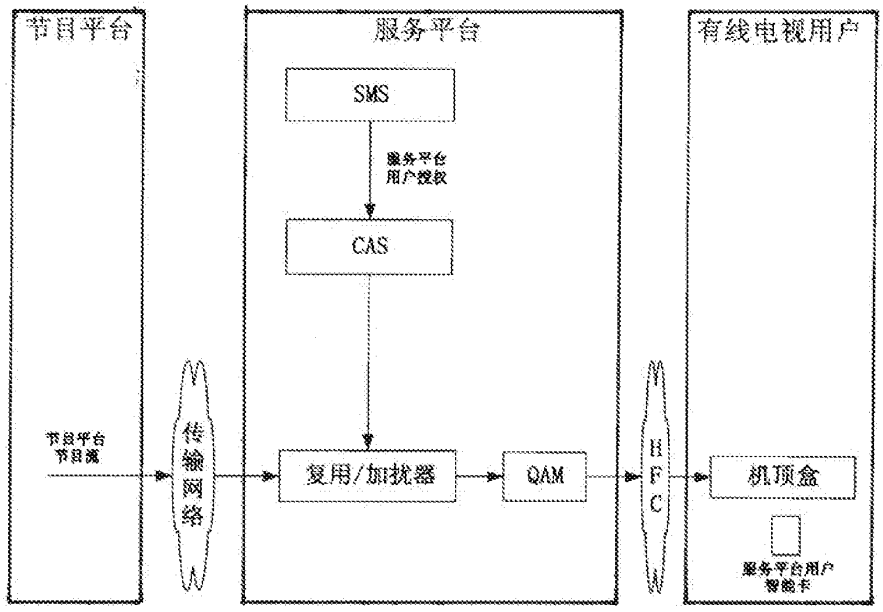

节目平台
服务平台
有线电视用户
SMS
服务平台
用户授权
CAS
节目平台
节目流
传输网络
复用/加扰器
QAM
HFC
机顶盒
服务平台用户
智能卡

图1

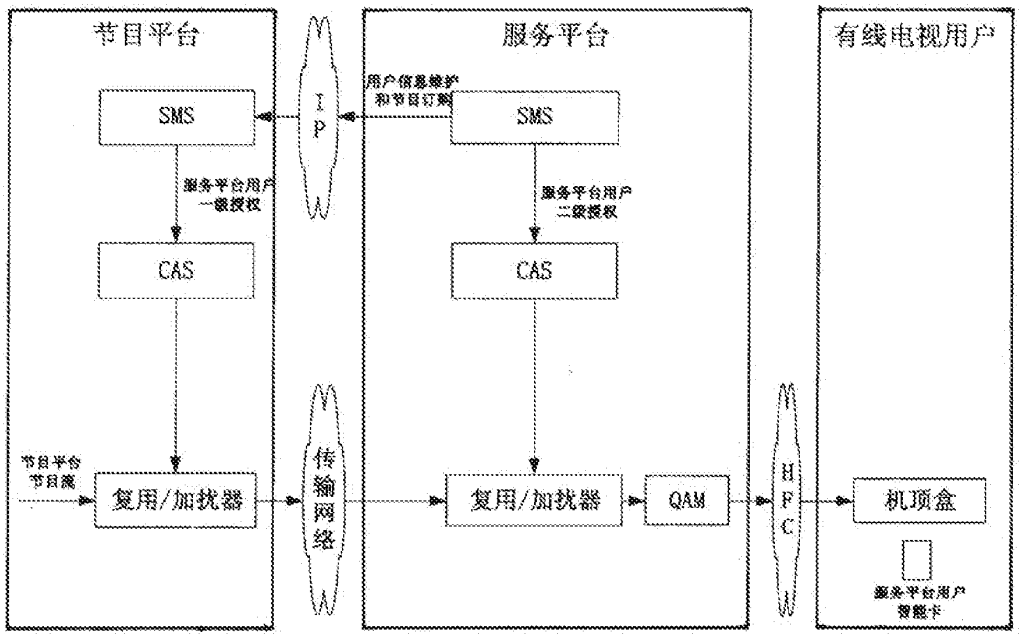

节目平台
服务平台
有线电视用户
SMS
IP
用户信息维护
和节目订购
SMS
服务平台用户
一级授权
服务平台用户
二级授权
CAS
CAS
节目平台
节目流
复用/加扰器
传输网络
复用/加扰器
QAM
HFC
机顶盒
服务平台用户
智能卡

图 2

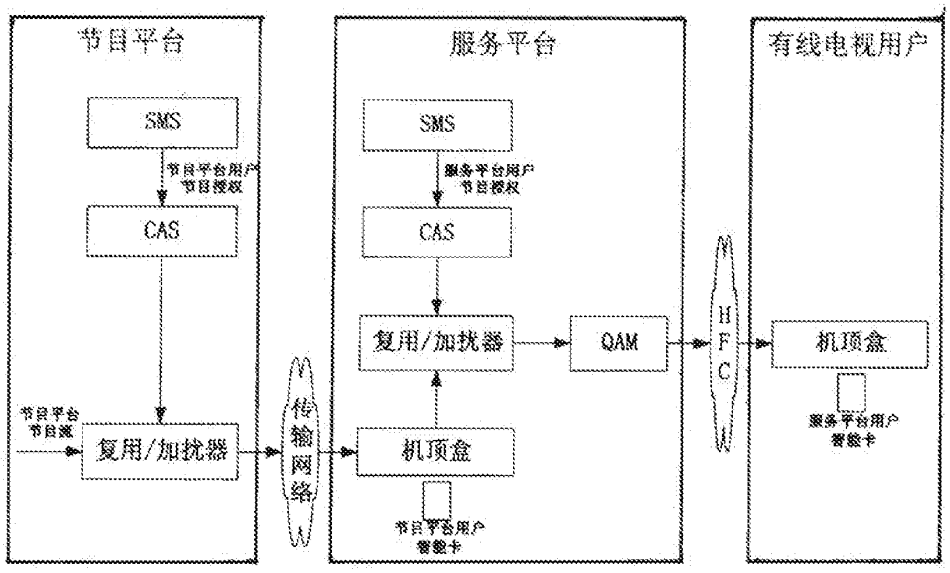

节目平台
SMS
节目平台用户节目授权
CAS
节目平台节目源
复用/加扰器
传输网络
服务平台
SMS
服务平台用户节目授权
CAS
复用/加扰器
QAM
机顶盒
节目平台用户智能卡
HFC
有线电视用户
机顶盒
服务平台用户智能卡

图 3

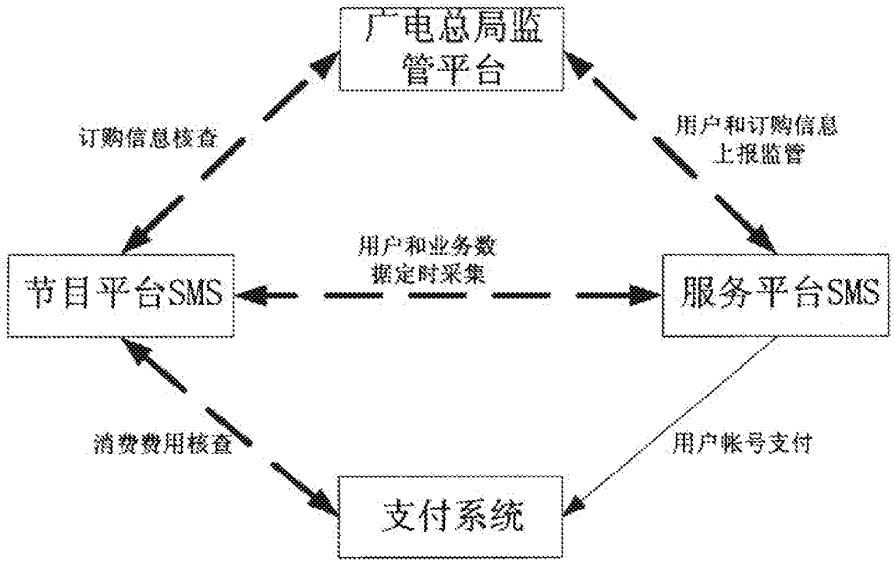

广电总局监管平台
订购信息核查
用户和订购信息上报监管
节目平台SMS
用户和业务数据定时采集
服务平台SMS
消费费用核查
用户帐号支付
支付系统

图 4

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 December 2011 (01.12.2011)

PCT

(10) International Publication Number
WO 2011/149532 A1

(51) International Patent Classification:
G01R 31/08 (2006.01)

(21) International Application Number:
PCT/US2011/000937

(22) International Filing Date:
25 May 2011 (25.05.2011)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

61/348,022	25 May 2010 (25.05.2010)	US
61/381,159	9 September 2010 (09.09.2010)	US
61/435,564	24 January 2011 (24.01.2011)	US

(71) Applicant *(for all designated States except US)*: **HEADWATER PARTNERS I LLC** [US/US]; 350 Marine Parkway, Suite 300, Redwood City, CA 94065 (US).

(72) Inventors: **RALEIGH, Gregory, G.**; 350 Marine Parkway, Suite 300, Redwood City, CA 94065 (US). **RAISSINIA, Ali**; 350 Marine Parkway, Suite 300, Redwood City, CA 94065 (US). **LAVINE, James**; 350 Marine Parkway, Suite 300, Redwood City, CA 94065 (US).

(74) Agents: **SOCKOL, Marc A.** et al.; Sheppard, Mullin, Richter & Hampton LLP, 390 Lytton Avenue, Palo Alto, CA 94301 (US).

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

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

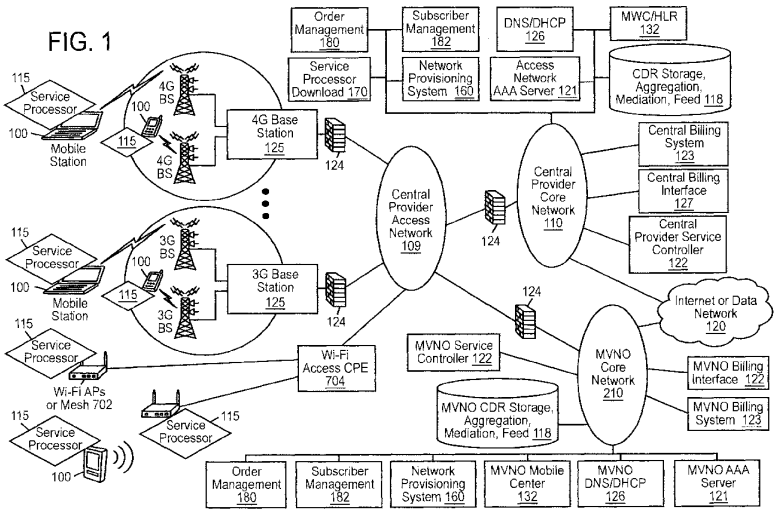
Published:

— *with international search report (Art. 21(3))*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

(54) Title: DEVICE- ASSISTED SERVICES FOR PROTECTING NETWORK CAPACITY

FIG. 1



(57) Abstract: Device Assisted Services (DAS) for protecting network capacity is provided. In some embodiments, DAS for protecting network capacity includes monitoring a network service usage activity of the communications device in network communication; classifying the network service usage activity for differential network access control for protecting network capacity; and associating the network service usage activity with a network service usage control policy based on a classification of the network service usage activity to facilitate differential network access control for protecting network capacity.

WO 2011/149532 A1

UNITED STATES PATENT APPLICATION

FOR

DEVICE-ASSISTED SERVICES FOR PROTECTING NETWORK CAPACITY

INVENTORS:

GREGORY G. RALEIGH

ALI RAISSINIA

JAMES LAVINE

PREPARED BY:

SHEPPARD MULLIN RICHTER & HAMPTON LLP
390 LYTTON AVENUE
PALO ALTO, CA 94301-1432

CUSTOMER NUMBER: 69849

ATTORNEY DOCKET NO.: 26WV-160509

EXPRESS MAIL LABEL NO.: EM 551709852 US

DEVICE-ASSISTED SERVICES FOR PROTECTING NETWORK CAPACITY

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application is a continuation-in-part of and incorporates by reference the following published U.S. pending nonprovisional patent applications: U.S. publication No. 2010/0188975, filed March 2, 2009, entitled "Verifiable Device Assisted Service Policy Implementation," U.S. publication No. 2010/0192170, filed March 2, 2009, entitled "Device Assisted Service Profile Management with User Preference, Adaptive Policy, Network Neutrality, and User Privacy," U.S. publication No. 2010/0191612, filed March 2, 2009, entitled "Verifiable Device Assisted Service Usage Monitoring with Reporting, Synchronization, and Notification," U.S. publication No. 2010/0191576, filed March 2, 2009, entitled "Verifiable Device Assisted Service Usage Billing with Integrated Accounting, Mediation Accounting, and Multi-Account," U.S. publication No. 2010/0188991, filed March 2, 2009, entitled "Network Based Service Policy Implementation with Network Neutrality and User Privacy," U.S. publication No. 2010/0188990, filed March 2, 2009, entitled "Network Based Service Profile Management with User Preference, Adaptive Policy, Network Neutrality and User Privacy," U.S. publication No. 2010/0192212, filed March 2, 2009, entitled "Automated Device Provisioning and Activation," U.S. publication No. 2010/0191604, filed March 2, 2009, entitled "Device Assisted Ambient Services," U.S. publication No. 2010/0191575, filed March 2, 2009, entitled "Network Based Ambient Services," U.S. publication No. 2010/0188993, filed March 2, 2009, entitled "Network Tools for Analysis, Design, Testing, and Production of Services," U.S. publication No. 2010/0190470, filed March 2, 2009, entitled "Roaming Services Network and Overlay Networks," U.S. publication No. 2010/0192120, filed March 2, 2009, entitled "Open Development System for Access Service Providers," U.S. publication No. 2010/0192207, filed March 2, 2009, entitled "Virtual Service Provider Systems," U.S. application serial No. 12/380,757, filed March 2, 2009, and entitled

"Service Activation Tracking System," U.S. publication No. 2010/0191613, filed March 2, 2009, entitled "Open Transaction Central Billing System," U.S. publication No. 2010/0188995, filed March 2, 2009, entitled "Verifiable and Accurate Service Usage Monitoring for Intermediate Networking Devices," U.S. publication No. 2010/0188994, filed March 2, 2009, entitled "Verifiable Service Billing for Intermediate Networking Devices," U.S. publication No. 2010/0191846, filed March 2, 2009, entitled "Verifiable Service Policy Implementation for Intermediate Networking Devices," U.S. publication No. 2010/0188992, filed March 2, 2009, entitled "Service Profile Management with User Preference, Adaptive Policy, Network Neutrality and User Privacy for Intermediate Networking Devices," U.S. publication No. 2010/0191847, filed March 2, 2009, entitled "Simplified Service Network Architecture," U.S. publication No. 2010/0197266, filed January 27, 2010, entitled "Device Assisted CDR Creation, Aggregation, Mediation, and Billing," U.S. publication No. 2010/0198698, filed January 27, 2010, entitled "Adaptive Ambient Services," U.S. publication No. 2010/0199325, filed January 27, 2010, entitled "Security Techniques for Device Assisted Services," U.S. publication No. 2010/0197267, filed January 27, 2010, entitled "Device Group Partitions and Settlement Platform," U.S. publication No. 2010/0198939, filed January 27, 2010, entitled "Device Assisted Services Install," U.S. publication No. 2010/0195503, filed January 27, 2010, entitled "Quality of Service for Device Assisted Services," U.S. publication No. 2010/0197268, filed January 28, 2010, entitled "Enhanced Roaming Services and Converged Carrier Networks with Device Assisted Services and a Proxy," and U.S. application serial No. 13/_____, filed May 25, 2011, and entitled "System and Method for Wireless Network Offloading."

[0002] This application seeks priority to and incorporates by reference the following U.S. pending provisional patent applications: U.S. provisional application serial No. 61/348,022, filed May 25, 2010, entitled "Device Assisted Services for Protecting Network Capacity," U.S. provisional application serial No. 61/381,159, filed September 9, 2010, entitled "Device Assisted

Services for Protecting Network Capacity," U.S. provisional application serial No. 61/381,162, filed September 9, 2010, entitled "Service Controller Interfaces and Workflows," U.S. provisional application serial No. 61/384,456, filed September 20, 2010, entitled "Securing Service Processor with Sponsored SIMs," U.S. provisional application serial No. 61/389,547, filed October 4, 2010, entitled "User Notifications for Device Assisted Services," U.S. provisional application serial No. 61/385,020, filed September 21, 2010, entitled "Service Usage Reconciliation System Overview," U.S. provisional application serial No. 61/387,243, filed September 28, 2010, entitled "Enterprise and Consumer Billing Allocation for Wireless Communication Device Service Usage Activities," U.S. provisional application serial No. 61/387,247, filed September 28, 2010, entitled "Secured Device Data Records," U.S. provisional application serial No. 61/407,358, filed October 27, 2010, entitled "Service Controller and Service Processor Architecture," U.S. provisional application serial No. 61/418,507, filed December 1, 2010, entitled "Application Service Provider Interface System," U.S. provisional application serial No. 61/418,509, filed December 1, 2010, entitled "Service Usage Reporting Reconciliation and Fraud Detection for Device Assisted Services," U.S. provisional application serial No. 61/420,727, filed December 7, 2010, entitled "Secure Device Data Records," U.S. provisional application serial No. 61/422,565, filed December 13, 2010, entitled "Service Design Center for Device Assisted Services," U.S. provisional application serial No. 61/422,572, filed December 13, 2010, entitled "System Interfaces and Workflows for Device Assisted Services," U.S. provisional application serial No. 61/422,574, filed December 13, 2010, entitled "Security and Fraud Detection for Device Assisted Services," U.S. provisional application serial No. 61/435,564, filed January 24, 2011, entitled "Framework for Device Assisted Services," and U.S. provisional application serial No. 61/472,606, filed April 6, 2011, entitled "Managing Service User Discovery and Service Launch Object Placement on a Device."

[0003] Further, this application incorporates by reference the following U.S. provisional patent applications: U.S. provisional application serial No. 61/206,354, filed January 28, 2009, entitled "Services Policy Communication System and Method," U.S. provisional application serial No. 61/206,944, filed February 4, 2009, entitled "Services Policy Communication System and Method," U.S. provisional application serial No. 61/207,393, filed February 10, 2009, entitled "Services Policy Communication System and Method," U.S. provisional application serial No. 61/207,739, filed February 13, 2009, entitled "Services Policy Communication System and Method," U.S. provisional application serial No. 61/270,353, filed July 6, 2009, entitled "Device Assisted CDR Creation, Aggregation, Mediation and Billing," U.S. provisional application serial No. 61/275,208, filed August 25, 2009, entitled "Adaptive Ambient Services," U.S. provisional application serial No. 61/237,753, filed August 28, 2009, entitled "Adaptive Ambient Services," U.S. provisional application serial No. 61/252,151, filed October 15, 2009, entitled "Security Techniques for Device Assisted Services," U.S. provisional application serial No. 61/252,153, filed October 15, 2009, entitled "Device Group Partitions and Settlement Platform," U.S. provisional application serial No. 61/264,120, filed November 24, 2009, entitled "Device Assisted Services Install," and U.S. provisional application serial No. 61/264,126, filed November 24, 2009, entitled "Device Assisted Services Activity Map."

BACKGROUND

[0004] With the advent of mass market digital communications, applications and content distribution, many access networks such as wireless networks, cable networks and Digital Subscriber Line (DSL) networks are pressed for user capacity, with, for example Evolution-Data Optimized (EVDO), High Speed Packet Access (HSPA), Long Term Evolution (LTE), Worldwide Interoperability for Microwave Access (WiMax), DOCSIS, DSL, and Wireless Fidelity (Wi-Fi) becoming user capacity constrained. In the wireless case, although network capacity will increase with new higher capacity wireless radio access technologies, such as Multiple-Input Multiple-Output (MIMO), and with more frequency spectrum and cell splitting being deployed in the future, these capacity gains are likely to be less than what is required to meet growing digital networking demand.

[0005] Similarly, although wire line access networks, such as cable and DSL, can have higher average capacity per user compared to wireless, wire line user service consumption habits are trending toward very high bandwidth applications and content 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.

[0006] The foregoing example of trends and issues is intended to be illustrative and not exclusive. Other limitations of the art will become apparent to those of skill in the relevant art upon a reading of the specification and a study of the drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] FIG. 1 illustrates a functional diagram of a network architecture for providing quality of service (QoS) for device assisted services (DAS) and/or for providing DAS for protecting network capacity in accordance with some embodiments.

[0008] FIG. 2 illustrates another functional diagram of another network architecture for providing quality of service (QoS) for device assisted services (DAS) and/or for providing DAS for protecting network capacity in accordance with some embodiments.

[0009] FIG. 3 illustrates a functional diagram of an architecture including a device based service processor and a service controller for providing quality of service (QoS) for device assisted services (DAS) and/or for providing DAS for protecting network capacity in accordance with some embodiments.

[0010] FIG.s 4A through 4C illustrates a functional diagram for providing quality of service (QoS) for device assisted services (DAS) in accordance with some embodiments.

[0011] FIG. 5 illustrates a functional diagram for generating a QoS activity map for quality of service (QoS) for device assisted services (DAS) in accordance with some embodiments.

[0012] FIG. 6 illustrates a functional diagram for quality of service (QoS) for device assisted services (DAS) for an end to end coordinated QoS service channel control in accordance with some embodiments.

[0013] FIG. 7 illustrates a flow diagram for quality of service (QoS) for device assisted services (DAS) in accordance with some embodiments.

[0014] FIGS. 8A through 8C each illustrate another flow diagram for quality of service (QoS) for device assisted services (DAS) in accordance with some embodiments.

[0015] FIG. 9 illustrates another flow diagram for quality of service (QoS) for device assisted services (DAS) in accordance with some embodiments.

[0016] FIG. 10 illustrates another flow diagram for quality of service (QoS) for device assisted services (DAS) in accordance with some embodiments.

[0017] FIG. 11 illustrates another flow diagram for quality of service (QoS) for device assisted services (DAS) in accordance with some embodiments.

[0018] FIG. 12 illustrates a device stack for providing various service usage measurement techniques in accordance with some embodiments.

[0019] FIG. 13 illustrates another device stack for providing various service usage measurement techniques in accordance with some embodiments.

[0020] FIG. 14 illustrates a flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments.

[0021] FIG. 15 illustrates another flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments.

[0022] FIG. 16 illustrates another flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments.

[0023] FIG. 17 illustrates another flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments.

[0024] FIG. 18 illustrates another flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments.

[0025] FIG. 19 illustrates another flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments.

[0026] FIG. 20 illustrates another flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments.

[0027] FIG. 21 illustrates another flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments.

[0028] FIG. 22 illustrates another flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments.

[0029] FIG. 23 illustrates a network capacity controlled services priority level chart for device assisted services (DAS) for protecting network capacity in accordance with some embodiments.

[0030] FIG. 24 depicts a diagram of a network capacity protection system utilizing device-assisted services (DAS).

[0031] FIG. 25 depicts a diagram an example of a differential access control notification system.

[0032] FIG. 26 depicts an example of a computer system on which techniques described in this paper can be implemented.

[0033] FIG. 27 depicts a diagram of an example of a system for application-specific differential network access control.

DETAILED DESCRIPTION

[0034] 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.

[0035] 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.

[0036] As the network capacity gains are less than what is required to meet growing digital networking demand, a network capacity crunch is developing due to increasing network

congestion on various wireless networks, such as mobile networks. The increasing popularity of various smart phone devices, net book devices, tablet computing devices, and various other wireless mobile computing devices, which are becoming increasingly popular on 3G, 4G, and other advanced wireless networks, is contributing to the network capacity crunch. Some network carriers have indicated that a relatively small number of users on such devices demand a disproportionately significant amount of their network capacity. For example, AT&T has recently indicated that about 3 percent of its smart phone device users (e.g., Apple iPhone® users) are generating approximately 40 percent of the operator's data traffic.

[0037] For example, in wireless networks, managing the wireless access connection capacity and network access connection resources is important to maintain network performance as network resources/capacity demand increases. Many network performance measures can be advantageously maintained or improved as network loading increases if capacity management and/or network resource management is employed. For example, these performance measures include network availability; the ability to deliver connections to all devices, users and/or applications seeking connections and enabled for service on the network; network access attempt success rate; the transmission speed experienced by one or more devices, users or applications; the average transmission speed experienced by all devices, users and/or applications; network bit error rate or packet error rate; the time delay from network access request to delivered access connection; the one-way delay or round-trip delay for a transmission; the delay timing jitter for a transmission; the time variation in transmission speed for one or more connections; the ability of the network to deliver various requested/needed levels of Quality of Service (QoS) to devices, users or applications that require differentiated connection QoS classes; the ability of the network to maintain efficiency (e.g., aggregated service throughput measured across all devices, users, and/or applications); the ability of the network to share or distribute a performance measure (e.g., the performance measures listed

above) uniformly or fairly across multiple devices, users, and/or applications that all have the same service quality class or the same service plan performance parameters.

[0038] For example, if there is a limited amount of shared bandwidth for a set of user devices (e.g., a set of devices on a wireless network, such as a given base station or base station controller or femto cell or pico cell; or a set of devices on a cable modem networks, etc.), and if multiple and/or all devices allow all applications to indiscriminately access or attempt to access network resources or transmit/receive traffic, then the network can generally become overloaded. As a result, a subset of users/devices or in some cases most or all users/devices obtain poor network performance. As another example, if one or more devices forming a subset of devices on the network allow multiple and/or all applications to indiscriminately access or attempt to access network resources or transmit/receive traffic, then the network can become overloaded. As a result, a subset of users/devices or in some cases most or all users/devices obtain poor network performance.

[0039] Traditionally, mobile devices typically have specialized designs that are optimized to preserve network capacity and protect network resources from being over taxed. For example, wireless devices that browse the Internet often use specialized protocols such as WAP and data traffic compression or low resolution techniques rather than standard HTTP protocols and traffic used in wired Internet devices.

[0040] However, the wireless devices that implement specialized methods for accessing the Internet and/or other networks often implement complex specifications provided by one or more wireless carriers that own the networks that the device is designed to connect to. Such complex specifications often require time consuming design, testing, and certification processes. These processes in part have the effect of narrowing the base of device suppliers to those qualified and willing to perform the specialized design work required, slowing time to market for new

devices, increasing the expense to develop new devices and reducing the types of applications that are supported.

[0041] Device OEMs have recently created wireless devices that are designed more like standard Internet devices and not fully optimized to preserve network capacity and resources. Many wireless service customers desire this type of device, and the OEMs generally want to reduce the complexity and time to market to deliver such devices. In addition, new market needs and new government requirements sometimes require that carriers offer a more open process for bringing new devices onto their network, in which the process does not require all of the specialized design and certification described above. These and various other factors are driving a growing need and trend for less complex and time consuming wireless device design and certification processes.

[0042] This trend has led many carriers to begin selling devices that are designed more as standard Internet service devices that connect to the Internet and other data networks through carrier wireless networks. As the cellular network is opened up to more and more new devices, applications and markets, there is a growing demand to allow general purpose Internet devices and applications to gain access to wireless networks without necessarily going through specialized design and certification process requirements to make the devices and applications efficient and authorized for access to such wireless networks.

[0043] However, general purpose Internet devices are not as frugal or sparing with wireless network access bandwidth. Moreover, with the advent of always on wide area network connections to the Internet has led to popular Internet services and applications that typically assume very inexpensive access and generally heed no attention to, for example, network busy state. As more general purpose Internet devices are provided for us on various wireless networks (e.g., mobile wireless networks), a high frequency of inefficient wireless network accesses continue to rise, which can reduce network capacity sometimes to levels that hinder

access to service for that device (e.g., user, device, software demand) and/or other devices on that wireless network and/or that wireless network segment. As discussed above, judicious use of wireless network bandwidth, capacity, and resources generally results in better service for all users, but at present, device manufacturers and wireless network providers (e.g., wireless network carriers or carriers) have not provided or implemented more intelligent bandwidth usage techniques. These factors generally result in less carrier control of device design, which poses a threat to longer term network capacity and performance preservation as the volume of devices with less optimized wireless designs continues to grow.

[0044] There are many network performance and user performance factors that are impacted by the efficiency of the network, including, for example, overall network congestion; the access network performance experienced by one or more groups of users, devices, applications, network service sources, communication protocols, and/or operating system functions; and/or the performance experienced by a given user, device, application, network service source, communication protocol, and/or operating system function. Under a relatively low capacity demand of a wireless network, network performance as experienced by a group of devices, applications, network service sources, communication protocols, operating system functions, and/or users or by a single device, application, network service source, communication protocol, operating system function, and/or user can degrade somewhat proportionally (e.g., aggregate traffic delivered by the network may be roughly proportional to the peak available network traffic) with incremental increases in network access and/or traffic demand from one or more groups of users, devices, applications, network service sources, communication protocols and/or operating system functions. However, as network resources/network capacity demand increases (e.g., more wireless network data traffic is demanded in aggregate; more devices are serviced by the network; more users are serviced by the network; more applications are serviced by the network; more network service sources are serviced by the network; more

operating system functions are serviced by the network; and/or more differentiated QoS sessions are serviced by the network), network availability/performance can decrease and/or the network may not adequately service one or more users, devices, applications, network service sources, communication protocols, and/or operating system functions, or may not service one or more groups of users, devices, applications, network service sources, communication protocols, and/or operating system functions.

[0045] There are many examples of how increasing network capacity demand can decrease network performance, including for example, to a decrease in average bandwidth offered per device (e.g., one or more users on a device, application, network service source, communication protocol, and/or operating system function executed/implemented on the device); an increase in traffic delivery latency; an increase in traffic delivery latency jitter; insufficient guaranteed or differentiated bandwidth for one or more differentiated QoS and/or dynamic QoS services (e.g., as described herein) to one or more devices, users, applications, network service sources, communication protocols, and/or operating system functions; increased latency for bandwidth reservation services; increased latency for QoS reservation services; performance problems with one or more communication protocols; unacceptable delays in user experience, and/or various other or similar consequences and device or user impacts resulting from reduced network availability and/or reduced network capacity. Examples of network communication protocols that can have degraded performance with excessive network loading or degraded network performance include, for example, Internet protocol (IP), HTML protocols, voice communication protocols including VOIP protocols, real-time video communication protocols, streaming media protocols (e.g., audio, video, etc), gaming protocols, VPN protocols, file download protocols, background service protocols, software update protocols, and/or various other network communication protocols. Thus, is it important to preserve/protect network capacity.

[0046] It is also important to control the number of transactions demanded from a given network resource (e.g., edge network segment, base station, base station controller, MAC resources, pico cell, femto cell, etc.) in a given period of time so that demand does not overcome the transaction servicing ability of that network resource. For example, network resources that should not be subjected to excess transaction demand can include base station or base station controller resources, media access control (MAC) resources, traffic transport resources, AAA resources, security or authentication resources, home agent (HA) resources, DNS resources, resources that play a part in network discovery, gateway or router resources, data session reservation or establishment resources (e.g., network resources required to manage, set up, conduct, and/or close service sessions, PPP sessions, communication flows, communication streams, QoS flows, radio access bearer reservation resources , tunnels, VPNs, APNs, special service routing, etc.), bandwidth reservation resources, QoS reservation or coordination resources, QoS transport resources, service charging resources, traffic analysis resources, network security resources, and/or various other or similar network resources. In some networks, the network performance degradation due to a given measure of incremental increase in network resource/capacity demand can become relatively large as various network resources become increasingly taxed due to either limited transaction processing capability or limited traffic bandwidth for one or more of the network resources that participate in establishing, servicing, conducting, maintaining, and/or closing the necessary network service connections and/or information exchanges required to conduct a service activity. For example, if the equipment required to establish a PPP session can only handle a certain number of new PPP session openings and/or closings per given period of time, and if device behavior is such that PPP sessions are often opened and/or closed, then the rate of PPP session transactions (e.g., openings and/or closings) can exceed the transaction capacity of the PPP session management resources. This is sometimes referred to as "flooding" or "overloading" a network resource with excess demand or excess connections, and, in such cases, the network resource may begin

falling behind in servicing transaction demand in a well controlled manner (e.g., the network resource may continue processing transactions at or near a maximum rate for that network resource), or in some cases, the resource may fall behind transaction demand in a less well controlled manner (e.g., the network resource may become overwhelmed such that its processing rate not only falls below aggregate transaction demand, but the transaction rate processing capability decreases under overload as well). In the PPP session establishment resource example, once the rate of requested transactions exceeds the resource maximum transaction rate, then unmet device demand can grow to a point where one or more devices experiences delays in connecting to and/or communicating (e.g., sending/receiving data) with the network.

[0047] As another example, in any type of random access bandwidth reservation protocol, MAC protocol, or bandwidth delivery protocol, in a network without proper management and/or control of traffic access reservations and/or transmissions, as the network demand increases there may be more collisions between reservation requests, traffic transmissions, application demands, network service source demands, communication protocol demands, and/or operating system function demands causing a decreasing network efficiency that can degrade user, device, application and/or network service performance so that performance falls below acceptable levels. As another example, in systems in which there is a QoS service session reservation system, uncontrolled and/or unmanaged QoS reservation requests and/or reservation grants can lead to a situation where the QoS reservation resources and/or QoS service delivery resources are over taxed to the point where QoS service performance falls below desired levels. As another example, in networks that require some form of minimum resource allocation for transmissions, reservations, or network resource transactions, the network can become inefficient if one or more devices, applications, network service sources, operating system functions, and/or communication protocols have a relatively high rate of

network resource access attempts, network accesses or data transmissions for small transmission payloads (e.g., minimum MAC reservation factors, minimum security overhead factors, minimum QoS reservation factors, minimum time responses for establishing a base station connection, minimum time responses for establishing or closing/being released from a session, etc). Even if the data packet comprising the access event is small, the network resources required to complete the access event are often busy servicing the access event for much longer periods of time than are required for the actual data transmission.

[0048] Another example of device service activity behavior that can have an impact on network performance is the way the device, device subsystem, and/or modem subsystem power cycling or transitions from one power save state to another. For example, establishing a basic connection from a device to a wireless base station consumes base station resources for a period of time and in some cases can also consume other network resources such as AAA, HLR, HA, gateway, billing, and/or charging gateway resources. If a device terminates the connection to the base station when the modem subsystem (e.g., or some other portion of the device) goes from active connection state to a power save state, then each time the device enters power save state and then exits power save state network resources are consumed, sometimes for time periods measured on the order of seconds or in extreme cases even minutes. If such a device has an aggressive power save algorithm that enters power save state after a short idle period, then the device behavior can consume a proportionally large amount of resources such that the network ability to support multiple devices is diminished, or such that the network cannot support very many similar devices on the network. Another similar example is the establishment of network sessions once the base station connection is established (e.g., establishing a PPP session between the device and a home agent (HA) or other gateway), in which network resources required to open and/or close the network session are ignorantly

consumed if a device exhibits aggressive power save state cycling or frequently terminates the data session for other reasons.

[0049] Another example of device service activity behavior that can impact network performance is applications that maintain persistent network communication that generates a relatively high frequency of network data packets. Some applications have persistent signaling that falls into this category. Specific examples include frequent device signaling sequences to update widgets on a desktop; synchronize user data such as calendars, contacts, email, and/or other information/content; check or update email or RSS feeds; access social networking websites or tools; online text, voice or video chat tools; update real-time information; and conduct other repetitive actions. Additional application behavior that can significantly tie up network resources and capacity include, for example, conference meeting services, video streaming, content update, software update, and/or other or similar application behavior. For example, even when the user is not directly interacting with or benefiting from this type of application, the application can be running in the background and continuing to consume potentially significant network resources.

[0050] For example, the types of service activities and/or device behavior that can reduce network capacity and/or network resource availability include software updates for OS and applications, frequent OS and application background network accesses and signaling, frequent network discovery and/or signaling (e.g., EtherType messages, ARP messages, and/or other messaging related to network access), cloud synchronization services, RSS feeds and/or other background information feeds, application (e.g., web browser) or device behavior reporting, background email downloads, content subscription service updates and downloads (e.g., music/video downloads, news feeds, etc.), text/voice/video chat clients, virus updates, peer to peer networking applications, inefficient network access sequences during frequent power cycling or power save state cycling, large downloads or other high bandwidth accesses, and/or

greedy application programs that continually and/or frequently access the network with small transmissions or requests for information. Various other examples will now be apparent to one of ordinary skill in the art.

[0051] Thus, not only can network capacity, network performance, and/or network resource availability be degraded by high device transmission bandwidth demand, but other types of persistent or frequent traffic resulting from network resource requests, network data accesses or other network interaction can also degrade network capacity, network performance, and/or network resource whether or not the aggregate bandwidth demand as measured by the total data throughput is high or not. Thus, techniques are needed to preserve network capacity by, for example, differentially controlling these types of network service usage activities in various ways depending on the type of service activity requesting network access and/or requesting transactions with network resources.

[0052] Smart phone and similar devices are exacerbating the problem by making frequent queries of the wireless network as such devices move among cell sites to while in transit, for example, push email, access social networking tools, and/or conduct other repetitive actions. While data traffic is also growing, signaling traffic is outpacing actual mobile data traffic by 30 percent to 50 percent by some estimates. For example, a Yahoo IM user may send a message but then wait a couple of seconds between messages. To preserve battery life, the smart phone typically moves into an idle mode. When the user pushes another message seconds later, the device has to set up a signaling path again, and even when the signaling resource is released by the smart phone, the network typically does not react fast enough to allow for the next station to use resources until several seconds and sometimes minutes. As a result, the base station controller in this example is spending a lot of its resources trying to process the signaling so it cannot perform other tasks, such as allocate additional resources for data

network usage, and such inefficiencies exacerbates the data network capacity crunch and dropped calls on such wireless networks.

[0053] One approach used by smart phone vendors to address this problem and save battery life on their devices is to implement a fast dormancy feature, which allows the mobile device to quickly make a query to the radio network controller to release the connection so that it can return to the idle state faster. In other words, the device is relaying the fact that the phone is going dormant saving device resources (e.g., signaling channel) rather than network resources. However, the fast dormancy feature can exacerbate this problem by prematurely requesting a network release only to follow on with a request to connect back to the network or by a request to re-establish a connection with the network.

[0054] Network carriers have typically attempted to manage network capacity using various purely central/core network based approaches. For example, some carriers have indicated a robust capacity planning process and sufficient investment is needed to alleviate this growing capacity crunch. Purely centralized network solutions with no assistance from a device based software agent (or service processor) can have several limitations. For example, for some device applications, OS functions or other service usage activities, if the activity is blocked somewhere in the network behind the base station after over the air (OTA) spectrum bandwidth is consumed to open or begin to open a communication socket, then there can still be an appreciable amount of network capacity or resources consumed even though the data transfer is not allowed to complete. In addition, if the service usage activity is aggressive in re-attempting to establish the network connection to transfer the data, and the network continues to allow the OTA portion of the connection establishment but blocks the connection somewhere in the network, then a large amount of capacity can be consumed by many devices exhibiting such behavior even though no useful service is being allowed. Accordingly, some embodiments for protecting network capacity include controlling network service usage activities at the source

of the demand – the device. Furthermore, in some embodiments, service usage is controlled in a manner that delays, prevents, or reduces the frequency of service usage activity re-try attempts to connect to the network.

[0055] In some cases, an additional drawback of purely centralized network solutions to protect network capacity arises when service usage activities are controlled, blocked, throttled, and/or delayed by central network equipment with no mechanisms or support to link to a device user interface (UI) to inform the user what is happening and why it is happening. This can lead to a frustrating user experience and reduced carrier customer satisfaction. Accordingly, in some embodiments, a device based UI is provided to provide the user with real time or near real time information regarding why a service usage activity is being controlled, blocked, throttled, and/or otherwise controlled in order to protect network capacity. In some embodiments, a UI is provided that also informs the user when there are options to set, control, override, or modify service usage controls for the purpose of protecting network capacity. In some embodiments, such user preference inputs also correspond to a change in service usage billing. In some embodiments, such changes in service usage billing due to capacity sparing service control changes by the user are communicated to the user via a UI notification sequence. In some embodiments, techniques for protecting network capacity employ user warnings when a service usage activity classified for differential user notification policies is likely to cause the user to go over service plan caps (e.g., total data byte count usage caps).

[0056] What is needed is intelligent network monitoring to provide real-time traffic monitoring network service usage (e.g., at the packet level/layer, network stack application interface level/layer, and/or application level/layer) of the wireless network (e.g., radio access networks and/or core networks) and to effectively manage the network service usage for protecting network capacity (e.g., while still maintaining an acceptable user experience). Using Device Assisted Services (DAS) techniques, and in some cases, network assisted/based techniques, to

provide for network service usage monitoring of devices, network carriers/operators would be provided greater insight into what devices, which users and what applications, and when and where network congestion problems occur, enabling operators to intelligently add additional resources to certain areas when necessary (e.g., offloading data traffic onto femto cells or WiFi hotspots and adding more network resources), to differentially control network service usage, and/or to differentially charge for network service usage based on, for example, a network busy state, for protecting network capacity.

[0057] Intelligent network monitoring of the wireless network to effectively manage network service usage for protecting network capacity can include providing Device Assisted Services (DAS) for protecting network capacity in accordance with various embodiments described herein. For example, intelligent network monitoring of the wireless network to effectively manage network service usage for protecting network capacity can include differentially controlling over the air software updates and/or performing software updates via wired connections only. As another example, intelligent network monitoring of the wireless network to effectively manage network service usage for protecting network capacity can include differentially controlling various applications that demand significant network resources or network capacity. As another example, intelligent network monitoring of the wireless network to effectively manage network service usage for protecting network capacity can include managing network access connection requests resulting from repeated power down modes in the modem, which can cause resource intensive re-connection and/or re-authentication processes. As another example, intelligent network monitoring of the wireless network to effectively manage network service usage for protecting network capacity can include techniques for keeping PPP sessions alive to avoid the need to consume network resources to re-establish PPP sessions (e.g., unless the application behavior analysis predicts that a mean access time is long enough for the PPP session to be dropped off and yet not causing overall network resource limitations).

[0058] Unlike traditional QoS techniques, which are used to establish a single end or end to end guaranteed service level(s) on a network, techniques disclosed herein for protecting network capacity facilitate implementation of services on a network to facilitate differential control of certain services to protect network capacity (e.g., to reduce network congestion, network capacity demand, network resource demand; and/or to increase network availability). As also disclosed herein, techniques disclosed herein for protecting network capacity facilitate implementation of services on a network to facilitate differential control of certain services to protect network capacity can also facilitate QoS implementations by maintaining needed levels of network capacity/availability to facilitate delivery of certain QoS levels/classes. For example, techniques disclosed herein for protecting network capacity can aggregate across multiple services and/or devices to facilitate differential control of certain services to protect network capacity. As another example, techniques disclosed herein for protecting network capacity can be used to provide for dynamic QoS classifications (e.g., dynamically assigning/classifying and reassigning/reclassifying (based on various criteria, events, and/or measures) network service usage activities to various QoS levels/classes, such as described herein) to facilitate differential control of certain services to protect network capacity.

[0059] Accordingly, Device Assisted Services (DAS) for protecting network capacity is provided. In some embodiments, DAS for protecting network capacity provides for protection of network capacity (e.g., network congestion and/or network access/resource demand and/or network availability on an edge element of the network, such as on the Radio Access Network (RAN) of a wireless network, and/or from a device to a base station/base station controller), such as by controlling network service activity usage activities of a device in wireless communication with the network to reduce demands on the network. For example, controlling network service usage activities can include classifying and/or controlling network access requests (e.g., IP address requests), network access reservation requests (e.g., a QoS

reservation/sequence), network capacity/resources usage (e.g., bandwidth usage), and/or any other network service usage activities. In some embodiments, applications, OS functions, and/or other network service usage activities that request IP addresses from network address server resources are classified and/or controlled so that the IP address requests are withheld, delayed, time windowed, reduced in frequency, aggregated or otherwise controlled. In some embodiments, such "IP address request control policies"" for one or more applications, OS functions, and/or other network service usage activities are set, updated, and/or modified before communicating it over a network connection to a network element (e.g., a service controller or another network element/function). In some embodiments, network service usage activities are generated/requested by applications, operating system (OS) functions, and/or other software/functions executed on a device in communication with the network. In some embodiments, it is desirable to apply a service usage control policy for the network service usage activities to protect network capacity (e.g., reduce network capacity demand). For example, some applications and/or OS functions have limited capabilities to defer certain traffic types based on fixed settings in the application, and such applications and/or OS functions typically cannot optimize network service usage activities based on a current network busy state (e.g., based on changing levels of network capacity and/or network performance available to the device). In some embodiments, the network busy state (e.g., or conversely the network availability state) is a characterization of the congestion (e.g., or conversely available capacity) of the network for one or more device connections. For example, the network busy state can provide a measure of how busy or congested the network or a network segment (e.g., network edge element) is for one or more device connections. As another example, network availability state can provide a measure of what network connection resources are available to one or more device connections. Thus, network busy state and network availability state can be viewed as converse ways of providing similar information, and as described herein with respect to various embodiments, these terms can be used interchangeably.

[0060] In some embodiments, techniques are provided for assigning a priority to a network service usage activity and controlling traffic associated with the network services usage activity based on the assigned priority. In some embodiments, techniques are provided for a implementing a differentiated and dynamic background services classification, for example, as a function of network availability state and/or network busy state.

[0061] In some embodiments, a service usage control policy is used for assisting in network access control of network service usage activities (e.g., deferring some or all of the network capacity demand from these source activities). In some embodiments, some or all of the network capacity demand is satisfied at a point where the network resources or capacity are more available or less busy. In some embodiments, techniques are provided for classifying network service activities associated with one or more applications or OS functions to a background service class and differentially controlling the background service class traffic. In some embodiments, techniques are provided for classifying one or more network service activities associated with an application or OS function to a background service class, while other network service activities associated with that application or OS function are classified to other service classes (e.g., or to different background service class priority levels).

[0062] In some embodiments, techniques are provided for determining a network busy state (e.g., for a network edge element connection to a device, such as for a RAN for the device's current wireless network access and/or to the current base station/base station controller in wireless communication with the device). In some embodiments, techniques are provided for implementing a service usage control policy to differentially control network services traffic based on a network busy state for an activity, a group of activities, or for a service class.

[0063] In some embodiments, DAS for protecting network capacity includes monitoring a network service usage activity of the communications device in network communication; classifying the network service usage activity for differential network access control for

protecting network capacity; and associating the network service usage activity with a network service usage control policy based on a classification of the network service usage activity to facilitate differential network access control for protecting network capacity.

[0064] In some embodiments, a network service usage activity is any activity by the device that includes wireless network communication. In some embodiments, an application, an operating system (OS), and/or other device function generates a network service usage activity. In some embodiments, an application, an operating system (OS), and/or other device function generates one or more network service usage activities. Examples of a network service usage activity include the following: a voice connection (e.g., coded voice connection or voice over IP (VOIP) connection), a device application or widget connection, a device OS function connection, an email text connection, an email download connection, a file download connection, a streaming media connection, a location service connection, a map services connection, a software update (e.g., application, operating system, and/or antimalware software update) or firmware update connection, a device backup connection, an RSS feed connection, a website connection, a connection to a server, a web browser connection, an Internet connection for a device based service activity, establishing a sync service account, a user data synchronization service, a device data synchronization service, a network connection flow or stream, a socket connection, a TCP connection, a destination/port assigned connection, an IP connection, a UDP connection, an HTTP or HTTPS connection, a TLS connection, an SSL connection, a VPN connection, a general network services connection (e.g., establishing a PPP session, authenticating to the network, obtaining an IP address, DNS service), and various other types of connections via wireless network communication as will be apparent to one of ordinary skill in the art.

[0065] In some embodiments, a network service usage activity is classified, associated with, and/or assigned to a background class (e.g., a background service or QoS class) to facilitate

differential network service usage control to protect network capacity. In some embodiments, differential network service usage control includes one or more of the following: monitoring network service usage activity; accounting for network service usage activity; reporting network service usage activity; generating a user notification for a network service usage activity; requesting a user preference for control of network service usage activity; accepting a user preference for network service usage activity; implementation of a network service usage activity policy (e.g., block/allow; traffic control techniques, such as throttle, delay, priority queue, time window, suspend, quarantine, kill, remove, and other well known traffic control techniques); implementing UI intercept procedures; generating a network busy state notification; generating a background class notification; generating a user notification for differential network service usage control of a network service usage activity; and various other techniques as described herein.

[0066] In some embodiments, a network availability state includes a state or measure of availability/capacity of a segment of a network (e.g., a last edge element of a wireless network). In some embodiments, a network busy state includes a state or measure of the network usage level or network congestion of a segment of a network (e.g., a last edge element of a wireless network). In some embodiments, network availability state and network busy state are inverse measures. As used herein with respect to certain embodiments, network availability state and network busy state can be used interchangeably based on, for example, a design choice (e.g., designing to assign background policies based on a network busy state or a network availability state yields similar results, but they are different ways to characterize the network performance and/or capacity and/or congestion). In some embodiments, network availability state and network busy state are dynamic measures as such states change based on network usage activities (e.g., based on a time of day, availability/capacity level, congestion level, and/or

performance level). In some embodiments, differential network service usage control of a network service usage activity is based on a network busy state or network availability state.

[0067] In some embodiments, certain network service usage activities are classified as background services. In some embodiments, lower priority and/or less critical (and/or based on various other criteria/measures) network service usage activities are classified as background services based on a network busy state and differentially controlled based on a network busy state to protect network capacity. In some embodiments, differential network service usage control policies are based on a time of day, a network busy state, background services and/or QoS class changes based on a time of day and/or a network busy state, a random back-off for access for certain network service usage activities, a deterministic schedule for certain network service usage activities, a time windowing in which network service usage control policies for one or more service activities or background/QoS classes changes based on time of day, network busy state, a service plan, and various other criteria, measures, and/or techniques as described herein.

[0068] In some embodiments, a network capacity controlled service or network capacity controlled services class includes one or more network services (e.g., background download services and/or various other types or categories of services as described herein) selected for differential network service usage control for protecting network capacity. In some embodiments, a network capacity controlled services classification includes one or more network services associated with a network capacity controlled service/class priority setting for differential network service usage control for protecting network capacity. In some embodiments, a network capacity controlled service or network capacity controlled services class includes one or more network services associated with a QoS class for differential network service usage control for protecting network capacity. In some embodiments, a network capacity controlled service or network capacity controlled services class includes one or more

network services associated with a dynamic QoS class for differential network service usage control for protecting network capacity.

[0069] For example, differentially controlling network service usage activities based on network capacity controlled services or dynamic QoS or QoS classifications can protect network capacity by, for example, improving network performance, increasing network availability, reducing network resources demand, and/or reducing network capacity demand (e.g., based on an individual device, aggregate devices connected to an edge element, and/or aggregate devices connected to many edge elements). In some embodiments, differentially controlling network service usage activities based on network capacity controlled services or dynamic QoS or QoS classifications can protect network capacity while maintaining proper device operation. In some embodiments, differentially controlling network service usage activities based on network capacity controlled services or dynamic QoS or QoS classifications can protect network capacity while maintaining an acceptable user experience (e.g., proper and/or expected device operation, proper and/or software/application/OS/function operation, avoiding (whenever possible) significant adverse impact on device functions, and/or user notifications to keep the user informed of various differential control implemented on the device).

[0070] In some embodiments, dynamic QoS classifications include QoS classifications that can be dynamically modified (e.g., reclassified, reprioritized, upgraded, and/or downgraded) based on various criteria, measures, settings, and/or user input as described herein (e.g., based on a time of day and/or day of week, based on a network busy state, based on a user preference, and/or based on a service plan). In some embodiments, the various techniques described herein related to DAS for providing network capacity and/or QoS for DAS are applied to dynamic QoS related techniques.

[0071] As wireless networks, such as mobile networks, evolve towards higher bandwidth services, which can include or require, for example, various levels of Quality of Service (QoS)

(e.g., conversational, interactive data, streaming data, and/or various (end-to-end) real-time services that may benefit from QoS), demands will increase for converged network services to facilitate such services for end-to-end services between networks (e.g., to allow for control and/or support for such services, for example, QoS support, across network boundaries, such as between wireless networks (such as various service provider networks) and IP networks (such as the Internet), and/or other networks). While various efforts have attempted to address such QoS needs, such as policy management frameworks for facilitating QoS end-to end solutions, there exists a need to facilitate various QoS requirements using Device Assisted Services (DAS).

[0072] Accordingly, Quality of Service (QoS) for Device Assisted Services (DAS) is provided. In some embodiments, QoS for DAS is provided.

[0073] To establish a QoS channel, differentiated services are typically available, in which one class/level of service has a higher priority than another to provide for differentiated services on a network, such as a wireless network. For example, in a wireless network, various network elements/functions can be provisioned and controlled to establish a single end or end to end QoS channel. In some embodiments, a centralized QoS policy coordination and decision function using DAS techniques to assist in coordinating the QoS channel setup and control among the various elements of a wireless network is provided.

[0074] In some embodiments, QoS channel refers to the logical communication channel connected to a device that provides a desired level of QoS service level. For example, the QoS channel can be created with one or more QoS links, in which each link represents a QoS enabled connection that spans a portion of the total end to end network communication path from a near end device to a far end device. For example, the far end device can be on the same network or on a different network, potentially with different access technology and/or a different access network carrier. In some embodiments, the QoS channel includes one or more

QoS links in which each link in the channel is QoS enabled, or one or more of the links in the channel is QoS enabled and others are not. As an example, a QoS channel can include the following links: a first device traffic path link, a first device to access network equipment element link (e.g., 2G/3G/4G wireless base station, WiFi access point, cable network head end, DSLAM, fiber aggregation node, satellite aggregation node, or other network access point/node), a first carrier core network, a long haul IPX network, a second carrier core network, a second device to access network equipment element link, and a second device traffic path link as similarly described herein with respect to various embodiments.

[0075] In some embodiments, each of the links described above have the ability to provide QoS services for that segment of an overall QoS channel. In some embodiments, the device traffic path link and/or the device to access network equipment element link are QoS enabled, but the carrier core network and/or IPX network links are not QoS enabled. In some embodiments, the core network and/or IPX network have sufficient over-provisioning of bandwidth that QoS is not limited by these network elements and, for example, can be limited by the device traffic link and/or the device to access network equipment element link do not have sufficient excess bandwidth making it desirable to QoS enable these QoS channel links. A common example is a 2G/3G/4G wireless network in which a device traffic path link and the device to access network element link (e.g., Radio Access Bearer (RAB)) are QoS enabled while the carrier core network and IPX network links are not (e.g., are provided at a best effort service level or other service levels).

[0076] In some embodiments, a QoS session refers to the QoS enabled traffic for a given device that flows over a QoS channel or QoS link. This QoS traffic supports a QoS service activity. In some embodiments, a QoS service activity includes a device service usage that is requested, configured, or preferably serviced with a given level of QoS. In some embodiments, a device QoS activity is a combination of one or more of the following: application, destination,

source, socket (e.g., IP address, protocol, and/or port), socket address (e.g., port number), URL or other similar service identifier, service provider, network type, traffic type, content type, network protocol, session type, QoS identifier, time of day, network capacity (e.g., network busy state), user service plan authorization or standing, roaming/home network status, and/or other criteria/measures as similarly described herein. For example, QoS service activities that are supported by QoS sessions can include VOIP traffic, streaming video traffic, differentiated access bandwidth during busy network periods, real-time interactive traffic, such as network connected multimedia meetings (e.g., shared presentations, picture, video, voice, and/or other such applications/services), best effort interactive, such as Internet browsing, time sensitive services, such as email message body delivery, near real-time interactive services, such as SMS or push to talk, background download services, such as email downloads and other file transfers (e.g., FTP), and/or truly background download services, such as software updates (e.g., OS or application software updates and/or antimalware updates including content/signature updates).

[0077] In some embodiments, various QoS levels or classes are supported. For example a conversation class can provide for real-time traffic, which is typically very delay sensitive but can tolerate bit errors and packet losses. The conversational class is typically used for Voice Over IP (VOIP) and video telephony, in which users of such services benefit from the short delay features of the conversational class. A streaming class is similar to the conversational class except that the streaming class typically can tolerate more delay than the conversational class. The streaming class is generally used for when one end of the connection is a user (e.g., human user) and the other end is a machine/computer (e.g., for streaming content applications, such as streaming of video, such as movies or other video content). An interactive class is generally intended for traffic that allows delay variation while requiring reasonably low response time (e.g., web browsing or other applications in which the channel can be unused for long

periods of time but when a user makes a request for a new page/data, the response time should be reasonably low). A background class is generally used for lowest priority service usages (e.g., typically used for e-mail with and without downloads/attachments, application software updates, OS software updates, and/or other similar applications/functions). In some embodiments, various QoS classes or services are applicable to the conversational class. In some embodiments, various QoS classes or services are also applicable to the streaming class. In some embodiments, various QoS classes or services are also applicable to the interactive class but typically not applicable to the background class. As will now be apparent to one of ordinary skill in the art, various other classes can be provided with lower or higher granularity based on service usage/channel requirements and/or network architectures.

[0078] In some embodiments, a QoS link or a QoS channel supports one QoS session. In some embodiments, a QoS link or a QoS channel supports multiple QoS sessions. In some embodiments, QoS link provisioning is provided to setup the QoS traffic level for a given QoS session or group of QoS sessions.

[0079] In some embodiments, a QoS channel is a single ended QoS channel or an end to end QoS channel. For example, if a QoS channel is end to end, then the QoS channel provisioning is accomplished in a coordinated manner for each QoS enabled link in the QoS channel. If a QoS channel is single ended, then the network elements and/or device participate in provisioning as much of one end of the QoS channel as possible, leaving provisioning of the QoS for the other end of the channel as the responsibility of the device and/or network elements that handle the traffic at the other end of the QoS channel. In some embodiments, a single ended QoS channel includes another single ended QoS channel at the other end. In some embodiments, only one end has single ended QoS channel enablement while the other end of the channel is a best effort service level, which, for example, can be used where one end of the QoS channel has tighter constraints on traffic capacity or quality than the other end (e.g., a

VOIP call with one end that is QoS enabled on a 3G wireless network that has relatively tight bandwidth compared to a lightly loaded cable modem network device on the other end which may not need to be QoS enabled in order to achieve adequate voice quality).

[0080] In some embodiments, a QoS request (e.g., a QoS channel request or QoS service request) is a request for a QoS provisioning event to enable a QoS channel for one or more QoS service activities. In some embodiments, QoS availability assessment includes determining whether one or more of the links in a possible QoS channel are available (e.g., based on network capacity and transmission quality) to provision the necessary level of QoS for a requested QoS channel. In some embodiments, a QoS request is initiated by a device, a user, an application, and/or a network element/function as similarly described herein.

[0081] In some embodiments, a service plan refers to the collection of access service capabilities, QoS capabilities, and/or network capacity controlled services that are associated with a communications device. In some embodiments, the access service capabilities, QoS capabilities, and/or network capacity controlled services are determined by the collection of access service control policies for the device. In some embodiments, these service control policies are implemented in the network equipment. In some embodiments, these access service control policies are implemented both in the device and in the network equipment. In some embodiments, these access service control policies are implemented in the device. In some embodiments, there are different levels of service control capabilities (e.g., policies) based on different levels of service plan payments or device standing or user standing. In some embodiments, there are different levels of service control policies based on network type, time of day, network busy status, and/or other criteria/measures as similarly described herein with respect to various embodiments. In some embodiments, the access control and QoS control policies are based on the type of service activity being sought. In some embodiments, the QoS level and access level available for a given service activity for a given device or user is

determined by the policies associated with the service plan. In some embodiments, a QoS authorization assessment is performed to determine whether a device or user has sufficient service plan standing to allow the requested level of QoS.

[0082] In some embodiments, before a QoS channel or link is provisioned (or before a QoS request is responded to or filled), a QoS availability assessment is performed to determine whether sufficient communication channel resources are available to provision the necessary level of QoS for the QoS channel or link. In some embodiments, this QoS availability assessment is determined by assessing the available QoS capacity for one or more necessary QoS links in the channel. For example, the available QoS link capacity can be assessed for one or more of a device traffic path, a device to access network equipment element link, a core network link, and/or an IPX network link. If the QoS assessment shows that the necessary channel capacity and quality is available for the desired QoS level for one or more desired QoS service activities, then a QoS channel request or QoS service request can be granted. In some embodiments, a QoS link or QoS channel reservation process is provided to reserve QoS capacity and quality in advance of link or channel provisioning to ensure that the available QoS resources are not assigned between the time of QoS availability assessment and QoS channel provisioning.

[0083] In some embodiments, the QoS availability assessment is performed after QoS authorization assessment. This prevents the unnecessary exercising of network elements when the device or user does not have sufficient service plan standing to receive the desired level of QoS even if it is available. This can be an important screening function performed on the device in the service processor, or by a centralized network function such as the service controller (e.g., or interchangeably, the home agent; Home Location Register (HLR); Authentication, Authorization, and Accounting (AAA) server/gateway/function; base station; one of the gateways, policy and charging rules function (PCRF), or other network element/function). In

some embodiments, QoS availability is assessed without conducting a QoS authorization assessment or before receiving the response to a QoS authorization assessment.

[0084] In some embodiments, a QoS channel is provisioned to create the QoS channel to support a QoS session (e.g., a QoS service activity). In some embodiments, QoS channel provision includes assigning, routing, and/or otherwise causing the QoS session traffic to flow over one or more QoS links in the assigned QoS channel.

[0085] In some embodiments, device assisted service traffic control and QoS apply readily and directly to the problems of managing a QoS device link for QoS channel provisioning. Accordingly, in some embodiments, a service provider is provided to assist in provisioning the device portion of the QoS channel. In some embodiments, the service processor provisions the device link portion of the QoS channel by placing a higher priority on higher QoS level traffic. In some embodiments, this QoS priority is implemented in a number of ways, including routing the higher priority QoS traffic into first priority in the downstream and/or upstream traffic queues. Upstream traffic queuing is performed directly in some embodiments by transmitting guaranteed bit rate traffic first at higher available throttling rates, differentiated QoS traffic second with a controlled throttling rate, best effort traffic third with possibly lower controlled throttled rates, and/or background traffic fourth when/if bandwidth not needed by the higher levels of QoS traffic and at lower controlled throttling rates. For example, downstream traffic can be handled by queuing traffic and delaying or preventing TCP acknowledgements to be returned for the lower levels of QoS priority, while immediately passing the traffic and TCP acknowledgements for higher levels of QoS priority. The device link portion of the QoS channel is thus provisioned by assigning policies for the queuing priority, delay, throttle rate, and TCP acknowledgement return rate for device traffic in accordance with the bandwidth that is available at any point in time for the device. In some embodiments, various device service processor traffic control capabilities

regulate or partially regulate QoS in accordance with a set of network policy instructions, including, in some embodiments, a service plan policy set.

[0086] In some embodiments the device service processor establishes multiple QoS channels through the device traffic path with each QoS channel having traffic control policies as described herein, with each QoS channel policy set creating a different class of QoS. In some embodiments, employing this multiple QoS channel approach, QoS for a given service activity is provided by routing the traffic for that QoS activity to the appropriate QoS channel with the appropriate QoS policy settings. The routing to the appropriate QoS channel can be provided using various techniques. For example, the routing can be provided by applying a common service traffic control policy set to traffic associated with all QoS service activities that require or request the QoS provided by the common service traffic control policy set. The application of the service traffic control policy set can be accomplished in a number of ways utilizing the embodiments described for the policy implementation agent and the policy control agent described herein. In such embodiments, the problem of assigning a QoS channel to a number of QoS service activities is reduced to applying a pre-determined set of service traffic control policies to each of the QoS service activities, with each pre-determined set of service traffic control policies representing a different QoS class. The device can then manage the overall QoS for all traffic based on the available traffic capacity and quality, the total aggregate traffic demand for each QoS traffic class and the policy rules that determine how each traffic class is provided with differential bit rate and traffic quality as compared to the other traffic classes for a given level of available traffic capacity and quality.

[0087] Based on the aggregate demand for each traffic QoS class, and the traffic capacity and quality level available to the device, the service processor can adjust the total available bit rate or percentage of available traffic capacity for each QoS class. For example, in some embodiments, the aggregate demand for the real-time interactive traffic control class (e.g.

services, such as VOIP, emergency communication services or high performance real-time competitive gaming) can be determined, and the QoS routing function on the device (e.g., a QoS router agent/function) can first allocate enough constant bit rate traffic capacity from the available traffic capacity to satisfy these services, with each QoS service activity that requires this QoS class being assigned to this QoS channel. As more QoS service activities require this traffic class, the capacity allocated to the QoS channel out of the available device capacity is increased, and when fewer QoS service activities require this traffic class the capacity for this QoS channel is released. In the event that the device does not have any more available capacity with a guaranteed bit rate QoS level, then additional QoS service activities that desire, require or request this QoS level will not be provided this QoS level, and instead will either be provided with a lower QoS level or will not be allowed to connect to the access network. In some embodiments, there can be a hierarchy among the possible QoS service activities so that if there is no more capacity available at a given service QoS level, then the available capacity for that QoS class is provided to the service activities requiring that QoS from highest priority to lowest, until the available QoS class capacity is consumed, and then one or more QoS service activities that are too low on the priority list to obtain service with that QoS class are either bumped to a lower QoS class or are denied access. In some embodiments, once the required capacity to satisfy the real-time constant rate traffic needs is satisfied, the remaining capacity available to the device is then divided among the other QoS channel classes in accordance with a priority policy, with the priority policy being based on the relative priority of each service class, the relative priority of each QoS service activity, or a combination of the relative priority of each QoS service class and each QoS service activity. For example, these relative priority policies can vary from device to device based on service plan selection, device type, user standing, user group, device location, device network connection, type of network, time of day, network busy state, and/or other criteria/measures.

[0088] In some embodiments, a QoS link is established between the device and an access network equipment element. For example, such equipment element embodiments can include a 2G/3G/4G wireless base station, a wireless access point, a cable network head end, a DSL network DSLAM, a fiber network device traffic aggregator, a satellite network device traffic aggregator, a frame relay aggregation node, an ATM aggregation node, and/or other network equipment. In some embodiments, a logical communication channel is created between the device and the network equipment element, with the logical communication channel supporting a given level of QoS or QoS class traffic policy set. For example, the logical channel can include a RAB formed between a 2G/3G/4G base station and a wireless end point device. The RAB can be formed by controlling the media access control (MAC) parameters of the base station radio channel so that a given level of QoS class policies can be implemented. For example, the RAB can support constant bit rate, low latency communication traffic for guaranteed bit rate real-time traffic, or a differentiated high priority access channel for streaming traffic, or a best effort random access channel for best effort traffic, or an available unused capacity traffic for background traffic. The QoS channel link created in this manner can be dedicated to a single device, or shared with a subset of devices, or available to all devices. The QoS channel link created in this manner can be used by the device to support a single QoS activity as described herein, or a group of QoS activities as described herein. It will now be apparent to one of ordinary skill in the art that similar settings for cable head end and cable modem MAC can yield similar QoS classes for QoS links for the cable modem case and that similar techniques can be applied for a wireless access point or a satellite system MAC to achieve similar QoS classes for QoS links. It will also now be apparent to one of ordinary skill in the art that by creating multiple logical channels in the device link, and/or adjusting the available access network capacity and quality for each logical device communication channel in the DSLAM or fiber aggregator, similar QoS class QoS links can be established for the DSL and fiber distribution network cases.

[0089] In some embodiments the device service processor serves to route QoS service activities to the appropriate logical communication channel established for the desired QoS class supported by a QoS link between the device and the access network equipment element. In some embodiments, the device service processor elements (e.g., the policy implementation agent and/or the policy control agent) can be used in some embodiments to assign the same QoS traffic control policies to one or more QoS service activities that require the same QoS level. In a similar manner, in some embodiments, the device service processor elements can be used to assign or route service activity traffic for a given QoS class to the correct logical communication channel between the device and the access network element (e.g., a 2G/3G/4G base station) that supports the traffic control policies for the desired QoS class. For example, a QoS service link that supports guaranteed bit rate and latency can be established with one or more RABs from a base station to the device, and a second QoS service link can be established that supports differentiated preferred access for streaming content using one or more differentiated access RABs, and a third best effort RAB can be used to support best effort traffic. Each of the required RABs is first requested and then provisioned as described herein based on the aggregate required capacity and quality for one or more QoS service activities that require or desire the specific QoS service class associated with the RAB logical channel policy parameters. Once the set of logical QoS channels is thus established, the service processor (e.g., QoS router agent/function) routes the traffic associated with each QoS service activity to the appropriate RAB. In some embodiments, the service processor can detect increases or decreases in aggregate QoS class demand for each QoS class as QoS activities are initiated or terminated for that QoS class, and the service processor can communicate the required increases or decreases in the RAB assignments required to support that logical QoS channel.

[0090] In some embodiments, the access QoS link is established by direct communication from the device in which the device requests the QoS channel or link from the access network

equipment element, or the device requests the QoS channel or link from an intermediate networking device, such as a service controller (e.g., or a readily substituted device with similar features, such as a home agent, an HLR, a mobile switching center, a base station, an access gateway, a AAA system, PCRF, or a billing system). In some embodiments, the device service processor bases the QoS channel or link request on an association the device performs to match a QoS service activity with a desired or required QoS class or QoS traffic control policy set. For example, this association of QoS class or QoS traffic control policy set with QoS service activity can be determined by a predefined policy mapping that is stored on the device and used by the service processor. In some embodiments, this policy mapping store is populated and/or updated by a service controller (e.g., or similar function as described herein). In some embodiments, the mapping is determined by a service controller (e.g., or similar function as described herein) based on a report from the device of the QoS service activity that needs the QoS channel or link.

[0091] In some embodiments, the required or desired QoS level for one or more QoS service activities is determined by a set of QoS service traffic control policies that are pre-assigned to various QoS service activities. For example, a given application can be pre-assigned a QoS class. As another example, a web service destination such as a VOIP service site can be assigned a QoS class. As another example, a given application can have one QoS assignment level for general Internet traffic but have a QoS assignment for real-time gaming traffic. As another example, a real-time broadcasting website can have a best effort QoS level assigned to programming information and general browsing and have a differentiated streaming QoS level for broadcast traffic content. In some embodiments, detection of QoS need or QoS assignment request for a given activity can be assigned by a device service processor according to a pre-defined QoS policy rules table (e.g., QoS activity table), or can be determined by a service controller based on information reported by the device, or can be requested by an application

through a QoS application interface (e.g., QoS API), or can be determined by the nature of incoming traffic.

[0092] In embodiments, in which both end points in the QoS channel participate in establishing an end to end QoS channel, the required QoS level is determined and/or communicated by the originating end point. In some embodiments, the required QoS level is determined and/or communicated by the receiving end point. In some embodiments the QoS level is determined and/or communicated by the originating end point service controller (e.g., or the access network element (such as a base station), the HLR, home agent, mobile switching center, AAA, gateway, or other network element/function). In some embodiments, the QoS level is determined and/or communicated by the receiving end point service controller (e.g., or alternatively the access network element (such as a base station), the HLR, home agent, mobile switching center, AAA, gateway, or other network element/function). In some embodiments, the receiving end point service controller (e.g., or the access network element (such as a base station), the HLR, home agent, mobile switching center, AAA, gateway or other network function) and the originating end point service controller (e.g., or other similar function) communicate with one another to coordinate establishment of the QoS channel between the end points.

[0093] In some embodiments, the near end or originating end device service processor contacts the far end or terminating device service processor to initiate a QoS channel. In some embodiments, the initiation of the QoS channel from the near end or originating device is performed automatically by the far end device when its service processor detects that a given level of QoS is needed for the communication between the two devices. In some embodiments, the near end or originating device service processor detects the need for a QoS channel to the far end or terminating device and contacts a central network resources, such as the service controller (e.g., or other equipment element with similar function for this purpose), and the

service controller provisions the far end of the QoS channel, either by communicating directly with the far end device or by communicating with the far end device's service controller (e.g., or other equipment element with similar function for this purpose). In some embodiments, in which the far end device service controller is contacted to assist in provisioning the QoS channel, there is a look up function to determine the address of the far end service controller based on a look up index formed from some aspect of the far end device credentials (e.g., phone number, SIM ID, MEID, IMSI, IP address, user name, and/or other device credentials).

[0094] In some embodiments, the mapping of QoS service activity to the desired level of QoS class or QoS traffic control policies is determined by providing a QoS API in the device service processor that applications use to request a QoS class or QoS channel connection. In some embodiments, an API is provided so that application developers can create application software that uses the standard interface commands to request and set up QoS channels. In some embodiments, the API does one or more of the following: accepts QoS requests from an application, formats the QoS channel request into a protocol appropriate for transmission to network equipment responsible for assessing QoS channel availability (e.g., including possibly the device traffic control system), coordinates with other network elements (e.g., including possibly the device traffic control system) to reserve a QoS channel, coordinates with other network elements (e.g., including possibly the device traffic control system) to provision a QoS channel, informs the application that the desired QoS channel can be created or not, and/or coordinates with other network elements (e.g., including possibly the device traffic control system) to connect the application with the desired QoS channel class. In some embodiments, the QoS API accepts the application QoS request and communicates and possibly coordinates with one or more QoS network equipment elements, such as a base station, cable head end or access point. In some embodiments, the QoS API accepts the QoS request from the application and communicate and possibly coordinates with an intermediate network element,

such as a service processor (e.g., or other similar function as described herein). In some embodiments the QoS API assesses the QoS service plan standing for the device or user before sending QoS channel requests to other network elements, and only initiates the QoS request sequence if required service plan authorization is in place. In this manner, the potentially complex process of establishing a QoS channel with all the specific equipment communication protocols that typically need to be supported to assess QoS channel availability and provision the QoS channel are simplified into a limited set of API commands that are easy for an application development community to learn about and use for QoS differentiated services and applications.

[0095] In some embodiments, local traffic control on the device service processor is combined with traffic control in the link between the device and the access network equipment element. In this manner, both the device traffic control path QoS link and the device to access network element QoS link can be coordinated for best device QoS performance results given the available capacity and quality of the access network traffic for the device. In some embodiments, the policies for how the device manages local traffic control, establishes access network element logical channels (e.g., RABs) and routes traffic to and from the access network element logical channels is all determined by predefined policy rules loaded onto the device by the service controller (or other equivalent network element). In some embodiments, these policies are determined in the service controller itself.

[0096] In some embodiments, a QoS user interface (e.g., QoS UI) is presented to the device user. In some embodiments, the QoS UI notifies the user what level of QoS services the device is authorized to receive based on the service plan selection. In some embodiments, the QoS UI notifies the user what level of QoS services are available on the present network the device is connected to at the present time. In some embodiments, the QoS UI notifies the user when a level of QoS service that is higher than that authorized by the user service plan is required or

desirable for a given service activity that the device has initiated. In some embodiments, the QoS UI provides the user with a set of one or more upgrade options to upgrade the service plan to include a higher level of QoS for one or more service activities. In some embodiments, the QoS UI provides the user with an opportunity to specify what level of QoS the user would like to employ for one or more service usage activities. In some embodiments, the QoS UI allows the user to specify a service plan setting that provides differentiated QoS during times when the network is busy. In some embodiments, the QoS UI allows the user to purchase one or more grades of service QoS with either a post-pay for a pre-defined service period and one or more pre-defined service usage limits by QoS class, a pre-pay for one or more pre-defined service usage limits by QoS class, or another payment system for differentiated QoS services. In some embodiments, the QoS UI provides the user with an opportunity to QoS enable or pay for QoS services for a connection that is initiated by an incoming connection to the device.

[0097] In some embodiments, QoS for DAS techniques include verifying that the device is properly implementing the QoS traffic control policies, for example, in accordance with a service plan. This ensures that errors, hacking, user device software settings manipulations, or other malware events do not result in inappropriate levels of QoS for a given device or group of devices. Accordingly, in some embodiments, the traffic control and QoS verification techniques described herein are employed to verify that the proper level of QoS is applied for a given service usage activity in accordance with a QoS priority policy. For example, verification of QoS channel request policy rules behavior can be implemented in a variety of ways including, as an example, monitoring device QoS channel requests and comparing the level of QoS requested with the level of QoS the device is authorized to receive in the service plan in effect for the device. Verification of proper QoS channel usage behavior by a device can be implemented in a variety of ways including, for example, monitoring network based reports of QoS service usage and comparing the network based reports against the service policy rules that should be

in effect given the device service plan. Verification of proper device traffic control to implement a QoS service policy that is in effect can be accomplished in a variety of ways by verifying that the appropriate traffic control policy rules are being properly implemented as described herein. In some embodiments, DAS for protecting network capacity techniques include various verification techniques (e.g., verifying monitoring, traffic controlling, reporting, and/or other functions implemented or performed by the device), as described herein.

[0098] In some embodiments, the QoS router prioritizes traffic on the device. In some embodiments, the QoS router connects the QoS enabled session to the RAB that has the proper QoS level. In some embodiments, one session is routed to the RAB. In some embodiments, more than one session can be routed to an RAB. In some embodiments, multiple RABs providing multiple QoS levels are created to the device, and the QoS router routes each service activity to the RAB dictated by the QoS policy rules in effect on the device.

[0099] In some embodiments, the network collects service usage charges for different QoS classes. In some embodiments, there is differentiated service charging for the different classes of QoS service usage. As an example, since guaranteed bit rate traffic consumes network resources whether the traffic capacity is used or not, there can be a time element involved in the charging calculations. As a more detailed example, guaranteed bit rate services can be charged by the total bandwidth provisioned to the device at a given time multiplied by the amount of time that that bandwidth is made available. In some embodiments, differentiated access traffic that has higher QoS than best effort traffic but is not guaranteed bit rate can be charged at a higher rate than best effort traffic but lower than guaranteed bit rate. In some embodiments, such traffic can be charged based on the time the QoS channel is made available and the total amount of data transmitted over the channel, or can only be based on the total amount of data transmitted over the channel. Best effort traffic is charged in some embodiments based only on the total amount of data used, with the data charges being less

than differentiated streaming access services. Background data services in some embodiments are charged at the lowest rate, possibly with only certain times of the day or periods of low network traffic demand being available for such services, and with the service being based on total data transmitted. In some embodiments, all QoS service levels can be charged based on a fixed price for a fixed charging period, possibly with a service usage cap with additional charges if the service cap is exceeded. In such fixed price scenario embodiments, the price charged is again higher for higher levels of QoS. In some embodiments, the network collects service usage charges for different network capacity controlled service classes. In some embodiments, there is differentiated service charging for the different classes of network capacity controlled service usage, as described herein.

[00100] In some embodiments, the network equipment (e.g., access network element, gateways, AAA, service usage storage systems, home agent, HLR, mobile data center, and/or billing systems) record and report service usage for one or more of the QoS service classes used by the device. In some embodiments, the device service processor records and reports service usage for one or more of the QoS service classes used by the device and reports the QoS service class usage to the service controller (e.g., or another substitute network element). In some embodiments, in which the device is recording reporting usage for one or more QoS service classes, it is important to verify the device service usage reports to ensure that the device usage reports are not distorted, tampered with, and/or otherwise in error. In some embodiments, verifying service usage reports against service usage that should be occurring given the service control policies in place on the device, service processor agent functional operation verification, test service usage events, agent query response sequences, device service processor software protection techniques, device service processor software environment checks, and several other techniques are provides as described herein. For example, using one or more of these verification techniques can provide a verifiable device

assisted QoS service usage charging system. As another example, using one or more of these verification techniques can provide a verifiable network capacity controlled service usage charging system. In some embodiments, the network equipment (e.g., access network element, gateways, AAA, service usage storage systems, home agent, HLR, mobile data center, and/or billing systems) record and report service usage for one or more of the network capacity controlled service classes used by the device, as described herein.

[00101] In some embodiments, device assisted traffic control is provided for managing network congestion as follows. For example, when a given base station or group of base stations experience traffic demand that is high relative to the available capacity and/or service quality that can be provided, and such a condition is determined (e.g., detected or reported) based on a network busy state assessment as described below and further herein, then a service controller (e.g., or another network function) can issue, send, and/or implement traffic control throttling policies to/for the devices in accordance with a measure of the excess traffic demand the one or more base stations is experiencing. For example, the device service processors connected to an overly busy base station can be instructed to reduce the traffic control priority for one or more classes of QoS traffic, reducing the queuing priority, throttling rate, delay and/or access allowance for some or all of one or more classes of traffic. As another example, the device service processors connected to an overly busy base station can be instructed to reduce the traffic control priority for one or more classes of network capacity controlled services traffic, reducing the queuing priority, throttling rate, delay and/or access allowance for some or all of one or more classes of such traffic. As another example, one or more classes of network capacity controlled services traffic, such as background download processes, which can include, for example, software updates can be turned off completely or throttled back significantly. As another example, best effort traffic such as Internet browsing can be throttled or reduced for a group of devices connected to base stations experiencing excess traffic

demand. As another example, a policy can be implemented on the devices connected to busy base stations in which the device is allowed to browse or conduct other best effort service activities at a relatively high throttling rate for a period of time, but if the device uses more than a certain amount of service (e.g., total data downloaded and/or uploaded) in a certain period of time then the device may be traffic controlled according to an adaptive throttling policy as described herein. In some embodiments, higher QoS level traffic cannot be throttled in such circumstances, such as VOIP traffic where real-time guaranteed bit rate is important to meet user service needs or expectations, while lower priority traffic such as interactive browsing and/or background download are throttled and/or blocked. In some embodiments, the QoS availability assessment processes described herein are adjusted so that higher QoS channels are not provided and provisioned in times or locations in which a given base station or group of base stations experience excess demand or demand above a given threshold.

[00102] In some embodiments, users or devices that have service plans with higher QoS levels, or service plans with higher priority during busy network periods have different traffic control policies (e.g., for QoS services and/or network capacity controlled services) applied to them that result in a higher level of traffic performance and/or a higher level of QoS service availability. For example, emergency service workers can be given higher traffic control access policies that result in differentiated services during peak busy times on the network or a portion of the network. In some embodiments, users can obtain a premium service plan for differentiated access during peak busy time periods or may use higher levels of QoS service settings and/or service plans to achieve differentiated service during peak busy periods. As another example, services that demand high levels of QoS classes, such as real-time voice services, instant messaging, push to talk, differentiated video streaming, and/or interactive gaming, are not traffic controlled to the same extent that other lower priority services or lower class service plans are traffic controlled during peak busy times. For example, this type of

service differentiation can also be applied based on device type, user group, user standing, user reward zone points, and/or other criteria/measures as similarly described herein.

[00103] In some embodiments, the decision to control (e.g., reduce, increase, and/or otherwise control in some manner) the access traffic control settings as described above is made by the device service processor based on the device's assessment of the network capacity, which can be determined using various techniques as described herein. In some embodiments, the decision to control the access traffic control settings as described above is made by a service controller (e.g., or other interchangeable network equipment element or elements as described herein) connected to the device that provides instructions to the device to adjust the access policy settings. For example, the service controller can obtain the network capacity information from access equipment elements, from device reports of traffic capacity and/or quality as described herein, or from reports on traffic capacity and/or quality obtained from dedicated devices used for the purpose of assessing network capacity. In some embodiments, the decision to control the access traffic control settings as described above is based on the time of day, the day of week, or both to accommodate cyclical patterns in network capacity and traffic demand.

[00104] In some embodiments, a service controller (e.g., or another network equipment element or elements, as described herein) assesses network busy state and then controls device traffic demand by reducing the offered capacity for one or more service classes (e.g., for QoS services and/or network capacity controlled services) supported by the access network equipment elements, such as a wireless base station. In such embodiments, the service controller (e.g., or similar function) gathers the network capacity information with one of the techniques described herein and instructs one or more of the access network equipment elements to reduce the offered capacity for one or more levels of QoS classes and/or network capacity controlled service classes, to one or more of the devices connected to the access

network equipment elements. For example, the determination of which devices to throttle back can be made based on an equal throttling of all devices of a given service plan status, or based on the device traffic usage patterns in the recent past as described herein, or based on a combination of service plan status and recent traffic usage patterns.

[00105] In some embodiments, the device is enabled with ambient services that have differentiated QoS services and/or network capacity controlled services as part of the ambient service offering. For example, ambient QoS techniques can be provided using the pre-assigned QoS policies for a given service activity set within the ambient service, or using an ambient service application that requests QoS through the QoS API. Other embodiments for providing QoS differentiated service activities within ambient service offerings will now be apparent to one of ordinary skill in the art. As another example, ambient network capacity controlled service techniques can be provided using the pre-assigned network capacity controlled policies for a given service activity set within the ambient service, monitoring and dynamically assigned techniques, and/or using an ambient service application that uses API or emulated API techniques, and/or other techniques as described herein.

[00106] In some embodiments, a QoS service control policy is adapted as a function of the type of network the device is connected to. For example, the QoS traffic control policies and/or the QoS service charging policies can be different when the device is connected to a wireless network (e.g., a 3G/4G network where there is in general less available QoS enabled traffic capacity) than when the device is connected to a wired network (e.g., a cable or DSL network where there is in general a higher level of QoS capacity available). In such embodiments, the device service processor and the service controller can coordinate to adapt the QoS service control policies and/or the QoS service charging policies to be different depending on which network the device is connected to. Similarly, the device QoS service control policy and/or QoS service charging policy can also be adapted based on whether the device is connected to a

home wireless network or a roaming wireless network. In some embodiments, a network capacity controlled service control policy and/or a network capacity controlled charging policy is adapted as a function of the type of network the device is connected to, as similarly described herein.

[00107] In some embodiments, various of the QoS related techniques and/or network capacity controlled services techniques described herein are performed on the device using DAS techniques and/or on the service controller in secure communication with a verified service processor executed on the device using DAS techniques. In some embodiments, various of the QoS related techniques and/or network capacity controlled services techniques described herein are performed by/in coordination/communication with one or more intermediate network elements/functions for assisting in various techniques (e.g., functions) for QoS techniques and/or network capacity controlled services techniques as described herein.

[00108] FIG. 1 illustrates a functional diagram of a network architecture for providing quality of service (QoS) for device assisted services (DAS) and/or for providing DAS for protecting network capacity in accordance with some embodiments. In some embodiments, QoS for DAS techniques described herein are implemented using the network architecture shown in FIG. 1. In some embodiments, DAS for protecting network capacity techniques described herein are implemented using the network architecture shown in FIG. 1.

[00109] 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 (e.g., via a firewall 124), 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, one or more of the devices 100 are in communication with other network element(s)/equipment that provides an access point, such as

a cable network head end, a DSL network DSLAM, a fiber network aggregation node, and/or a satellite network aggregation node. In some embodiments, each of the wireless devices 100 includes a service processor 115 (as shown) (e.g., executed on a processor of the wireless device 100), and each service processor connects through a secure control plane link to a service controller 122 (e.g., using encrypted communications).

[00110] In some embodiments, service usage information includes network based service usage information (e.g., network based service usage measures or charging data records (CDRs), which can, for example, be generated by service usage measurement apparatus in the network equipment), which is obtained from one or more network elements (e.g., BTS/BSCs 125, RAN Gateways (not shown), Transport Gateways (not shown), Mobile Wireless Center/HLRs 132, AAA 121, Service Usage History/CDR Aggregation, Mediation, Feed 118, or other network equipment). In some embodiments, service usage information includes micro-CDRs. In some embodiments, micro-CDRs are used for CDR mediation or reconciliation that provides for service usage accounting on any device activity that is desired. In some embodiments, each device activity that is desired to be associated with a billing event is assigned a micro-CDR transaction code, and the service processor 115 is programmed to account for that activity associated with that transaction code. In some embodiments, the service processor 115 periodically reports (e.g., during each heartbeat or based on any other periodic, push, and/or pull communication technique(s)) micro-CDR usage measures to, for example, the service controller 122 or some other network element. In some embodiments, the service controller 122 reformats the heartbeat micro-CDR usage information into a valid CDR format (e.g., a CDR format that is used and can be processed by an SGSN or GGSN or other network elements/equipment used/authorized for generating or processing CDRs) and then transmits it to a network element/function for CDR mediation (e.g., CDR Storage, Aggregation, Mediation, Feed 118).

[00111] In some embodiments, CDR mediation is used to account for the micro-CDR service usage information by depositing it into an appropriate service usage account and deducting it from the user device bulk service usage account. For example, this technique provides for a flexible service usage billing solution that uses pre-existing solutions, infrastructures, and/or techniques for CDR mediation and billing. For example, the billing system (e.g., billing system 123 or billing interface 127) processes the mediated CDR feed from CDR mediation, applies the appropriate account billing codes to the aggregated micro-CDR information that was generated by the device, and then generates billing events in a manner that does not require changes to the existing billing systems (e.g., using new transaction codes to label the new device assisted billing capabilities). In some embodiments, network provisioning system 160 provisions various network elements/functions for authorization in the network, such as to authorize certain network elements/functions (e.g., CDR storage, aggregation, mediation, feed 118 or other network elements/functions) for providing micro-CDRs, reformatted micro-CDRs, and/or aggregated or reconciled CDRs.

[00112] As shown in Figure 1, a CDR storage, aggregation, mediation, feed 118 is provided. In some embodiments, the CDR storage, aggregation, mediation, feed 118 receives, stores, aggregates and mediates micro-CDRs received from mobile devices 100. In some embodiments, the CDR storage, aggregation, mediation, feed 118 also provides a settlement platform using the mediated micro-CDRs, as described herein. In some embodiments, another network element provides the settlement platform using aggregated and/or mediated micro-CDRs (e.g., central billing interface 127 and/or another network element/function).

[00113] In some embodiments, various techniques for partitioning of device groups are used for partitioning the mobile devices 100 (e.g., allocating a subset of mobile devices 100 for a distributor, an OEM, a MVNO, and/or another partner or entity). As shown in Figure 1, a MVNO core network 210 includes a MVNO CDR storage, aggregation, mediation, feed 118, a MVNO

billing interface 122, and a MVNO billing system 123 (and other network elements as shown in Figure 1). In some embodiments, the MVNO CDR storage, aggregation, mediation, feed 118 receives, stores, aggregates and mediates micro-CDRs received from mobile devices 100 (e.g., MVNO group partitioned devices).

[00114] Those of ordinary skill in the art will appreciate that various other network architectures can be used for providing device group partitions and a settlement platform, and Figure 1 is illustrative of just one such example network architecture for which device group partitions and settlement platform techniques described herein can be provided.

[00115] In some embodiments, 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 apparatus/systems attached to one or more of the sub-networks shown in Figure 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 Figure 1, service usage 118 provides 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 Figure 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 and embodiments described herein by one of ordinary skill in the art. Also, as shown in Figure 1, the service controller 122 is in communication with the central billing interface 127 (e.g., sometimes referred to as the external billing management interface or billing communication interface), which is in communication with the central billing system 123. As shown in Figure 1, 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.

[00116] In some embodiments, a service processor download 170 is provided, which provides for periodical downloads/updates of service processors (e.g., service processor 115). In some embodiments, verification techniques include periodically updating, replacing, and/or updating an obfuscated version of the service processor, or performing any of these techniques in response to an indication of a potential compromise or tampering of any service processor functionality (e.g., QoS functionality and/or network capacity controlled services functionality) executed on or implemented on the device 100.

[00117] 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) collects device generated/assisted service

usage information (e.g., micro-CDRs) for one or more devices on the wireless network (e.g., devices 100); and provides the device generated service 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, as described herein, the CDR storage, aggregation, mediation, feed 118 collects/receives micro-CDRs for one or more devices on the wireless network (e.g., devices 100). In some embodiments, the CDR storage, aggregation, mediation, feed 118 (e.g., or other network elements and/or various 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 service usage information. In some embodiments, 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 (network based) CDRs and/or micro-CDRs for the one or more devices on the wireless network; applies a set of rules to the aggregated CDRs and/or micro-CDRs using a rules engine (e.g., bill by account, transactional billing, revenue sharing model, 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, a revenue sharing platform is provided using various techniques described herein. In some embodiments, QoS usage accounting/charging and/or network capacity controlled services usage accounting/charging is provided using various techniques described herein.

[00118] 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 (e.g., aggregated and mediated CDRs and/or micro-CDRs that are then translated into standard CDRs for a given wireless network) for the one or more devices on the wireless network to a billing interface (e.g., central billing interface 127) or a billing system (e.g., central billing system 123). 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 (e.g., service controller 122) to collect the device generated service usage information (e.g., micro-CDRs) 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 service usage information 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 transport gateway and/or a Radio Access Network (RAN) gateway to collect the network generated/based service usage information for the one or more devices on the wireless network. In some embodiments, the service controller 122 communicates the device assisted service usage information (e.g., micro-CDRs) to the CDR storage, aggregation, mediation, feed 118 (e.g., or other network elements and/or various combinations of network elements).

[00119] In some embodiments, the CDR storage, aggregation, mediation, feed 118 (e.g., or other network elements and/or various combinations of network elements) performs rules for performing a bill by account aggregation and mediation function. 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 service billing function, as described herein, and/or for performing a service/transactional revenue sharing function, as described herein. 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 assisted service usage information (e.g., micro-CDRs). In some embodiments, a rules engine device in communication with the CDR storage, aggregation, mediation, feed 118 (e.g., or other network elements and/or various combinations of network elements) performs a rules engine for aggregating and mediating the device assisted service usage information (e.g., QOS service usage information and/or network capacity controlled services usage information).

[00120] 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.

[00121] In some embodiments, a settlement platform service is provided. For example, micro-CDRs can be aggregated and mediated to associate service usage for one or more services used by a communications device (e.g., a user of the communications device). A rules engine or another function can determine a revenue share allocation for the service usage for a particular service to determine the settlement for such service usage for the revenue sharing allocation/model and to distribute accounting and settlement information to one or more of

carriers, distribution partners, MVNOs, wholesale partners, and/or other partners or entities. In some embodiments, the service is a transactional service.

[00122] 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., 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.

[00123] 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 assisted 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.

[00124] 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 assisted service usage information (e.g., micro-CDRs) includes a transaction type field or transaction code (e.g., indicating a type of service for the associated service usage information). For example, the rules engine can apply a rule or a set of rules based on the identified service associated with the device generated service 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).

[00125] 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).

[00126] In some embodiments, the service controller 122 sends the device generated CDRs to the rules engine (e.g., a service usage data store and rules engine, such as CDR storage, aggregation, mediation, feed 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 (e.g., by network provision system 160) and behaves substantially similar to other CDR generators on the network).

[00127] In some embodiments, the service controller 122 is provisioned as a new type of networking function that is recognized as a valid, authorized, and secure source for CDRs by

the other necessary elements in the network (e.g., CDR storage, aggregation, mediation, feed 118). In some embodiments, if the necessary network apparatus only recognize CDRs from certain types of networking equipment (e.g. a RAN gateway or transport gateway), then the service controller 122 provides authentication credentials to the other networking equipment that indicate that it is one of the approved types of equipment for 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.

[00128] 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 provides the device assisted service usage information (e.g., device based CDRs or micro-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), as it is not required to mediate network based CDRs and device assisted CDRs), and the device based service usage information is provided to the central billing interface 127 or the central billing system 123.

[00129] In some embodiments, the device based CDRs (e.g., micro-CDRs) and/or new CDRs generated based on execution of a rules engine as described herein are provided only for devices that are managed and/or based on device group, service plan, or any other criteria, categorization, and/or grouping, such as based on ambient service or ambient service provider or transactional service or transactional service provider.

[00130] In some embodiments, QoS for DAS includes a service processor (e.g., any device assisted element/function) that facilitates coordination for and/or provisions wireless access/radio access bearers (e.g., RABs). In some embodiments, the service processor determines whether a request for QoS is authorized (e.g., according to QoS service level, user standing, available local network capacity (e.g., as reported by other device(s) and/or network)).

In some embodiments, device QoS capacity demand reports provide and/or augment network capacity demand reports.

[00131] In some embodiments, QoS for DAS includes a service controller (e.g., any network device based service control element/function) that facilitates coordination for and/or provisions wireless access/radio access bearers (e.g., RABs) on a device (e.g., a communications device, such as a mobile wireless communications device and/or an intermediate networking device), on network, and/or on device plus network. In some embodiments, the service controller provides device QoS capacity demand reports to other network equipment/elements/functions, and then also provisions the RAB channel based on various criteria and determinations.

[00132] In some embodiments, QoS for DAS provides for device assisted monitoring, information, and/or functionality to facilitate QoS without and/or to assist network based monitoring, information, and/or functionality (e.g., Deep Packet Inspection (DPI) and/or provides such monitoring, information, and/or functionality that may not be available via network based monitoring, information, and/or functionality (e.g., encrypted activities on the device may not be accessible by DPI or other network based techniques). For example, QoS for DAS can assist in the QoS setup to facilitate the QoS setup and provide such information that may not otherwise be available using network based only techniques. For example, device assisted activity and/or service monitoring techniques can assist in classifying the QoS for the monitored activity and/or service using, for example, a QoS activity map (e.g., as described herein or other similar techniques). For example, using such device assisted techniques eliminates and/or minimizes DPI or other network based techniques that can give rise to privacy concerns/issues, network neutrality concerns/issues, and/or otherwise may not be able to provide similar or equivalent granular service/activity monitoring, as discussed above, and/or also off loads such processing from the network (e.g., network elements/devices/functionality) to the communications devices (e.g., at least for such communications devices that can perform such functions, based on their

processing and/or memory capabilities, as would be apparent to one of ordinary skill in the art). In some embodiments, QoS for DAS includes the service provider for providing an initial authorization/clearance for a QoS request (e.g., using various techniques described herein), and the service controller determines if the QoS request should be authorized (e.g., based on various QoS authorization/clearance/approval criteria (e.g., QoS activity maps and/or QoS request rule) and/or network capacity, as described herein). In some embodiments, QoS for DAS includes the service provider for providing a QoS request including a QoS class to the service controller, and the service controller determines if the QoS request should be authorized, as described herein. In some embodiments, DAS for protecting network capacity provides for device assisted monitoring, information, and/or functionality to facilitate protecting network capacity without and/or to assist network based monitoring, information, and/or functionality (e.g., Deep Packet Inspection (DPI) and/or provides such monitoring, information, and/or functionality that may not be available via network based monitoring, information, and/or functionality (e.g., encrypted activities on the device may not be accessible by DPI or other network based techniques). In some embodiments, DAS for protecting network capacity provides for device assisted monitoring, information, and/or functionality to facilitate protecting network capacity without solely relying upon DPI and/or without any use or any significant use of DPI wireless network, which conserves network resources and network capacity by controlling device network access behavior at the device instead of deep in the core network at a DPI gateway (e.g., DPI based techniques consume over the air wireless network capacity even if chatty device behavior is blocked at a DPI gateway, in contrast, DAS for protecting network capacity techniques that do not use DPI based techniques for controlling device service usage can, for example, providing a device based usage notification and service selection UI that does not consume over the air wireless network capacity).

[00133] In some embodiments, QoS for DAS and/or DAS for protecting network capacity includes providing or facilitating reports for base station (BTS) for network capacity (e.g., sector, channel, busy state information or network capacity usage/availability, and/or network capacity expected demand) based on, for example, one or more of the following: monitored application usage on the communications device, monitored user activity on the communications device, location of the communications, other available networks, and/or other monitored or determined activity, service usage measure, and/or metric. In some embodiments, at or after execution of an application that is determined to require network service usage (e.g., may require increased wireless network bandwidth, such as based on a service usage activity map), QoS for DAS sends information to the network (e.g., a network controller or other network device element/function) that capacity demand is forthcoming for the communications device (e.g., potentially initiating a provisioning of a QoS radio access bearer (RAB) or other type of RAB).

[00134] In some embodiments, network capacity (e.g., busy state information) is collected from one or more communications devices in communication with a wireless network (e.g., network capacity/usage information measured from each respective communications device's perspective is determined and stored by the service processor on each respective communications device) and reported to the service controller, and the service controller (e.g., or another network element/function) uses this information to determine what resources are available for allocation to various levels of QoS (e.g., to respond to/facilitate various QoS requests) and/or to workload balance across multiple base stations and/or networks (e.g., wired networks, cellular, Wi-Fi, and/or other wireless networks).

[00135] In some embodiments, the service processor executed on the communications device sends a QoS request (e.g., a wireless network bearer channel reservation request or Radio Access Bearer (RAB) request) to the service controller. The service controller verifies the request using various verification techniques as described herein. In some embodiments, the

service controller facilitates coordination of various device QoS requests with one or more base stations (BTSs) in communication with the communications device to provide for the requested QoS reservation to facilitate the new QoS session. In some embodiments, the service controller provides a QoS routing function by, for example, providing various QoS routing instructions to a device service processor (e.g., aggregating, prioritizing, queuing, authorizing, allocating reservations/RABs, denying, re-routing (such as to other BTSs and/or other networks) and/or otherwise managing QoS requests), in which the BTS may or may not be QoS aware. For example, QoS priority can be based on activity (e.g., service usage and/or application), service level, user standing, network capacity, time of day, and/or QoS priority can be purchased on a transaction basis, a session basis, a pre-pay basis or a plan basis. As another example, QoS priority can also vary by device type, user within a group, group, application type, content type, or any other criteria or measure and/or any combination thereof. In some embodiments, the service controller also facilitates coordination of various device QoS requests with other network elements/functions for QoS implementation and management to provide for an end to end QoS solution.

[00136] In some embodiments, QoS can be symmetric for two mobile devices or asymmetric. In some embodiments, QoS resource availability can be from communications devices, BTS(s), other network functions (e.g., service control, service controller and/or any other network elements/functions) or any combination thereof. In some embodiments, the service controller provides QoS demand information to another network element/function. In some embodiments, the service controller provides the central aggregator and policy decision point (PDP). In some embodiments, the service controller controls (e.g., at least in part) QoS related functions for communications devices, BTS(s), and/or a combination of both.

[00137] In some embodiments, charging (e.g., monitoring and/or determining associating charging or billing) for QoS service usage/transactions and/or network capacity controlled

services usage/transactions is determined using various techniques described herein. For example, the service processor can assist in charging for QoS and/or network capacity controlled activities. In some embodiments, the service processor uses device assisted Charging Data Records (CDRs) or micro-CDRs to assist in charging for QoS and/or network capacity controlled activities (e.g., using QoS class related transaction codes and/or network capacity controlled related transaction codes), as described herein with respect to various embodiments. In some embodiments, charging for QoS and/or network capacity controlled services is performed in whole or in part by one or more network elements/functions (e.g., service controller, SGSN/GGSN/other gateways, and/or billing interfaces/servers).

[00138] In some embodiments, service usage information includes network based service usage information. In some embodiments, the network based service usage information includes network based CDRs. In some embodiments, service usage information includes device based service usage information. In some embodiments, device based service usage information includes device assisted CDRs, also referred to herein as micro-CDRs, as described herein. In some embodiments, micro-CDRs are used for CDR mediation or reconciliation that provides for service usage accounting on any device activity that is desired (e.g., providing granular service usage information, such as based on application layer service usage monitoring, transaction service usage monitoring, QoS activities/sessions/transactions, network capacity controlled activities/sessions/transactions, and/or other types of service usage information). In some embodiments, each device includes a service processor (e.g., a service processor executed on a processor of a communications device, such as a mobile device or an intermediate networking device that can communicate with a wireless network).

[00139] In some embodiments, each device activity that is desired to be associated with a billing event (e.g., for a QoS related billing event) is assigned a micro-CDR transaction code, and the service processor is programmed to account for that activity associated with that

transaction code (e.g., various transaction codes can be associated with service usage associated with certain services, applications, and/or based on QoS classes or priorities, respectively, which can be used for providing granular service usage for these various Internet/network based services/sites/transactions and/or any other Internet/network based services/sites, which can include transactional based services). For example, using these techniques, as described herein, essentially any type of device activity (e.g., including QoS classes and prioritization and/or network capacity controlled classes and prioritization) can be individually accounted for and/or controlled (e.g., throttled, restricted, and/or otherwise controlled as desired). In some embodiments, the service processor periodically reports (e.g., during each heartbeat or based on any other periodic, push, and/or pull communication technique(s)) micro-CDR usage measures to, for example, a service controller or some other network element/function. In some embodiments, the service controller reformats the heartbeat micro-CDR usage information into a valid CDR format (e.g., a CDR format that is used and can be processed by an SGSN or GGSN or some other authorized network element/function for CDRs) and then transmits the reformatted micro-CDRs to a network element/function for performing CDR mediation.

[00140] In some embodiments, CDR mediation is used to properly account for the micro-CDR service usage information by depositing it into an appropriate service usage account and deducting it from the user device bulk service usage account. For example, this technique provides for a flexible service usage billing solution that uses pre-existing solutions for CDR mediation and billing. For example, the billing system can process the mediated CDR feed from CDR mediation, apply the appropriate account billing codes to the aggregated micro-CDR information that was generated by the device, and then generate billing events in a manner that does not require changes to existing billing systems, infrastructures, and techniques (e.g., using new transaction codes to label the new device assisted billing capabilities).

[00141] In some embodiments, the various QoS techniques performed on or by the communications device (e.g., using a service processor to provide or assist in providing QoS session provisioning, QoS policy management, QoS policy enforcement, and/or QoS accounting/charging, such as QoS charging records and reports) are verified (e.g., using various verification techniques described herein). In some embodiments, the various network capacity controlled services techniques performed on or by the communications device (e.g., using a service processor to provide or assist in providing network capacity controlled services policy management, network capacity controlled services policy enforcement, and/or network capacity controlled services charging, such as network capacity controlled services charging records and reports) are verified (e.g., using various verification techniques described herein).

[00142] For example, a QoS request, QoS related policy rules (e.g., QoS activity map, QoS related service plan and/or service policy settings) and implementation, QoS policy enforcement, and QoS charging are verified (e.g., periodically, per transaction, and/or based on some other criteria/metric). In some embodiments, verification techniques include one or more of the following: compare a network based service usage measure with a first service policy associated with the communications device, compare a device assisted service usage measure with the first service policy, compare the network based service usage measure to the device assisted service usage measure, perform a test and confirm a device assisted service usage measure based on the test, perform a User Interface (UI) notification (e.g., which can include a user authentication, password, question/answer challenge, and/or other authentication technique), and/or other similar verification techniques as will now be apparent to one of ordinary skill in the art. Accordingly, in some embodiments, QoS for DAS "closes the loop" for verification of various QoS related techniques, such as QoS requests, QoS grants, QoS usage, and/or QoS charging. In some embodiments, the service processor and the service controller serve as a verifiable QoS management/coordination system for other QoS elements/functions in

network. In some embodiments, if such or other verification techniques determine or assist in determining that a QoS request, QoS report, and/or QoS policy behavior (e.g., or similarly, network capacity controlled services monitoring, reporting, and/or policy behavior) does not match expected requests, reports, and/or policy, then responsive actions can be performed, for example, the communications device (e.g., and/or suspect services) can be suspended, quarantined, killed/terminated, and/or flagged for further analysis/scrutiny to determine whether the device is malfunctioning, needs updating, has been tampered with or compromised, is infected with malware, and/or if any other problem exists.

[00143] In some embodiments, the communications device (e.g., the service processor) maintains a QoS flow table that associates or maps device activity to QoS level/class to RAB/QoS channel, and in some embodiments, the communications device also informs a QoS management network function/element of the relative priority of the QoS flows for the communications device (e.g., based on or using the QoS flow table). In some embodiments, the service controller receives or collects information from the communications device and maintains such a QoS flow table for the communications device and, in some embodiments, the service controller also informs a QoS management network function/element of the relative priority of the QoS flows for the communications device (e.g., based on or using the QoS flow table). In some embodiments, flows can be assigned to activities originating at the communications device in a transparent way, or simply by activity class or user preference, or using other techniques.

[00144] In some embodiments, the communications device maintains a table of QoS billing rates, scheduled transmission times, and/other QoS related information to implement an overlay MAC at the data networking level to manage QoS on legacy networks that are not QoS MAC enabled and/or do not have the various functionality to support QoS controls (e.g., and such techniques can also be used to provide for QoS functionality across different networks). In

some embodiments, QoS related policies are exchanged between roaming and home service controllers to facilitate QoS support while roaming on a non-home network(s).

[00145] In some embodiments, the communications device serves as a network capacity indicator (e.g., collecting network capacity information for a local cell and communicating or reporting that network capacity information to the service controller). For example, permanent local cell communications devices can be placed in local cell areas to augment legacy equipment for such network capacity indicator/reporting functions. Various other techniques for determining network capacity and/or network availability are described herein.

[00146] In some embodiments, service partners and/or service providers can subsidize in whole or in part to upgrade a given user or group of users to better QoS related service level agreement(SLA)/class for a preferred destination. In some embodiments, based on monitored service usage and/or other monitored behavior of the communications device, such subsidized QoS upgrade/offers can be presented to a user of the communications device (e.g., as an incentive/reward for desired or preferred user behavior or for other reasons). Similarly, in some embodiments, these techniques are also applied to network capacity controlled services.

[00147] In some embodiments, QoS charging is based on QoS channel/reservation, service flow, or RAB charging (e.g., single flow per RAB, multi-flow per RAB, multi-RAB per flow). In some embodiments, charging (e.g., for QoS and/or for network capacity controlled services) is based on one or more of the following: network busy state, time criteria, user service class request, traffic volume and class, time and class, network capacity (e.g., network busy state) and class, time of day and class, location, traffic type, application type, application class, destination, destination type, partner service, and/or other criteria/measures. In some embodiments, QoS charging is verified using the various verification techniques described herein (e.g., test charging events). In some embodiments, network capacity controlled services charging is verified using the various verification techniques described herein (e.g., test

charging events). In some embodiments, QoS charging is by data usage (e.g., by Megabyte (MB)), service flow by time by QoS class, speed by time, network busy state, time of day/day of week, service plan, current network, and/or other criteria/measures. In some embodiments, network capacity controlled services charging is by data usage (e.g., by Megabyte (MB)), service flow by time by network capacity controlled services class, speed by time, network busy state, time of day/day of week, service plan, current network, and/or other criteria/measures.

[00148] In some embodiments, QoS for DAS includes coordinating functions with one or more of the following: DAS elements/functions, Radio Access Network (RAN), Transport network, Core network, GRX network, IPX network, and/or other networks/elements/functions.

[00149] Figure 2 illustrates another functional diagram of another network architecture for providing quality of service (QoS) for device assisted services (DAS) and/or for providing DAS for protecting network capacity in accordance with some embodiments. In some embodiments, QoS for DAS techniques described herein are implemented using the network architecture shown in Figure 2. In some embodiments, DAS for protecting network capacity techniques described herein are implemented using the network architecture shown in Figure 2.

[00150] As shown, Figure 2 includes various devices 100 including service processors 115. For example, devices 100 can include various types of mobile devices, such as phones, PDAs, computing devices, laptops, net books, tablets, cameras, music/media players, GPS devices, networked appliances, and any other networked device; and/or devices 100 can include various types of intermediate networking devices, as described herein. The devices 100 are in communication with service control 210 and central provider access and core networks 220. Service policies and accounting functions 230 are also provided in communication with the central provider access and core networks 220. For example, devices 100 can communicate via the central provider access and core networks 220 to the Internet 120 for access to various

Internet sites/services 240 (e.g., Google sites/services, Yahoo sites/services, Blackberry services, Apple iTunes and AppStore, Amazon.com, FaceBook, and/or any other Internet service or other network facilitated service).

[00151] In some embodiments, Figure 2 provides a wireless network architecture that supports various DAS for protecting network capacity techniques as described herein. Those of ordinary skill in the art will appreciate that various other network architectures can be used for providing various DAS for protecting network capacity techniques as described herein, and Figure 2 is illustrative of just another such example network architecture for which DAS for protecting network capacity techniques as described herein can be provided.

[00152] Figure 3 illustrates another functional diagram of an architecture 300 including a device based service processor 115 and a service controller 122 for providing quality of service (QoS) for device assisted services (DAS) and/or for providing DAS for protecting network capacity in accordance with some embodiments. In some embodiments, QoS for DAS techniques described herein are implemented using the functions/elements shown in Figure 3. In some embodiments, DAS for protecting network capacity techniques described herein are implemented using the functions/elements shown in Figure 3.

[00153] For example, the architecture 300 provides a relatively full featured device based service processor implementation and service controller implementation. As shown, this corresponds to a networking configuration in which the service controller 122 is connected to the Internet 120 and not directly to the access network 1610. As shown, a data plane (e.g., service traffic plane) communication path is shown in solid line connections and control plane (e.g., service control plane) communication path is shown in dashed line connections. As will be apparent to one of ordinary skill in the art, 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 Figure 3 are described below with respect to, for example, Figures 4, 12, and 13 as well as Figures 5 through 11 (e.g., QoS for DAS related embodiments) and Figures 14 through 23 (e.g., DAS for protecting network capacity related embodiments).

[00154] As shown in Figure 3, 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.

[00155] As shown in Figure 3, 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 Figure 3, 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.

[00156] In some embodiments, the service control server link 1638 provides for securing, signing, encrypting and/or otherwise protecting the communications before sending such communications over the service control link 1653. For example, the service control server link 1638 can send to the transport layer or directly to the link layer for transmission. In another example, the service control server link 1638 further secures the communications with transport layer encryption, such as TCP TLS or another secure transport layer protocol. As another example, the service control server link 1638 can encrypt at the link layer, such as using IPSEC, various possible VPN services, other forms of IP layer encryption and/or another link layer encryption technique.

[00157] As shown in Figure 3, the service controller 122 includes an access control integrity server 1654 (e.g., service policy security server). 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 (e.g., QoS policy violation and/or a network capacity controlled services policy violation) or a system integrity breach is suspected.

[00158] 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 (e.g., service policy security agent) reports and error conditions. Many of the access control integrity agent 1654 checks can be accomplished by the server. For example, the access control integrity agent 1654 checks include one or more of the following: service usage measure against usage range consistent with policies (e.g., usage measure from the network and/or from the device); configuration of agents; operation of the agents; and/or dynamic agent download.

[00159] 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 (e.g., a QoS policy and/or a network capacity controlled services policy). For example, device service policy implementations can include measuring total QoS data passed, QoS 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.

[00160] In some embodiments, the access control integrity server 1654 (e.g., and/or some other agent of service controller 122) verifies device service policy, and the verification error conditions that can indicate a mismatch in QoS service measure and QoS 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 QoS 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 (e.g., a QoS policy and/or a network capacity controlled services policy).

[00161] As shown in Figure 3, service controller 122 includes a service history server 1650 (e.g., charging server). 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 (e.g., CDR feed and CDR mediation). 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.

[00162] As shown in Figure 3, service controller 122 includes a policy management server 1652 (e.g., policy decision point (PDP) server) for managing service usage policies, such as QoS policies and/or a network capacity controlled services policies. 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.

[00163] 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 the 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, and/or other sensitive information) 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, and/or otherwise obtains a measure of network availability/capacity and adjusts traffic shaping policy and/or other policy settings based on available network availability/capacity (e.g., a network busy state).

[00164] As shown in Figure 3, 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 some embodiments, the network traffic analysis server 1656 estimates the service quality and/or service usage for the network under variable settings on potential service policies. In some 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. In some embodiments, the network traffic analysis server 1656 estimates the network availability/capacity for the network under variable settings on potential service policies. In some embodiments, the network traffic analysis server 1656 identifies actual or potential service behaviors by one or more devices that are impacting and/or causing problems for overall network availability/capacity.

[00165] As shown in Figure 3, Service Analysis, Test & Download 122B includes a beta test server 1658 (e.g., policy creation point and beta test server). 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, such as for protecting network capacity.

[00166] As shown in Figure 3, service controller 122 includes a service download control server 1660 (e.g., a service software download control server). In some embodiments, the service download control server 1660 provides a download function to install and/or update service software elements (e.g., the service processor 115 and/or agents/components of the service processor 115) on the device, as described herein.

[00167] As shown in Figure 3 service controller 122 includes a billing event server 1662 (e.g., micro-CDR server). 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.

[00168] As shown in Figure 3, the Access Network HLR 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 the device service history 1618).

[00169] As shown in Figure 3, 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 (e.g., to verify service usage charging). In some embodiments, the device service history 1618 is used to synchronize and/or verify the local service usage counter (e.g., to verify service usage accounting).

[00170] As shown in Figure 3, the central billing 1619 (e.g., central provider billing server) 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.

[00171] As shown in Figure 3, in some embodiments, modem selection and control 1811 (e.g., in communication with connection manager 1804 as shown) 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 (e.g., 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 (e.g., potentially for higher service payments) than other users). As another example, ambient services (e.g., as similarly described herein) can be provided for the hotspot for verified service processors.

[00172] 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 (e.g., or 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.

[00173] As shown in Figure 3, 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 Figure 3, 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.

[00174] As shown in Figure 3, service processor 115 includes an API and OS stack interface 1693. In some embodiments, the API and OS stack interface 1693 provides the QoS API functionality as similarly described herein with respect to various embodiments. In some embodiments, a QoS API is used to report back QoS availability to applications. In some embodiments, the API and OS stack interface 1693 provides the network capacity controlled API and/or emulated API functionality as similarly described herein with respect to various embodiments. As shown, service processor 115 also includes a router 1698 (e.g., a QoS router agent/function and/or a network capacity controlled services router agent/function) and a policy decision point (PDP) agent 1692. In some embodiments, the router 1698 provides QoS router functionality as similarly described herein with respect to various embodiments. In some embodiments, the router 1698 provides network capacity controlled services router functionality as similarly described herein with respect to various embodiments. In some embodiments, the QoS router supports multiple QoS channels (e.g., one or more provisioned/allocated QoS links forming a QoS channel between the device and the desired end point, such as an access

point/BTS/gateway/network for a single ended QoS channel or other communication device for an end to end QoS channel, depending on the QoS connection/network support/availability/etc.). In some embodiments, the QoS router supports multiple QoS channels, which can each have different QoS classes/levels. In some embodiments, the QoS router routes application/service usage traffic to an appropriate QoS channel. In some embodiments, the QoS router determines the routing/mapping based on, for example, one or more of the following: a QoS API request, a QoS activity map, a user request, a service plan, a service profile, service policy settings, network capacity, service controller or other intermediate QoS network element/function/device, and/or any other criteria/measure, as similarly described herein with respect to various embodiments. In some embodiments, multiple different applications/services are routed to a particular QoS channel using various techniques described herein. In some embodiments, different applications/services are routed to different QoS channels using various techniques described herein. In some embodiments, the QoS router assists in managing and/or optimizing QoS usage for the communications device. In some embodiments, the QoS router assists in managing and/or optimizing QoS usage across multiple communications devices (e.g., based on network capacity for a given cell area/base station or other access point). In some embodiments, PDP agent 1692 provides the PDP agent functionality as similarly described herein with respect to various embodiments. As shown, architecture 300 also includes a suspend resume interface 320, network QoS provisioning interfaces 330 (e.g., for providing the various QoS techniques described herein), and an activation/suspend resume server 340 and billing interface server 350 in the service controller 122A.

[00175] 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 (e.g., charging agent), 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 (not shown), 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 socket (such as by IP address, protocol, and/or port), by socket id (such as port address/number), by port number, by content type, by application or application type, and/or any other service usage activity classification/categorization) with associated IP addresses and/or other criteria/measures. 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 for providing QoS for DAS and/or for providing DAS for protecting network capacity. 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, and/or any of the various other DAS related techniques as described herein with respect to various embodiments.

[00176] 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 (e.g., 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 (e.g., 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 (e.g., security credentials). In some embodiments, the ability to load at least a portion of service processor 115 software into protected non-volatile memory also requires a secure key and/or signature and/or requires that the service processor 115 software

components being loaded into non-volatile memory are also securely encrypted and appropriately signed by an authority that is trusted by a secure software downloader function, such as service downloader 1663 as shown in Figure 3. 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.

[00177] Figures 4A through 4C illustrates a functional diagram for providing quality of service (QoS) for device assisted services (DAS) in accordance with some embodiments. In some embodiments, QoS for DAS techniques described herein are implemented using the network architecture shown in Figures 4A through 4C.

[00178] Referring to Figure 4A, in some embodiments, QoS functionality is performed at the communications device 100 using service processor 115 as similarly described herein. For example, the service processor 115 determines whether or not a QoS request is authorized (e.g., based on the associated service plan and/or other criteria/measures). If the QoS request is authorized, then the service processor 115 communicates with the base station (BTS) 125 to send the QoS request (e.g., a RAB or multi-RAB reservation request) to the local BTS. The BTS determines whether to accept or deny the QoS request (e.g., based on network capacity, such as using a first come first service QoS/network bandwidth or best effort access policy or other techniques, and/or other criteria/measures). The BTS responds to the QoS request accordingly. If the QoS request is granted, the QoS session can be initiated as similarly described herein. In some embodiments, the service processor 115 also performs various QoS charging functions using various techniques described herein, and the service processor 115 periodically sends QoS charging records or reports to the service controller 122 (e.g., and/or another network element/function). In some embodiments, the service processor 115 and the

QoS related functions performed by the service processor 115 are periodically verified using the various techniques described herein.

[00179] Referring to Figure 4B, Figure 4B is similar to Figure 4A except that the service controller 122 is also shown to be in communication with the service processor 115 of the communications device 100, which can provide for the download and periodically updating of the QoS rules and/or other service plan/profile/policy information that can include QoS related information. In some embodiments, the service processor 115 also performs various QoS charging functions using various techniques described herein, and the service processor 115 periodically sends QoS charging records or reports to the service controller 122 (e.g., and/or another network element/function). In some embodiments, the service processor 115 and the QoS related functions performed by the service processor 115 are periodically verified using the various techniques described herein.

[00180] Referring to Figure 4C, at 410, the service processor 115 sends a QoS request to the service controller 122 (e.g., the service processor can also (at least in part) determine whether the QoS request is authorized as similarly described with respect to Figure 4A). At 420, the service controller 122 sends the QoS request to the BTS 125 if it is determined that the QoS request is authorized using various techniques described herein and/or whether the BTS 125 has network capacity for the QoS request. For example, the service controller can provide a central policy decision point function for QoS related activities (e.g., based on QoS prioritization, network capacity, and/or other criteria/measures/policies). At 430, the service controller 122 communicates the response to the QoS request accordingly. At 440, if the QoS request was approved, the device 100 initiates the QoS session (e.g., using a RAB or multi-RAB reservation) via the BTS 125. In some embodiments, the service processor 115 also performs various QoS charging functions using various techniques described herein, and the service processor 115 periodically sends QoS charging records or reports to the service controller 122 (e.g., and/or

another network element/function). In some embodiments, the service processor 115 and the QoS related functions performed by the service processor 115 are periodically verified using the various techniques described herein.

[00181] In some embodiments, QoS techniques as described herein are implemented in the device (e.g., using the service processor 115) and one or more other network elements/functions, such as the BTS 125, service controller 125, RAN, SGSN/GGSN/other gateways and/or other network elements/functions, in which various of the QoS related functions can be distributed or allocated to such network elements/functions based on various design/network architecture approaches as will now be apparent to one of ordinary skill in the art, in which QoS related activities and/or functions at the device 100 are verified using various verification techniques described herein.

[00182] In some embodiments, the device determines QoS availability by directly querying QoS link reservation equipment in the network (e.g., an access point, such as the BTS 125). In some embodiments, the device determines QoS availability based on an intermediate network function that coordinates QoS requests with one or more network QoS link resources. In some embodiments, the device requests a QoS reservation in advance of QoS link establishment with one or more QoS network link resources. In some embodiments, in response to a QoS request, a QoS channel is reported as available only if/after it is determined that the necessary one or more QoS links required to create the QoS channel are available, and, for example, the QoS channel can then be reserved based on a confirmation or automatically be reserved in response to the QoS request.

[00183] Figure 5 illustrates a functional diagram for generating a QoS activity map for quality of service (QoS) for device assisted services (DAS) in accordance with some embodiments. In particular, Figure 5 illustrates techniques for mapping a service plan or a set of service plan policies/rules for QoS 510 to a set of QoS activity rules 530. As shown, a set of QoS rules/QoS

related device state information 510 (e.g., a set of associated service plan, service plan usage, other state such as network capacity or forecasted demand or time of day/day of week, activity usage, QoS level, and/or user preferences) is mapped using a QoS mapping function to a set of QoS activity rules 530 using various techniques described herein. At 530, activity rules (e.g., activity policy rules instructions) 530 are determined using the mapping function 520. In some embodiments, DAS for network capacity controlled services techniques can similarly be implemented using the techniques described with respect to Figure 5 (e.g., for generating and implementing a network capacity controlled services activity map).

[00184] In some embodiments, the service plan includes a list of activity policies, and each activity policy in the service plan specifies how the activity policy is modified by rules state information. In some embodiments, each activity policy then becomes the instruction for the engine (e.g., QoS mapping function 520) that maps the activity policy to QoS activity rules 530. In some embodiments, service controller 122 downloads QoS mapping function 520, which is implemented by service processor 115.

[00185] In some embodiments, the service processor determines (e.g., and classifies) application/service usage activity demand with or without granular application/service usage activity (e.g., depending on various user/service plan/service provider/network/legal and/or other privacy restrictions and/or any other related requirements or settings). For example, policies (e.g., service policy settings and/or service profile settings) can be downloaded to provide such application/service usage activity monitoring rules and a QoS activity map for assigning such monitored activities to various QoS classes or priorities, and, in some embodiments, such monitoring and the QoS activity map can also be implemented using various verification techniques described herein (e.g., periodically audited, tested, compared with network service usage information). In some embodiments, the QoS activity map is based on a service plan, service profile, and/or service policy settings associated with the communications device. In

some embodiments, the QoS activity map is based on a device group and/or user group. In some embodiments, the QoS activity map is based on user input (e.g., a user of the communications device can identify QoS classes/service levels for various applications and/or service activities, in response to requests for user input, based on user configurations, user defined rules (e.g., to eliminate or mitigate privacy and/or net neutrality concerns/issues), and/or confirmed monitored user behavior QoS related patterns or preferences). In some embodiments, the QoS activity map includes mappings/associations based on one or more of the following: a user preference for a given destination, destination class, application, application class (e.g., by application class instead of with respect to a specific application can also eliminate or mitigate privacy and/or net neutrality concerns/issues), flow, traffic or flow class, time period, time of day, location, network busy state (e.g., provide QoS when you can, then charge more when busy, notify user of busy state), device type, user type, user plan, user group, user standing, partner service, tokens, service type, and/or other criteria or measures.

[00186] In some embodiments, various techniques described herein are managed for device 100 for incoming and/or outgoing QoS requests. In some embodiments, as shown in Figure 6, QoS for DAS includes establishing an end to end coordinated QoS service channel control.

[00187] Figure 6 illustrates a functional diagram for quality of service (QoS) for device assisted services for an end to end coordinated QoS service channel control in accordance with some embodiments. As shown in Figure 6, a wireless communications device 100A includes a service processor 115A in secure communication with service controller 122A. A wireless communications device 100B includes a service processor 115B in secure communication with service controller 122B. In some embodiments, when, for example, device 100A initiates a QoS request for a QoS class session in communication with device 100B (e.g., a VOIP call or another application service requiring or possibly using a QoS class/level session, such as a conversational or other QoS type of class/level), as sequence of actions are performed using

service controller 122A and service controller 122B to facilitate/setup an end to end coordinated QoS service channel control. In some embodiments, as similarly described herein, assuming that service processor 115A and service controller 122A determine that the QoS request from device 100A is authorized for that device, then the service controller 122A contacts registry 650 (e.g., a device registry, such as an HLR, mobile services center, or other central database or registry including, for example, service controller mappings by device/IP address/other) to determine the service controller associated with/responsible for managing QoS/service control for device 100B. The registry 650 provides the service controller 122B information (e.g., IP address/other address) based on this lookup determination. In some embodiments, service controller 122A then initiates the QoS request with service controller 122B to determine if the device 100B is authorized and/or available for the QoS session requested by device 100A. In some embodiments, service controllers 122A/B communicate with BTSs 125A/B to determine whether the QoS request can be facilitated (e.g., based on network capacity) as similarly described herein. In some embodiments, the service controllers 122A and 122B provide the central QoS coordination function and can request appropriate QoS channels directly from the respective local BTSs. In some embodiments, the service controllers 122A and 122B also communicate with one or more of the following network elements/functions as shown in Figure 6 in order to facilitate an end to end coordinated QoS service channel control: RAN 610/670, Core Network 620/660, and IPX network 630. In some embodiments, service controllers 122A and 122B communicate with various necessary network elements for provisioning to facilitate session provisioning through the carrier core network as similarly discussed above. In some embodiments, service controllers 122A and 122B communicate with various necessary network elements for provisioning to facilitate session provisioning through the IPX network as similarly discussed above. As will be apparent to one of ordinary skill in the art, QoS for DAS techniques as described herein can be similarly implemented using these or similar techniques to various other network architectures.

[00188] Figure 7 illustrates a flow diagram for quality of service (QoS) for device assisted services (DAS) in accordance with some embodiments. At 702, the process begins. At 704, QoS rules are received or determined (e.g., a service processor receives or requests the QoS rules, which may be included in service plan, service profile, and/or service policy settings associated with the communications device). In some embodiments, the QoS rules are verified using various techniques as described herein (e.g., periodically updated, replaced, downloaded, obfuscated, and/or tested using by a service controller and/or using other verification techniques). In some embodiments, a QoS API is also used by various applications to initiate a QoS request, as described herein with respect to various embodiments. In some embodiments, the QoS rules are implemented in the form of a QoS activity map in accordance with various embodiments described herein. At 706, the communications device's standing for QoS is determined using various techniques described herein (e.g., based on the service plan, service profile, service policy settings, QoS rules, based on QoS class, current service usage, current billing standing, and/or any other criteria/measure). In some embodiments, in addition to verifying the device/user standing for the QoS request, whether the device is following or in compliance with an assigned QoS reservation request policy is also verified using various techniques described herein. If the device is determined to not be eligible for QoS, then at 708, the device User Interface (UI) provides information concerning the denial/ineligibility for QoS session(s) (e.g., denial/ineligibility explanation and/or options for providing for one or more QoS options, such as a service plan upgrade or payment for a certain/set of/period of time for QoS session(s) access). If the device is determined to be eligible for QoS, then at 710, QoS availability is determined (e.g., based on network capacity, which may be determined at the device, via communication with the service controller, via communication with the BTS, and/or any combination thereof, using the various techniques described herein). If QoS is determined to not be available, then at 712, the UI provides information and/or options concerning the QoS availability (e.g., unavailability explanation and/or options for providing for one or more QoS

options, such as a service plan upgrade or payment for a certain/set of/period of time for QoS session(s) access). If QoS is determined to be available, then at 714, a request for network resources for the QoS session is sent to one or more network resources (e.g., service controller, BTS, gateway, core/transport network, IPX/GRX networks, and/or other network elements/functions/resources). At 716, a confirmation of the approved QoS session is received to close the loop for the QoS for DAS (e.g., a QoS schedule is received that provides the QoS session confirmation information, such as a scheduled RAB/multi-RAB and/or other reserved network resource(s) by schedule/other criteria). At 718, one or more verification techniques are performed to verify the QoS for DAS implementation on the device using various verification techniques described herein (e.g., comparing QoS service usage reports from a network source with the associated device policy; comparing QoS service usage reports from a network source with the QoS service usage reports from the device, and/or using other verification techniques as similarly described herein). At 720, the process is completed.

[00189] Figures 8A through 8C each illustrate another flow diagram for quality of service (QoS) for device assisted services (DAS) in accordance with some embodiments. Figure 8A illustrates another flow diagram for quality of service (QoS) for device assisted services (DAS) in accordance with some embodiments. At 802, the process begins. In some embodiments, the QoS policies are implemented on the device (e.g., service processor collects/receives an associated service plan that defines/specifies basic policies for QoS, which can include a QoS activity map, which, for example, maps QoS classes based on application, service usage, flow type, destination, time of day, network capacity, and/or other criteria/measures, as similarly described herein). In some embodiments, a QoS API is also used by various applications to initiate a QoS request, as described herein with respect to various embodiments. In some embodiments, the QoS rules are implemented in the form of a verified QoS activity map in accordance with various embodiments described herein. At 804, a QoS request is determined

(e.g., by QoS class for a particular associated service/application). In some embodiments, the QoS request is determined at least in part by using the QoS activity map using various techniques described herein, for example, based on service/application usage monitoring on the device (e.g., by the service processor service usage monitoring agent). In some embodiments, the QoS request is determined based on the QoS API. In some embodiments, the QoS request is determined to be associated with an outgoing connection or an incoming connection. At 806, whether the QoS request is authorized is determined (e.g., whether the QoS request supported by the service plan, sufficient charging credit exists for this QoS request, and/or other criteria/measures). If not, then at 808, the UI provides a responsive notification and/or option as similarly described herein. If the QoS request is approved, then at 810, a request for network resources for the QoS session is sent to one or more network resources (e.g., service controller, BTS, gateway, core/transport network, IPX/GRX networks, a/another service controller in communication with another communications device such as for setting up a conversational class QoS connection with the other communications device, and/or other network elements/functions/resources). If the device is determined to be eligible for QoS, then at 810, QoS availability is determined (e.g., based on network capacity, which may be determined at the device, via communication with the service controller, via communication with the BTS or another network element/function, and/or any combination thereof, using the various techniques described herein). If QoS is determined to not be available, then at 812, the UI provides information and/or options concerning the QoS availability (e.g., unavailability explanation and/or options for providing for one or more QoS options, such as a service plan upgrade or payment for a certain/set of/period of time for QoS session(s) access). If QoS is determined to be available, then at 814, a request for network resources for the QoS session is sent to one or more network resources (e.g., service controller, BTS, gateway, core/transport network, IPX/GRX networks, and/or other network elements/functions/resources, to setup, for example, a QoS end to end connection – coordinate all resources end to end for the approved and verified

QoS flow). At 816, a confirmation of the approved QoS session is received to close the loop for the QoS for DAS (e.g., a QoS schedule is received that provides the QoS session confirmation information, such as a scheduled RAB/multi-RAB and/or other reserved network resource(s) by schedule/other criteria). At 818, a QoS router is executed/performed on the communications device to assist in implementing QoS for DAS using various verification techniques described herein (e.g., to perform QoS queuing, throttling, and/or other QoS router related functions as described herein). At 820, verified QoS charging is performed (e.g., at least in part) on the device using various techniques described herein (e.g., using the service processor, such as the charging/service usage monitoring and/or other agents as described herein). In some embodiments, QoS charging records and/or reports are provided to one or more network elements for managing QoS billing and/or other QoS management/billing related service control functions (e.g., to the service controller and/or the billing interface or billing server). In some embodiments, QoS for DAS also facilitates reestablishing the QoS session/connection/channel/stream if the QoS session/connection/channel/stream is lost or goes down, using similar techniques to those described herein as would be apparent to one of ordinary skill in the art. At 822, the process is completed. In some embodiments, the QoS provisioning channel is closed when the device session is over to, for example, free up various resources.

[00190] Figure 8B illustrates another flow diagram for quality of service (QoS) for device assisted services (DAS) in accordance with some embodiments. In some embodiments, QoS for DAS includes identifying the QoS requirements (e.g., QoS level or QoS class) for a service activity. At 824, the process begins. In some embodiments, the QoS policies are implemented on the device (e.g., service processor collects/receives an associated service plan that defines/specifies basic policies for QoS, which can include a QoS activity map, which, for example, maps QoS classes based on application, service usage, flow type, destination, time of

day, network capacity, and/or other criteria/measures, as similarly described herein). In some embodiments, the QoS rules are implemented in the form of a verified QoS activity map in accordance with various embodiments described herein. At 826, the device monitors device activity, such as service/application usage activities. In some embodiments, the device detects the relevant activities based on various service usage monitoring techniques described herein. At 828, a QoS request is determined, for example, using various techniques described herein. At 830, a QoS level is determined based on the application and/or various device monitored service usage/application activities associated with the QoS request using various techniques described herein. For example, the QoS level can be determined using the QoS activity map, which provides a QoS policy defined by a table associating various QoS levels with a variety of activities that include various device monitored service usage/application activities. In some embodiments, the QoS activity map includes QoS level mappings based on one or more of the following: application, destination/source, traffic type, connection type, content type, time of day/day of week, network capacity, activity usage, service plan selection, current standing, user class, device class, home/roaming, network capabilities, and/or other criteria/measures as similarly described herein. In some embodiments, at 832, if the QoS level cannot be determined and/or in order to confirm a QoS level or selection among multiple potential appropriate/approved QoS levels, the UI presents options for a user to select the QoS level. At 834, the QoS request is initiated for the determined QoS level (e.g., QoS class and/or priorities). At 836, the process is completed.

[00191] Figure 8C illustrates another flow diagram for quality of service (QoS) for device assisted services (DAS) in accordance with some embodiments. In some embodiments, QoS for DAS includes determining whether the network should grant the QoS request for a given device activity. At 842, the process begins. At 844, QoS request is determined. At 846, the communications device's standing for QoS is determined using various techniques described

herein (e.g., a service processor in combination with a service controller or based on a communication for authorization of the QoS request sent to the service controller determines whether the QoS request is authorized, which can be based on the service plan, service profile, service policy settings, QoS rules, based on QoS class, current service usage, current billing standing, and/or any other criteria/measure). If the device is determined to not be eligible for QoS, then at 848, the device User Interface (UI) provides information concerning the denial/ineligibility for QoS session(s) (e.g., denial/ineligibility explanation and/or options for providing for one or more QoS options, such as a service plan upgrade or payment for a certain/set of/period of time for QoS session(s) access). If the device is determined to be eligible for QoS, then at 850, QoS availability is determined (e.g., based on network capacity, which may be determined at the device, via communication with the service controller, via communication with the BTS or another network element/function, and/or any combination thereof, using the various techniques described herein). If QoS is determined to not be available, then at 852, the UI provides information and/or options concerning the QoS availability (e.g., unavailability explanation and/or options for providing for one or more QoS options, such as a service plan upgrade or payment for a certain/set of/period of time for QoS session(s) access). If QoS is determined to be available, then at 854, a request for network resources for the QoS session is sent to one or more network resources (e.g., service controller, BTS, gateway, core/transport network, IPX/GRX networks, and/or other network elements/functions/resources can be queried directly and/or a centralized QoS resource/network function/element/database can be queried for determining such network resources and coordinating such scheduling). At 856, a confirmation of the approved QoS session is received to close the loop for the QoS for DAS (e.g., a QoS schedule is received that provides the QoS session confirmation information, such as a scheduled RAB/multi-RAB and/or other reserved network resource(s) by schedule/other criteria). At 858, a QoS router is performed. In some embodiments, the QoS router is performed on the device (e.g., service

processor), on a network element/function (e.g., service controller), and/or in combinations thereof. In some embodiments, the QoS router prioritizes multiple QoS requests across a given communications device. In some embodiments, the QoS router prioritizes multiple QoS requests across multiple communications devices and/or across multiple BTSs. In some embodiments, the QoS router performs various QoS class degradation, promotion, and/or other throttling related techniques as similarly described herein (e.g., based on session priority, network capacity, workload balancing, QoS priority rules, and/or other criteria/measures/rules). At 860, the process is completed.

[00192] Figure 9 illustrates another flow diagram for quality of service (QoS) for device assisted services (DAS) in accordance with some embodiments. In some embodiments, QoS for DAS includes QoS session provision for a service activity. At 902, the process begins. At 904, a new QoS session is granted and/or confirmed. At 906, a device service processor (e.g., policy decision point (PDP) agent, also referred to herein as a policy control agent) maps the QoS session grant to a QoS monitoring policy (e.g., based on a service controller provided QoS related policy, based on a service plan associated with the device, user, device/user group, and/or other criteria/measures, as similarly described herein). At 908, the QoS monitoring policy provides commands/instructions to a policy enforcement point (PEP) (e.g., PEP agent, also referred to herein as a policy implementation agent) for managing/enforcing the new QoS priorities/sessions. At 910, the PEP determines whether to allow, block, throttle, and/or queue priority (e.g., and/or otherwise control using various traffic control related techniques) a session based on the QoS monitoring policy. At 912, the process is completed.

[00193] Figure 10 illustrates another flow diagram for quality of service (QoS) for device assisted services (DAS) in accordance with some embodiments. In some embodiments, Radio Access Bearer (RAB) support is available, and the following process is performed in accordance with some embodiments. At 1002, the process begins. At 1004, the device service processor

detects a QoS request or QoS need (e.g., a QoS API request, a QoS request or need/benefit of QoS session based on service usage monitoring, such as by application and/or another service usage measure/activity). At 1006, the service processor and/or the service processor in communication with the service controller determines if the service plan allows/supports the requested QoS. If not, then at 1008, a UI event is generated (e.g., notifying the device user that such QoS/QoS level/class is not available, and potentially offering a QoS/service plan upgrade/purchase for that QoS/QoS level/class). At 1010, the service processor communicates the QoS request to the service controller (e.g., using a secure service control link or secure communication channel, as similarly described herein) to request the QoS level/class. At 1012, the service controller determines whether network resources are available using various techniques as described herein. In some embodiments, network capacity is determined using various techniques, such as local device measurements; dedicated local device measurement reports; BTS reports; other network element reports; by assessing, for example, a combination of one or more of available bandwidth, traffic delay or latency, available QoS level, variability in available bandwidth, variability in latency, and/or variability in available QoS level; and/or other techniques as described herein. At 1014, the service controller responds to the QoS request (e.g., grants or denies the QoS request). In some embodiments, another UI event is generated if the QoS request is denied as similarly described herein. At 1016 (assuming the QoS request is granted), the device requests a QoS channel from the BTS. In some embodiments, the request includes a QoS request authorization code received from the service controller. In some embodiments, the service controller provides a notification of the QoS request approval for the communications device to the BTS, so that the BTS can verify the approval of the QoS request. In some embodiments, the BTS confirms the device QoS channel request directly with the service controller. For example, various other techniques for verifying the QoS channel request can also be used as similarly described herein and as would be apparent to one of ordinary skill in the art. In some embodiments, the device service processor and/or service

controller provides QoS related reports informing the BTS of how many QoS channels (e.g., RABs) to provision and how many best effort resources to provision based on device demand projections. At 1018 (assuming the QoS channel request is verified), the QoS session is initiated based on an allocated RAB or multi-RAB reservation received from the BTS (e.g., and/or other network elements as similarly described herein). At 1020, the process is completed.

[00194] Figure 11 illustrates another flow diagram for quality of service (QoS) for device assisted services (DAS) in accordance with some embodiments. In some embodiments, RAB support is not available, and the following process is performed in accordance with some embodiments. At 1102, the process begins. At 1104, the device service processor detects a QoS request or QoS need (e.g., a QoS API request, a QoS request or need/benefit of QoS session based on service usage monitoring, such as by application, or other service usage measure/activity). At 1106, the service processor and/or the service processor in communication with the service controller determines if the service plan allows/supports the requested QoS. If not, then at 1108, a UI event is generated (e.g., notifying the device user that such QoS/QoS level/class is not available, and potentially offering a QoS/service plan upgrade/purchase for that QoS/QoS level/class). At 1110, the service processor communicates the QoS request to the service controller (e.g., using a secure service control link or secure communication channel, as similarly described herein) to request the QoS level/class. At 1112, the service controller determines whether network resources are available using various techniques as described herein. In some embodiments, network capacity is determined using various techniques, such as local device measurements, BTS reports, other network element reports, and/or other techniques as described herein. In some embodiments, the service controller throttles other devices on the link so that the requested QoS level can be achieved (e.g., as RAB support is not available). In some embodiments, the service controller time slots

traffic from the device end in synchronization with a BTS clock or absolute clock to facilitate the requested QoS level and to achieve necessary network capacity to support/facilitate the requested QoS level (e.g., minimizing jitter/inter-packet delay variation) based on current/forecasted network capacity on the link. At 1114, the service controller responds to the QoS request (e.g., grants or denies the QoS request). In some embodiments, another UI event is generated if the QoS request is denied as similarly described herein. At 1116 (assuming the QoS request is granted), the device initiates the QoS session. At 1118, the device service processor and/or the device service processor in secure communication with the service controller monitors and verifies the QoS session using various monitoring and verification techniques described herein (e.g., checks CDRs to determine if the QoS channel is properly implemented by the device). In some embodiments, a UI event is generated to notify the device user if there are potential problems with the QoS session implementation, to periodically inform the user of QoS charging, and/or other events/information related to QoS activities. At 1120, the process is completed.

[00195] Figure 12 illustrates a device stack for providing various service usage measurement techniques in accordance with some embodiments. Figure 12 illustrates a device stack providing various service usage measurement from various points in the networking stack for a service monitor agent (e.g., for monitoring QoS related activities and/or for monitoring network capacity controlled services as described herein), a billing agent, and an access control integrity agent to assist in verifying the service usage measures, QoS related activities and functions, and billing reports in accordance with some embodiments. As shown in Figure 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/detect 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 driver/agent 1690 (e.g., policy enforcement point driver/agent), 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.

[00196] 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.

[00197] It will be appreciated that although the implementation/use of any or all of the measurement points illustrated in Figure 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).

[00198] Referring to Figure 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 certain embodiments to differentiate the traffic or service activity taking place through one modem from that of one or more of the other modems. In some embodiments, measurement point VI, or another measurement point, is located over, within or below one or more of the individual modem drivers. The respective modem buses for each modem reside

between example measurement points V and VI. In the next higher layer, a modem selection & control layer for multimode device based communication is provided. In some embodiments, this layer is controlled by a network decision policy that selects the most desirable network modem for some or all of the data traffic, and when the most desirable network is not available the policy reverts to the next most desirable network until a connection is established provided that one of the networks is available. In some embodiments, certain network traffic, such as verification, control, redundant or secure traffic, is routed to one of the networks even when some or all of the data traffic is routed to another network. This dual routing capability provides for a variety of enhanced security, enhanced reliability or enhanced manageability devices, services or applications. In the next higher layer, a modem firewall is provided. For example, the modem firewall provides for traditional firewall functions, but unlike traditional firewalls, in order to rely on the firewall for verifiable service usage control, such as access control and security protection from unwanted networking traffic or applications, the various service verification techniques and agents described herein are added to the firewall function to verify compliance with service policy and prevent/detect 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 and described herein. 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 (e.g., QoS IP queuing and routing layer and/or a network capacity controlled services 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 QoS IP queuing and routing and/or for network capacity controlled services 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 Figure 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 Figure 12.

[00199] As shown in Figure 12, the application service interface layer (e.g., QoS application service interface layer and/or network capacity controlled services 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.

[00200] As shown in Figure 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.

[00201] Figure 13 illustrates another device stack for providing various service usage measurement techniques in accordance with some embodiments. Figure 13 illustrates an embodiment similar to Figure 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 Figure 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 Figure 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 functions on the modem subsystem (e.g., and such an approach can be applied to one or more modems). For example, the service processor can be distributed as a standard feature set contained in a modem chipset hardware of software package or modem module hardware or software package, and such a configuration can provide for easier adoption or development by device OEMs, a higher level of differentiation for the chipset or modem module manufacturer, higher levels of performance or service usage control implementation integrity or security, specification or interoperability standardization, and/or other benefits.

[00202] Referring to Figure 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 Figure 13.

[00203] Additional Embodiments of DAS for Protecting Network Capacity

[00204] In some embodiments, DAS for protecting network capacity includes classifying a service activity as a network capacity controlled service and implementing a network capacity controlled services policy. In some embodiments, DAS for protecting network capacity includes device assisted/based techniques for classifying a service activity as a network capacity controlled service and/or implementing a network capacity controlled services policy. In some embodiments, DAS for protecting network capacity includes network assisted/based techniques (e.g., implemented on a network element/function, such as a service controller, a DPI gateway, a BTS/BTSC, etc., or a combination of network elements) for classifying a service activity as a network capacity controlled service and/or implementing a network capacity controlled services policy. In some embodiments, DAS for protecting network capacity includes providing a network access API or an emulated or virtual network access API (e.g., such an API can provide network busy state information and/or other criteria/measures and/or provide a mechanism for allowing, denying, delaying, and/or otherwise controlling network access). In some embodiments, DAS for protecting network capacity includes implementing a service plan

that includes a network capacity controlled services policy (e.g., for differential network access control and/or differential charging for network capacity controlled services, which can also be based on a network busy state and/or other criteria/measures).

[00205] In some embodiments, DAS for protecting network capacity techniques also provide improved user privacy and facilitate network neutrality requirements. In contrast, network based techniques (e.g., DPI based techniques) can give rise to user privacy and network neutrality concerns and problems as discussed above. In some embodiments, DAS for protecting network capacity techniques include allowing a user to specify (e.g., permit or not permit) whether the network is aware of the user's Internet behavior (e.g., using UI input). In some embodiments, DAS for protecting network capacity techniques include allowing a user to select how they want their traffic usage and service plan costs to be managed.

[00206] Figure 14 illustrates a flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments. At 1402, the process begins. At 1404, monitoring a network service usage activity of a device in network communication (e.g., wireless network communication) is performed. At 1406, whether the monitored network service usage activity is a network capacity controlled service is determined. At 1408 (the monitored network service usage activity was determined not to be a network capacity controlled service), the network service usage activity is not classified for differential network access control. At 1410, (the monitored network service usage activity was determined to be a network capacity controlled service), the network service usage activity is classified (e.g., into one or more network capacity controlled services) for differential network access control for protecting network capacity. In some embodiments, classifying the network service usage activity includes classifying the network service usage activity into one or more of a plurality of classification categories for differential network access control for protecting network capacity (e.g., one or more network capacity controlled service classifications and/or a priority state

classification, such as a background services classification and/or a background priority state classification). At 1412, associating the network service usage activity with a network capacity controlled services control policy based on a classification of the network service usage activity to facilitate differential network access control for protecting network capacity is performed. At 1414, implementing differential network access control for protecting network capacity by implementing different traffic controls for all or some of the network service usage activities (e.g., based on a network busy state or another criteria/measure) is performed. At 1416, the process is completed.

[00207] Figure 15 illustrates another flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments. At 1502, the process begins. At 1504, monitoring network service usage activities of a device in network communication is performed. At 1506, monitored network service usage activity of the device is reported (e.g., to a network element/function). At 1508, a statistical analysis of a reported network service usage activities across a plurality of devices is performed (e.g., by a network element/function). At 1510, the device receives a network service usage activity classification list (e.g., a network capacity controlled services list, which can be generated, for example, based on the monitored network service usage activities and the statistical analysis as well as other criteria/measures, including, for example, a service plan and/or a network busy state) from the network element. At 1512, implementing differential network access control based on the network service usage activity classification list for protecting network capacity is performed. At 1514, the process is completed. In some embodiments, DAS for protecting network capacity further includes associating the network service usage activity with a network service usage control policy (e.g., a network capacity controlled services policy) based on a classification of the network service usage activity to facilitate differential network access control for protecting network capacity. In some embodiments, DAS for protecting network capacity further includes

differentially controlling the network service usage activity (e.g., network capacity controlled service) based on the service usage activity classification list.

[00208] Figure 16 illustrates another flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments. At 1622, the process begins. At 1624, a first report of network service usage activity of a first device is received (e.g., at a network element/function) from the first device. At 1626, a second report of network service usage activity of a second device (e.g., at a network element/function) from the second device is received. At 1628, a statistical analysis of a plurality of reported service usage activities across a plurality of devices, including the first device and the second device, is performed (e.g., by a network element/function). At 1630, a network service usage activity classification list (e.g., a network capacity controlled services classification list) is sent to the first device (e.g., from a network element/function) for classifying network service usage activities (e.g., network capacity controlled services) based on the network service usage activity classification list for differential network access control for protecting network capacity. At 1632, a network service usage activity classification list is sent to the second device (e.g., from a network element/function) for classifying network service usage activities based on the network service usage activity classification list for differential network access control for protecting network capacity. At 1634, the process is completed. In some embodiments, DAS for protecting network capacity further includes associating the network service usage activity with a service usage control policy (e.g., a network capacity controlled services policy) based on a classification of the network service usage activity to facilitate differential network access control for protecting network capacity. In some embodiments, DAS for protecting network capacity further includes differentially controlling the network service usage activity (e.g., network capacity controlled service) based on the service usage activity classification list (e.g., network capacity controlled services classification list). In some embodiments, classifying network service usage activities is based

on which network to which the device is connected. In some embodiments, the network service usage control policy is based on which network to which the device is connected.

[00209] Figure 17 illustrates another flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments. At 1702, the process begins. At 1704, monitoring a network service usage activity of a plurality of devices in network communication using network based techniques is performed. At 1706, a statistical analysis of monitored network service usage activities across the plurality of devices is performed. At 1708, a network service usage activity classification list (e.g., a network capacity controlled services classification list) is sent to each of the plurality of devices for classifying network service usage activities (e.g., network capacity controlled services) based on the service usage activity classification list for differential network access control for protecting network capacity. At 1710, the process is completed.

[00210] Figure 18 illustrates another flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments. At 1802, the process begins. At 1804, monitoring network service usage activities of a device in network communication is performed. At 1806, associating a network service usage activity (e.g., a network capacity controlled service) with a service usage control policy (e.g., a network capacity controlled services policy) based on a classification of the network service usage activity (e.g., a network capacity controlled services classification list) for differential network access control for protecting network capacity is performed. At 1808, a user notification based on the service usage control policy is generated. At 1810, the process is completed.

[00211] In some embodiments, the service usage control policy includes a service usage notification policy. In some embodiments, the user notification includes one or more of the following: a notification that the application to be downloaded and/or launched is a network capacity controlled service; a list of one or more service activities (e.g., applications, OS/other

software functions/utilities, and/or other functions/utilities as described herein) that have a network capacity controlled services classification; type of service policy in effect for one or more network capacity controlled services; notification that a service activity belongs to a network capacity controlled services class; notification that a service activity that is classified as network capacity controlled service can have the service class changed; notification that if the service class is changed for a service activity the service charges will change; notification that one or more networks are available (e.g., one or more alternative networks and/or network busy state information and/or charging information and/or incentives associated with such networks), a service plan upgrade/downgrade offer/option; and an offer for a service plan that rewards a user that responds to the notification a service plan is lower cost/discounted for responding to notification to use or not to use service activity based on usage level warning notification. In some embodiments, the user notification includes a user preference selection, including one or more of the following: a provision to associate an access policy control with the application (e.g., allow/block, notify of usage, notify of usage at a given threshold, traffic control settings, allow during certain times, allow when network not busy, and/or other policy controls as described herein), an over-ride option for selecting the service usage control policy; a modify option to select the service usage control policy; a select option to select a new service plan (e.g., an option to review and select alternative/new service plan upgrade/downgrade options), and an acknowledgement request (e.g., to confirm/acknowledge receipt of the notification, in which the acknowledgement can be transmitted to a network element/function and/or stored locally for later reference/transmission).

[00212] In some embodiments, before a given device application, process, function, OS service or other service activity is allowed to start, the intention to start is intercepted by a launch manager, the background service policy set or the network protection service policy set for the service activity is retrieved, and any necessary user notification or service launch control

policies are implemented prior to allowing the service activity to launch. In such embodiments, a launch intercept manager may be used to implement this functionality. In some embodiments, this launch intercept manager is provided with a list identifying the service activities (e.g. application identifiers, OS function identifiers, aggregate service activity identifiers, and/or component service activity identifiers) that have a launch control policy in effect. In some embodiments, the list of launch control policies includes blocking or delaying launch of the one or more service activities. In some embodiments, the launch control policy includes a user notification before, during or after the service activity is launched. In some embodiments, the user is informed that a service activity that has a background service control policy in effect or a network protection service control policy in effect is attempting to launch, is about to launch or has launched. In a further set of embodiments, the launch is held up until the user is notified and is allowed to decide if they would like to launch the service activity. In some embodiments, the user notification includes a message that the service activity attempting to launch consumes a large amount of service usage and asks the user if they would like to continue (e.g. "This application consumes a large amount of data, would you like to continue?", "This application consumes data even when you are not using it, would you like to continue?" "This application consumes data while you are roaming which adds cost to your usage bill, would you like to continue?", etc). In some embodiments, the decision on whether or not to launch a service activity is pre-programmed into the list identifying the service activities (e.g. application identifiers, OS function identifiers, aggregate service activity identifiers, and/or component service activity identifiers) that have a launch control policy in effect. In some embodiments a portion of the list is pre-programmed by the user in accordance with user preference for controlling usage of service activities. In some embodiments, a portion of the list is pre-programmed by a network element (e.g. a service controller) in accordance with network background service or network protection service policies specified by a service policy design management system operated by a service provider as described herein. In some

embodiments, the policy implementation defined by the list identifying the service activities (e.g. application identifiers, OS function identifiers, aggregate service activity identifiers, and/or component service activity identifiers) that have a launch control policy in effect is verified to ensure that the user or malicious software has not defeated the policy enforcement specified in the list. In some embodiments the list identifying the service activities that have a launch control policy in effect includes launch policies that are a function of one or more of: background service state, network busy state (or performance state or QoS state), type of network the device is connected to, home or roaming connection, time of day or day of week.

[00213] In some embodiments, the various design techniques described herein that allow for intercepting a service activity intention to launch, and applying a background service policy set or a network protection service policy set can be designed into the OS itself. For example, the intercept and policy implementation functions can be designed into the activity manager, broadcast intent manger, media service manager, service manager, or other application or service activity management function in the Android OS. One of ordinary skill in the art will recognize that similarly, the various design techniques described herein that allow for intercepting a service activity intention to launch, and applying a background service policy set or a network protection service policy set can be designed into application launch management functions in the iPhone OS, windows mobile OS, windows PC OS, Blackberry OS, Palm OS, and other OS designs.

[00214] In some embodiments, the pre-launch user notification information indicates one or more of: typical service usage or cost, or projected service usage or cost for the service activity attempting to launch. In some embodiments, the user sets limitations on access for one or more service activities and once this limit is hit then when the service activities with exceeded limits attempt to launch the user is notified. In some embodiments, the user chooses from a set of service restrictions rather than simply blocking or allowing service activity launch, with

example service restrictions including but not limited to: a pre-configured set of restriction policies to chose from (e.g. full access, limited access, highly restricted access or block access), block, throttle, delay, aggregate and hold, limit amount of usage per unit time, cap usage, set limit for additional notification, specify type of network, specify busy state (performance, QoS) or background state, or choose from pre-configured settings options.

[00215] In some embodiments, the user notification occurs after the user attempts to download or load an application onto the device (e.g., an application downloaded from the web or an online application store for a smart phone or other wireless/network computing device, such as an Apple iPhone or iPad, or Google Android/Chrome based device). In some embodiments, the user notification occurs after the user attempts to run the service activity or to initiate usage of a cloud based service/application (e.g., Google or Microsoft cloud service based apps). In some embodiments, the user notification occurs after one or more of the following: the service usage activity hits a usage threshold event, the service usage activity attempts a network service usage that satisfies a pre-condition, an update to a network capacity protection service activity classification list or policy set, and a network message is sent to the device triggering the notification. In some embodiments, the user notification provides information on the service usage activity that is possible, typical, or likely for the service usage activity. In some embodiments, the user notification includes a user option for obtaining more information about the service usage of the service activity (e.g., a message that the service usage activity may result in a high service usage and/or that the service usage activity may or will result in a high service usage as compared in some way to a limit of the current service plan) to make informed user preference settings.

[00216] In some embodiments, a user notification includes displaying (e.g., and as applicable, allowing users to provide UI input) one or more of the following: current and/or past/historical/logged network service usage activity list, current and/or past/historical/logged

network capacity controlled service usage activities, current activity policy settings, current or available networks, service plan options (e.g., for how to treat one or more network capacity controlled service traffic types), selection option(s) to assign a network capacity controlled service activity into a different priority traffic control and/or charging buckets, network service usage by activity (e.g., network capacity controlled services and other services), network busy state (e.g., and with resulting policies in force), service activity policy setting vs. busy state and time/day/week, network service activity priority, network service activity usage statistics (e.g., vs. network busy state and/or network service usage control policy state).

[00217] In some embodiments, a UI notification is displayed when user attempts a network capacity controlled service activity during a network busy state (e.g., that modifies a network capacity controlled services policy). In some embodiments, the UI notification includes information on service plan choice and a network capacity controlled services policy over-ride option (e.g., one time, time window, usage amount, permanent by activity, and/or all), charging information based on a user selection, and/or service plan upgrade information and options.

[00218] In some embodiments, a UI notification is displayed for user input for preferences/configurations for multiple networks (e.g., WiFi, 4G, 3G, and/or other wired or wireless access networks) including charging policy. In some embodiments, a UI notification is displayed when a specified network traffic service usage activity (e.g., based on network capacity controlled services classification, QoS classification, priority classification, time based criteria, network capacity, service plan, charging criteria, and/or other criteria/measures) is being attempted or is occurring and providing options (e.g., allow, block, delay, throttle, and/or other options).

[00219] In some embodiments, a UI fuel gauge is displayed (e.g., to depict current and/or historical network service usage, for example, relative to a service plan for the device, by network, relative to network busy state, time based criteria, and/or other criteria/measures). In

some embodiments, a user notification includes a communication sent to the user (e.g., an email, SMS or other text message, voice message/call, and/or other electronic form of communication). In some embodiments, the communication sent to the user includes network service usage information, network capacity controlled service usage related information, and/or an instruction to log into a web page or send a communication for more information (e.g. regarding an information update and/or alert or warning message, such as related to network service usage and/or charging for network service usage).

[00220] In some embodiments, a notification (e.g., a user or network service cloud notification) is generated based on an aggregate service activity reports usage (e.g., allows network provider to generate user notifications and/or to notify application provider/service activity provider). In some embodiments, a notification (e.g., a user or network service cloud notification) is generated based on a publishing of an updated/new network capacity controlled services list based on an aggregate monitored activity (e.g., based on a service plan, velocity, sockets opening frequency/rate (e.g., messaging layer behavior), total data usage, peak busy time usage to formulate or update black list for monitoring, notifying, and/or controlling, which can be applied to one, multiple, group, or all devices). In some embodiments, a notification (e.g., a user or network service cloud notification) is generated based on data usage trends for particular device relative to an associated service plan and/or other comparable devices or data usage thresholds/statistical based data usage measures.

[00221] In some embodiments an application is actually composed of several component applications, processes or functions. Examples of this include but are not limited to: the components of a Java application JAR file; applications that use OS functions; applications that use a proxy service function; applications, functions or processes that coordinate with one another to implement a composite process, function or application; and OS process functions that support an application or overall OS function. In such embodiments it is important to be

able to categorize all applications, functions and processes on a device that contribute to the service usage of a service activity so that the service activity can be monitored for service usage, have the service usage accounted for, implement the appropriate user notification when one or more service activity components attempts to start or use the network, implement the appropriate user notification when one or more service activity components reaches a pre-determined service usage level that requires user notification, and implement the appropriate background service or network protection service usage controls as specified herein ((including but not limited to for example: block network access, restrict network access, throttle network access, delay network access, aggregate and hold network access, select for time of day network access restrictions, select network type restrictions, select roaming network access restrictions, select service usage restrictions such as a usage limit, select service cost restrictions such as a cost limit or otherwise place on another form of background service status or network usage restriction as described herein). In the case of service activity components that belong exclusively to one aggregate service activity (e.g. an application, application JAR file or OS function), this may be accomplished by including each of the component service activities on a list that identifies the service activity components that belong to the aggregate service activity, and then monitoring, possibly controlling and providing user notifications based on the aggregate or component behavior of each service activity in accordance with the policies specified for the aggregate service activity. For example, it is necessary to group all application launch behavior and/or network access behavior under the monitoring, launch, notification, accounting and background service controls or network protection service controls (or other background or network protection service policies as specified herein) in accordance with the background service or network protection service policies for the aggregate application that the JAR file supports. As another example, if an OS network synch or update function utilizes various software components or processes to implement the network synch or update function, then each of the software components or process must be monitored and aggregated under the

background service policies or network protection service policies for the aggregate OS synch or update function.

[00222] In some embodiments, this ability to group usage for a related set of service activity components dedicated to an aggregate service activity as described herein is used to improve usage reporting of service activities to a service controller for the purpose of statistically identifying service activities that are candidates for background service policy controls or network protections service policy controls.

[00223] In some cases, multiple applications, processes, functions, OS services or other service activities can utilize a common set of component software applications, processes, functions or OS services. In such cases, in order to implement background service policies and/or network protection service policies for service activity monitoring and accounting, service activity launch control, user notification, or network access control as described herein, it is necessary to associate the specific network access data or information flows to and from the common component software applications, processes or functions that belong to the specific initiating application, process, function or other service activity that is to be managed according to a background service or network protection service policy set. In what follows, a specific set of examples are provided on how to map common component service activity for a set of common OS functions referred to as proxy service functions to a specific application, process, function, OS service or other service activity for the purpose of implementing a background service policy set or a network protection service policy set as described herein. Once these examples are reviewed, it will be obvious to one of ordinary skill in the art how to apply similar mapping of service activity for a common set of components to a service activity that is to be managed in accordance with a background service policy set or a network protection service policy set as described herein.

[00224] In some embodiments, this ability to group usage for a common set of service activity components as described herein is used to improve usage reporting of service activities to a service controller for the purpose of statistically identifying service activities that are candidates for background service policy controls or network protections service policy controls.

[00225] In some embodiments, a proxy network service manager refers to an intermediary data flow function in a device operating system that sits on a data path between a device application and a device networking stack interface to provide a level of network service abstraction from the network stack interface, a higher level service function above the network stack interface, enhanced or special traffic processing functions, media service transfer management, file download service, HTTP proxy service functions, QoS differentiation, or other similar or related higher level traffic processing. Example Proxy Service Managers include the following: media service manager (e.g. android media service library function), email service manger, DNS function, software download service manager, media download manager (e.g. audio player, streaming media player, movie downloader, media service OS function, etc), data download service manager, Android "media" library function, Android.net library function, Jave.net library function, Apache library function, other similar software/library functions or services in other device operating systems, SMTP/IMAP/POP proxy, HTTP proxy, IM proxy, VPN service manager, SSL proxy, etc. Herein these alternative network access data flows that are initiated by an application are termed application proxy service flows. In such embodiments an app can sometimes simply requests a network access service activity from an OS component such as a proxy service component rather then directly accessing the network. In such embodiments, in order to implement background service controls or user notification of application service usage, it is necessary to monitor the application proxy service flows, classify them as being initiated by or belonging to a particular application or service activity, and implement the proper background service classifications, user notifications, application process

launch intercept, background service accounting, and background service usage restrictions as described herein in accordance with the policies intended for the initiating application or service activity. This is accomplished by inserting service usage monitors that allow a mapping of (i) the initiating application identifier (e.g. app name, app fingerprint, application identification tag, application process number, application credential, or other secure or non-secure application or process identifier) to (ii) the request to the proxy service and subsequently to (iii) the network service flows between the proxy service and the network elements that service the information communications. Once this mapping is accomplished, the service usage flows of the proxy service can then be accounted back to the initiating application, device software process or other service activity, the proper policies can then be applied to each service usage flow for user notification, service activity launch control, service activity background accounting (including variable charge rating dependent on background service state and/or sponsored service charging), service activity background service controls or network usage restrictions as described herein (including but not limited to for example: block network access, restrict network access, throttle network access, delay network access, aggregate and hold network access, select for time of day network access restrictions, select network type restrictions, select roaming network access restrictions, select service usage restrictions such as a usage limit, select service cost restrictions such as a cost limit or otherwise place on another form of background service status or network usage restriction as described herein).

[00226] In some embodiments, this ability to track service usage for an service activity through a proxy service as described herein is used to improve usage reporting of service activities to a service controller for the purpose of statistically identifying service activities that are candidates for background service policy controls or network protections service policy controls.

[00227] In some embodiments, the various design techniques described herein that allow for monitoring, accounting for and/or implementing service policy for component service activities

that belong to an aggregate service activity can be designed into the OS itself. For example, in certain current mobile OS implementations (e.g. Android, iPhone, Blackberry, etc) there are some applications available in the market that allow a user to get an estimate for how much data a certain subset of applications are consuming on a wireless service provider network, but it is not possible for the user or application to get an indication of the service usage for certain OS functions, whereas the embodiments disclosed herein will allow for this. As another example, in certain current mobile OS implementations it is not possible to associate proxy service usage (e.g. media download and media streaming proxy library software functions) with the specific applications that use the proxy service, so while the user can be informed of generic common OS functions or proxy services (e.g. in the case of Android: "media service", "media", "gallery", "google service framework" and other generic common OS software library functions or proxy services), there is no way for the user to determine what applications widgets or other service activities are actually generating this common service function usage, whereas the invention described herein permits the user full visibility on such usage monitoring examples. Furthermore, if the OS is retrofitted with the intercept and policy implementation functions can be designed into the activity manager, broadcast intent manger, media service manager, service manager, or other application or service activity management function in the Android OS. One or ordinary skill in the art will recognize that similarly, the various design techniques described herein that allow for intercepting a service activity intention to launch, and applying a background service policy set or a network protection service policy set can be designed into application launch management functions in the iPhone OS, windows mobile OS, windows PC OS, Blackberry OS, Palm OS, and other OS designs.

[00228] Figure 19 illustrates another flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments. At 1902, the process begins. At 1904, determining a network busy state of one or more networks is performed. In

some embodiments, the one or more networks are selected from an access network, a wired network, and a wireless network. At 1906, classifying a network service usage activity (e.g., a network capacity controlled service) of a device based on the network busy state determination is performed to facilitate differential network access control for protecting network capacity of the one or more networks. In some embodiments, the network busy state is based on one or more of the following: network performance, network congestion, network availability, network resource availability, network capacity, or any other network service usage measure, and one or more time windows (e.g., time based criteria). In some embodiments, protecting network capacity of the one or more networks includes protecting network capacity of a last edge segment of a wireless network (e.g., RAN, BTS, BTSC, and/or other network elements). In some embodiments, the determining and classifying are performed using device assisted/based techniques. In some embodiments, the determining and classifying are performed using network assisted/based techniques (e.g., implemented on a network element/function, such as a service controller, a DPI gateway, a BTS/BTSC, etc., or a combination of network elements). In some embodiments, the determining and classifying are performed using a combination of device assisted/based techniques and network assisted/based techniques. At 1908, implementing differential traffic controls is performed based on the service usage activity classification for protecting network capacity is performed. At 1910, the process is completed. In some embodiments, a network busy state is determined based on one or more of the following: a time of day, a network reported busy state, and/or a device (e.g., near-end and/or far-end) determined/reported network busy state. In some embodiments, a network busy state is determined using one or more of the following: a network probe, a device query, a network probe report (e.g., including a BTS and/or BTSC), a network probe analysis, a device analysis based on performance of native traffic without probe such as TCP timeout, UDP retransmissions, a multiple network test, a device monitored network congestion based on network service usage activity (e.g., application based network access performance data)

performed for a network to which the device is connected and/or one or more alternative networks. In some embodiments, a network congestion state is associated with a network busy state (e.g. a network busy state setting/level). For example, a network congestion level of 40% of network usage can be associated with a network busy state setting of 4, a network congestion level of 80% of network usage can be associated with a network busy state setting of 8, and so forth.

[00229] Figure 20 illustrates another flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments. At 2002, the process begins. At 2004, monitoring a network service usage activity of a device in network communication is performed. At 2006, classifying the network service usage activity (e.g., based on a classification of the network service usage activity for protecting network capacity, for example, as a network capacity controlled service) for protecting network capacity is performed. At 2008, accounting for network capacity controlled services (e.g., accounting for the network service usage activity based on a classification of the network service usage activity for protecting network capacity) is performed. At 2010, charging for network capacity controlled services is performed. At 2012, the process is completed. In some embodiments, DAS for protecting network capacity further includes classifying the network service usage activity as a network capacity controlled service. In some embodiments, DAS for protecting network capacity includes differentially accounting and/or differentially charging for network capacity controlled services and foreground services. In some embodiments, the network service usage control policy includes policies for differentially controlling, accounting, and/or charging for network capacity controlled services (e.g., based on a network busy state, a time based criteria, a service plan, network to which the device or network service usage activity is gaining access from, and/or other criteria/measures). In some embodiments, accounting for network capacity controlled services includes differentially collecting service usage for one or more network

capacity controlled service classes in which the accounting is modified/varies (e.g., dynamically) based on one or more of the following: network busy state (e.g., modify/credit accounting during network congestion not satisfying the user preference), network service activity, access network (e.g., the network to which the device/service activity is currently connected), user preference selection, time based criteria (e.g., current time of day/day of week/month), associated service plan, option to time window. In some embodiments, charging for network capacity controlled services includes mapping an accounting to a charging report. In some embodiments, charging for network capacity controlled services includes sending the charging report to a network element (e.g., a service controller, a service cloud, a billing interface/server, and/or another network element/function). In some embodiments, charging for network capacity controlled services includes mediating or arbitrating CDRs/IPDRs for network capacity controlled service(s) vs. other network service usage activities or bulk network service usage activities. In some embodiments, charging for network capacity controlled services includes converting a charging report to a billing record or billing action. In some embodiments, charging for network capacity controlled services includes generating a user notification of network capacity controlled service charges upon request or based a criteria/measure (e.g., a threshold charging level and/or a threshold network service usage level). In some embodiments, charging for network capacity controlled services includes charge by application based on a charging policy (e.g., bill by application according to billing policy rules, such as for billing to a user or to a sponsored service provider, carrier, and/or other entity).

[00230] Figure 21 illustrates another flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments. In some embodiments, DAS for protecting network capacity includes providing a device service access API that provides an interface for applications, OS functions, and/or other service usage activities to a network access connection (e.g., or stack) for providing differential network access for

protecting network capacity. In some embodiments, the differential network access is determined by one or more of the following: a service priority of the service usage activity and a network busy state. At 2102, the process begins. At 2104, a device service access API request is received. At 2106, the device service access API request is responded to. In some embodiments, the differential network access (e.g., for network capacity controlled services and/or based on network busy state and/or other criteria/measures) is implemented by one or more of the following: providing network busy state information to the service usage activity, receiving network busy state information, receiving network capacity demands for the service usage activity, receiving a scheduled time/time slot demand from the service usage activity, receiving and/or providing network location and/or physical location information (e.g., base station, communication channel, cell sector, roaming or non-roaming network to which the device is connected, and/or GPS or other physical location data), providing information to the service usage activity informing it when it is allowed to access the network, providing information to the service usage activity informing it what traffic controls must be applied/implemented, providing information to the service usage activity informing it when the network is available to it for access, and providing information to the service usage activity of its scheduled access time/time slot (e.g., based on one or more of the following: priority, network busy state, and time of day) (e.g., with a specified performance level or service level, such as data transfer size, speed, network capacity controlled service priority level, QoS level, data transfer type, scheduling time(s), and/or network connection parameters), and instructing the device and/or service usage activity to transition to a different state (e.g., power save state, sleep state dormant, idle, wait state, and/or an awake state). At 2108, differential network access is implemented. At 2110, the process is completed. In some embodiments, the device service access API is a programmatic interface, a virtual interface, and/or an emulated interface that provides instructions for differential access to a network to protect network capacity, as described herein.

[00231] In some embodiments, the API is served or located on the device, on a network element (e.g., using a secure communication between the device and the network element for the API communication, such as HTTPS, TLS, SSL, an encrypted data connection or SS7 control channel, and/or other well known secure communication techniques), and/or both/partly in both. In some embodiments, a network based API is an API that facilitates an API or other interface communication (e.g. secure communication as discussed above) between an application executing on the device and a network element and/or service cloud for protecting network capacity. For example, a network API can provide an interface for an application to communicate with a service cloud (e.g., network server) for obtaining network access control information (e.g., network busy state, multiple network information based on available networks and/or network busy state information of available networks, network capacity controlled service priorities and availability, scheduled time/time slots for network access based on network busy state, service plan, network capacity controlled service, and/or other criteria/measures). As another example, a network API can facilitate an application provider, central network/service provider, and/or a third party with access to communicate with the application to provide and/or request information (e.g., physical location of the application, network location of the application, network service usage information for the application, network busy state information provided to the application, and/or other criteria/measures). As yet another example, a network API can facilitate a broadcast to one or more applications, OS functions, and/or devices (e.g., partitioned based on geography, network, application, OS function, and/or any other criteria/measure) with network capacity related information (e.g., network busy state, availability based on network capacity controlled service classification and/or priority level, scheduled time/time slots for certain network capacity controlled service classification and/or priority level, emergency/high priority software/antimalware/vulnerability update and scheduled time/time slots for such software updates, and/or other criteria/measures). In some embodiments, the network access API for protecting network capacity is an open API or standard/required API (e.g., required or

standardized for applications for a certain network service provider, such as to be provided via the Verizon application store or the Apple AppStore) published for application and OS developers so that the applications and OS functions are designed to understand and implement the network access API for protecting network capacity. For example, a certification program can be established to provide application and OS developers with test specifications, working implementations, and/or criteria to make sure the network access API is properly implemented and is functioning in accordance with the specified requirements. In some embodiments, the network access API is an interface for communication with a service controller (e.g., service controller 122) or another network element/function (e.g., a service usage API for communication with a service usage server or billing interface/server or another network element/function that facilitates a secure communication for sending/receiving or otherwise communicating network access related information for protecting network capacity). In some embodiments, the network API provides for sponsored billing (e.g., reverse billing) of all, classified, and/or a subset of network service usage charges to a sponsored partner associated with the network service usage activity (e.g., application) that accesses the network API. In some embodiments, the network API provides for a sponsored service in which the network service usage activity (e.g., application) that accesses the network API provides a sponsored service partner credential to the network API, the credential is used as a billing mechanism to charge the sponsored partner, the user account is mediated to remove the sponsored partner charge, and the network API provides access service and/or information service (e.g., location information, local information, content information, network information, and/or any other information).

[00232] Figure 22 illustrates another flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments. At 2202, the process begins. At 2204, network service usage activities of a device are monitored (e.g., using a

verified/verifiable service processor). At 2206, a network busy state (e.g., a measure of network capacity, availability, and/or performance) is determined based on the monitored network service usage activities (e.g., using various techniques as described herein). In some embodiments, a service processor on the device is used to determine (e.g., measure and/or characterize) a network busy state experienced by the device (e.g., which can be used to determine the network access control policy for one or more network capacity controlled services). At 2208, a network busy state report is sent to a network element/function (e.g., a service controller and/or another network element/function as described herein). At 2210, the process is completed. In some embodiments, the service processor is verified using various techniques described herein. In some embodiments, the network busy state report includes one or more of the following: data rate, latency, jitter, bit error rate, packet error rate, number of access attempts, number of access successes, number of access failures, QoS level availability, QoS level performance, and variability in any of the preceding parameters. In some embodiments, the network busy state report includes one or more of the following: base station ID, cell sector ID, CDMA ID, FDMA channel ID, TDMA channel ID, GPS location, and/or physical location to identify the edge network element that is associated with the network busy state report to a network element. In some embodiments, the monitoring of network service usage activities includes measuring the network performance for traffic the device is transmitting/receiving and/or generating network performance testing traffic. In some embodiments, the network busy state is collected (e.g., and/or used to assist, supplement, and/or verify device based network busy state measures) by one or more network elements that can measure and/or report network busy state (e.g., BTS, BTSC, base station monitor, and/or airwave monitor). For example, airwave monitors and/or base station monitors can be provided to facilitate a reliable characterization of network busy state in a coverage area of one or more base stations and/or base station sectors, such as affixed mobile terminals (e.g., trusted terminals that can include additional network busy state monitoring and/or reporting

functionality) installed (e.g., temporarily or permanently) in the coverage area of one or more base stations and/or base station sectors (e.g., in which a sector is the combination of a directional antenna and a frequency channel) so that the affixed mobile terminals perform network busy state monitoring and reporting to the service controller, the local base station, and/or other network element(s)/function(s) as similarly described herein. In some embodiments, the permanently affixed mobile terminals provide network monitors for reporting, for example, network busy state, to a central network element, such as the service controller, which can, for example, aggregate such network busy state information to determine network busy state for one or more network coverage areas. In some embodiments, the permanently affixed mobile terminals are always present in these locations where installed and always on (e.g., performing network monitoring), and can be trusted (e.g., the permanently affixed mobile terminals can be loaded with various hardware and/or software credentials). For example, using the permanently affixed mobile terminals, a reliable characterization of network busy state can be provided, which can then be reported to a central network element and aggregated for performing various network busy state related techniques as described herein with respect to various embodiments. In some embodiments, the network element/function uses the network busy state report (e.g., and other network busy state reports from other devices connected to the same network edge element) to determine the network busy state for a network edge element connected to the device. In some embodiments, network element/function sends a busy state report for the network edge element to the device (e.g., and to other devices connected to the same network edge element), which the device can then use to implement differential network access control policies (e.g., for network capacity controlled services) based on the network busy state. In some embodiments, a network busy state is provided by a network element (e.g., service controller or service cloud) and broadcast to the device (e.g., securely communicated to the service processor).

[00233] Figure 23 illustrates a network capacity controlled services priority level chart for device assisted services (DAS) for protecting network capacity in accordance with some embodiments. In some embodiments, various applications, OS functions, and/or other utilities/tools installed/loaded onto and/or launched/executing/active on a communications device (e.g., device 100) are classified as network capacity controlled services for protecting network capacity. In some embodiments, one or more of the network capacity controlled services are assigned or classified with network capacity controlled service levels or priority levels for protecting network capacity. In some embodiments, one or more of the network capacity controlled services are dynamically assigned or classified with network capacity controlled service levels or priority levels based on one or more criteria/measures (e.g., dynamic criteria/measures), such as network busy state, current access network, time based criteria, an associated service plan, and/or other criteria/measures. In some embodiments, a higher priority level means that the application or utility/function is granted higher relative priority for network access (e.g., a priority level 10 can provide for guaranteed network access and a priority level 0 can provide a blocked network access, while priority levels between 1 through 9 can provide relatively increasing prioritized network access potentially relative to allocated network access and other services requesting network access).

[00234] As shown in Figure 23, the network capacity controlled services are dynamically assigned or classified with network capacity controlled service levels or priority levels based on the network busy state of the current access network. For example, an email application, Microsoft Outlook, is assigned different priority levels for protecting network capacity based on the network busy state, as shown: a priority level 6 for a network busy state (NBS) level of 10% (e.g., up to about 10% of the network capacity is being utilized based on current or recently/last measured/detected/determined network capacity/resources usage using various techniques as described herein), a priority level 5 for a network busy state (NBS) level of 25%, a priority level 4

for a network busy state (NBS) level of 50%, a priority level 3 for a network busy state (NBS) level of 75%, and a priority level 2 for a network busy state (NBS) level of 90%. As also shown, an antivirus (AV) software update application/utility/function is assigned different priority levels for protecting network capacity based on the network busy state: a priority level 9 for a network busy state (NBS) level of 10%, a priority level 7 for a network busy state (NBS) level of 25%, a priority level 5 for a network busy state (NBS) level of 50%, a priority level 3 for a network busy state (NBS) level of 75%, and a priority level 1 for a network busy state (NBS) level of 90%. Various other applications and utilities/functions are shown with various priority level assignments/classifications based on the network busy state levels shown in the network capacity controlled services priority level chart of Figure 23. As will be apparent to one of ordinary skill in the art, various assignments and/or techniques for dynamically assigning priority levels for network access based on network busy state levels can be applied for protecting network capacity (e.g., based on user preferences, service plans, access networks, a power state of device, a device usage state, time based criteria, and various other factors such as higher priority for urgent software and/or security updates, such as a high priority security or vulnerability software patch or update, and/or urgent or high priority emails or other communications, such as a 911 VOIP call).

[00235] Referring again to Figures 1 through 3, DAS for protecting network capacity is implemented using a service processor (e.g., a service processor 115) of the device (e.g., a device 100) using various DAS techniques as described herein to facilitate differential network service access control (e.g., for network capacity controlled services) to assist in protecting network capacity in accordance with some embodiments. In some embodiments, the service processor and/or one or more agents of the service processor is/are verified using one or more of the following verification techniques (e.g., and/or to specifically verify monitoring the network service usage activity, classifying one or more service activities into one or more network

capacity controlled service classes, associating the one or more network capacity controlled service classes with one or more differential service activity policies, and/or determining a network busy state): compare a network based service usage measure with a service policy and/or service plan associated with the device, compare a device assisted service usage measure with the service policy and/or service plan associated with the device, compare the network based service usage measure to the device assisted service usage measure, compare a first device assisted service usage measure to a second device assisted service usage measure, verify presence of the service processor and/or one or more agents of the service processor, verify configuration of the service processor, verify service usage activities are reported properly (e.g., using test service usages to generate service usage events/reports for analysis and confirmation), verify billing events are reported properly, compare the network based service usage measure with reported device billing data, verify reporting of a test billing event, verify reporting of the communications device reports billing events from a transaction server, verify presence of an activation tracking system, verify device configuration or operation, verify device standing or service plan standing, verify proper operation of the service processor, verify service processor heartbeat response reports, verify monitoring of a test service event, download a new service processor (e.g., and/or one or more agents or new configuration settings of the service processor) and perform integrity checks, verify a service processor code configuration with agent self-diagnosis checks, verify that the communications device uses the first service only after being authorized, verify user standing, verify a network busy state (e.g., compare and/or statistically process network busy state measures from more than one device in which the network busy state monitoring apparatus, for example, is located in a secure execution environment on the device), verify various differential network access control implementations (e.g., network capacity controlled services are properly monitored/determined/detected, controlled, accounted for, and/or charged for), verify various QoS implementations (e.g., as discussed above), and verify an agent communications log.

Various other verification techniques are described herein and similar and other verification techniques for providing DAS for protecting network capacity using device based implementations (e.g., service processors and/or other device based agents or software/hardware techniques) will now be apparent to one of ordinary skill in the art in view of the various embodiments described herein.

[00236] In some embodiments, the service processor is secured using various hardware and software techniques described herein, including, for example, implementing all and/or portions of the service processor in a secure virtual machine, protected execution environment, secure storage (e.g., secure memory), secure modem, and/or other secure implementation techniques as described herein and/or other or similar techniques as will now be apparent to one of ordinary skill in the art in view of the various embodiments described herein. For example, the service processor can be implemented in software and executed in a protected area of an OS executed on the device and/or executed in protected execution partitions (e.g., in CPU, APU, SIM chipset, modem, modem secure execution partition, SIM, other hardware function on the device, and/or any combination of the above).

[00237] In some embodiments, a network service usage counter is embedded into a secure execution environment (e.g., a program store in secure non-volatile memory located on a modem card and/or a modem chip not accessible by device applications, secure CPU environment for executing program and/or secure program operation for data path monitoring and/or control that cannot be bypassed by device applications to get to the modem connection to the network) in a device modem (e.g., using measurement points V, VI, and/or other measurement points of Figure 12). In some embodiments, the service usage counter counts data traffic (e.g., bytes and/or any other measure of service usage, such as file transactions, message transactions, connection time, time of connection or duration of connection, and/or traffic passed or transactions passed for a given QoS or network capacity controlled service

priority level), traffic as a function of time, traffic according to a network service activity classification (e.g., by application, destination/source, port, traffic type, content type, time of day, network busy state, and/or any other criteria/measure). In some embodiments, the service usage counter counts data traffic (e.g., as discussed above) while coordinating with a VPN layer established, for example, for both layer-III (e.g., IPSEC) and layer-II (e.g., L2TP tunnel) so that precise over the air service usage measure is counted for billing mediation and/or network service usage charging (e.g., customer billing, sponsored service bill by service and/or any other charging or billing). In some embodiments, the service usage counter counts data traffic (e.g., as discussed above) while coordinating with accelerator software (e.g., a compression/decompression engine) which transforms frames for more efficient over the air transmission. As similarly discussed above, service processor coordination with the accelerator layer facilitates a precise over the air service usage measure for billing mediation and/or network service usage charging. In some embodiments, the service usage counter counts data traffic (e.g., as discussed above) while coordinating with both the VPN layer and accelerator software layer to facilitate a precise over the air service usage measure for billing mediation and/or network service usage charging.

[00238] In some embodiments, the service usage counter reports the service usage to a network element (e.g., a service controller, charging gateway, PCRF, AAA, HA, billing system, mediation system, traffic accounting database, base station or base station controller, and/or another network element/function or central network element/function). In some embodiments, the information reported to the network element is encrypted or signed with a corresponding key known by the network element. In some embodiments, the communication link to the network element to pass the service usage count is conducted over a wireless network specific channel such as SMS, MMS, SS-7, or another specialized control channel. In some embodiments, the communications link to the network element to pass the service usage count is conducted over

a network channel (e.g., via IP, TCP, UDP, HTTP, HTTPS, TLS, SSL, point to point signed variants of TLS or SSL, or another data network channel via the network control channel connection to the device). In some embodiments, the data network control channel traffic is injected into the PPP stream at the modem. In some embodiments, the data network control channel traffic is passed up to the device networking stack for connection to the network. In some embodiments, a signed or encrypted service usage count from the modem subsystem is coordinated to provide a service usage count for a time period that also corresponds to a similar time period for a service processor heartbeat report that includes a service usage measure or count. For example, this provides the service controller or another network element with a secondary set of information that can be used to verify and/or secure the service usage measures reported by the service processor. Various techniques can be used to synchronize the time period for the modem service usage count and the service processor service usage count. For example, the service processor can request a latest count message from the modem, in which the modem counts all service usage since the previous request for latest count until the present request for latest count, encrypts the latest count message so that the service processor or other application software or OS software on the device cannot decode and/or tamper with the message, and the modem service usage counter then passes the encrypted message to the service processor. The service processor can then pass the encrypted service usage count message from the modem to the service controller along with the service processor service usage accounting message(s) for the same or similar time period. The service controller can then decode both service count messages from the secure modem subsystem and the service processor and correlate the two measures to verify the service usage reporting by, for example, looking for discrepancies that would indicate service usage control or charging errors or device service processor tampering. In some embodiments, the secure modem subsystem records byte counts for streams (e.g., and/or flows, socket connections, or combinations of IP destination/source/ports), potentially along with time of day, network busy

state, QoS level, and/or other criteria/measures, and reports these counts for each stream that had traffic activity during the current reporting interval. For example, the service controller can then correlate the stream service usage information with the service usage information provided by the service processor heartbeat service usage report to verify that the service processor service usage report is consistent with the independent measure made in the modem subsystem. In some embodiments, service usage reports (e.g., certified service usage reports) are correlated on the device and/or in the network (e.g., using one or more network elements/functions, such as the service controller).

[00239] In some embodiments, a deeper analysis of traffic can be conducted in the modem subsystem service usage count. For example, a layer 7 analysis of the service usage can be conducted for HTTP or HTTPS traffic flowing through the modem in which the modem subsystem service usage counter performs an HTTP level analysis of the traffic to associate web traffic gets and other transfers with a given higher level service classification (e.g., ad server, content server, proxy server, and/or traffic that is referred by the local host serving up a web page). In some embodiments, the modem subsystem service usage count can be augmented for HTTPS, SSL or TLS traffic by including a trusted proxy server embedded in the modem system. For example, the proxy server can be trusted by the device stack so that the encryption keys for HTTPS, TLS or SSL are known by the proxy server allowing the modem based proxy server, located, for example, in a secure execution environment, to perform layer 7 analysis of encrypted traffic in a manner similar to that described above. In some embodiments, the embedded proxy server generates server SSL certificates for each connection to a specific remote host in real time based on a root certificate trusted by the device (e.g., and/or by network service usage activity, such as by application) and also trusted by the embedded proxy server, and the proxy server then becomes a middle man emulating a remote SSL host on one side and emulating the device (e.g., and/or network service usage activity, such as application) on the

other side, decrypting the traffic, analyzing it and re-encrypting before forwarding to and from the remote host. Similarly, as in the case of layer 3 and 4 traffic analysis performed by the modem service usage counting subsystem, the layer 7 service usage count messages can be encrypted and passed to the service controller via various channels. In some embodiments, the layer 7 modem subsystem service usage counting system records service usage counts for a reporting time period that is similar to the reporting time period used by the service processor so that the service controller can correlate the service processor accounting messages against the modem accounting messages with layer 7 information.

[00240] In some embodiments, the secure service usage reporting system elements are located in a secure execution environment that includes the modem driver. In some embodiments, all traffic that gets to the modem for the network traffic being controlled or accounted for is required to go through the secure modem driver so that an independent count can be generated and reported to the service controller as described above without the need to embed the secure service usage counting and reporting elements in the modem.

[00241] In some embodiments, the secure service usage reporting system elements are located in a secure execution environment that includes the modem driver and modem hardware interface controller driver (e.g. USB controller for 2/3/4G and SDIO controller for WiFi). In some embodiments, all traffic that gets to the modem for the network traffic being controlled or accounted for is required to go through the secure modem driver and modem hardware interface controller driver (e.g. USB controller for 2/3/4G and SDIO controller for WiFi) so that precise count can be generated by either the modem driver and/or modem hardware interface controller driver (e.g. USB controller for 2/3/4G and SDIO controller for WiFi) and passed to the secure service usage reporting element to send it to the service controller for customer charging/billing. This scheme provides flexibility (e.g., most of the device software and operation system and its services/applications need not be located/executed in the secure

execution environment) while ensuring usage counting to occur securely as it pertains to the customer accounting and billing.

[00242] In some embodiments, the layer 7 proxy server traffic accounting and reporting techniques used for processing HTTPS, TLS, and SSL traffic, as discussed above, are also used in the service processor itself to allow a detailed accounting of encrypted layer 7 traffic by the device. In some embodiments, the information thus obtained is filtered so that private user information is not transmitted to the network (e.g., service controller, PCRF, and/or any other network element/function) but only service usage information sufficient to allow for accounting of service plan usage, to verify service control policy implementation, or to verify service charging policy implementation is transmitted to the network (e.g., service controller, PCRF, and/or any other network element/function). In some embodiments, the layer 7 proxy server for processing secure or in the clear device service usage accounting messages is located in secure hardware execution environments in the device application processor or within secure software partitions in the operating system.

[00243] Various techniques can be used to verify and/or secure service usage controls or service usage charging reports. For example, if the secondary service usage reports indicate that service usage is outside of the service usage policy limits that are intended to be in effect (e.g., based on a service plan and/or service policy associated with the device), then the service controller can indicate an error flag for further analysis and action (e.g., implementing various verification and responsive actions as described herein, such as blocking the activity, throttling the activity, quarantining the device, updating/replacing the service processor, and/or monitoring the device using various additional DAS and/or network assisted monitoring techniques). As another example, if the service usage reports from the service processor do not match up with the secondary service usage reports, then the service controller can indicate an error flag for further analysis and action. For example, the correlation can be based on bulk measures of

service usage (e.g., total bytes over a given period of time), or using finer grain measures of service usage (e.g., verifying the accounting between one group of service usage activities, such as application, destination/source, port, content type, time of day, network busy state, QoS level, and/or other criteria/measures) charged to one service plan charging record versus the accounting for another group of service usage activities charged to another service plan charging record. In some embodiments, the correlation process between the two service usage accounting reports is performed continuously on all device traffic in real time or near real time as the usage accounting reports are received. In some embodiments, the usage accounting reports are stored and analyzed or correlated later (e.g., periodically, based on a request or audit, and/or based on certain events, such as threshold network service usage events and/or any other events based on various criteria/measures). In some embodiments, only an audit of a portion of time is used to correlate the two usage accounting reports, which, for example, can reduce network traffic and/or network processing load in the service controller.

[00244] In some embodiments, correlation techniques are applied by the service controller to compare two different service usage measures as described above based on one or more of the following: total amount of data (e.g., bytes for file transfers, sessions, and/or other measures), amount of data per unit time, total number of accesses, number of accesses per unit time or frequency of accesses, accesses during a time interval (e.g., peak time), accesses during a network busy state, access requests, and individual versus group transmissions at a point in time (e.g., each for a given set of destinations or destinations and traffic types).

[00245] In some embodiments, service usage monitoring includes characterizing service usage activities by streams, flows, destination/port, packet inspection, and/or other criteria/measures using the various techniques as described herein and/or other or similar techniques as would be apparent to one of ordinary skill in the art. In some embodiments, service usage monitoring includes characterizing service usage activities by streams, flows, destination/port, packet

inspection, and/or other criteria/measures and then correlating to find network service usage behavior patterns that identify likely association of behavior with one or more service activities being managed.

[00246] In some embodiments, DAS for network capacity control includes classifying traffic to determine which network service usage activity(ies) are causing traffic (e.g., increasing network capacity/resources usage beyond a threshold), and then determining if access network service usage activity(ies) are violating any rules (e.g., service usage policies or service plan settings associated with the device/user). In some embodiments, DAS for network capacity control includes generating a list for network capacity controlled services that specifies behavioral characteristics for one or more network service usage activities with expected access limits based on access control policy for each managed network service usage activity (e.g., based on service usage policies or service plan settings associated with the device/user). In some embodiments, DAS for network capacity control includes monitoring and/or controlling network service usage activities based on limits, which, for example, can be based on one or more of the following: total access traffic counters, counters for different types of access traffic, destinations, ports, frequency of accesses, access behavior during a given time, access behavior during a given busy state, access behavior for groups of activities (e.g., verify clumping), and/or other criteria/measures.

[00247] Accordingly, in some embodiments, a second secure and trusted service usage measure is provided that the service controller (e.g., or another network element/function) can use to verify or secure the service control or service charging reports for the service processor. In some embodiments, the secure and trusted service usage measure also provides for enhanced verification and service security in cases, in which, for example, network based service usage measures are available for additional correlation with the service processor service usage reports. In cases in which network based service usage measures are either not

available or are only available at widely spaced time intervals (e.g., roaming networks or other networks with no timely network based service usage measure), these techniques facilitate real time or near real time verification or security for the device assisted service controls and charging.

[00248] In some embodiments, a SIM card performs a portion or all of the secure environment processing described above, with the device modem traffic, or a copy of the device modem traffic, being directed to the SIM secure subsystem for traffic accounting and reporting. In some embodiments, a SIM card is used to store QoS classifications and/or network capacity controlled services classifications for various service usage activities so that the user behavior in using certain network service usage activities and/or the user preferences in controlling certain network service usage activities do not need to be relearned or redownloaded as the user swaps the SIM between different devices. In some embodiments, the SIM keeps a local record of service usage activity for multiple devices that belong to the user or the user family plan, so that the service usage notification and policies can be immediately updated on a given device as the user swaps the SIM from device to device. In some embodiments, the manner in which this service usage history is stored on the SIM is secure so that it cannot be tampered with. In some embodiments, the SIM card is used to implement various application management and/or traffic control techniques described herein. In some embodiments, the SIM card is used to inspect traffic, classify traffic, create reports (e.g., certified service activity usage reports), encrypt the report, send the report to a network element/function, and the network element/function correlates the reports (e.g., using network assisted measures for comparisons and/or using various other techniques as described herein). In some embodiments, a SIM card performs a portion or all of the secure environment processing described above using one or more modem measurement points. For example, the traffic that is to be classified can be routed through the SIM and correlated with what is measured by the

modem. In some embodiments, network assisted/based network service usage activity classifications are compared SIM based/assisted classifications for service usage monitoring/reporting verification (e.g., detected inconsistencies in monitored/reported network service usage activities can be identified, such as based on total traffic, streams/flows/sockets activities, and/or other criteria/measures). In some embodiments, the reports include a verified sequence so that reports cannot be spoofed and/or missing reports can be determined.

[00249] In some embodiments, a portion or all of the secure environment processing described above are applied to implement and/or verify QoS for DAS techniques and/or DAS for network capacity controlled services techniques as described herein.

[00250] In some embodiments, the reports include one or more of the following: a number of times the device is cycled from or to a power cycle state in the modem, a number of times during a time window or network busy state, a power cycle versus number of streams initiated during the cycle, and a power cycle versus the streams that are transmitted during that cycle, In some embodiments, device power cycle events trigger generating of a report.

[00251] In some embodiments, monitoring, reporting, control, accounting, charging, and/or policy implementation for network capacity controlled services is verified (e.g., using various verification techniques described herein). If any of the verification techniques determine or assist in determining that the network capacity controlled services monitoring, reporting, control, accounting, and/or charging, and/or policy implementation has been tampered with, disabled, and/or is not properly implemented or functioning, then responsive actions can be performed, for example, the device (e.g., and/or suspect services) can be suspended, quarantined, killed/terminated, and/or flagged for further analysis/scrutiny to determine whether the device is malfunctioning, needs updating, has been tampered with or compromised, is infected with malware, and/or if any other problem exists.

[00252] In some embodiments, the service processor monitors a network service usage activity of a device. In some embodiments, monitoring of the service usage activity includes monitoring for multiple networks (e.g., to determine which networks are available and/or a network busy state of the available networks). In some embodiments monitoring a network service usage activity is performed by and/or assisted by a service cloud (e.g., one or more network elements that provide such a service). In some embodiments, monitoring the network service usage activity includes identifying the network service usage activity, measuring the network service usage of the network service usage activity, and/or characterizing the network service usage of the network service usage activity (e.g., using device assisted/based techniques, network assisted/based techniques, testing/offline monitoring/analysis techniques, and/or a combination thereof).

[00253] In some embodiments, the service processor implements differential network access service control (e.g., for network capacity controlled services), network service usage accounting, network service usage charging, and/or network service usage notification on the device to facilitate DAS for protecting network capacity.

[00254] In some embodiments, the service processor (e.g., a service processor 115) is updated, communicated with, set, and/or controlled by a network element (e.g., a service controller 122). In some embodiments, the service processor receives service policy information from a network function selected from a base station (e.g., a base station 125), a RAN gateway, a core gateway, a DPI gateway, a home agent (HA), a AAA server (e.g., AAA server 121), a service controller, and/or another network function or combinations of network functions as described herein and/or as will now be apparent to one of ordinary skill in the art in view of the various embodiments described herein. In some embodiments, the service processor is updated through over the air or over the network OS software updates or application software updates or device firmware updates. In some embodiments, the service

processor uses an IP connection, SMS connection, and/or MMS connection, for a control channel with a service controller. In some embodiments, the service processor queries a service controller to determine the association of a monitored network service usage activity with a network service usage control policy. In some embodiments, the device (e.g., service processor) maintains a network capacity controlled services list and/or network capacity controlled services policy for one or more of the active services (e.g., actively executing and/or previously installed/downloaded to the device) that have been classified as a network capacity controlled service (e.g., as the number of applications continues to grow, as hundreds of thousands of applications are already available on certain platforms, maintaining a list specific and/or a set of policies unique or specific to each application is not efficient). In this embodiment, when a new application is active/launched and/or downloaded to the device, the device can request an updated network capacity controlled services list and/or an updated network capacity controlled services policy accordingly (e.g., and/or periodically refresh such lists/policies).

[00255] In some embodiments, differential network access control for protecting network capacity includes controlling network services traffic generated by the device (e.g., network capacity controlled services based on a network service usage control policy (e.g., a network capacity controlled services policy). In some embodiments, differential network access control for protecting network capacity includes providing assistance in control of the distribution of bandwidth among devices, network capacity controlled services (e.g., applications, OS operations/functions, and various other network services usage activities classified as network capacity controlled services), a differentiated QoS service offering, a fair sharing of capacity, a high user load network performance, and/or preventing one or more devices from consuming so much network capacity that other devices cannot receive adequate performance or performance in accordance with various threshold and/or guaranteed service levels. In some embodiments,

differential network access control for protecting network capacity includes applying policies to determine which network the service activity should be connected to (e.g., 2G, 3G, 4G, home or roaming, WiFi, cable, DSL, fiber, wired WAN, and/or another wired or wireless or access network), and applying differential network access control rules (e.g., traffic control rules) depending on which network to which the service activity is connected. In some embodiments, differential network access control for protecting network capacity includes differentially controlling network service usage activities based on the service usage control policy and a user input (e.g., a user selection or user preference). In some embodiments, differential network access control for protecting network capacity includes differentially controlling network service usage activities based on the service usage control policy and the network the device or network service activity is gaining access from.

[00256] In some embodiments, the network service usage control policy is dynamic based on one or more of the following: a network busy state, a time of day, which network the service activity is connected to, which base station or communication channel the service activity is connected to, a user input, a user preference selection, an associated service plan, a service plan change, an application behavior, a messaging layer behavior, random back off, a power state of device, a device usage state, a time based criteria (e.g., time/day/week/month, hold/delay/defer for future time slot, hold/delay/defer for scheduled time slot, and/or hold/delay/defer until a busy state/availability state/QoS state is achieved), monitoring of user interaction with the service activity, monitoring of user interaction with the device, the state of UI priority for the service activity, monitoring the power consumption behavior of the service activity, modem power cycling or power control state changes, modem communication session set up or tear down, and/or a policy update/modification/change from the network. In some embodiments, the network service usage control policy is based on updated service usage behavior analysis of the network service usage activity. In some embodiments, the network

service usage control policy is based on updated activity behavior response to a network capacity controlled service classification. In some embodiments, the network service usage control policy is based on updated user input/preferences (e.g., related to policies/controls for network capacity controlled services). In some embodiments, the network service usage control policy is based on updates to service plan status. In some embodiments, the network service usage control policy is based on updates to service plan policies. In some embodiments, the network service usage control policy is based on availability of alternative networks. In some embodiments, the network service usage control policy is based on policy rules for selecting alternative networks. In some embodiments, the network service usage control policy is based on network busy state or availability state for alternative networks. In some embodiments, the network service usage control policy is based on specific network selection or preference policies for a given network service activity or set of network service activities.

[00257] In some embodiments, associating the network service usage activity with a network service usage control policy or a network service usage notification policy, includes dynamically associating based on one or more of the following: a network busy state, a time of day, a user input/preference, an associated service plan (e.g., 25 MB data plan, 5G data plan, or an unlimited data plan or other data/service usage plan), an application behavior, a messaging layer behavior, a power state of device, a device usage state, a time based criteria, availability of alternative networks, and a set of policy rules for selecting and/or controlling traffic on one or more of the alternative networks.

[00258] In some embodiments, a network service usage control policy (e.g., a network capacity controlled services policy) includes defining the network service usage control policy for one or more service plans, defining network access policy rules for one or more devices or groups of devices in a single or multi-user scenarios such as family and enterprise plans, defining network access policy rules for one or more users or groups of users, allowing or disallowing network

access events or attempts, modulating the number of network access events or attempts, aggregating network access events or attempts into a group of access events or attempts, time windowing network access events or attempts, time windowing network access events or attempts based on the application or function being served by the network access events or attempts, time windowing network access events or attempts to pre-determined time windows, time windowing network access events or attempts to time windows where a measure of network busy state is within a range, assigning the allowable types of access events or attempts, assigning the allowable functions or applications that are allowed network access events or attempts, assigning the priority of one or more network access events or attempts, defining the allowable duration of network access events or attempts, defining the allowable speed of network access events or attempts, defining the allowable network destinations for network access events or attempts, defining the allowable applications for network access events or attempts, defining the QoS rules for one or more network access events or attempts, defining or setting access policy rules for one or more applications, defining or setting access policy rules for one or more network destinations, defining or setting access policy rules for one or more devices, defining or setting access policy rules for one or more network services, defining or setting access policy rules for one or more traffic types, defining or setting access policy rules for one or more QoS classes, and defining or setting access policy rules based on any combination of device, application, network destination, network service, traffic type, QoS class, and/or other criteria/measures.

[00259] In some embodiments, a network service usage control policy (e.g., a network capacity controlled services policy) includes a traffic control policy. In some embodiments, the traffic control policy includes a traffic control setting. In some embodiments, the traffic control policy includes a traffic control/tier, and the traffic control/tier includes the traffic control setting. In some embodiments, the traffic control policy includes one or more of the following: block/allow

settings, throttle settings, adaptive throttle settings, QoS class settings including packet error rate, jitter and delay settings, queue settings, and tag settings (e.g., for packet tagging certain traffic flows). In some embodiments, QoS class settings, include one or more of the following: throttle level, priority queuing relative to other device traffic, time window parameters, and hold or delay while accumulating or aggregating traffic into a larger stream/burst/packet/group of packets. In some embodiments, the traffic control policy includes filters implemented as indexes into different lists of policy settings (e.g., using cascade filtering techniques), in which the policy filters include one or more of the following: a network, a service plan, an application, a time of day, and a network busy state. For example, a two dimensional traffic control implementation scheme can be provided using a network busy state and/or a time of day as an index into a traffic control setting (e.g., a certain application's priority level can be increased or decreased based on a network busy state and/or time of day). In some embodiments, the traffic control policy is used for selecting the network from a list of available networks, blocking or reducing access until a connection is made to an alternative network, and/or modifying or replacing a network stack interface of the device to provide for intercept or discontinuance of network socket interface messages to applications or OS functions.

[00260] In some embodiments, a traffic control setting is selected based on the network service usage control policy. In some embodiments, the traffic control setting is implemented on the device based on the network service usage control policy. In some embodiments, the implemented traffic control setting controls traffic/traffic flows of a network capacity controlled service. In some embodiments, the traffic control setting is selected based on one or more of the following: a time of day, a day of week, a special time/date (e.g., a holiday or a network maintenance time/date), a network busy state, a priority level associated with the network service usage activity, a QoS class associated with the network service usage activity (e.g., emergency traffic), which network the network service activity is gaining access from, which

networks are available, which network the network service activity is connected to, which base station or communication channel the network service activity is connected to, and a network dependent set of traffic control policies that can vary depending on which network the service activity is gaining access from (e.g., and/or various other criteria/measures as described herein). In some embodiments, the traffic control setting includes one or more of the following: allow/block, delay, throttle, QoS class implementation, queue, tag, generate a user notification, random back off, clear to send received from a network element, hold for scheduled transmission time slot, selecting the network from the available networks, and blocking or reducing access until a connection is made to an alternative network. In some embodiments, the traffic control setting is selected based on a network capacity controlled services priority state of the network service usage activity and a network busy state. In some embodiments, the traffic control setting is selected based on a network capacity controlled services priority state of the network service usage activity and a network busy state and is global (e.g., the same) for all network capacity controlled services activities or varies based on a network service usage activity priority, user preferences or option selection, an application, a time based criteria, a service plan, a network the device or service activity is gaining access from, a redetermination of a network congestion state after adapting to a previously determined network busy state, and/or other criteria/measures as described herein.

[00261] In some embodiments, network capacity controlled services traffic (e.g., traffic flows) is differentially controlled for protecting network capacity. For example, various software updates for an OS and one or more applications on the device can be differentially controlled using the various techniques described herein. As another example, security/antimalware software (e.g., antivirus, firewall, content protection, intrusion detection/prevention, and/or other security/antimalware software) can be differentially controlled using the various techniques described herein. As yet another example, network backups/imaging, content downloads (e.g.,

exceeding a threshold individually and/or in aggregate, such as for image, music, video, eBook content, email attachments, content/media subscriptions, RSS/news feeds, text/image/video chat, software updates, and/or other content downloads) can be differentially controlled using the various techniques described herein.

[00262] For example, using the DAS for protecting network capacity techniques described herein an adaptive policy control for protecting network capacity can be provided. A network capacity controlled services list can be generated, updated, reported, and/or received by the device and stored on the device (e.g., the list can be based on adapted to the service plan associated with the device). If a monitored network service usage activity is not on the list, then the device can report the monitored network service usage activity to a network element (e.g., for a monitored network service usage activity that also exceeds a certain threshold, based on a network busy state, based on a time based criteria, and/or other criteria/measure). As an example, monitored network service usage activity can be reported if/when the monitored network service usage activity exceeds a data usage threshold (e.g., 50 MB total data usage per day, a socket opening frequency/rate, velocity of data usage at an instant in time, or more complicated thresholds over time, over peak periods, by content and time, by various other parameters/thresholds). As another example, the monitored network service usage activity can be reported based on testing of the network service usage behavior and/or application developer characterization input. The report can include information that identifies the network service usage activity and various network service usage parameters.

[00263] In some embodiments, a notification setting is selected based on a service usage notification policy. In some embodiments, a notification setting includes a user notification setting (e.g., various user notifications settings as described above with respect to Figure 18).

[00264] In some embodiments, classifying the network service usage activity further includes classifying the network service usage activity (e.g., using a usage threshold filter and/or

cascading filter techniques) into one or more of a plurality of classification categories for differential network access control for protecting network capacity. In some embodiments, classifying the network service usage activity, further includes classifying the network service usage activity into one or more network capacity controlled services in which the network capacity controlled services include one or more of the following: applications requiring data network access, application software updates, applications requiring network information, applications requiring GPS or physical location, operating system software updates, security software updates, network based backups, email downloads, and a set of activities configured as network capacity controlled service activities based on a service profile and/or user input (e.g., and/or various other types of network service usage activities as described herein and as will now be apparent to one of ordinary skill in the art). For example, network capacity controlled services can include software updates for OS and applications, OS background network accesses, cloud synchronization services, RSS feeds & other background information feeds, browser/application/device behavior reporting, background email downloads, content subscription service updates and downloads (e.g., music/video downloads, news feeds), text/voice/video chat clients, security updates (e.g., antimalware updates), peer to peer networking application updates, inefficient network access sequences during frequent power cycling or power save state cycling, large downloads or other high bandwidth accesses, and greedy application programs that constantly/repeatedly access the network with small transmissions or requests for information. In some embodiments, a network capacity controlled services list is static, adaptive, generated using a service processor, received from a network element (e.g., service controller or service cloud), received from a network element (e.g., service controller or service cloud) and based at least in part on device activity reports received from the service processor, based on criteria set by pre-testing, report of behavior characterization performed by the application developer, and/or based at least in part on user

input. In some embodiments, the network capacity controlled services list includes one or more network service activity background (QoS) classes.

[00265] In some embodiments, classifying the network service usage activity further includes classifying the network service usage activity based on one or more of the following: application or widget (e.g., Outlook, Skype, iTunes, Android email, weather channel weather widget, iCal, Firefox Browser, etc), application type (e.g., user application, system application/utility/function/process, OS application/utility/function/process, email, browser, widget, malware (such as a virus or suspicious process), RSS feed, device synchronization service, download application, network backup/imaging application, voice/video chat, peer to peer content application or other peer to peer application, streaming media feed or broadcast reception/transmission application, network meeting application, chat application or session, and/or any other application or process identification and categorization), OS/system function (e.g., any system application/utility/function/process and/or OS application/utility/function/process, such as a OS update and/or OS error reporting), modem function, network communication function (e.g., network discovery or signaling, EtherType messages, connection flow/stream/session set up or tear down, network authentication or authorization sequences, IP address acquisition, and DNS services), URL and/or domain, destination/source IP address, protocol, traffic type, socket (e.g., IP address, protocol, and/or port), socket address/label/identifier (e.g., port address/port number), content type (e.g., email downloads, email text, video, music, eBooks, widget update streams, and download streams), port (e.g., port number), QoS classification level, time of day, on peak or off peak, network time, network busy state, access network selected, service plan selected, user preferences, device credentials, user credentials, and/or status, modem power cycling or power state changes, modem authentication processes, modem link set up or tear down, modem management communications, modem software or firmware updates, modem power management

information, device power state, and modem power state. In some embodiments, classifying the network service usage activity further includes associating the classified network service usage activity with an ID (e.g., an application ID, which can be, for example, a unique number, name, and/or signature). In some embodiments, classifying the network service usage activity further includes classifying the network service usage activity using a plurality of classification parameters, including one or more of the following: application ID, remote IP (e.g., URL, domain, and/or IP address), remote port, protocol, content type, a filter action class (e.g., network busy state class, QoS class, time of day, network busy state, and/or other criteria/measures), and access network selected. In some embodiments, classifying the network service usage activity further includes using a combination of parameters as discussed above to determine the classification of the network service usage activity.

[00266] In some embodiments, classifying the network service usage activity further includes classifying the network service usage activity as a network capacity controlled service, a non-network capacity controlled service, a blocked or disallowed service, and/or a not yet classified/identified service (e.g., unknown/yet to be determined classification or pending classification). In some embodiments, an application connection, OS connection, and/or other service activity is classified as a network capacity controlled service activity when the device has been inactive (e.g., or in a power save state) for a period of time (e.g., when the user has not interacted with it for a period of time, when it has not displayed user notification policy, and/or a user input has not been received for a period of time, and/or when a power save state is entered). In some embodiments, an application connection, OS connection, and/or other service activity is classified as a network capacity controlled service activity when the monitored network service usage activity exceeds a data usage threshold for more than one application connection, OS connection, and/or other service activity (e.g., aggregated data usage exceeds the data usage threshold); or for a specific application connection. In some embodiments, an

application connection, OS connection, and/or other service activity is classified as a network capacity controlled service activity when the monitored network service usage activity exceeds a data usage threshold based on a predetermined list of one or more data usage limits, based on a list received from a network element, usage time limit (e.g., based on a period of time exceeding a usage limit), and/or based on some other usage related criteria/measures. In some embodiments, classifying the network service usage activity further includes classifying the network service usage activity as a network capacity controlled service based on a network peak time, a network busy state, or a network connection to the device falls below a certain performance level (e.g., higher/lower priorities assigned based on various such criteria/other input/factors).

[00267] In some embodiments, one or more of the network capacity controlled services are associated with a different network access policy set for one or more networks and/or one or more alternative networks. In some embodiments, one or more of the network capacity controlled services are associated with a different notification policy set for one or more networks and/or one or more alternative networks. In some embodiments, the network capacity controlled services list is stored on the device. In some embodiments, the network capacity controlled services list is received/periodically updated from a network element and stored on the device. In some embodiments, the network capacity controlled services list includes network capacity controlled services, non-network capacity controlled services (e.g., foreground services or services based on various possibly dynamic criteria are not classified as network capacity controlled services), and an unclassified set of services (e.g., grey list including one or more network service activities pending classification based on further analysis and/or input, such as from a network element, service provider, and/or user). In some embodiments, the network capacity controlled services list is based on one or more of the following: predefined/predesignated (e.g., network, service plan, pre-test and/or characterized by an

application developer) criteria; device assisted/based monitoring (e.g., using a service processor); network based monitoring (e.g., using a DPI gateway); network assisted analysis (e.g., based on device reports of DAS activity analysis). For example, the device can report device monitored network service usage activities (e.g., all monitored network service usage activities or a subset based on configuration, threshold, service plan, network, and/or user input) to the network element. As another example, the network element can update the network capacity controlled services list and send the updated list to the device. As yet another example, the network element can perform a statistical analysis of network service activities across a plurality of devices based on the device based and/or network based network service usage activity monitoring/reporting. In some embodiments, a network service usage activity is determined to be an active application or process (e.g., based on a user interaction with the device and/or network service usage activity, such as a pop-up and/or other criteria/measures).

[00268] In some embodiments, implementing traffic control for network capacity controlled services is provided using various techniques. In some embodiments, the device includes a service processor agent or function to intercept, block, modify, remove or replace UI messages, notifications or other UI communications generated by a network service activity that whose network service usage is being controlled or managed (e.g., using various measurement points as shown in and described with respect to Figures 12 and 13). For example, this technique can be used to provide for an improved user experience (e.g., to prevent an application that is being controlled for protecting network capacity from generating repeated and/or confusing messages/alerts to the user). In some embodiments, a network stack interface of the device is replaced or modified to provide for intercept or discontinuance of network socket interface messages to applications or OS functions or other functions/software.

[00269] In some embodiments, implementing traffic control for network capacity controlled services using DAS techniques is provided using various techniques in which the network

service usage activity is unaware of network capacity control (e.g., does not support an API or other interface for implementing network capacity control). For example, network service application messaging interface based techniques can be used to implement traffic control. Example network service application messaging interfaces include the following: network stack API, network communication stream/flow interface, network stack API messages, EtherType messages, ARP messages, and/or other messaging or other or similar techniques as will now be apparent to one of ordinary skill in the art in view of the various embodiments described herein. In some embodiments, network service usage activity control policies or network service activity messages are selected based on the set of traffic control policies or service activity messages that result in reduced or modified user notification by the service activity due to network capacity controlled service policies applied to the network service activity. In some embodiments, network service usage activity control policies or network service activity messages are selected based on the set of traffic control policies or service activity messages that result in reduced disruption of device operation due to network capacity controlled service activity policies applied to the network service activity. In some embodiments, network service usage activity control policies or network service activity messages are selected based on the set of traffic control policies or service activity messages that result in reduced disruption of network service activity operation due to network capacity controlled service activity policies applied to the network service activity. In some embodiments, implementing traffic control for network capacity controlled services is provided by intercepting opens/connects/writes. In some embodiments, implementing traffic control for network capacity controlled services is provided by intercepting stack API level or application messaging layer requests (e.g., socket open/send requests). For example, an intercepted request can be copied (e.g., to memory) and queued (e.g., delayed or throttled) or dropped (e.g., blocked). As another example, an intercepted request can be copied into memory and then a portion of the transmission can be retrieved from memory and reinjected (e.g., throttled). As yet another example, intercepting messaging

transmissions can be parsed inline and allowed to transmit (e.g., allowed), and the transmission or a portion of the transmission can be copied to memory for classifying the traffic flow. In some embodiments, implementing traffic control for network capacity controlled services is provided by intercepting or controlling or modulating UI notifications. In some embodiments, implementing traffic control for network capacity controlled services is provided by killing or suspending the network service activity. In some embodiments, implementing traffic control for network capacity controlled services is provided by deprioritizing the process(es) associated with the service activity (e.g., CPU scheduling deprioritization).

[00270] In some embodiments, implementing traffic control for network capacity controlled services using DAS techniques for network service usage activities that are unaware of network capacity control is provided by emulating network API messaging (e.g., effectively providing a spoofed or emulated network API). For example, an emulated network API can intercept, modify, block, remove, and/or replace network socket application interface messages and/or EtherType messages (e.g., EWOULDBLOCK, ENETDOWN, ENETUNREACH, EHOSTDOWN, EHOSTUNREACH, EALRADY, EINPROGRESS, ECONNREFUSED, EINPROGRESS, ETIMEDOUT, and/other such messages). As another example, an emulated network API can modify, swap, and/or inject network socket application interface messages (socket(), connect(), read(), write(), close(), and other such messages) that provide for control or management of network service activity service usage behavior. As yet another example, before a connection is allowed to be opened (e.g., before a socket is opened), transmission, or a flow/stream is initiated, it is blocked and a message is sent back to the application (e.g., a reset message in response to a sync request or another message that the application will understand and can interpret to indicate that the network access attempt was not allowed/blocked, that the network is not available, and/or to try again later for the requested network access). As yet another example, the socket can be allowed to open but after some point in time (e.g., based on network

service usage, network busy state, time based criteria, and/or some other criteria/measure), the stream is blocked or the socket is terminated. As yet another example, time window based traffic control techniques can be implemented (e.g., during non-peak, not network busy state times), such as by allowing network access for a period of time, blocking for a period of time, and then repeating to thereby effectively spread the network access out either randomly or deterministically. Using these techniques, an application that is unaware of network capacity control based traffic control can send and receive standard messaging, and the device can implement traffic controls based on the network capacity control policy using messaging that the network service usage activity (e.g., application or OS or software function) can understand and will respond to in a typically predictable manner as would now be apparent to one of ordinary skill in the art.

[00271] In some embodiments, implementing traffic control for network capacity controlled services using DAS techniques is provided using various techniques in which the network service usage activity is aware of network capacity control (e.g., the network service usage activity supports an API or other interface for implementing network capacity control). For example, a network access API as described herein can be used to implement traffic control for network capacity controlled services. In some embodiments, the API facilitates communication of one or more of the following: network access conditions, network busy state or network availability state of one or more networks or alternative networks, one or more network capacity controlled service policies (e.g., the network service can be of a current network access setting, such as allow/block, throttle, queue, scheduled time/time slot, and/or defer, which can be based on, for example, a current network, a current network busy state, a time based criteria, a service plan, a network service classification, and/or other criteria/measures), a network access request from a network service activity, a query/polled request to a network service activity, a network access grant to a network service activity (e.g., including a priority setting and/or network

capacity controlled service classification, a scheduled time/time slot, an alternative network, and/or other criteria/measures), a network busy state or a network availability state or a network QoS state.

[00272] In some embodiments, implementing traffic control for network capacity controlled services using network assisted/based techniques is provided using various techniques in which the network service usage activity is unaware of network capacity control (e.g., does not support an API or other interface for implementing network capacity control). In some embodiments, DPI based techniques are used to control network capacity controlled services (e.g., to block or throttle network capacity controlled services at a DPI gateway).

[00273] In some embodiments, implementing traffic control for network capacity controlled services using network assisted/based techniques is provided using various techniques in which the network service usage activity is aware of network capacity control (e.g., does support an API or other interface for implementing network capacity control). In some embodiments, the application/messaging layer (e.g., a network API as described herein) is used to communicate with a network service activity to provide associated network capacity controlled service classifications and/or priorities, network busy state information or network availability of one or more networks or alternative networks, a network access request and response, and/other criteria/measures as similarly described herein.

[00274] In some embodiments, DAS for protecting network capacity includes implementing a service plan for differential charging based on network service usage activities (e.g., including network capacity controlled services). In some embodiments, the service plan includes differential charging for network capacity controlled services. In some embodiments, the service plan includes a cap network service usage for network capacity controlled services. In some embodiments, the service plan includes a notification when the cap is exceeded. In some embodiments, the service plan includes overage charges when the cap is exceeded. In some

embodiments, the service plan includes modifying charging based on user input (e.g., user override selection as described herein, in which for example, overage charges are different for network capacity controlled services and/or based on priority levels and/or based on the current access network). In some embodiments, the service plan includes time based criteria restrictions for network capacity controlled services (e.g., time of day restrictions with or without override options). In some embodiments, the service plan includes network busy state based criteria restrictions for network capacity controlled services (e.g., with or without override options). In some embodiments, the service plan provides for network service activity controls to be overridden (e.g., one time, time window, usage amount, or permanent) (e.g., differentially charge for override, differentially cap for override, override with action based UI notification option, and/or override with UI setting). In some embodiments, the service plan includes family plan or multi-user plan (e.g., different network capacity controlled service settings for different users). In some embodiments, the service plan includes multi-device plan (e.g., different network capacity controlled service settings for different devices, such as smart phone v. laptop v. net book v. eBook). In some embodiments, the service plan includes free network capacity controlled service usage for certain times of day, network busy state(s), and/or other criteria/measures. In some embodiments, the service plan includes network dependent charging for network capacity controlled services. In some embodiments, the service plan includes network preference/prioritization for network capacity controlled services. In some embodiments, the service plan includes arbitration billing to bill a carrier partner or sponsored service partner for the access provided to a destination, application, or other network capacity controlled service. In some embodiments, the service plan includes arbitration billing to bill an application developer for the access provided to a destination, application or other network capacity controlled service.

[00275] In some application scenarios, excess network capacity demand can be caused by modem power state changes on the device. For example, when an application or OS function attempts to connect to the network for any reason when the modem is in a power save state wherein the modem is not connected to the network, it can cause the modem to change power save state, reconnect to the network, and then initiate the application network connection. In some cases, this can also cause the network to re-initiate a modem connection session (e.g., PPP session) which in addition to the network capacity consumed by the basic modem connection also consumes network resources for establishing the PPP session. Accordingly, in some embodiments, network service usage activity control policies are implemented that limit or control the ability of applications, OS functions, and/or other network service usage activities (e.g., network capacity controlled services) from changing the modem power control state or network connection state. In some embodiments, a service usage activity is prevented or limited from awakening the modem, changing the power state of the modem, or causing the modem to connect to the network until a given time window is reached. In some embodiments, the frequency a service usage activity is allowed to awakening the modem, changing the power state of the modem, or causing the modem is limited. In some embodiments, a network service usage activity is prevented from awakening the modem, changing the power state of the modem, or causing the modem until a time delay has passed. In some embodiments, a network service usage activity is prevented from awakening the modem, changing the power state of the modem, or causing the modem until multiple network service usage activities require such changes in modem state, or until network service usage activity is aggregated to increase network capacity and/or network resource utilization efficiency. In some embodiments, limiting the ability of a network service usage activity to change the power state of a modem includes not allowing the activity to power the modem off, place the modem in sleep mode, or disconnect the modem from the network. In some embodiments, these limitations on network service usage activity to awaken the modem, change the power state of the modem, or cause the

modem to connect to a network are set by a central network function (e.g., a service controller or other network element/function) policy communication to the modem. In some embodiments, these power control state policies are updated by the central network function.

[00276] FIG. 24 depicts a diagram of a network capacity protection system 2400 utilizing device-assisted services (DAS). The system 2400 includes wireless devices 2402-1 to 2402-N (referred to collectively as the wireless devices 2402), wireless networks 2404-1 to 2404-N (referred to collectively as the wireless networks 2404), a network traffic analysis engine 2406, a network service usage classification engine 2408, and a differential network access control engine 2410.

[00277] The wireless devices 2402 will at a minimum include a processor, memory (though the memory could be implemented in the processor), a radio, and a radio interface (though the radio interface could be implemented as "part of" the radio). In order to make the wireless devices 2402 useful, they will typically have at least one input device and at least one output device, including input and output interfaces, if applicable.

[00278] The wireless devices 2402 can be implemented as stations. A station, as used herein, may be referred to as a device with a media access control (MAC) address and a physical layer (PHY) interface to the wireless medium that comply with, e.g., the IEEE 802.11 standard. A station can be described as "IEEE 802.11-compliant" when compliance with the IEEE 802.11 standard is intended to be explicit. (I.e, a device acts as described in at least a portion of the IEEE 802.11 standard.) One of ordinary skill in the relevant art would understand what the IEEE 802.11 standard comprises today and that the IEEE 802.11 standard can change over time, and would be expected to apply techniques described in this paper in compliance with future versions of the IEEE 802.11 standard if an applicable change is made. IEEE Std 802.11™-2007 (Revision of IEEE Std 802.11-1999) is incorporated by reference. IEEE

802.11k-2008, IEEE 802.11n-2009, IEEE 802.11p-2010, IEEE 802.11r-2008, IEEE 802.11w-2009, and IEEE 802.11y-2008 are also incorporated by reference.

[00279] In alternative embodiments, one or more of the wireless devices 2402 may comply with some other standard or no standard at all, and may have different interfaces to a wireless or other medium. It should be noted that not all standards refer to wireless devices as "stations," but where the term is used in this paper, it should be understood that an analogous unit will be present on all applicable wireless networks. Thus, use of the term "station" should not be construed as limiting the scope of an embodiment that describes wireless devices as stations to a standard that explicitly uses the term, unless such a limitation is appropriate in the context of the discussion.

[00280] The wireless networks 2404 will typically include an internetworking unit (IWU) that interconnects wireless devices on the relevant one of the wireless networks 2404 with another network, such as a wired LAN. The IWU is sometimes referred to as a wireless access point (WAP). In the IEEE 802.11 standard, a WAP is also defined as a station. Thus, a station can be a non-WAP station or a WAP station. In a cellular network, the WAP is often referred to as a base station.

[00281] The wireless networks 2404 can be implemented using any applicable technology, which can differ by network type or in other ways. The wireless networks 2404 can be of any appropriate size (e.g., metropolitan area network (MAN), personal area network (PAN), etc.). Broadband wireless MANs may or may not be compliant with IEEE 802.16, which is incorporated by reference. Wireless PANs may or may not be compliant with IEEE 802.15, which is incorporated by reference. The wireless networks 2404 can be identifiable by network type (e.g., 2G, 3G, WiFi), service provider, WAP/base station identifier (e.g., WiFi SSID, base station and sector ID), geographic location, or other identification criteria.

[00282] The wireless networks 2404 may or may not be coupled together via an intermediate network. The intermediate network can include practically any type of communications network, such as, by way of example but not limitation, the Internet, a public switched telephone network (PSTN), or an infrastructure network (e.g., private LAN). The term "Internet" as used herein refers to a network of networks which uses certain protocols, such as the TCP/IP protocol, and possibly other protocols such as the hypertext transfer protocol (HTTP) for hypertext markup language (HTML) documents that make up the World Wide Web (the web).

[00283] In the example of FIG. 24, the network traffic analysis engine 2406 is coupled to the wireless device 2402-1. In a specific implementation, the network traffic analysis engine 2406 is implemented on a server and is coupled to the wireless device 2402-1 through the Internet. However, at least a portion of the network traffic analysis engine 2406 can alternatively be implemented on the wireless device 2402-1, with or without a connection to a server that includes another portion (e.g., a server portion) of the network traffic analysis engine 2406.

[00284] As used in this paper, an engine includes a dedicated or shared processor and, typically, firmware or software modules that are executed by the processor. Depending upon implementation-specific or other considerations, an engine can be centralized or its functionality distributed. An engine can include special purpose hardware, firmware, or software embodied in a computer-readable medium for execution by the processor. As used in this paper, a computer-readable medium is intended to include all mediums that are statutory (e.g., in the United States, under 35 U.S.C. 101), and to specifically exclude all mediums that are non-statutory in nature to the extent that the exclusion is necessary for a claim that includes the computer-readable medium to be valid. Known statutory computer-readable mediums include hardware (e.g., registers, random access memory (RAM), non-volatile (NV) storage, to name a few), but may or may not be limited to hardware.

[00285] The network traffic analysis engine 2406 analyzes a subset of traffic between the wireless device 2402-1 and a source or destination. The analyzed traffic may or may not be limited to a network segment, such as between a cellular phone and a base station. The network traffic analysis engine 2406 can analyze traffic for a subset of devices in the wireless network 2404-1 service area. The analyzed traffic may or may not be limited to subscribers.

[00286] In the example of FIG. 24, the network service usage classification engine 2408 is coupled to the network traffic analysis engine 2406. In a specific implementation, the network service usage classification engine 2408 is implemented on a server, which may or may not be the same server on which the network traffic analysis engine 2406 is implemented. However, at least a portion of the network service usage classification engine 2408 can alternatively be implemented on the wireless device 2402-1, with or without a connection to a server that includes another portion (e.g., a server portion) of the network service usage classification engine 2408.

[00287] The network service usage classification engine 2408 can categorize traffic based upon the service class (e.g., conversational, streaming, interactive, background, or some other service class) requested or needed for a service. The categorization facilitates identification of a snapshot of service class use at a given time, and, in some implementations, predictions of future service class use based upon the snapshot (e.g., making an assumption that future service class use is at least somewhat related to service class use of the snapshot), historical data analysis (e.g., service class usage at certain times of day/days of the week), identification of trends, or the use of some other predictive technology.

[00288] In the example of FIG. 24, the differential network access control engine 2410 is coupled to the network service usage classification engine 2408. In a specific implementation, the network access control engine 2410 is implemented on a server, which may or may not be the same server on which the network traffic analysis engine 2406 and/or the network service

usage classification engine 2408 are implemented. However, at least a portion of the network access control engine 2410 can alternatively be implemented on the wireless device 2402-1, with or without a connection to a server that includes another portion (e.g., a server portion) of the network access control engine 2410.

[00289] The differential network access control engine 2410 uses the predicted service class use from the network service usage classification engine 2408 to dynamically adjust resources allocated to service classes. For example, the differential network access control engine 2410 can perform a service class availability assessment to determine whether service class capacity for service classes on a channel are sufficient for predicted service usage, and either add resources if service class availability is insufficient for predicted service usage or reduce resources if service class availability is more than sufficient for predicted service usage.

[00290] Alternatively, the differential network access control engine 2410 can instead or in addition control applications on devices such that the applications change service usage levels or delay consumption of wireless resources (e.g., by delaying software updates until more resources become available). In an embodiment, a service usage control policy is implemented on the wireless device 2402-1. This may be necessary in some cases to ensure the wireless device 2402-1 can adjust application settings that are normally fixed, optimize network service usage activation based on network state (e.g., if the network is busy), control over-the-air software updates, throttle resource-hungry applications, manage network service usage requests from repeated power down modes, keep PPP sessions active, or otherwise facilitate dynamic service class adjustments or other device behavior.

[00291] In a specific implementation, subscribers can be incented to change service classes by, for example, charging more for higher service classes. The differential network access control engine 2410 can send a notification of differential charges for service classes. Alternatively, the charges could be implemented via subscriber account settings or preferences.

[00292] In the example of FIG. 24, in operation, the network traffic analysis engine 2406 analyzes traffic from one or more devices, including the wireless device 2402-1. The network service usage classification engine 2408 predicts the amount of resources needed for service classes, and the differential network access control engine 2410 dynamically allocates resources on an as-needed basis to adjust the service classes that are available to the one or more devices and/or adjusts device behavior for a subset of the one or more devices or instructs a subset of the one or more devices to adjust device behavior such that the device consumes service class-specific resources in accordance with an access control policy appropriate for the resources allocated to the applicable service classes.

[00293] FIG. 25 depicts a diagram an example of a differential access control notification system 2500. In the example of FIG. 25, the system 2500 includes a network service usage analysis engine 2502, a network service usage classification engine 2504, a differential network access control engine 2506, a network service usage control policy datastore 2508, a network service usage notification engine 2510, a user interface 2512, and a service plan update engine 2514.

[00294] In the example of FIG. 25, the network service usage analysis engine 2502 analyzes network service usage activity. The analysis can include an analysis of traffic sent to or from a device, an application running on a device, a request for services, or other analysis that is informative of past, current, or future network service usage. For example, the network service usage activity can include an attempt to download or load an application onto the communications device, an attempt to execute the network service activity or the network service usage activity attempts to access the network, meeting or exceeding a network service usage threshold, satisfying a network service usage pre-condition, an update to a network capacity controlled service activity classification list, an update to a network capacity controlled services policy, and a network message is sent to the device triggering the notification, to name

several by way of example. The analysis can occur on a non-WAP station, a WAP or base station, a server, or partly on one of these devices or some other device.

[00295] In the example of FIG. 25, the network service usage classification engine 2504 is coupled to the network service usage analysis engine 2502. The network service usage classification engine 2504 classifies the analyzed network service usage into one or more service classes. The classification can occur on a non-WAP station, a WAP or base station, a server, or partly on one of these devices or some other device.

[00296] In the example of FIG. 25, the differential network access control engine 2506 is coupled to the network service usage classification engine 2504. The differential network access control engine 2506 determines network access parameters using the service classes associated with the network service usage activity and network service usage control policies stored in the network service usage control policy datastore 2508. The determination can occur on a non-WAP station, a WAP or base station, a server, or partly on one of these devices or some other device. The network service usage control policy datastore 2508 can be implemented on a wireless device, but it is also possible to maintain the datastore remotely relative to the device (e.g., on a server). In a specific implementation, even if the network service usage control policy datastore 2508 is maintained remotely relative to the wireless device, the wireless device will still have a network service usage control policy implemented.

[00297] A datastore can be implemented, for example, as software embodied in a physical computer-readable medium on a general- or specific-purpose machine, in firmware, in hardware, in a combination thereof, or in an applicable known or convenient device or system. Datastores in this paper are intended to include any organization of data, including tables, comma-separated values (CSV) files, traditional databases (e.g., SQL), or other applicable known or convenient organizational formats. Datastore-associated components, such as database interfaces, can be considered "part of" a datastore, part of some other system

component, or a combination thereof, though the physical location and other characteristics of datastore-associated components is not critical for an understanding of the techniques described in this paper.

[00298] Datastores can include data structures. As used in this paper, a data structure is associated with a particular way of storing and organizing data in a computer so that it can be used efficiently within a given context. Data structures are generally based on the ability of a computer to fetch and store data at any place in its memory, specified by an address, a bit string that can be itself stored in memory and manipulated by the program. Thus some data structures are based on computing the addresses of data items with arithmetic operations; while other data structures are based on storing addresses of data items within the structure itself. Many data structures use both principles, sometimes combined in non-trivial ways. The implementation of a data structure usually entails writing a set of procedures that create and manipulate instances of that structure.

[00299] In the example of FIG. 25, the network service usage notification engine 2510 is coupled to the differential network access control engine 2506 and the network service usage control policy datastore 2508. The network service usage notification engine 2510 is configured to generate a notification sufficient to indicate relevant access control information. For example, the notification could indicate what network service usage activities are network capacity controlled services, the type of network service policy in effect for one or more network capacity controlled services, that a network service activity belongs to a network capacity controlled services classification, that a service activity that is classified as network capacity controlled services classification can have the classification changed, that if the service class is changed for the network service activity that the associated network service usage charges will change, a service plan upgrade/downgrade offer, and an offer for a service plan that provides discounts

and/or incentives for responding to one or more user notifications for protecting network capacity, to name several by way of example.

[00300] The notification may or may not also include a user preference selection. For example, the notification could include a provision to associate a network service usage control policy with the network service usage activity, an over-ride option for selecting the network service usage control policy, a modify option to select the service usage control policy, and a select option to select a new service plan, to name several by way of example. Other examples include network service usage activity information for one or more network capacity controlled services, predicted network service usage activity information for one or more network capacity controlled services, an option for obtaining more information about the network service usage of the network service usage activity, a message that the network service usage activity may result in network service usage that exceeds a threshold for a service plan associated with the device, an option to review or select an alternative service plan, an acknowledgement request, and an option to submit the acknowledgement request, to name several more by way of example.

[00301] In the example of FIG. 25, the user interface 2512 is coupled to the network service usage notification engine 2510. It may be noted that notifications can be disposed of by consulting user preferences (e.g., when a user indicates that maximum performance or minimum cost should be automatically selected). However, unless subscriber preferences are set as a default, a user is likely to have notifications displayed in the UI 2512. The notification can be in an applicable known or convenient form, such as SMS, email, a popup window, or the like. To the extent a response is permitted, a user can input a response to the notification using an input device (not shown).

[00302] In the example of FIG. 25, the service plan update engine 2514 is coupled to the UI 2512. As was previously mentioned, the UI can be bypassed because of, e.g., user preferences that are determinative of a selection provided in the notification. Regardless of how the

selection associated with the notification is made, the service plan update engine 2514 can update a service plan, network service usage control policy, user preferences, or other parameters in accordance with the selection. The service plan update engine 2514 can also update accounting if costs accrue.

[00303] FIG. 26 depicts an example of a computer system 2600 on which techniques described in this paper can be implemented. The computer system 2600 may be a conventional computer system that can be used as a client computer system, such as a wireless client or a workstation, or a server computer system. The computer system 2600 includes a computer 2602, I/O devices 2604, and a display device 2606. The computer 2602 includes a processor 2608, a communications interface 2610, memory 2612, display controller 2614, non-volatile storage 2616, and I/O controller 2618. The computer 2602 may be coupled to or include the I/O devices 2604 and display device 2606.

[00304] The computer 2602 interfaces to external systems through the communications interface 2610, which may include a modem or network interface. It will be appreciated that the communications interface 2610 can be considered to be part of the computer system 2600 or a part of the computer 2602. The communications interface 2610 can be an analog modem, ISDN modem, cable modem, token ring interface, satellite transmission interface (e.g. "direct PC"), or other interfaces for coupling a computer system to other computer systems.

[00305] The processor 2608 may be, for example, a conventional microprocessor such as an Intel Pentium microprocessor or Motorola power PC microprocessor. The memory 2612 is coupled to the processor 2608 by a bus 2670. The memory 2612 can be Dynamic Random Access Memory (DRAM) and can also include Static RAM (SRAM). The bus 2670 couples the processor 2608 to the memory 2612, also to the non-volatile storage 2616, to the display controller 2614, and to the I/O controller 2618.

[00306] The I/O devices 2604 can include a keyboard, disk drives, printers, a scanner, and other input and output devices, including a mouse or other pointing device. The display controller 2614 may control in the conventional manner a display on the display device 2606, which can be, for example, a cathode ray tube (CRT) or liquid crystal display (LCD). The display controller 2614 and the I/O controller 2618 can be implemented with conventional well known technology.

[00307] The non-volatile storage 2616 is often a magnetic hard disk, an optical disk, or another form of storage for large amounts of data. Some of this data is often written, by a direct memory access process, into memory 2612 during execution of software in the computer 2602. One of skill in the art will immediately recognize that the terms "machine-readable medium" or "computer-readable medium" includes any type of storage device that is accessible by the processor 2608 and also encompasses a carrier wave that encodes a data signal.

[00308] The computer system 2600 is one example of many possible computer systems which have different architectures. For example, personal computers based on an Intel microprocessor often have multiple buses, one of which can be an I/O bus for the peripherals and one that directly connects the processor 2608 and the memory 2612 (often referred to as a memory bus). The buses are connected together through bridge components that perform any necessary translation due to differing bus protocols.

[00309] Network computers are another type of computer system that can be used in conjunction with the teachings provided herein. Network computers do not usually include a hard disk or other mass storage, and the executable programs are loaded from a network connection into the memory 2612 for execution by the processor 2608. A Web TV system, which is known in the art, is also considered to be a computer system, but it may lack some of the features shown in FIG. 26, such as certain input or output devices. A typical computer

system will usually include at least a processor, memory, and a bus coupling the memory to the processor.

[00310] In addition, the computer system 2600 is controlled by operating system software which includes a file management system, such as a disk operating system, which is part of the operating system software. One example of operating system software with its associated file management system software is the family of operating systems known as Windows® from Microsoft Corporation of Redmond, Washington, and their associated file management systems. Another example of operating system software with its associated file management system software is the Linux operating system and its associated file management system. The file management system is typically stored in the non-volatile storage 2616 and causes the processor 2608 to execute the various acts required by the operating system to input and output data and to store data in memory, including storing files on the non-volatile storage 2616.

[00311] FIG. 27 depicts a diagram of an example of a system 2700 for application-specific differential network access control. In the example of FIG. 27, the system 2700 includes a network service consuming application 2702, a network service usage analysis engine 2704, an application behavior datastore 2706, a network service usage classification engine 7708, an application traffic prioritization engine 2710, a network service usage control policy datastore 2712, a differential network access control engine 2714, an application traffic cache 2716, an application traffic override engine 2718, and a network interface 2720. The system 2700 is intended to represent a specific implementation of techniques described previously in this paper for illustrative purposes. The techniques may be applicable to an applicable known or convenient (wired or wireless) device for which there is a motivation to control network service usage.

[00312] In the example of FIG. 27, the network service consuming application 2702 is a application that is implemented on a device. In an expected use, the application is a software

application stored at least in part in memory on a wireless device, though kernel-level instructions could be implemented as firmware or even hardware. The application can be referred to as "running" on the device or as being "executed" by the device in accordance with known uses of those terms. Wireless media are known to have more bandwidth constraints, which is why a wireless device is an expected use, though the technique may be applicable to wired devices in certain situations.

[00313] In the example of FIG. 27, the network service usage analysis engine 2704 is coupled to the network service consuming application 2702. The network service usage analysis engine 2704 analyzes traffic from the network service consuming application 2702 and stores relevant data in the application behavior datastore 2706. The data can include all traffic that is sent by the application, or a subset of the traffic (e.g., that which has a certain QoS classification or priority, that which has high resource consumption due to frequent transmission from the application, that which is sent to a particular destination, etc.) The data can also include traffic that is received for the application. The application behavior datastore 2706 can alternatively or in addition be implemented as a traffic source/destination datastore, which can be valuable if differential access control is based upon the source and/or destination of traffic. The application behavior datastore 2706 includes data structures (e.g., records) representative of data that is organized with implementation-specific granularity. For example, the data structures could be representative of frames (L2), packets (L3), or messages. (It may be noted that the term "packets" is often used to mean collections of data that are not limited to L3.) The desired granularity may depend upon where the network service usage analysis engine 2704 is located. Whether the data structures are changed over time (e.g., to change data associated with a record), replaced as records age, or maintained as historical data is also implementation-specific.

[00314] In the example of FIG. 27, the network service usage classification engine 2708 is coupled to the network service usage analysis engine 2704 and the application behavior datastore 2706. The network service usage classification engine 2708 can categorize the traffic stored in the application behavior datastore 2706 based on, e.g., network type, time of day, connection cost, whether home or roaming, network busy state, QoS, and whether the particular service usage activity is in foreground of user interaction or in the background of user interaction, or other characteristics that are obtained from network service usage analysis or through other means. Classification rules can include, for example, examining if one or more of the following has taken place within a specified period of time: user has interacted with the device, user has interacted with the service usage activity, user has picked up the device, service usage activity UI content is in the foreground of the device UI, audio or video information is being played by the service usage activity, a certain amount of data has been communicated by the service usage activity, service usage activity is or is not on a foreground or background service list. Rules that define which service usage activities to classify as, e.g., background service usage activities can be user-selected, set by a service provider, or through some other applicable means.

[00315] Advantageously, the network service usage analysis engine 2704 can examine a particular service usage activity and the network service usage classification engine 2708 can determine if the particular service usage activity fits a set of one or more classification rules that define the particular service usage activity as, e.g., a background service usage activity.

[00316] In the example of FIG. 27, the application traffic prioritization engine 2710 uses a policy stored in the network service usage control policy datastore 2712 to determine an appropriate prioritization for traffic to and/or from the network service consuming application 2702. Prioritization can enable the system 2700 to fine-tune the amount of network resources consumed by the network service consuming application 2702, or the rate of network resource

consumption. The control policy can require applications to throttle network resource consumption, prohibit the use of network resources by certain applications, etc.

[00317] Advantageously, the application traffic prioritization engine 2710 can determine a particular service usage activity has a particular characteristic, such as being a background service usage activity. This can involve checking whether a condition is satisfied.

[00318] In the example of FIG. 27, the differential network access control engine 2714 is coupled to the application traffic prioritization engine 2710 and the network service usage control policy datastore 2712. The differential network access control engine 2714 causes the network service consuming application 2702 traffic to be queued in the application traffic cache 2716. (If no throttling is required to follow the control policy, of course, the traffic need not be cached anywhere other than is typical, such as in an output buffer.) The application traffic cache 2716 is intended to represent a cache that is implemented on top of an output buffer or other standard caching device, and is used by the differential network access control engine 2714 to facilitate control over "rogue" applications, applications having anomalous behavior, or applications that must otherwise be controlled to conform with the control policy.

[00319] Advantageously, the differential network access control engine can restrict network access of a particular service usage activity when a condition is satisfied, such as when the service usage activity is a background activity.

[00320] In the example of FIG. 27, the application traffic override engine 2718 is coupled to the differential network access control engine 2714 and the application traffic cache 2716. The application traffic override engine 2718 enables a user or device to deviate from the control policy. Such deviation can be prompted by, for example, an incentive offer or a notification of cost.

[00321] In an illustrative example, the device 2700 blocks chatter for an application running in the background that is attempting to report device or user behavior. The application traffic prioritization engine 2710 determines that the chatter has zero priority, such that the network service consuming application 2702 is prevented from consuming any resources. The user can be sent a notification by the application traffic override engine 2718 that their control policy prohibits the application from consuming network resources, but that the user can opt to deviate from the control policy if they are willing to pay for the consumed resources. If the user is willing to pay for the resources, traffic can be sent at a certain rate from the application traffic cache 2716 through the network interface 2720, or perhaps sent without using the application traffic cache 2716.

[00322] As another illustrative example, the device 2700 could identify application traffic as a software update. The differential network access control engine 2714 may determine that software updates can be received at a throttled rate (perhaps even slower than the lowest QoS categorization). The application traffic override engine 2718 can receive an indication from the user, from user preferences, service provider settings, or the like that the updates can ignore the control policy for a particular application (or for all applications).

[00323] Advantageously, the control policy can set up a priority to communicate cached elements, set minimum update frequencies, provide control policy overrides (typically for payment), or the like to fine-tune differential network access control policies. This can enable the system 2700 to encourage certain behavior, such as sending low QoS traffic when it is cheaper (e.g., when the network does not have a busy state, at historically low-use times of day, when on a certain type of network, such as Wi-Fi, as opposed to another, such as cellular, etc.).

[00324] Some portions of the detailed description are presented in terms of algorithms and symbolic representations of operations on data bits within a computer memory. These algorithmic descriptions and representations are the means used by those skilled in the data

processing arts to most effectively convey the substance of their work to others skilled in the art. An algorithm is here, and generally, conceived to be a self-consistent sequence of operations leading to a desired result. The operations are those requiring physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical or magnetic signals capable of being stored, transferred, combined, compared, and otherwise manipulated. It has proven convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers, or the like.

[00325] It should be borne in mind, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities. Unless specifically stated otherwise as apparent from the following discussion, it is appreciated that throughout the description, discussions utilizing terms such as "processing" or "computing" or "calculating" or "determining" or "displaying" or the like, refer to the action and processes of a computer system, or similar electronic computing device, that manipulates and transforms data represented as physical (electronic) quantities within the computer system's registers and memories into other data similarly represented as physical quantities within the computer system memories or registers or other such information storage, transmission or display devices.

[00326] The present invention, in some embodiments, also relates to apparatus for performing the operations herein. This apparatus may be specially constructed for the required purposes, or it may comprise a general purpose computer selectively activated or reconfigured by a computer program stored in the computer. Such a computer program may be stored in a computer readable storage medium, such as, but is not limited to, read-only memories (ROMs), random access memories (RAMs), EPROMs, EEPROMs, magnetic or optical cards, any type of

disk including floppy disks, optical disks, CD-ROMs, and magnetic-optical disks, or any type of media suitable for storing electronic instructions, and each coupled to a computer system bus.

[00327] The algorithms and displays presented herein are not inherently related to any particular computer or other apparatus. Various general purpose systems may be used with programs in accordance with the teachings herein, or it may prove convenient to construct more specialized apparatus to perform the required method steps. The required structure for a variety of these systems will appear from the description below. In addition, the present invention is not described with reference to any particular programming language, and various embodiments may thus be implemented using a variety of programming languages.

[00328] 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.

CLAIMS

We claim:

1. A system, comprising:

a processor of a communications device configured to:

monitor a network service usage activity of the communications device in network communication;

classify the network service usage activity for differential network access control for protecting network capacity; and

associate the network service usage activity with a service usage control policy based on a classification of the network service usage activity to facilitate differential network access control for protecting network capacity; and

a memory coupled to the processor and configured to provide the processor with instructions.

2. A system, comprising:

a processor of a communications device configured to:

monitor a network service usage activity of the communications device in wireless network communication;

report the network service usage activity of the communications device to a network element, wherein the network element performs statistical analysis of a plurality of reported network service usage activities across a plurality of devices;

receive a network service usage activity classification list from the network element; and

classify the network service usage activity based on the network service usage activity classification list for differential network access control for protecting network capacity; and

a memory coupled to the processor and configured to provide the processor with instructions.

3. The system recited in claim 2, wherein the processor of the communications device is further configured to:

associate the network service usage activity with a network service usage control policy based on a classification of the network service usage activity to facilitate differential network access control for protecting network capacity.

4. The system recited in claim 2, wherein the processor of the communications device is further configured to:

associate the network service usage activity with a network service usage control policy based on a classification of the network service usage activity to facilitate differential network access control for protecting network capacity; and

differentially control the network service usage activity based on the network service usage activity classification list, wherein the network service usage activity is a network capacity controlled service.

5. A system, comprising:

a processor of a network device configured to:

receive a first report of network service usage activities of a first device from the first device;

receive a second report of network service usage activities of a second device from the second device;

perform a statistical analysis of a plurality of reported service usage activities across a plurality of devices, including the first device and the second device; and

send a network service usage activity classification list to the first device and the second device for classifying network service usage activities based on the service usage activity classification list for differential network access control for protecting network capacity; and

a memory coupled to the processor and configured to provide the processor with instructions.

6. The system recited in claim 5, wherein the processor of the network device is further configured to:

associate the network service usage activity with a network service usage control policy based on a classification of the network service usage activity to facilitate differential network access control for protecting network capacity.

7. The system recited in claim 5, wherein the processor of the network device is further configured to:

associate the network service usage activity with a network service usage control policy based on a classification of the network service usage activity to facilitate differential network access control for protecting network capacity; and

differentially control the network service usage activity based on the service usage activity classification list for protecting network capacity.

8. A system, comprising:

a processor of a communications device configured to:

associate a network service usage activity of the communications device with a network service usage control policy based on a classification of the network service usage activity for differential network access control for protecting network capacity; and

generate a user notification based on the network service usage control policy; and

a memory coupled to the processor and configured to provide the processor with instructions.

9. The system recited in claim 8, wherein the network service usage control policy includes a network service usage notification policy.

10. The system recited in claim 8, wherein the user notification includes one or more of the following: one or more service activities classified as network capacity controlled services, type of network service policy in effect for one or more network capacity controlled services, notification that a network service activity belongs to a network capacity controlled services classification, notification that a service activity that is classified as network capacity controlled services classification can have the classification changed, notification that if the service class is changed for the network service activity that the associated network service usage charges will change, a service plan upgrade/downgrade offer, and an offer for a service plan that provides discounts and/or incentives for responding to one or more user notifications for protecting network capacity.

11. The system recited in claim 8, wherein the user notification includes a user preference selection, including one or more of the following: a provision to associate a network service usage control policy with the network service usage activity, an over-ride option for selecting the

network service usage control policy, a modify option to select the service usage control policy, and a select option to select a new service plan.

12. The system recited in claim 8, wherein the user notification occurs after one or more of the following: an attempt to download or load an application onto the communications device, an attempt to execute the network service activity or the network service usage activity attempts to access the network, a network service usage activity meets or exceeds a network service usage threshold, a network service usage activity attempts a network service usage that satisfies a pre-condition, an update to a network capacity controlled service activity classification list, an update to a network capacity controlled services policy, and a network message is sent to the device triggering the notification.

13. The system recited in claim 8, wherein the user notification includes one or more of the following: network service usage activity information for one or more network capacity controlled services, predicted network service usage activity information for one or more network capacity controlled services, an option for obtaining more information about the network service usage of the network service usage activity, a message that the network service usage activity may result in network service usage that exceeds a threshold for a service plan associated with the device, an option to review or select an alternative service plan, an acknowledgement request, and an option to submit the acknowledgement request.

14. A system, comprising:

a processor of a communications device configured to:

determine a network busy state of a wireless network; and

classify a network service usage activity of the communications device based on the network busy state to facilitate differential network access control for protecting network capacity of the wireless networks; and

a memory coupled to the processor and configured to provide the processor with instructions.

15. The system recited in claim 14, wherein the network busy state is based on one or more of the following: network performance, network congestion, network availability, network resource availability, network capacity, and a time based criteria.

16. The system recited in claim 14, wherein protecting network capacity of the wireless network includes protecting network capacity of a last edge segment of the wireless network, and the processor is further configured to:

send the network busy state to a network element.

17. A system, comprising:

a processor of a communications device configured to:

monitor a network service usage activity of a device in wireless network communication;

classify the network service usage activity to facilitate differential network access control for protecting network capacity; and

account for the network service usage activity based on a classification of the network service usage activity for differential network service usage accounting; and

a memory coupled to the processor and configured to provide the processor with instructions.

18. The system recited in claim 17, wherein the processor of the communications device is further configured to:

charge for the network service usage activity based on the classification of the network service usage activity for differential network service usage charging, wherein charging for the network service usage activity includes mediating CDR/IPDR charging records for network capacity controlled services and non-capacity controlled services.

19. A system, comprising:

a processor of a communications device configured to:

receive an API request from a network service usage activity for wireless network access;

respond to the API request from the network service usage activity; and

implement differential network access for the network service usage activity for protecting network capacity, wherein the differential network access is based on a priority level associated with the network service usage activity and a network busy state; and

a memory coupled to the processor and configured to provide the processor with instructions.

20. The system recited in claim 19, wherein a response to the API request includes providing one or more of the following to the network service usage activity: a network busy state, whether the network service usage activity is allowed to access the network, which access network to which the network service usage activity is granted network access, what traffic controls the network service usage activity is required to implement for network access, when the network is available to the network service usage activity for access, a schedule for network access for the network service usage activity, a reservation for network access for the network

service usage activity with a specified performance level, an instruction to transition to a dormant or power save state, and an instruction to awake from a dormant or power save state.

21. A system, comprising:

a processor of a network device configured to:

receive an API request from a network service usage activity of a communications device for wireless network access; and

respond to the API request from the network service usage activity for implementing differential network access for protecting network capacity;

wherein the differential network access is based on a priority level associated with the network service usage activity and a network busy state; and

a memory coupled to the processor and configured to provide the processor with instructions.

22. The system recited in claim 21, wherein a response to the API request includes providing one or more of the following to the network service usage activity: a network busy state, whether the network service usage activity is allowed to access the network, which access network to which the network service usage activity is granted network access, what traffic controls the network service usage activity is required to implement for network access, when the network is available to the network service usage activity for access, a schedule for network access for the network service usage activity, a reservation for network access for the network service usage activity with a specified performance level, an instruction to transition to a dormant or power save state, and an instruction to awake from a dormant or power save state.

23. The system recited in claim 21, wherein the API is a network element API that is in secure communication with the communications device, and wherein the communications device

implements the differential network access, and the differential network access implementation is verified.

24. The system recited in claim 21, wherein the busy state information is obtained from one or more network elements.

25. A system, comprising:

a processor of a communications device configured to:

monitor a plurality of network service usage activities of the communications device;

determine a network busy state based on the monitored plurality of network service usage activities;

send a network busy state report to a network element; and

a memory coupled to the processor and configured to provide the processor with instructions.

26. The system recited in claim 25, wherein the communications device includes a verified service processor, and wherein the verified service processor monitors the plurality of network service usage activities of the communications device and determines the network busy state based on the monitored plurality of network service usage activities.

27. The system recited in claim 25, wherein determining the network busy state includes one or more of the following: data rate, latency, jitter, bit error rate, packet error rate, number of network access attempts, number of network access successes, number of network access failures, QoS level availability, QoS level performance, and variability in any of the preceding parameters.

28. A system, comprising:

a processor of a network device configured to:

collect network busy state information for one or more access networks for a plurality of communications devices; and

implement differential network access for one or more network capacity controlled services for the plurality of communications devices based on the network busy state information associated with each of the one or more access networks for protecting network capacity; and

a memory coupled to the processor and configured to provide the processor with instructions.

29. The system recited in claim 28, wherein the network busy state information is collected from a plurality of network based measures transmitted to the network device, wherein the network based measures are received from one or more of the following: a base station, a base station monitor, an airwave monitor, and a base station controller.

30. A system, comprising:

a processor of a communications device configured to:

monitor a network service usage activity of the communications device in network communication;

classify the network service usage activity for differential network access control for protecting network capacity; and

associate the network service usage activity with a network service usage control policy based on a classification of the network service usage activity to facilitate differential network access control for protecting network capacity; and

a memory coupled to the processor and configured to provide the processor with instructions.

31. The system recited in claim 30, wherein the communications device is a mobile communications device, and the service includes one or more Internet based services, and wherein the mobile communications device includes one or more of the following: a mobile phone, a PDA, an eBook reader, a music device, an entertainment/gaming device, a computer, laptop, a net book, a tablet, and a home networking system.

32. The system recited in claim 30, wherein the processor of the communications device is further configured to:

implement differential network access for the network service usage activity for protecting network capacity; and

verify implementation of the differential network access for the network service usage activity.

33. The system recited in claim 30, wherein the processor of the communications device is further configured to:

implement differential network access for the network service usage activity for protecting network capacity using a verified service processor.

34. The system recited in claim 30, wherein the processor of the communications device is further configured to:

implement differential network access for the network service usage activity for protecting network capacity using an emulated network access API.

35. The system recited in claim 30, wherein the processor of the communications device is further configured to:

monitor the network service usage activity based on a service profile; and

determine that the network service usage activity is a network capacity controlled service based on the monitored use of the network service usage activity based on the service profile using a verified service processor.

36. The system recited in claim 30, wherein the processor of the communications device is further configured to:

determine if network access for the network service usage activity is authorized based on a service plan associated with the communications device, a network capacity controlled service priority level associated with the network service usage activity, and a network busy state.

37. The system recited in claim 30, wherein the processor is further configured to:

execute a router for dynamically managing one or more network capacity controlled services and/or QoS sessions for the communications device.

38. The system recited in claim 30, wherein the processor is further configured to:

execute a router for dynamically managing one or more network capacity controlled services and/or QoS sessions for the communications device; and

send network busy state information to a service controller, wherein the service controller provides a policy decision point for management for a plurality of communications devices in communication with one or more base stations.

39. The system recited in claim 30, wherein the processor is further configured to:

execute a router for dynamically managing one or more network capacity controlled services and/or QoS sessions for the communications device;

send network busy state information to a service controller, wherein the service controller provides a policy decision point for management for a plurality of communications devices in communication with one or more base stations; and

receive router traffic control instructions from the service controller, wherein the service controller provides the router traffic control instructions to assist in dynamically managing network capacity usage for the plurality of communications devices in communication with the one or more base stations for protecting network capacity of one or more access networks.

40. The system recited in claim 30, wherein the classifying is based on a current access network and/or the network service usage control policy is based on a current access network.

41. The system recited in claim 30, wherein classifying includes dynamically assigning a network capacity controlled services priority level based on a network busy state.

42. The system recited in claim 30, wherein classifying includes querying a network element for determining a network capacity controlled services classification and/or associating includes querying a network element for determining an association with the network service usage control policy.

43. The system recited in claim 30, wherein the network service usage control policy includes one or more of the following: block/allow settings, throttle settings, adaptive throttle settings, QoS class settings, packet error rate, jitter and delay settings, queue settings, and tag settings.

44. The system recited in claim 30, wherein the network service usage control policy includes traffic control policy filters.

45. The system recited in claim 30, wherein the network service usage control policy includes traffic control policy filters implemented as cascading filters.

46. The system recited in claim 30, wherein the network service usage control policy includes traffic control policy filters using a network busy state and/or a time of day as an index into a traffic control setting.

47. The system recited in claim 30, wherein the processor is further configured to:

differentially control the network service usage activity based on the network service usage control policy based on a network busy state, wherein the network service usage activity is classified as a network capacity controlled service.

48. The system recited in claim 30, wherein the processor is further configured to:

differentially control the network service usage activity based on the network service usage control policy based on a user input and/or a current access network, wherein the network service usage activity is classified as a network capacity controlled service.

49. The system recited in claim 30, wherein the processor is further configured to:

modify or replace a network stack interface of the communications device to provide for intercept or discontinuance of network access messaging for implementing traffic control for network capacity controlled services for protecting network capacity.

50. The system recited in claim 30, wherein the processor is further configured to:

store a network capacity controlled service list, wherein the network capacity controlled service list is periodically updated based on monitored network service usage activities.

51. A method, comprising:

monitoring a network service usage activity of the communications device in network communication;

classifying the network service usage activity for differential network access control for protecting network capacity; and

associating the network service usage activity with a network service usage control policy based on a classification of the network service usage activity to facilitate differential network access control for protecting network capacity.

52. A computer program product, the computer program product being embodied in a computer readable storage medium and comprising computer instructions for:

monitoring a network service usage activity of the communications device in network communication;

classifying the network service usage activity for differential network access control for protecting network capacity; and

associating the network service usage activity with a network service usage control policy based on a classification of the network service usage activity to facilitate differential network access control for protecting network capacity.

53. A method comprising:

examining a particular service usage activity to determine if the particular service usage activity fits a set of one or more classification rules that define the particular service usage activity as a background service usage activity;

determining whether a condition is satisfied, the condition including a finding that the particular service usage activity is determined to be a background service usage activity; and

when the condition is satisfied, restricting network access of the particular service usage activity.

54. The method of claim 53, wherein the set of one or more classification rules examines at least one of network type, time of day, connection cost, whether home or roaming, network busy state, QoS, and whether the particular service usage activity is in foreground of user interaction or in the background of user interaction.

55. The method of claim 53, wherein the set of one or more classification rules includes examining if one or more of the following has taken place within a specified period of time: user has interacted with the device, user has interacted with the service usage activity, user has picked up the device, service usage activity UI content is in the foreground of the device UI, audio or video information is being played by the service usage activity, a certain amount of data has been communicated by the service usage activity, service usage activity is or is not on a foreground or background service list.

56. The method of claim 53, further comprising obtaining user selection of rules that define which service usage activities to classify as background service usage activities.

57. The method of claim 56, wherein the user selection of classification rules includes user selection of specific service usage activities to classify as background service usage activities.

58. The method of claim 56, further comprising obtaining user selection of rules that define more than one level of service background class for the user to choose from.

59. The method of claim 56, wherein the obtaining user selection includes presenting usage information for service usage activities to aid in determining which to define as background service usage activities.

60. The method of claim 56, wherein the obtaining user selection includes presenting cost information for service usage activities to aid in determining which to define as background service usage activities.

61. The method of claim 53, wherein the condition includes enabling the user to select a network for background service usage activities.

62. The method of claim 61, wherein the selection of the network is based on the time of day.

63. The method of claim 61, wherein the selection of the network is based on connection cost.

64. The method of claim 53, wherein the user can modify the set of one or more classification rules.

65. The method of claim 53, wherein the condition includes
detecting when the service usage activity was initiated or attempted to be initiated;
notifying the user that this is a background service usage activity; and
provides the user with an option to implement the step of restricting.

66. The method of claim 65, further comprising
informing the user of what the restriction options are; and

implementing the restriction if the user chooses to implement a restriction option; and disabling the restriction if the user chooses to proceed.

67. The method of claim 66, wherein a network element sets the classification rules.

68. The method of claim 67, wherein the setting of the set of one or more classification rules is based on network manager input.

69. The method of claim 67, wherein the setting the set of one or more classification rules is based on characterizing application usage behavior.

70. The method of claim 66, wherein the setting the set of one or more classification rules is based on a policy instruction provided from a network element to the device.

71. The method of claim 53, wherein the examining takes place on the device.

72. The method of claim 53, wherein the set of one or more classification rules includes determining if an app is an OS function, client/server data sharing/update function, software update or download, background file download, email or calendar or contact update or synch function.

73. The method of claim 53, wherein the restricting includes one or more of: blocking, delaying, implementing a time window, aggregating/holding/transmitting, throttling, restricting to a range of NBS level, restricting to certain network types, restricting based on whether home or roaming, restricting to a certain time period, waiting for lower cost condition, waiting for specified

network, waiting for home network, waiting for time of day, and waiting for network background state.

74. The method of claim 53, wherein the background service usage activity data that needs to be communicated via the device is cached until the condition is modified, reduced or removed.

75. The method of claim 74, wherein the cached data is prioritized so that most important data is communicated first when the condition is modified, reduced or removed.

76. The method of claim 53, wherein the restricting occurs on the device, and the app is unaware that it might be subjected to background service restrictions.

77. The method of claim 53, further comprising modifying or repressing app notification messages about lack of network connectivity.

77. The method of claim 53, wherein an app is provided with network state indications that are differential for different apps according to app background class or priority.

78. The method of claim 53, wherein an app is made aware that it might be subjected to background service restrictions.

79. The method of claim 78, wherein the awareness is provided via a background service API.

80. The method of claim 53, wherein an app has rules defining in which background states it should transmit.

81. The method of claim 53, wherein an app has a capability to override background service rules for high priority data.

82. The method of claim 53, wherein an app background service status API indicates one or more of: background transmission permission status, background class or classes allowed to transmit, NBS, QoS, apps allowed to transmit, service classes allowed to transmit, type of network, time of day, geography, and whether home or roaming.

82. The method of claim 53, wherein the restricting allows a minimum connectivity for background services.

83. The method of claim 53, wherein the user is charged less for background services that are implemented with background service policy controls.

84. The method of claim 53, wherein the user can override background service policy enforcement for high priority communication.

85. The method of claim 53, wherein the user pays a higher price when background service policy enforcement is overridden.

86. The method of claim 53, wherein a sponsored service partner is charged less for background services that are implemented with background service policy controls.

87. The method of claim 53, wherein a sponsor can override background service policy enforcement for high priority communication.

88. The method of claim 53, wherein a sponsor programs override decision conditions into an app.

89. The method of claim 53, wherein a sponsor programs override decision conditions into a network element.

90. The method of claim 53, wherein a sponsor app or network element can override background service policy.

91. The method of claim 53, wherein a sponsor pays a higher price when background service policy enforcement is overridden.

92. The method of claim 53, wherein a restriction occurs in the network.

93. The method of claim 92, wherein an app is not aware that it might be subjected to background service restrictions.

94. The method of claim 92, further comprising modifying or repressing app notification messages about lack of network connectivity.

95. The method of claim 92, further comprising providing an app with network state indications that are differential for different apps according to app background class or priority.

96. The method of claim 92, further comprising informing an app that it might be subjected to background service restrictions.

97. The method of claim 96, wherein a background service API performs the informing.

98. The method of claim 92, wherein an app has rules for which background states it should transmit.

99. The method of claim 92, wherein an app has a capability to override background service rules for high priority data.

100. The method of claim 92, wherein an app background service status API indicates one or more of: background transmission permission status, background class or classes allowed to transmit, NBS, QoS, apps allowed to transmit, service classes allowed to transmit, type of network, time of day, geography, and whether home or roaming.

101. The method of claim 92, wherein the price for a sponsored service for background service usage activities is reduced when background service policies are followed.

102. The method of claim 92, wherein a sponsor device app determines background classification state and determines whether or not to restrict communication.

103. The method of claim 92, wherein an app determines background state from a device API.

104. The method of claim 92, wherein an app determines background state from a network API.

105. The method of claim 92, wherein an app determines background state from an NBS monitor.

106. The method of claim 92, wherein a sponsor price is increased if background policies are overridden by a sponsor app.

107. The method of claim 92, wherein a sponsor server determines background classification state and determines whether to restrict communication.

108. The method of claim 92, wherein a network element determines background state from a device API.

109. The method of claim 92, wherein a network element determines background state from a network API.

110. The method of claim 92, wherein a network element determines background state from an NBS monitor.

111. The method of claim 92, wherein a sponsor price is increased if background policies are overridden by a sponsor network element.

112. The method of claim 92, wherein a background service state indication API on the device makes background service state available to apps or network elements so they can decide when to communicate.

113. The method of claim 92, wherein a background service state indication API on a network element provides API background service state information to device apps or partner servers so they can decide when to communicate.

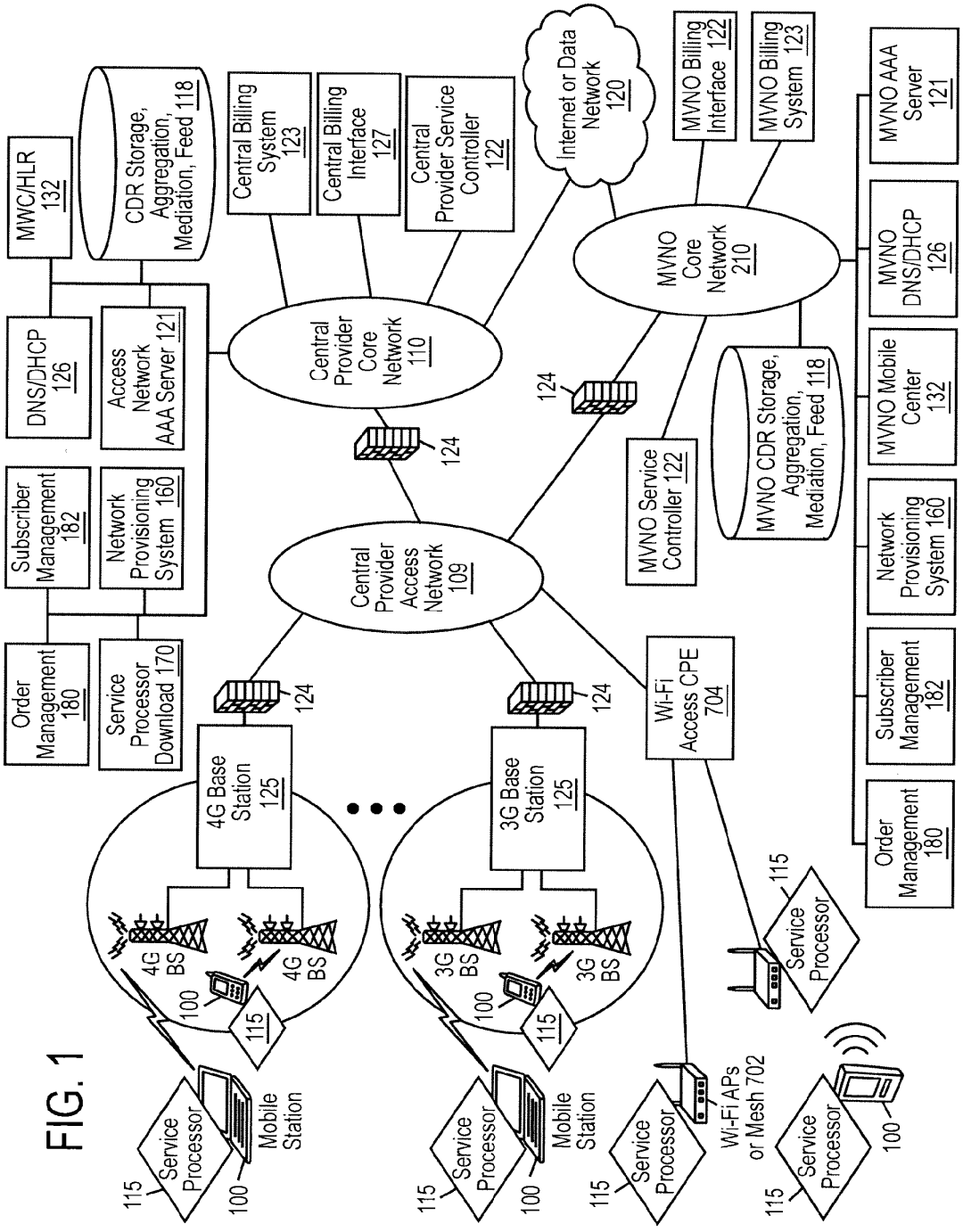

MWC/HLR 132
CDR Storage, Aggregation, Mediation, Feed 118
Central Billing System 123
Central Billing Interface 127
Central Provider Service Controller 122
Internet or Data Network 120
MVNO Billing Interface 122
MVNO Billing System 123
MVNO AAA Server 121
DNS/DHCP 126
Access Network AAA Server 121
Central Provider Core Network 110
MVNO Core Network 210
MVNO DNS/DHCP 126
Subscriber Management 182
Network Provisioning System 160
MVNO Mobile Center 132
MVNO Service Controller 122
MVNO CDR Storage, Aggregation, Mediation, Feed 118
Order Management 180
Service Processor Download 170
Central Provider Access Network 109
Wi-Fi Access CPE 704
4G Base Station 125
3G Base Station 125
4G BS
3G BS
100
115
124
Service Processor
Mobile Station
Wi-Fi APs or Mesh 702

FIG. 1

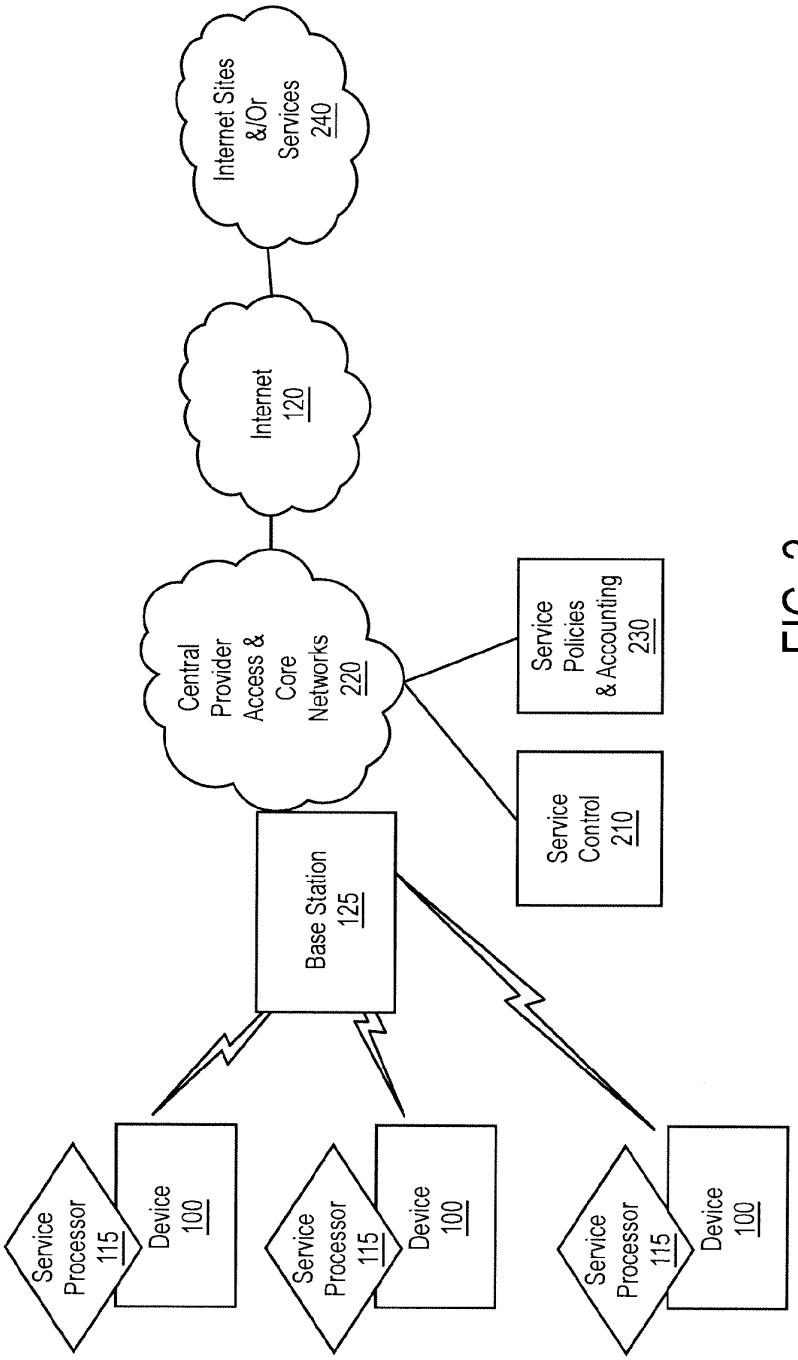

Internet Sites &/Or Services 240
Internet 120
Central Provider Access & Core Networks 220
Service Policies & Accounting 230
Service Control 210
Base Station 125
Service Processor 115
Device 100
Service Processor 115
Device 100
Service Processor 115
Device 100

FIG. 2

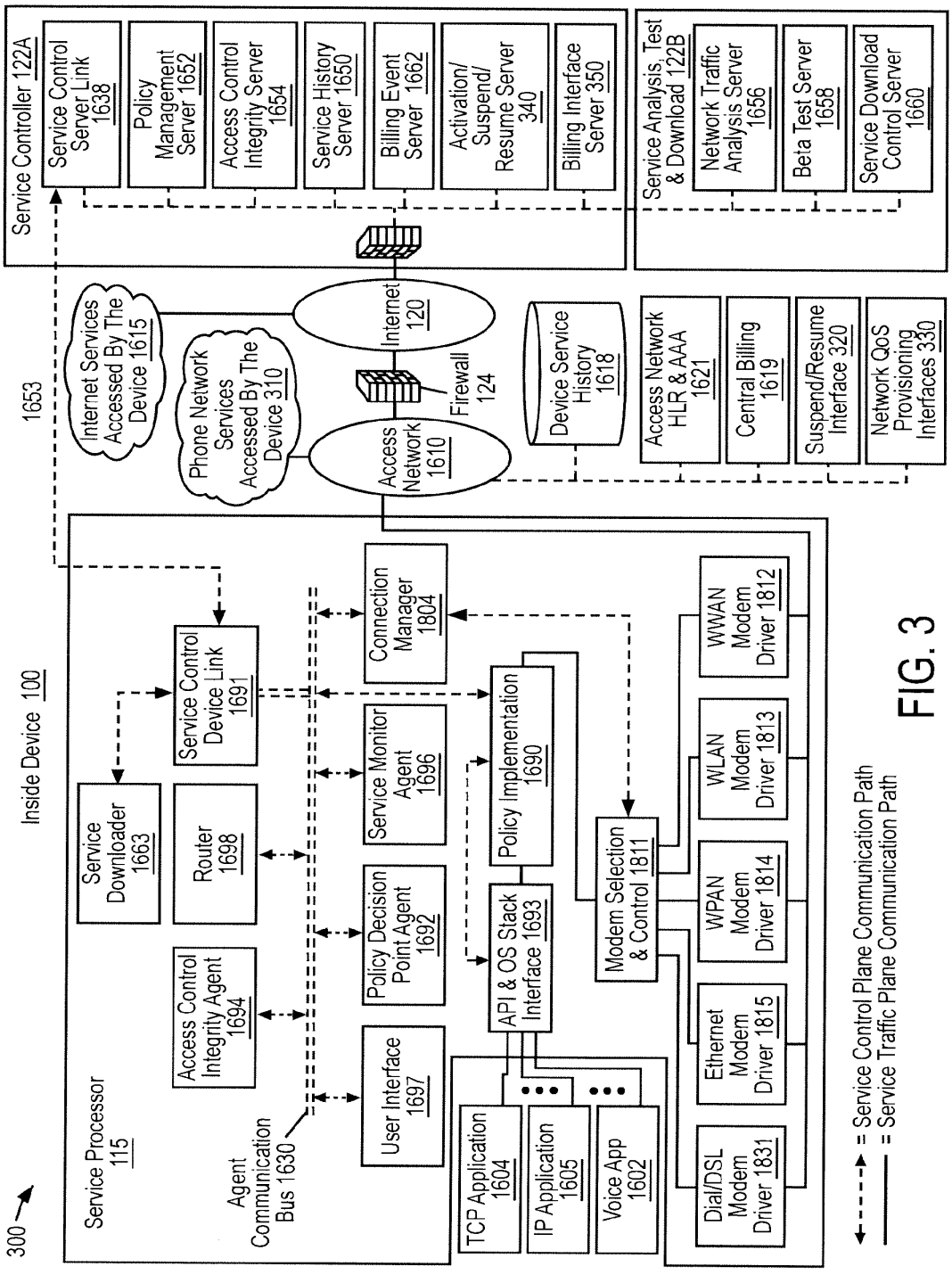

300
Service Processor 115
Inside Device 100
Agent Communication Bus 1630
Service Downloader 1663
Router 1698
Service Control Device Link 1691
Connection Manager 1804
Service Monitor Agent 1696
Policy Implementation 1690
Access Control Integrity Agent 1694
Policy Decision Point Agent 1692
API & OS Stack Interface 1693
Modem Selection & Control 1811
User Interface 1697
TCP Application 1604
IP Application 1605
Voice App 1602
Dial/DSL Modem Driver 1831
Ethernet Modem Driver 1815
WPAN Modem Driver 1814
WLAN Modem Driver 1813
WWAN Modem Driver 1812
1653
Internet Services Accessed By The Device 1615
Phone Network Services Accessed By The Device 310
Access Network 1610
Firewall 124
Internet 120
Device Service History 1618
Access Network HLR & AAA 1621
Central Billing 1619
Suspend/Resume Interface 320
Network QoS Provisioning Interfaces 330
Service Controller 122A
Service Control Server Link 1638
Policy Management Server 1652
Access Control Integrity Server 1654
Service History Server 1650
Billing Event Server 1662
Activation/ Suspend/ Resume Server 340
Billing Interface Server 350
Service Analysis, Test & Download 122B
Network Traffic Analysis Server 1656
Beta Test Server 1658
Service Download Control Server 1660
= Service Control Plane Communication Path
= Service Traffic Plane Communication Path

FIG. 3

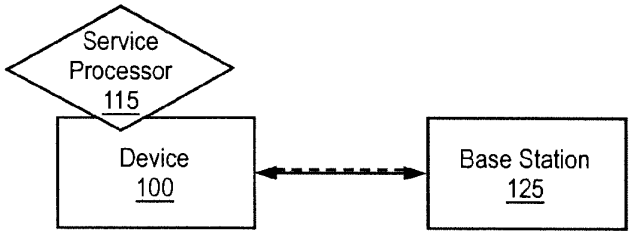


FIG. 4A

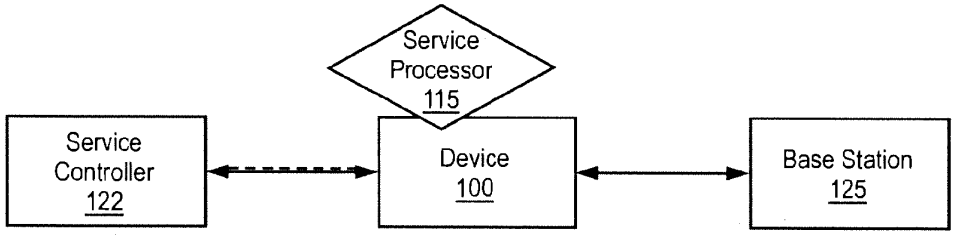


FIG. 4B

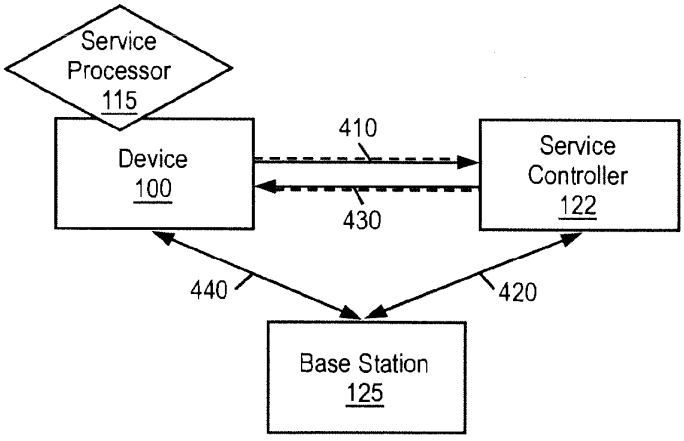


FIG. 4C

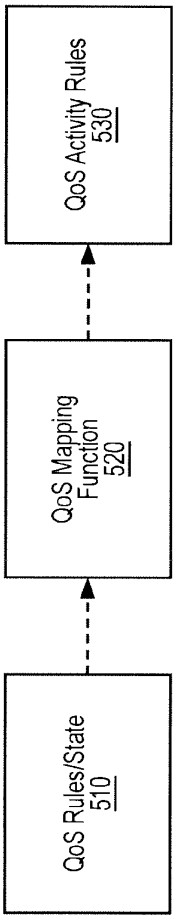

QoS Activity Rules
530
QoS Mapping
Function
520
QoS Rules/State
510

FIG. 5

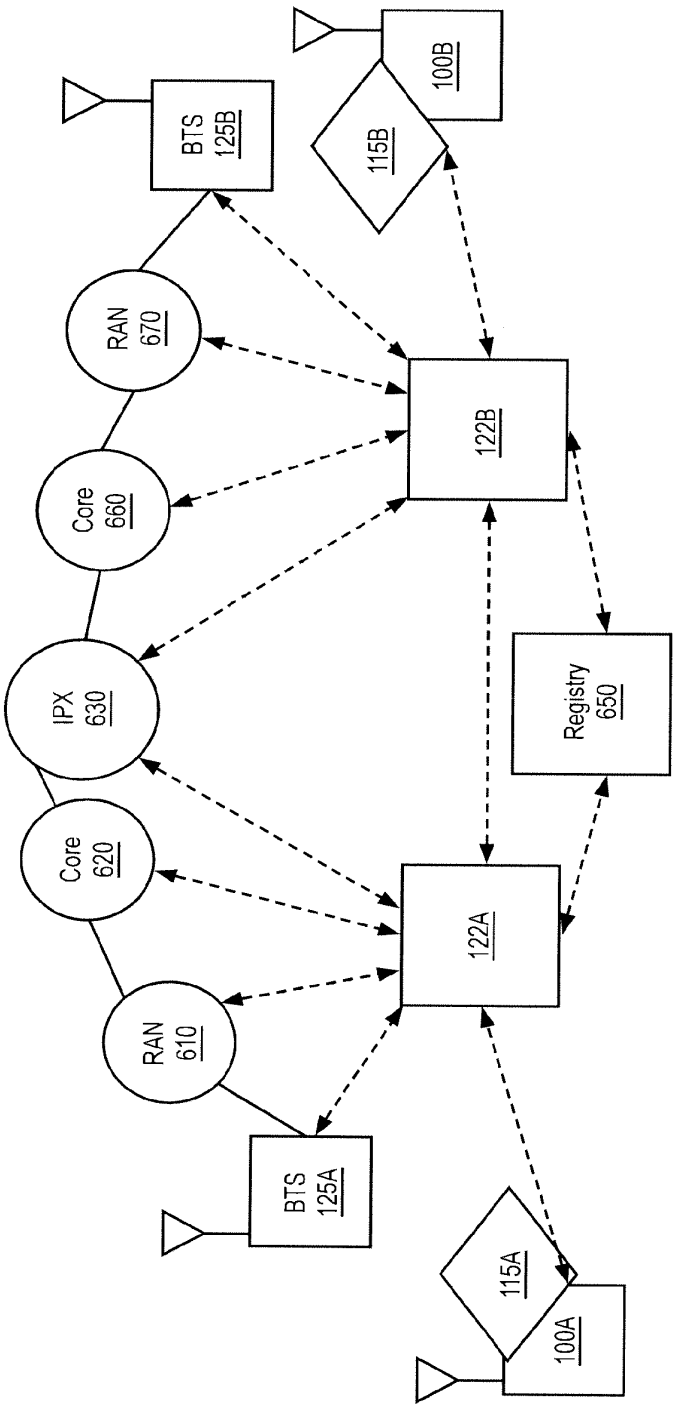

100B
115B
BTS 125B
RAN 670
Core 660
122B
IPX 630
Registry 650
Core 620
122A
RAN 610
BTS 125A
115A
100A

FIG. 6

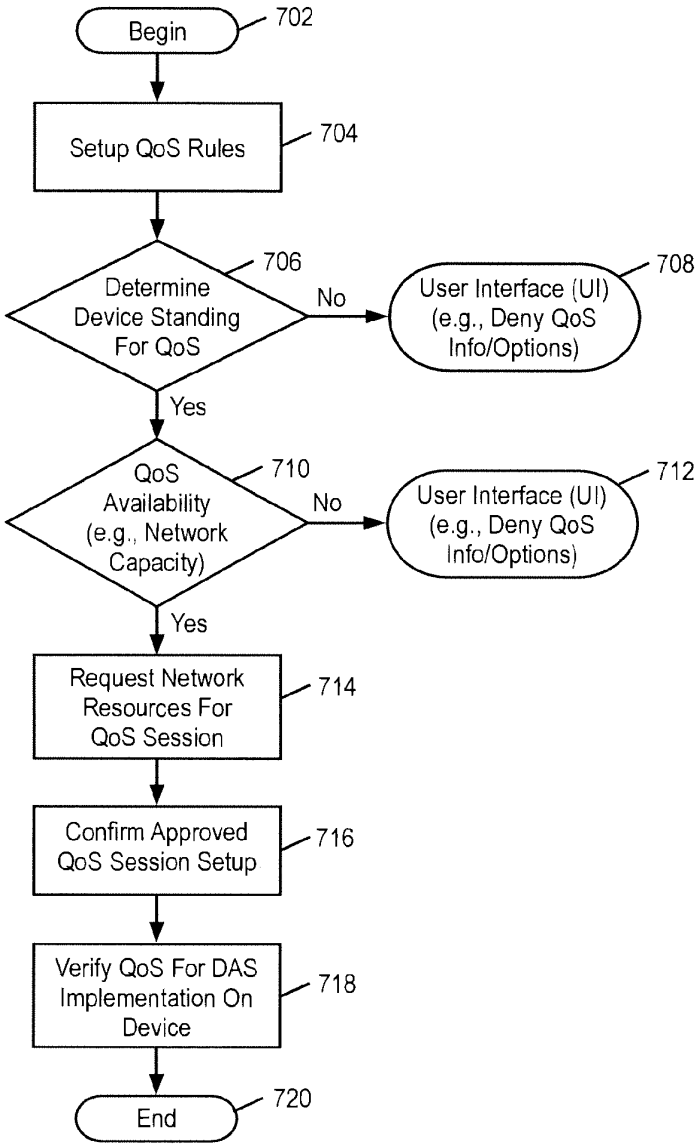

Begin
702
Setup QoS Rules
704
Determine Device Standing For QoS
706
No
User Interface (UI) (e.g., Deny QoS Info/Options)
708
Yes
QoS Availability (e.g., Network Capacity)
710
No
User Interface (UI) (e.g., Deny QoS Info/Options)
712
Yes
Request Network Resources For QoS Session
714
Confirm Approved QoS Session Setup
716
Verify QoS For DAS Implementation On Device
718
End
720

FIG. 7

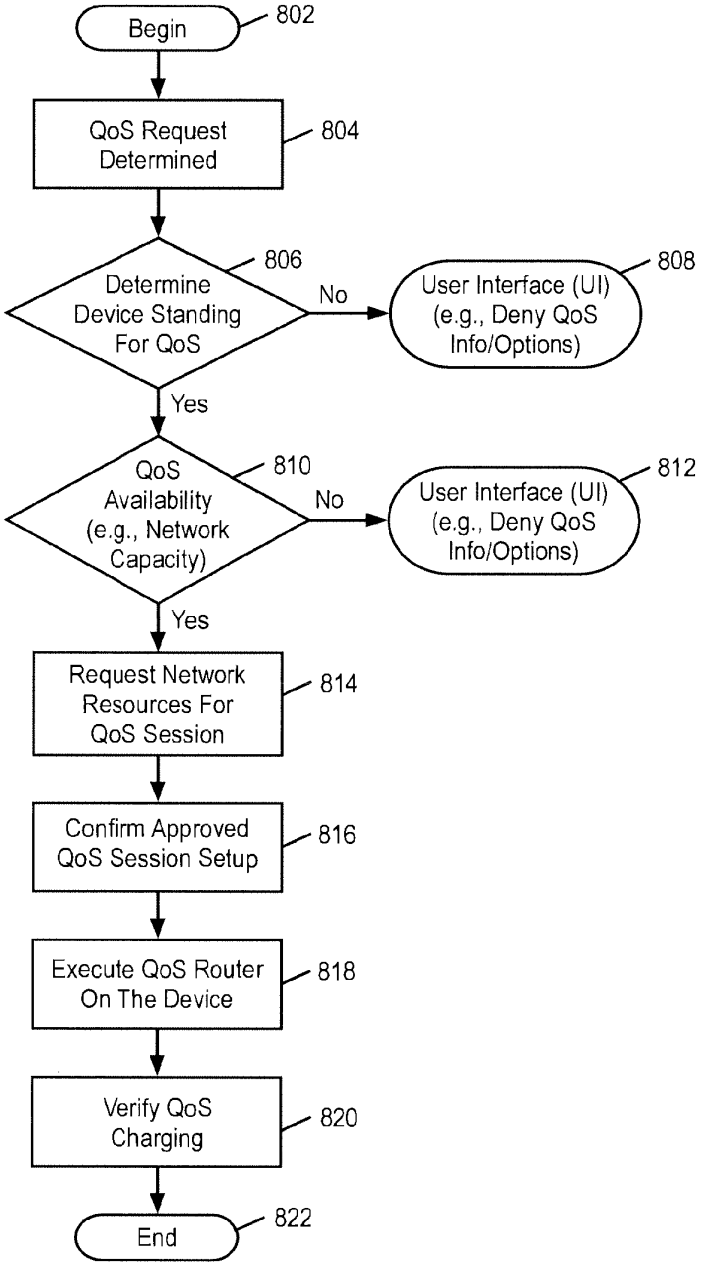

Begin
802
QoS Request Determined
804
Determine Device Standing For QoS
806
No
User Interface (UI) (e.g., Deny QoS Info/Options)
808
Yes
QoS Availability (e.g., Network Capacity)
810
No
User Interface (UI) (e.g., Deny QoS Info/Options)
812
Yes
Request Network Resources For QoS Session
814
Confirm Approved QoS Session Setup
816
Execute QoS Router On The Device
818
Verify QoS Charging
820
End
822

FIG. 8A

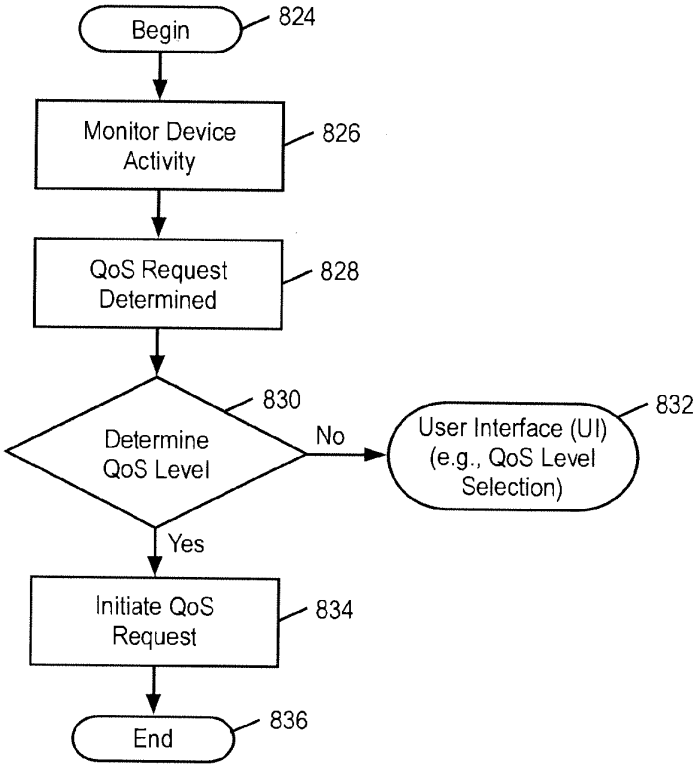

Begin
824
Monitor Device Activity
826
QoS Request Determined
828
Determine QoS Level
830
No
User Interface (UI) (e.g., QoS Level Selection)
832
Yes
Initiate QoS Request
834
End
836

FIG. 8B

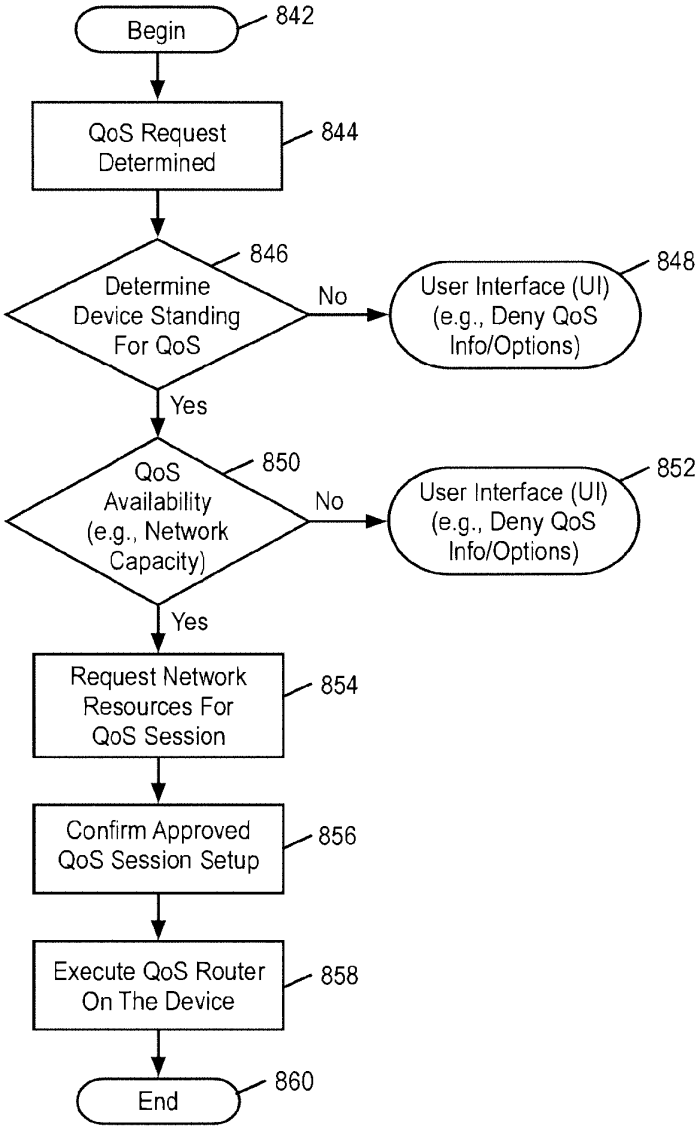

Begin
842
QoS Request Determined
844
Determine Device Standing For QoS
846
No
User Interface (UI) (e.g., Deny QoS Info/Options)
848
Yes
QoS Availability (e.g., Network Capacity)
850
No
User Interface (UI) (e.g., Deny QoS Info/Options)
852
Yes
Request Network Resources For QoS Session
854
Confirm Approved QoS Session Setup
856
Execute QoS Router On The Device
858
End
860

FIG. 8C

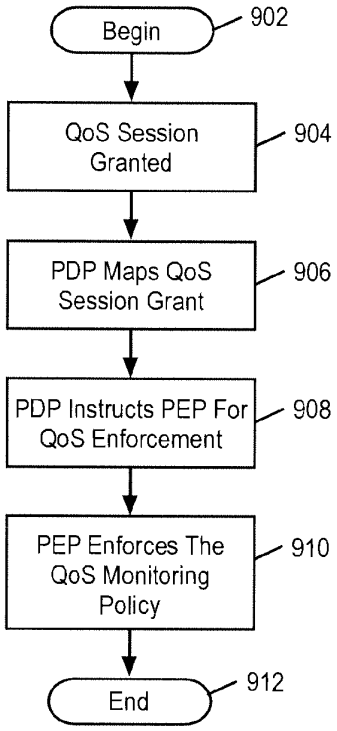

Begin
902
QoS Session Granted
904
PDP Maps QoS Session Grant
906
PDP Instructs PEP For QoS Enforcement
908
PEP Enforces The QoS Monitoring Policy
910
End
912

FIG. 9

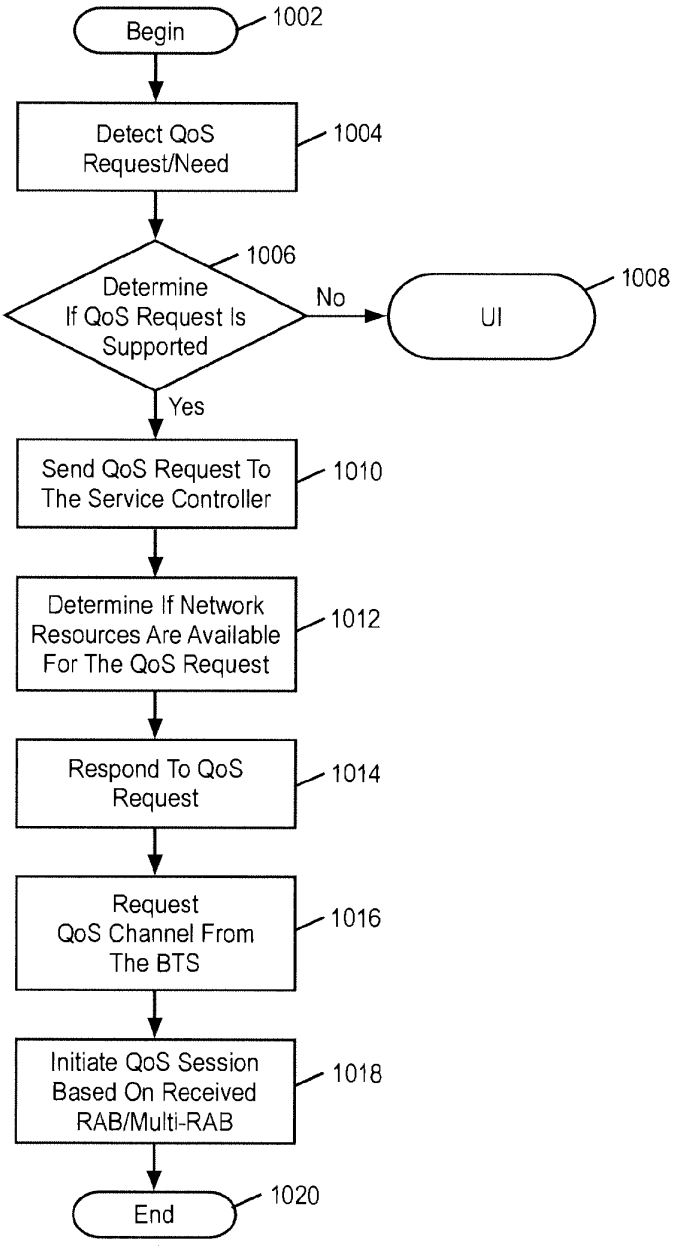

Begin
1002
Detect QoS Request/Need
1004
Determine If QoS Request Is Supported
1006
No
UI
1008
Yes
Send QoS Request To The Service Controller
1010
Determine If Network Resources Are Available For The QoS Request
1012
Respond To QoS Request
1014
Request QoS Channel From The BTS
1016
Initiate QoS Session Based On Received RAB/Multi-RAB
1018
End
1020

FIG. 10

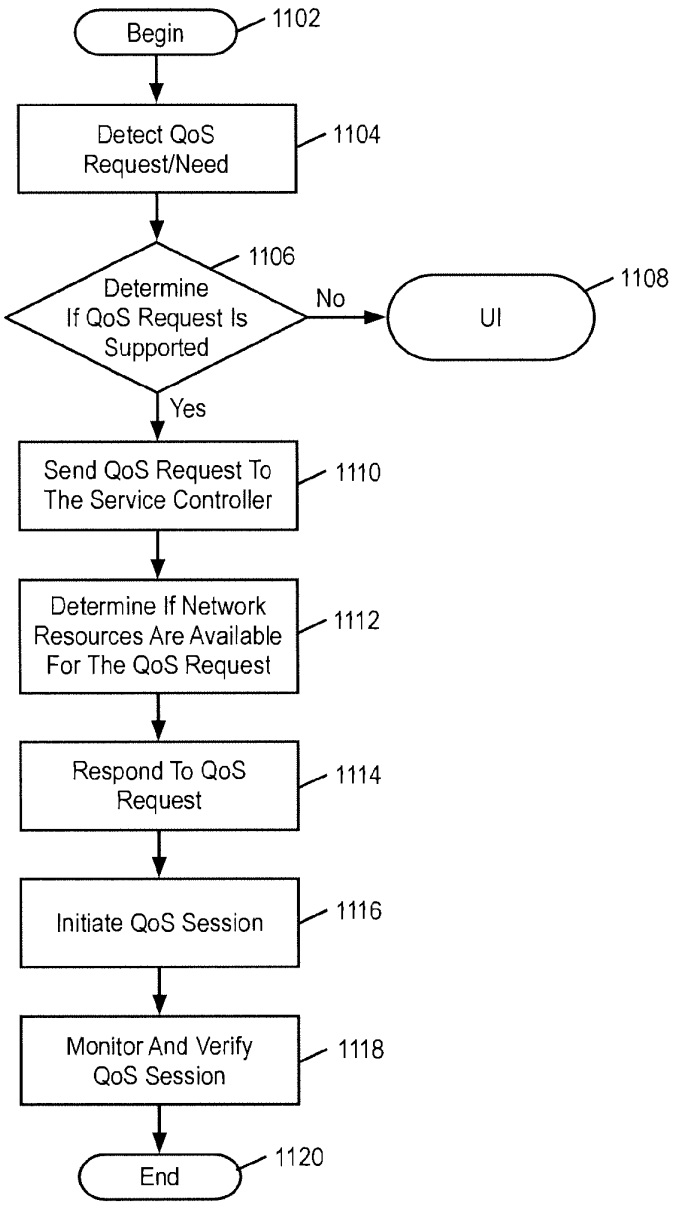

Begin
1102
Detect QoS Request/Need
1104
Determine If QoS Request Is Supported
1106
No
UI
1108
Yes
Send QoS Request To The Service Controller
1110
Determine If Network Resources Are Available For The QoS Request
1112
Respond To QoS Request
1114
Initiate QoS Session
1116
Monitor And Verify QoS Session
1118
End
1120

FIG. 11

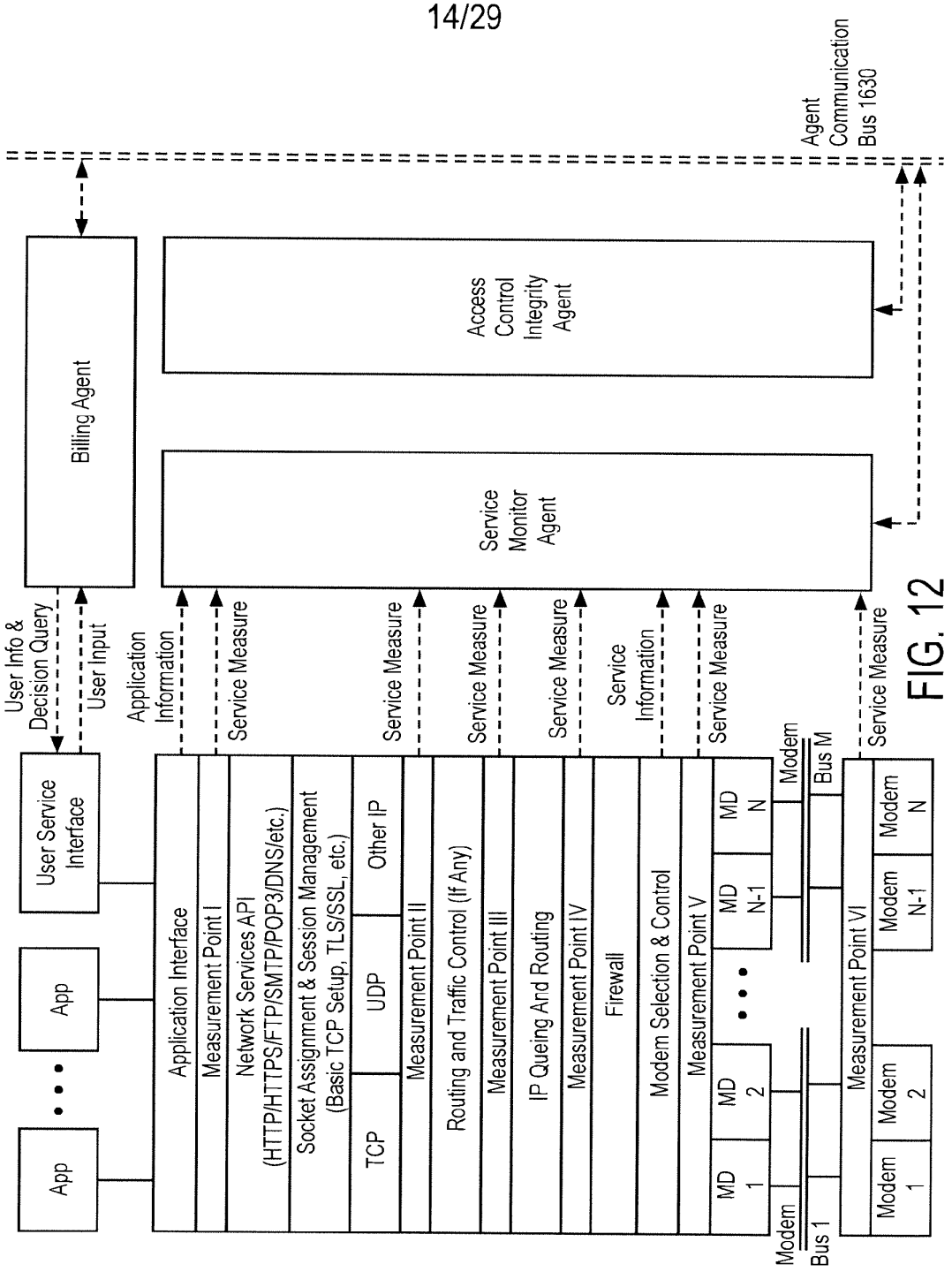

Agent Communication Bus 1630
Billing Agent
Access Control Integrity Agent
Service Monitor Agent
User Info & Decision Query
User Input
Application Information
Service Measure
Service Measure
Service Measure
Service Measure
Service Information
Service Measure
Service Measure
User Service Interface
App
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 Queing And Routing
Measurement Point IV
Firewall
Modem Selection & Control
Measurement Point V
MD 1
MD 2
MD N-1
MD N
Modem
Bus M
Modem
Bus 1
Measurement Point VI
Modem 1
Modem 2
Modem N-1
Modem N

FIG. 12

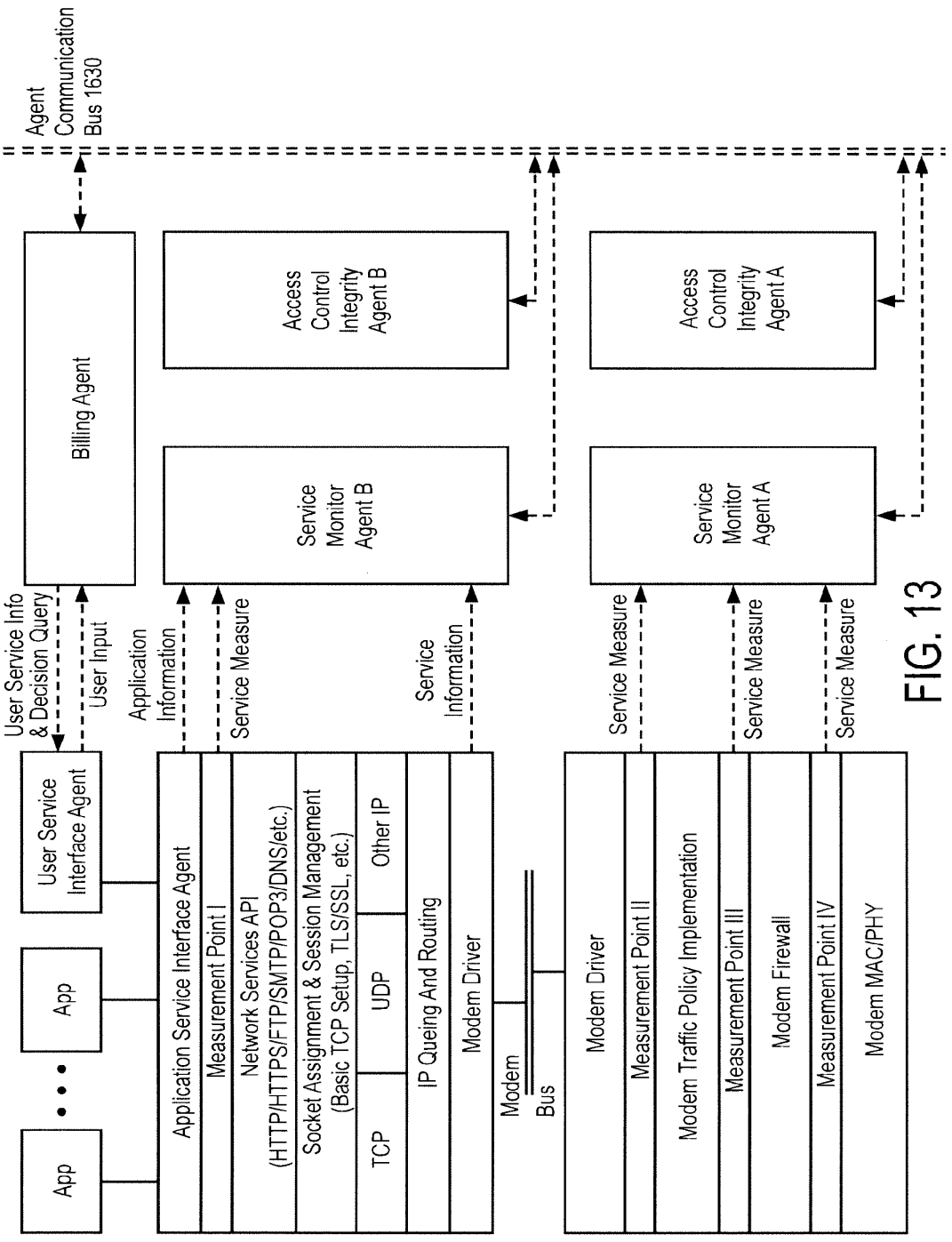

Agent Communication Bus 1630
Billing Agent
Access Control Integrity Agent B
Access Control Integrity Agent A
Service Monitor Agent B
Service Monitor Agent A
User Service Info & Decision Query
User Input
Application Information
Service Measure
Service Information
Service Measure
Service Measure
Service 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 Queing 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

FIG. 13

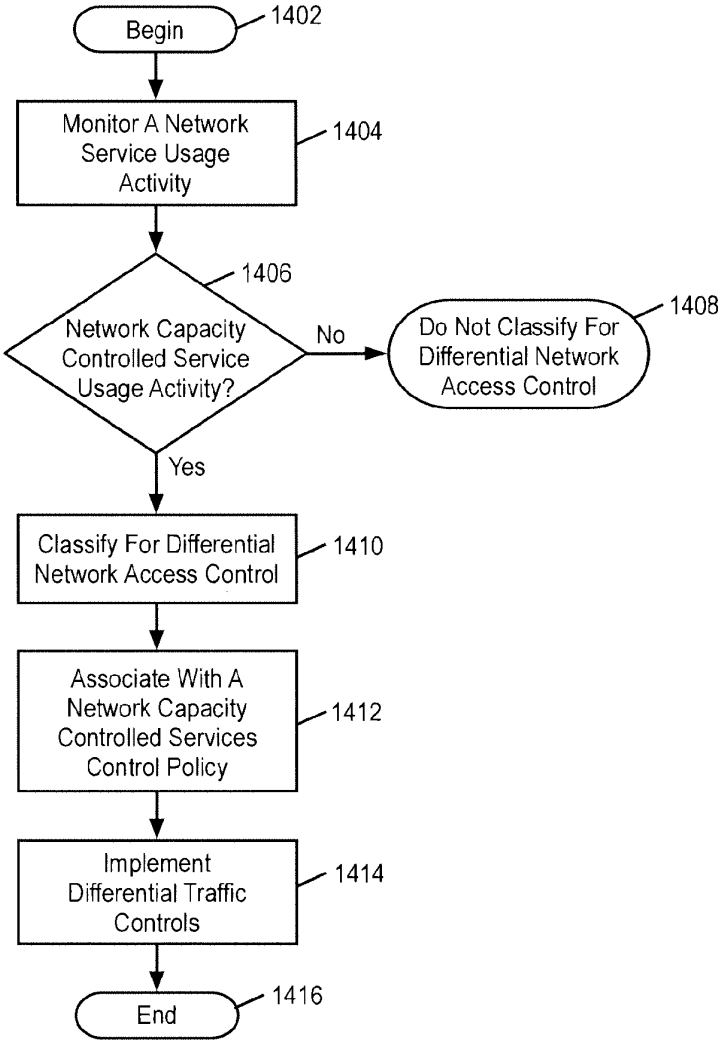

Begin
1402
Monitor A Network Service Usage Activity
1404
1406
Network Capacity Controlled Service Usage Activity?
No
Do Not Classify For Differential Network Access Control
1408
Yes
Classify For Differential Network Access Control
1410
Associate With A Network Capacity Controlled Services Control Policy
1412
Implement Differential Traffic Controls
1414
End
1416

FIG. 14

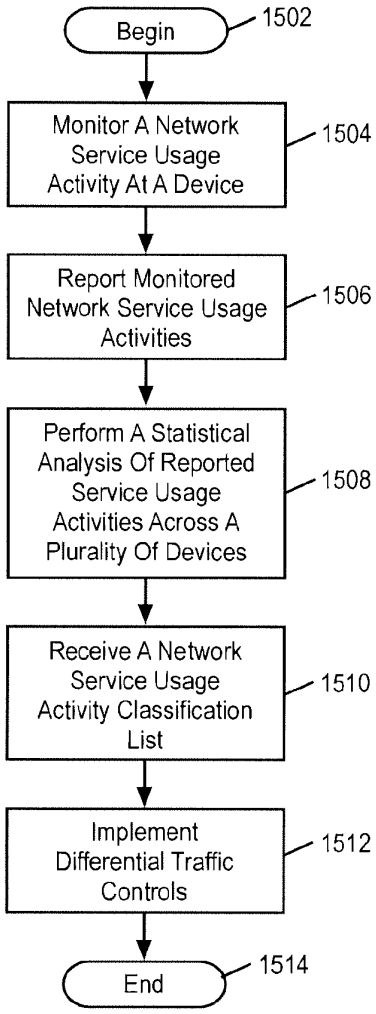

Begin
1502
Monitor A Network Service Usage Activity At A Device
1504
Report Monitored Network Service Usage Activities
1506
Perform A Statistical Analysis Of Reported Service Usage Activities Across A Plurality Of Devices
1508
Receive A Network Service Usage Activity Classification List
1510
Implement Differential Traffic Controls
1512
End
1514

FIG. 15

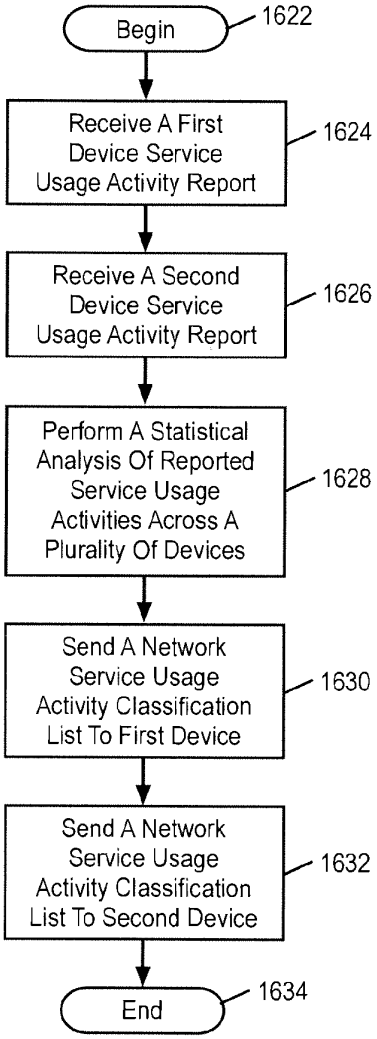

Begin
1622
Receive A First Device Service Usage Activity Report
1624
Receive A Second Device Service Usage Activity Report
1626
Perform A Statistical Analysis Of Reported Service Usage Activities Across A Plurality Of Devices
1628
Send A Network Service Usage Activity Classification List To First Device
1630
Send A Network Service Usage Activity Classification List To Second Device
1632
End
1634

FIG. 16

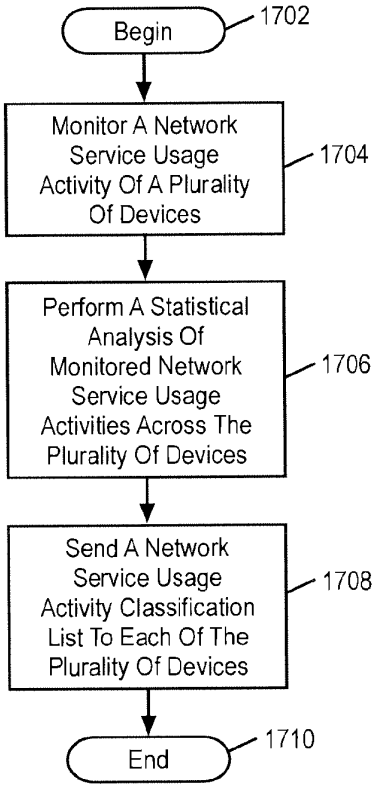

Begin
1702
Monitor A Network Service Usage Activity Of A Plurality Of Devices
1704
Perform A Statistical Analysis Of Monitored Network Service Usage Activities Across The Plurality Of Devices
1706
Send A Network Service Usage Activity Classification List To Each Of The Plurality Of Devices
1708
End
1710

FIG. 17

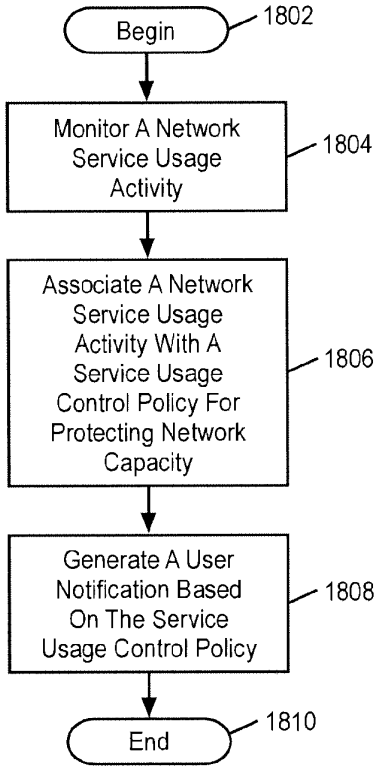

Begin
1802
Monitor A Network Service Usage Activity
1804
Associate A Network Service Usage Activity With A Service Usage Control Policy For Protecting Network Capacity
1806
Generate A User Notification Based On The Service Usage Control Policy
1808
End
1810

FIG. 18

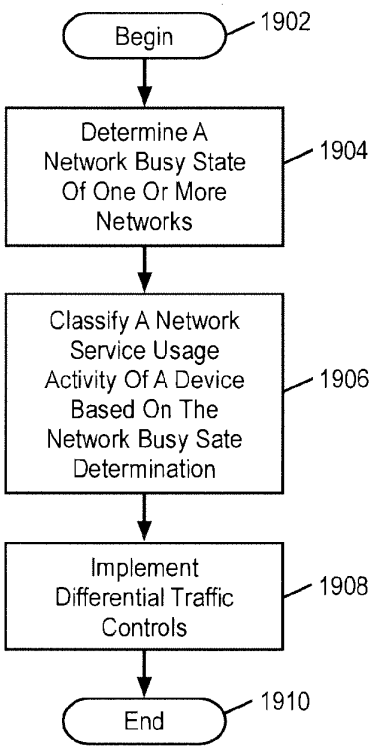

Begin
1902
Determine A Network Busy State Of One Or More Networks
1904
Classify A Network Service Usage Activity Of A Device Based On The Network Busy Sate Determination
1906
Implement Differential Traffic Controls
1908
End
1910

FIG. 19

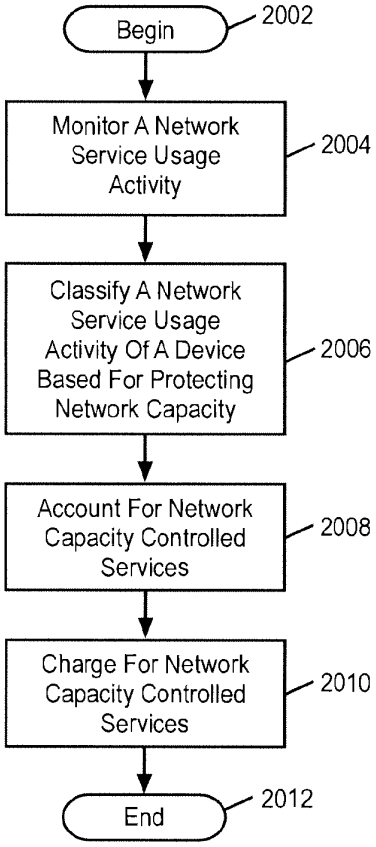

Begin
2002
Monitor A Network Service Usage Activity
2004
Classify A Network Service Usage Activity Of A Device Based For Protecting Network Capacity
2006
Account For Network Capacity Controlled Services
2008
Charge For Network Capacity Controlled Services
2010
End
2012

FIG. 20

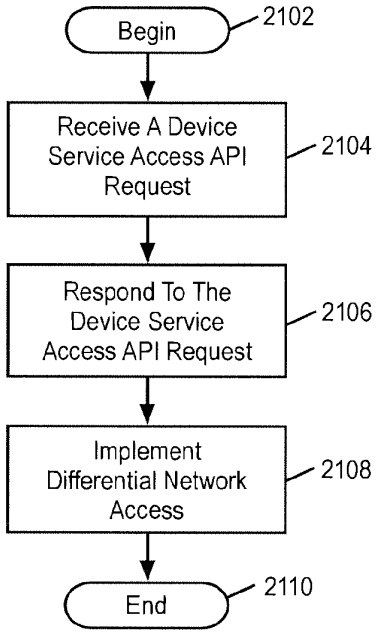

Begin
2102
Receive A Device Service Access API Request
2104
Respond To The Device Service Access API Request
2106
Implement Differential Network Access
2108
End
2110

FIG. 21

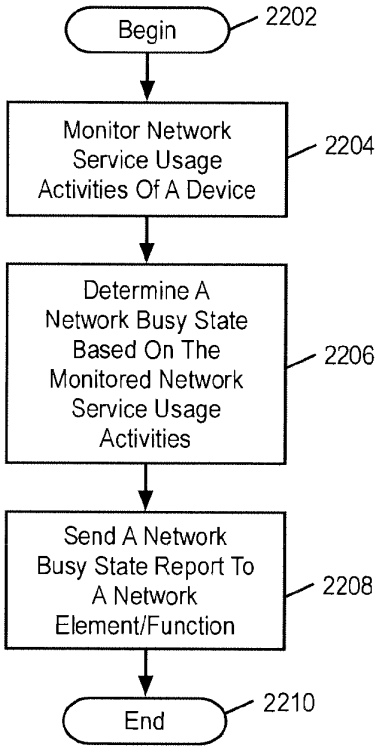

Begin
2202
Monitor Network Service Usage Activities Of A Device
2204
Determine A Network Busy State Based On The Monitored Network Service Usage Activities
2206
Send A Network Busy State Report To A Network Element/Function
2208
End
2210

FIG. 22

	NBS 10%	NBS 25%	NBS 50%	NBS 75%	NBS 90%
Outlook	6	5	4	3	2
Skype	7	6	2	1	0
Safari	5	4	3	2	1
Pandora	5	4	3	2	1
FaceBook	4	3	2	1	0
iTunes	7	6	3	1	0
QuickTime	8	6	4	1	0
AV Software	9	7	5	3	1
Online Backup	3	2	1	1	0
OS Update	2	1	0	0	0

FIG. 23

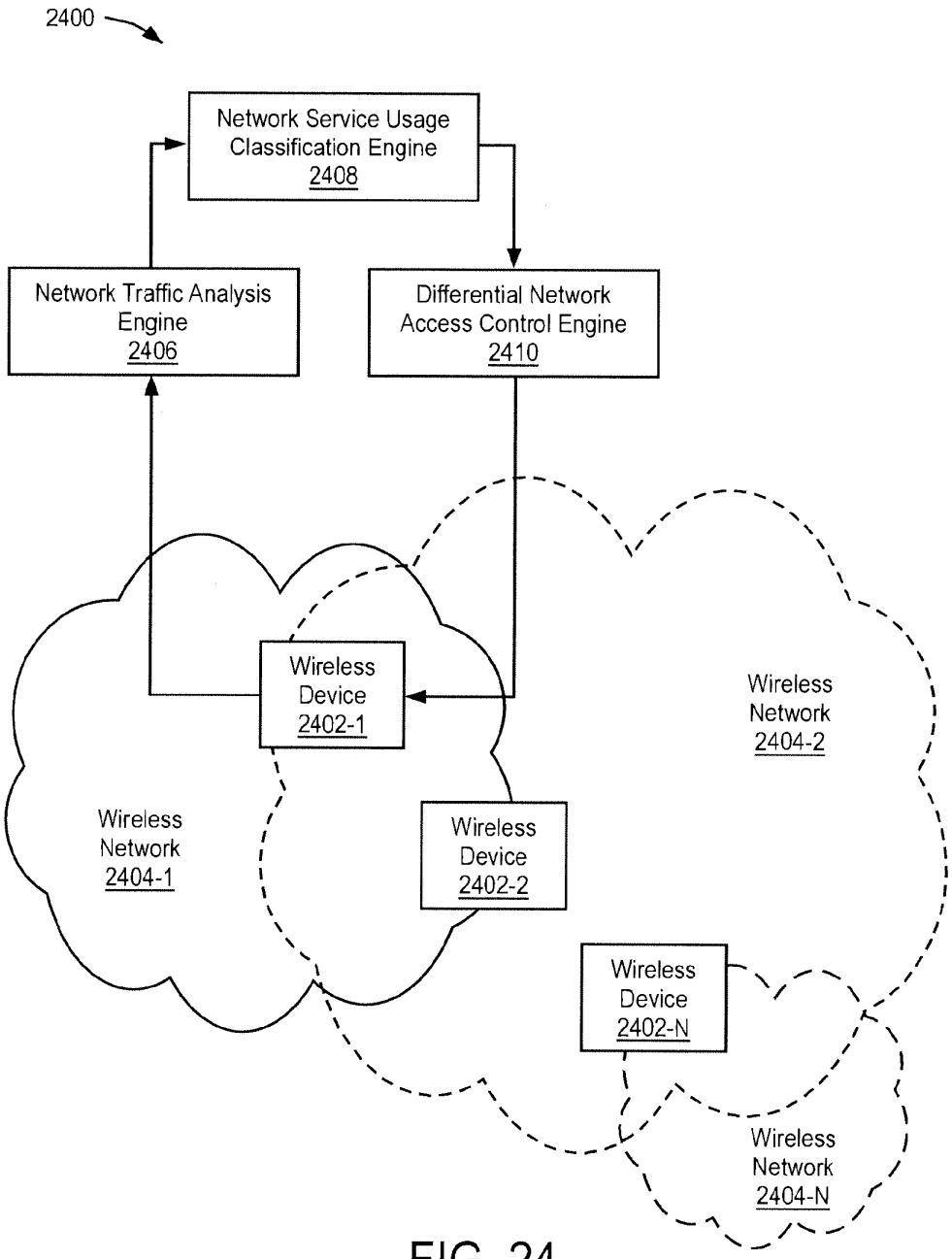

2400
Network Service Usage Classification Engine 2408
Network Traffic Analysis Engine 2406
Differential Network Access Control Engine 2410
Wireless Device 2402-1
Wireless Network 2404-1
Wireless Device 2402-2
Wireless Network 2404-2
Wireless Device 2402-N
Wireless Network 2404-N

FIG. 24

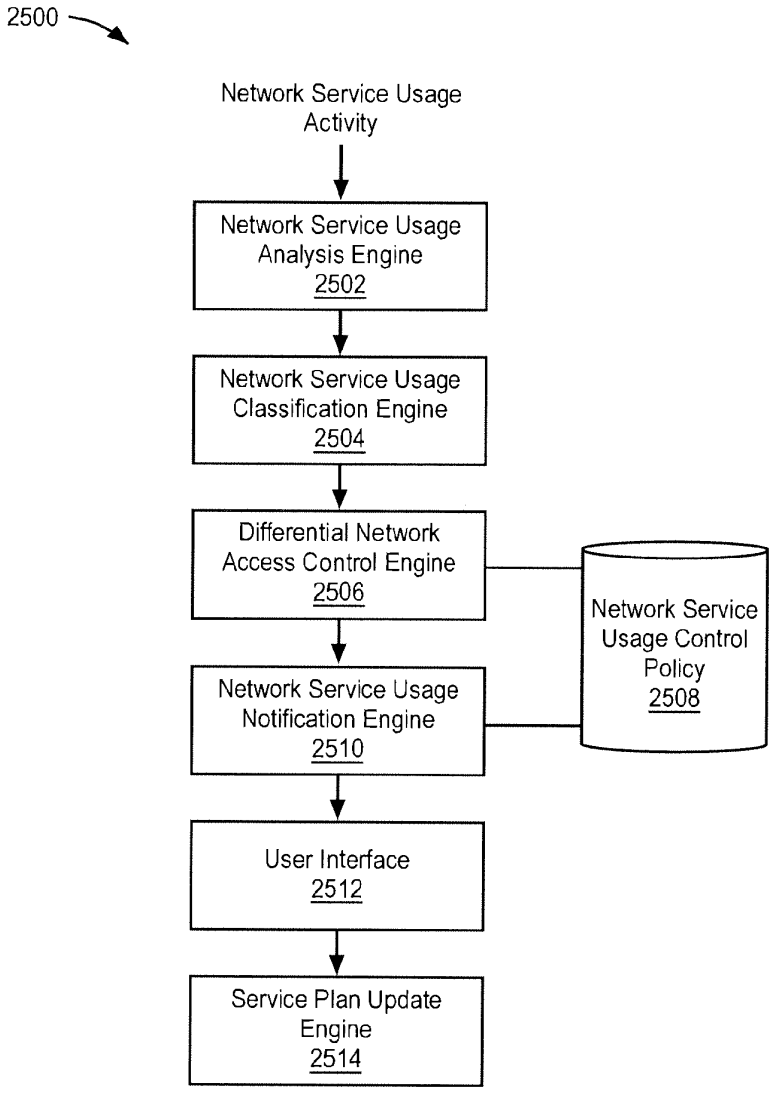

2500
Network Service Usage Activity
Network Service Usage Analysis Engine 2502
Network Service Usage Classification Engine 2504
Differential Network Access Control Engine 2506
Network Service Usage Control Policy 2508
Network Service Usage Notification Engine 2510
User Interface 2512
Service Plan Update Engine 2514

FIG. 25

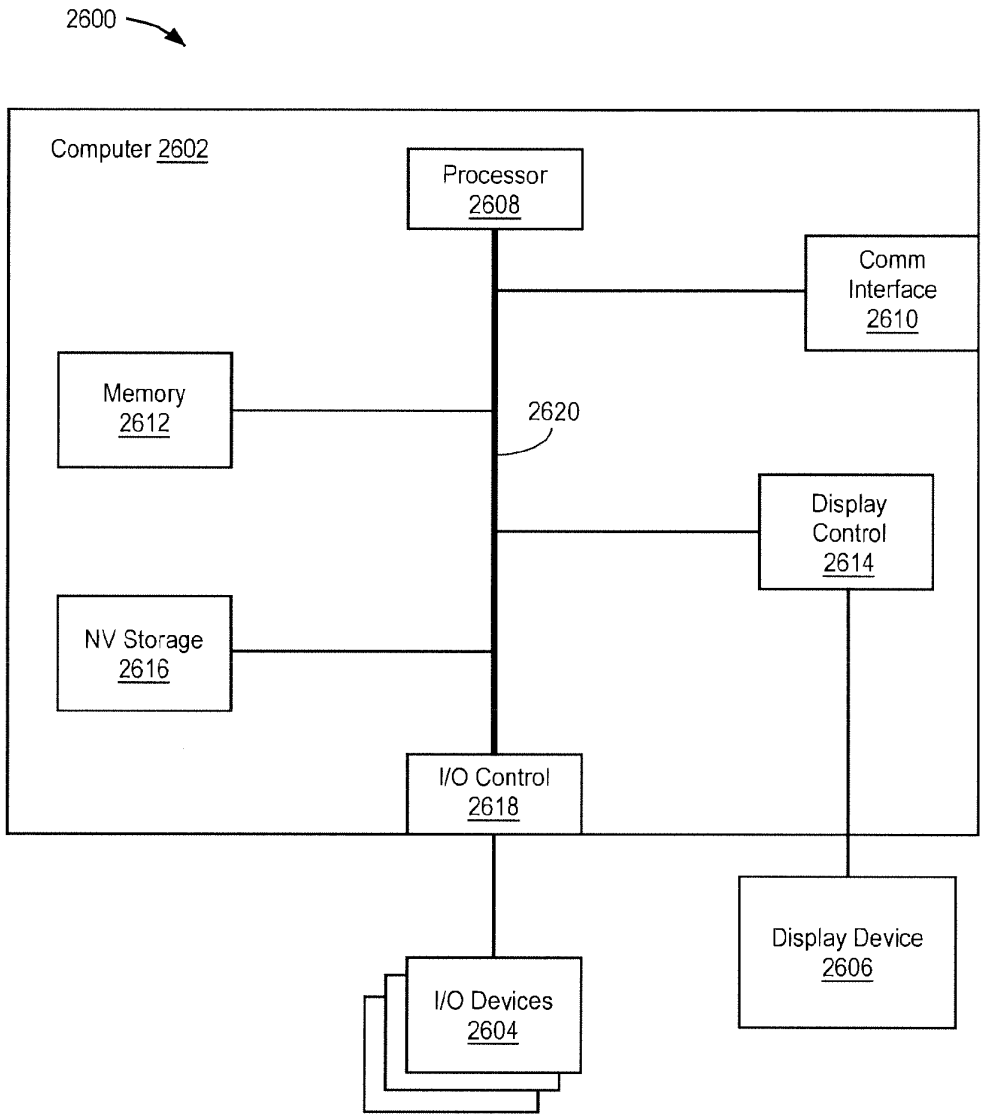

2600
Computer 2602
Processor 2608
Comm Interface 2610
Memory 2612
2620
Display Control 2614
NV Storage 2616
I/O Control 2618
Display Device 2606
I/O Devices 2604

FIG. 26

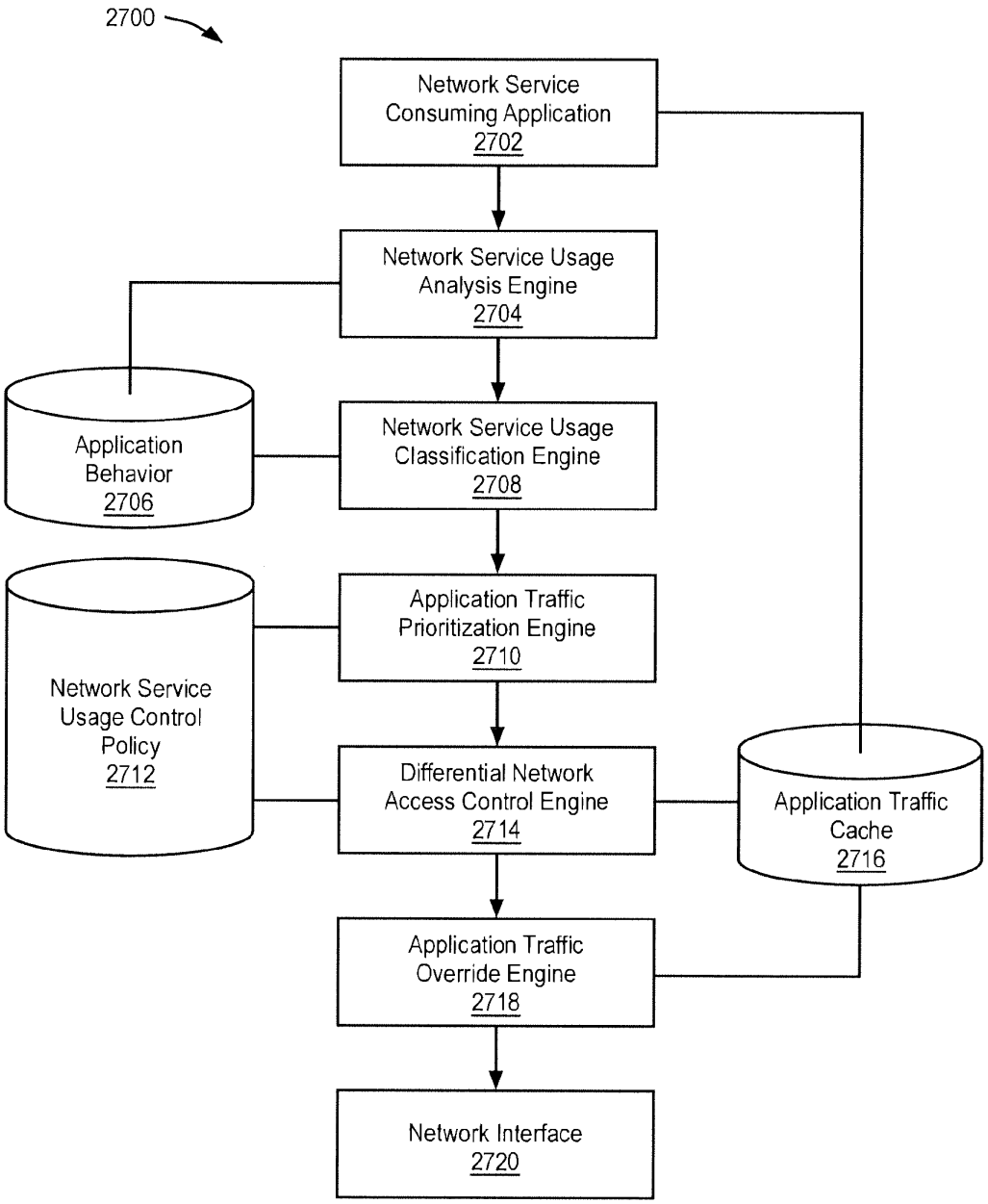

2700
Network Service Consuming Application 2702
Network Service Usage Analysis Engine 2704
Application Behavior 2706
Network Service Usage Classification Engine 2708
Network Service Usage Control Policy 2712
Application Traffic Prioritization Engine 2710
Differential Network Access Control Engine 2714
Application Traffic Cache 2716
Application Traffic Override Engine 2718
Network Interface 2720

FIG. 27

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 11/00937

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G01R 31/08 (2011.01)
USPC - 370/252
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC(8) - G01R 31/08 (2011.01)
USPC - 370/252

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC - 370/241, 252, 254, 259 (keyword limited - see terms below)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Electronic Databases: PubWEST(PGPB,USPT,USOC,EPAB,JPAB); Google Patents/Scholar
Search terms used: Communication, network, usage, activity, service, capacity, access, protect, classification

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X — Y	US 7,322,044 B2 (Hrastar) 22 January 2008 (22.01.2008), entire document, especially col. 7, ln. 35-40; col. 14, ln. 37-59; col. 29, ln. 13-33	1-18, 25, 28, 30-32, 40, 42, 47-52 --- 19-24, 26, 27, 29, 33-39, 41, 43-46, 53-113
Y	US 2008/0318547 A1 (Ballou et al.) 25 December 2008 (25.12.2008), para. [0101], [0170]	26, 33, 35
Y	US 7,180,855 B1 (Lin) 20 February 2007 (20.02.2007), abstract, col. 6, ln. 1-5	27, 37-39, 43
Y	US 2009/0257379 A1 (Robinson et al.) 15 October 2009 (15.10.2009), para. [0095], [0099]	19-24, 34
Y	US 2008/0162637 A1 (Adamczyk et al.) 03 July 2008 (03.07.2008), para. [0256]-[0274]	19-24, 36, 41
Y	US 2007/0259673 A1 (Willars et al.) 08 November 2007 (08.11.2007), para. [0036], [0039], [0047]	29, 44-46
Y	US 2010/0082431 A1 (Ramer et al.) 01April 2010 (01.04.2010), entire document, especially para. [0191], [0205]	53-113
A	US 20090180391 A1 (Petersen et al.) 16 July 2009 (16.07.2009), entire document	1-113
A	US 7,324,447 B1 (Morford) 29 January 2008 (29.01.2008), entire document	1-113
A	US 2007/0263558 A1 (Salomone) 15 November 2007 (15.11.2007), entire document	53-113

☐ Further documents are listed in the continuation of Box C. ☐

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 September 2011 (28.09.2011)	17 OCT 2011
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (July 2009)

Electronic Acknowledgement Receipt

EFS ID:	19597255
Application Number:	14082040
International Application Number:	
Confirmation Number:	1015
Title of Invention:	Device-Assisted Services for Protecting Network Capacity
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	Krista Susan Jacobsen
Filer Authorized By:	
Attorney Docket Number:	RALEP032C1
Receipt Date:	16-JUL-2014
Filing Date:	15-NOV-2013
Time Stamp:	15:21:57
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	P032C1IDS.pdf	612302 c8dc027faeb63371b55ec78b11f4de87081b667d	no	4

Warnings:	
Information:	

2	Foreign Reference	Jiang.pdf	10963497 3beb6debdf2ebd6470e65bb7d92def5fd16d49ae	no	34
Warnings:					
Information:					
3	Foreign Reference	Raleigh.pdf	5227173 abf39a10aa9302a631c02c725b5937a58682176c	no	240
Warnings:					
Information:					
			Total Files Size (in bytes):	16802972	

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

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

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

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

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

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

Application Number	14082040
Filing Date	2013-11-15
First Named Inventor	Gregory G. Raleigh
Art Unit	2447
Examiner Name	not yet assigned
Attorney Docket Number	RALEP032C1

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	6185576	B1	2001-02-06	Mcintosh, Lowrie	
	2	7320029	B2	2008-01-15	Rinne et al.	
	3	7539132	B2	2009-05-26	Werner et al.	
	4	7805606	B2	2010-09-28	Birger et al.	
	5	8175574	B1	2012-05-08	Panda et al.	
	6	8180881	B2	2012-05-15	Seo et al.	
	7	8191124	B2	2012-05-29	Wynn et al.	
	8	8275415	B2	2012-09-25	Huslak, Nicholas S.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	9	8300575	B2	2012-10-30	Willars, Per	
	10	8315593	B2	2012-11-20	Gallant et al.	
	11	8347378	B2	2013-01-01	Merkin et al.	
	12	8375128	B2	2013-02-12	Tofighbakhsh et al.	
	13	8527410	B2	2013-09-03	Markki et al.	
	14	8539561	B2	2013-09-17	Gupta et al.	
	15	8554876	B2	2013-10-08	Winsor, Gerald W.	
	16	8666395	B2	2014-03-04	Silver, Andrew	
	17	8391834	B2	2013-03-05	Raleigh, Gregory G.	

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	1	20110238545		2011-09-29	Fanaian, Nabil Ruh et al.	
	2	20040170191	A	2004-09-02	Guo et al.	
	3	20040203833	A	2004-10-14	Rathunde, Dale F. et al.	
	4	20050186948	A	2005-08-25	Gallagher et al.	
	5	20070147317	A	2007-06-28	Smith et al.	
	6	20080025230	A	2008-01-31	Patel et al.	
	7	20080056273	A	2008-03-06	Pelletier et al.	
	8	20080270212	A	2008-10-30	Blight et al.	
	9	20100030890	A	2010-02-04	Dutta et al.	
	10	20110110309	A	2011-05-12	Bennett, James D.	
If you wish to add additional U.S. Published Application citation information please click the Add button. Add						
FOREIGN PATENT DOCUMENTS Remove						

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] ¡	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	1310401	CN	A	2001-08-29	Wang, Di Xing		☐
	2	2466831	EP	A1	2012-06-20	Openet Telecom Ltd. - Mcnamee et al.		☐
	3	2007133844	WO	A	2007-11-22	Camiant, Inc.		☐
	4	1999027723	WO	A1	1999-06-03	Telefonaktiebolaget LM Ericsson		☐

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

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	"End to End QoS Solution for Real-time Multimedia Application;" Computer Engineering and Applications, 2007, 43 (4): 155-159, by Tan Zu-guo, Wang Wen-juan; Information and Science School, Zhanjian Normal College, Zhan jiang, Guangdong 524048, China	☐
	2	"ASA/PIX: Allow Split Tunneling for VPN Clients on the ASA Configuration Example," Document ID 70917, January 10, 2008	☐

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

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

CERTIFICATION STATEMENT

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

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

OR

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

☐ See attached certification statement.

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

☒ None

SIGNATURE

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

Signature	/Krista S. Jacobsen/	Date (YYYY-MM-DD)	2014-05-22
Name/Print	Krista S. Jacobsen	Registration Number	59374

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 2 466 831 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
20.06.2012 Bulletin 2012/25

(51) Int Cl.:
H04L 12/56 *(2006.01)* ***H04L 29/08*** *(2006.01)*
H04L 29/06 *(2006.01)*

(21) Application number: **11193499.8**

(22) Date of filing: **14.12.2011**

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA ME

(30) Priority: **16.12.2010 US 42398610 P**
07.06.2011 US 201113494300
01.12.2011 US 201113309221

(71) Applicant: **Openet Telecom Ltd.**
12 Dublin (IR)

(72) Inventors:
- **McNamee, Alan**
  Dublin, 9 (IE)
- **Dunne, Cameron Ross**
  County Kildare (IE)
- **McCann, Fergus**
  Dublin, 12 (IE)
- **O'Sullivan, Michael**
  Dublin, 12 (IE)
- **Byrne, Niall**
  Dublin, 12 (IE)
- **Hogan, Joe**
  County Dublin (IE)

(74) Representative: **Kelly, Madeleine**
FRKelly
27 Clyde Road
Ballsbridge
Dublin 4 (IE)

(54) Methods, systems and devices for pipeline processing

(57) Methods, servers and systems for communicating signaling information in a telecommunications signaling network implement methods that include receiving a first message encoding signaling information from a source component and processing the message using a fixed pipeline having a plurality of modules, each module having at least one procedure for performing a specific set of tasks. Application level routing operations may be performed to identify a suitable destination component. Information contained in the first message may be used to generate a second message encoding signaling information, which is sent to the identified destination component.

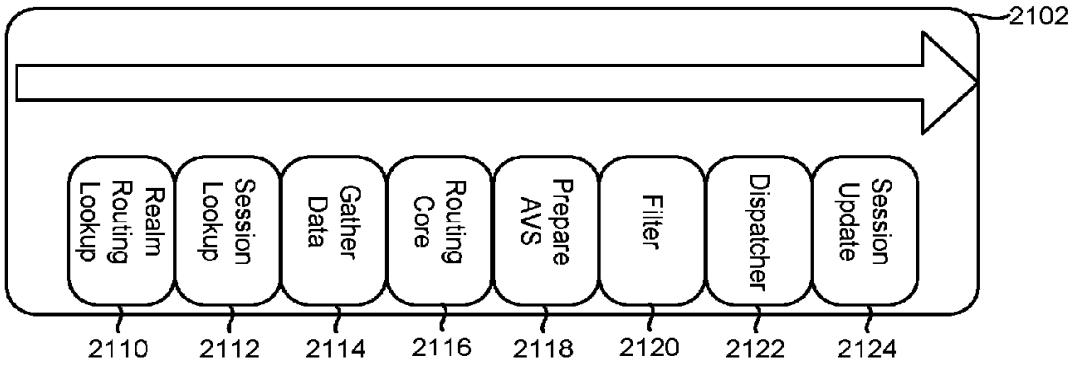


FIG. 21

EP 2 466 831 A1

Printed by Jouve, 75001 PARIS (FR)

Description

BACKGROUND

[0001] Wireless and cellular communication technologies have seen dramatic improvements over the past few years. Cellular service providers now offer users a wide array of services, higher usage limits and attractive subscription plans. Wireless dongles and embedded wireless modem cards allow users to use tablet computers, netbooks and laptops to access wireless Internet protocol (IP) and data services through the cellular networks. Internet-enabled smart phones, tablets and gaming consoles have become essential personal accessories, connecting users to friends, work, leisure activities and entertainment. Users now have more choices and expect to have access to content, data and communications at any time, in any place. As more users utilize these services, telecommunication system operator networks must expand to meet the increase in user demand, support the array of new services and provide fast, reliable communications. This expansion has greatly increased the complexity of wireless and cellular networks, and the efficient routing and management of signalling traffic is becoming an ever more challenging task.

SUMMARY

[0002] The various embodiments provide methods, devices and systems for enabling communications between multiple instances of components in a telecommunications network. The various embodiments provide protocol agnostic interfaces that allow communications between source and destination nodes in a telecommunication system operator network. Routing and load-balancing decisions may be made dynamically based on a context and content of the information being communicated. Messages being communicated may be opened and the information contained therein used to make intelligent connection management and control/rules routing decisions. Calls may be made to external systems requesting additional information for a specific message being communicated. Information from external systems may be used to modify the contents of the information being communicated or to aid in routing and/or load balancing operations within the operator's network. Information specific to a particular network node, protocol, application, message or message type may be stored in an internal memory and referenced for future routing and/or load balancing operations. Routing and load balancing algorithms may be updated as internal/external data changes.

[0003] The various embodiments include methods of communicating signaling information in a telecommunications signaling network that may include receiving, in a first processor, a first message encoding signaling information from a source component, decoding the received first message into an internal representation of the message, processing the internal representation of the message via a pipeline having a plurality of stages, in which each stage may contain one or more procedures for performing a specific set of tasks, performing application level routing operations using contextual information derived from the internal representation to identify a destination component, encoding the signaling information contained in the internal representation into a second message, and sending the second message encoding the signaling information to the identified destination component. In an embodiment, performing application level routing operations using contextual information derived from the internal representation to identify a destination component includes using at least one pipeline stage to make a routing decision using a discrete number of configurable procedures. In a further embodiment, the pipeline type is one of a request handler pipeline, a response handler pipeline, a failover handler pipeline, or a redirect handler pipeline. In a further embodiment, the pipeline type and instance is selected on a per message type or on a per application basis. In a further embodiment, the pipeline may have a plurality of stages that include at least one stage from the group consisting of a realm routing lookup stage, a session lookup stage, a gather data stage, a routing core stage, a prepare AVS stage, a filter stage, a dispatcher stage, a session update stage, and a redirect stage.

[0004] Further embodiments include a server configured with server-executable instructions to perform operations that may include receiving a first message encoding signaling information from a source component, decoding the received first message into an internal representation of the message, processing the internal representation of the message via a pipeline having a plurality of stages, in which each stage may contain one or more procedures for performing a specific set of tasks, performing application level routing operations using contextual information derived from the internal representation to identify a destination component, encoding the signaling information contained in the internal representation into a second message, and sending the second message encoding the signaling information to the identified destination component. In an embodiment, the processor may be configured with processor-executable instructions to perform operations such that performing application level routing operations using contextual information derived from the internal representation to identify a destination component includes using at least one pipeline stage to make a routing decision using a discrete number of configurable procedures. In a further embodiment, the processor may be configured with processor-executable instructions to perform operations such that the pipeline type is one of a request handler pipeline, a response handler pipeline, a failover handler pipeline, or a redirect handler pipeline. In a further embodiment, the processor may be configured with processor-executable instructions to perform operations such that the pipeline type and instance is selected on a per message type

or on a per application basis. In a further embodiment, the pipeline may feature a plurality of stages that include at least one stage from the group consisting of a realm routing lookup stage, a session lookup stage, a gather data stage, a routing core stage, a prepare AVS stage, a filter stage, a dispatcher stage, a session update stage, and a redirect stage.

[0005] Further embodiments include a non-transitory server-readable storage medium having stored thereon server-executable instructions configured to cause a server to perform operations that may include receiving a first message encoding signaling information from a source component, decoding the received first message into an internal representation of the message, processing the internal representation of the message via a pipeline having a plurality of stages, in which each stage may contain one or more procedures for performing a specific set of tasks, performing application level routing operations using contextual information derived from the internal representation to identify a destination component, encoding the signaling information contained in the internal representation into a second message, and sending the second message encoding the signaling information to the identified destination component. In an embodiment, the stored server-executable instructions may be configured to cause a server to perform operations such that performing application level routing operations using contextual information derived from the internal representation to identify a destination component includes using at least one pipeline stage to make a routing decision using a discrete number of configurable procedures. In a further embodiment, the stored server-executable instructions may be configured to cause a server to perform operations such that the pipeline type is one of a request handler pipeline, a response handler pipeline, a failover handler pipeline, or a redirect handler pipeline. In a further embodiment, the stored server-executable instructions may be configured to cause a server to perform operations such that the pipeline type and instance is selected on a per message type or on a per application basis. In a further embodiment, the stored server-executable instructions may be configured to cause a server to perform operations such that the pipeline has a plurality of stages that include at least one stage from the group consisting of a realm routing lookup stage, a session lookup stage, a gather data stage, a routing core stage, a prepare AVS stage, a filter stage, a dispatcher stage, a session update stage, and a redirect stage.

BRIEF DESCRIPTION OF THE DRAWINGS

[0006] The accompanying drawings, which are incorporated herein and constitute part of this specification, illustrate exemplary aspects of the invention, and, together with the general description given above and the detailed description given below, serve to explain features of the invention.

[0007] FIG. 1 is a communication system block diagram illustrating network components of a communication system having an evolved packet core (EPC) architecture suitable for use in the various embodiments.

[0008] FIG. 2 is a communication system block diagram illustrating network components of an example communication-system having a policy and charging control (PCC) network in accordance with the various embodiments.

[0009] FIG. 3 is a network architectural diagram illustrating logical components and information flows in an example policy and charging control network.

[0010] FIG. 4 is a network architectural diagram illustrating logical components and communication protocols in an example policy and charging control network.

[0011] FIG. 5 is an illustration of an example message structure for communicating signaling information suitable for use with an embodiment.

[0012] FIG. 6 is a network architectural diagram illustrating an expanded policy and charging control network having multiple instances of the same logical components.

[0013] FIG. 7A is a network architectural diagram illustrating an expanded policy and charging control network that includes a Diameter routing agent (DRA).

[0014] FIG. 7B is an architectural diagram illustrating an expanded policy and charging control network that includes a dynamic context router (DCR) in accordance with various embodiments.

[0015] FIG. 8 is a component block diagram illustrating the logical components and communication links of an example dynamic context router system in accordance with various embodiments.

[0016] FIG. 9 is an architectural diagram illustrating example signaling and message flows in a network that includes a dynamic context router system in accordance with the various embodiments.

[0017] FIG. 10A is a process flow diagram illustrating an embodiment dynamic context router method for receiving, processing and transmitting signaling messages in accordance with various embodiments.

[0018] FIG. 10B is a process flow diagram illustrating an embodiment dynamic context router method for determining if a specific instance of a destination node is required to perform load balancing and context routing operations in accordance with various embodiments.

[0019] FIG. 11 is an architectural diagram illustrating example logical components and information flows of an example dynamic context router system in accordance with an embodiment.

[0020] FIG. 12 is an illustration of an example dynamic context router topology tree that may be used for performing routing and load balancing operations by hierarchy in accordance with various embodiments.

[0021] FIG. 13 is a process flow diagram illustrating an embodiment dynamic context router method for processing Diameter messages in accordance with various embodiments.

[0022] FIG. 14 is a process flow diagram illustrating an embodiment dynamic context router method for performing hunting operations in accordance with various embodiments.

[0023] FIGs. 15A-17C are network architectural diagrams illustrating logical components and information flows of example dynamic context router systems configured to perform failover operations in accordance with various embodiments.

[0024] FIG. 18 is a network architectural diagram illustrating example logical components and information flows of an example dynamic context router system configured to perform fork routing operations.

[0025] FIG. 19 is a process flow diagram illustrating an embodiment dynamic context router method for performing fork routing operations in accordance with various embodiments.

[0026] FIG. 20 is a component block diagram illustrating the logical components and interfaces of an example dynamic context router system in accordance with the various embodiments.

[0027] FIG. 21 is an illustration of an example request message processing pipeline in a dynamic context router system.

[0028] FIG. 22 is an illustration of an example response message processing pipeline in a dynamic context router system.

[0029] FIG. 23 is an illustration of an example failover message processing pipeline in a dynamic context router system.

[0030] FIG. 24 is an illustration of an example message redirect processing pipeline in a dynamic context router system.

[0031] FIG. 25 is a component block diagram of a server suitable for use with an embodiment.

DETAILED DESCRIPTION

[0032] The various embodiments will be described in detail with reference to the accompanying drawings. Wherever possible, the same reference numbers will be used throughout the drawings to refer to the same or like parts. References made to particular examples and implementations are for illustrative purposes, and are not intended to limit the scope of the invention or the claims.

[0033] The word "exemplary" is used herein to mean "serving as an example, instance, or illustration." Any implementation described herein as "exemplary" is not necessarily to be construed as preferred or advantageous over other implementations.

[0034] The terms "mobile device," "wireless device" and "user equipment (UE)" may be used interchangeably and refer to any one of various cellular telephones, smartphones (e.g., iPhone®), personal data assistants (PDA's), palm-top computers, tablet computers, laptop computers, wireless electronic mail receivers (e.g., Blackberry®), VoIP phones, wire-line devices, devices implementing Machine-to-Machine (M2M) technologies, multimedia/Internet enabled cellular telephones, and similar electronic devices capable of sending and receiving wireless communication signals. A wireless device may include a programmable processor and memory. In a preferred embodiment, the wireless device is a cellular handheld device (e.g., a mobile device), which can communicate via a cellular telephone communications network.

[0035] The phrases "Diameter reference points," "Diameter applications," and "Diameter interfaces" may be used interchangeably and refer to specific implementations of the Diameter protocol. However, when possible, the phrase "Diameter application" is used to describe an extension of the Diameter base protocol (which is built on top of the Diameter base protocol) and the phrase "Diameter reference point" is used to describe an interface between network components that employ the Diameter protocol to realize communications (i.e., network components realize communications over a reference point). Diameter applications may use the same name as Diameter reference points (e.g., Gx reference point and Gx Diameter application), the distinction being that at each end of the reference point there may be a client node and a server node.

[0036] As used herein, the word "domain" refers to a logical entity configured entirely within the DCR system that can be used to represent any routing destination based on a scenario. It should be understood that the domains discussed herein differ from, and provide functionality over and above those provided by, the domain-like concepts present in the Diameter protocol standard. Examples include the "Destination-Realm" and "Destination-Host" attribute-value-pairs (AVPs).

[0037] The term "attribute value stream" and its acronym "AVS" are used herein to refer to a message structure that stores information corresponding to information carried by a telecommunications network message (e.g., a Diameter message). Each AVS may include one or more structured fields (e.g., a session identification field, a policy and charging rules function identification field, a domain field, an origin-host field, a subscriber identification field, an address field, etc.), and may be used by a dynamic context router (DCR) system as internal representation of a telecommunications network message (e.g., a Diameter message).

[0038] A number of different cellular and mobile communication services and standards are available or contemplated in the future, all of which may implement and benefit from the various embodiments. Such services and standards include, e.g., third generation partnership project (3GPP), long term evolution (LTE) systems, third generation wireless mobile communication technology (3G), fourth generation wireless mobile communication technology (4G), global system for mobile communications (GSM), universal mobile telecommunications system (UMTS), 3GSM, general packet radio service (GPRS), code division multiple access (CDMA) systems (e.g., cdmaOne, CDMA2000TM), enhanced data rates

for GSM evolution (EDGE), advanced mobile phone system (AMPS), digital AMPS (IS-136/TDMA), evolution-data optimized (EV-DO), digital enhanced cordless telecommunications (DECT), Worldwide Interoperability for Microwave Access (WiMAX), wireless local area network (WLAN), Wi-Fi Protected Access I & II (WPA, WPA2), and integrated digital enhanced network (iden). Each of these technologies involves, for example, the transmission and reception of signaling and content messages. It should be understood that any references to terminology and/or technical details related to an individual standard or technology are for illustrative purposes only, and are not intended to limit the scope of the claims to a particular communication system or technology unless specifically recited in the claim language.

[0039] The various embodiments provide methods, devices and systems for managing communications in a network. The various embodiments provide a dynamic context router (DCR) that operates as a flexible, protocol agnostic, application-level router and load balancer. The dynamic context router may perform message routing, relay, and redirect operations. The dynamic context router may identify communication partners and/or determine resource availability. The dynamic context router may make routing and load-balancing decisions dynamically based on the context and content of the information being communicated. The dynamic context router may look inside the messages being communicated and make intelligent decisions based on the content of the messages. The dynamic context router may make calls to external systems requesting additional information for a specific message being communicated. The dynamic context router may request information from external systems and use the information to modify the contents of the information being communicated or to aid in the routing and/or load balancing operations. The dynamic context router may store information specific to a particular network node, protocol, application, message or message type in an internal memory and reference the internal memories when processing future communications related to that node, protocol, application, message or message type. The dynamic context router may update its routing and load balancing algorithms as internal/external data changes.

[0040] In an embodiment, the dynamic context router may provide pipelining, topology hunting, and/or message forking operations.

[0041] In an embodiment, the dynamic context router may access subscriber information stored in subscriber profile repositories (SPRs) and use the subscriber information to aid its routing and load balancing operations. In an embodiment, the dynamic context router may modify the contents of the messages being communicated with subscriber information retrieved from a subscriber profile repository. In an embodiment, the dynamic context router may access online charging systems (OCSs) or off-line changing systems (OFCSs), and use charging and/or billing information from those systems to aid its routing and load balancing operations and/or to modify the contents of the messages being communicated. In an embodiment, the dynamic context router may access additional business support systems (BSS)/operations support systems (OSS) to aid its routing and load balancing operations and/or to modify the contents of the messages being communicated.

[0042] In an embodiment, the dynamic context router (DCR) may generate, procure and/or use a topology tree, referred to herein as a "DCR topology tree." The DCR topology tree may be used to efficiently identify and locate nodes in the network. In an embodiment, the dynamic context router may use the DCR topology tree to perform routing and load balancing operations by hierarchy.

[0043] In an embodiment, the dynamic context router may perform message destination hunting operations to identify a correct instance of a destination node that cannot otherwise be ascertained from information included within the message or otherwise available. In an embodiment, the dynamic context router may use the DCR topology tree to performing hunting operations by hierarchy.

[0044] In an embodiment, the dynamic context router may communicate with a dictionary to receive decoding rules that can be used for decoding message types with which the dynamic context router is unfamiliar. In an aspect, the dictionaries may be implemented as databases, and the dictionary databases may be internal to the dynamic context router or external to the dynamic context router (e.g., may exist on dictionary servers). In an embodiment, the external dictionaries may be hosted "in the cloud" as part of a cloud computing implementation. In an embodiment, external dictionary servers may be used to centralize the configuration of the protocol capabilities. In an embodiment, the dynamic context router may access partial dictionaries to receive only the minimum amount of a rule or rules required to successfully decode messages, reducing latency and improving processing speeds.

[0045] In an embodiment, the dynamic context router may decode messages in multiple phases. For example, the dynamic context router may decode only a small portion of a message in a first phase and, if necessary, perform more extensive decoding operations in a second phase. In an embodiment, the need for the second phase of decoding may be determined based on the first phase decoding results and/or any combination of contextual and static information.

[0046] In an embodiment, the dynamic context router may incrementally decode messages. In this embodiment, incremental decoding may begin with decoding an initial portion of the message, and determining if the decoded portion identifies a destination component or if the destination component can be derived from the decoded portion. When it is determined that the previously decoded portions do not identify the destination component and/or that the destination component cannot be derived using the previously decoded portions, the dynamic con-

text router may then recursively decode subsequent portions of the message. The need for the continued decoding of additional portions of the message may be based on whether or not information extracted from the decoded portions may be used by the dynamic context router to identify a destination component.

[0047] In an embodiment, the dynamic context router may perform opaque proxy operations. In this embodiment, if the dynamic context router receives a message that is either partially syntactically or semantically invalid (and thus "opaque"), instead of sending an error message, the dynamic context router may decode only a portion of the message, leaving the rest of the message in the original format (e.g., binary wire format), package the message into a network transparent container, and send the container including the message to the destination node. In this manner, the dynamic context router may operate in a loose, tolerant mode that improves processing speeds, while supporting network nodes that do not fully comply with a particular standard.

[0048] In an embodiment, the dynamic context router may perform protocol translation operations. In an embodiment, the dynamic context router may include a flexible protocol translator module which converts received messages from a first protocol into a second protocol. In various embodiments, the first protocol may be the same as the second protocol, a subset of the second protocol, a superset of the second protocol, compatible with the second protocol, or completely independent of the second protocol.

[0049] In an embodiment, the dynamic context router may perform protocol translation operations even when the first and second protocols are the same.

[0050] Often, network nodes vary in their implementation of the same set of standards. This often occurs when the nodes are manufactured by different vendors or are operating different versions of software. For example, a vendor's implementation of a standard may not fully comply with the standards, the standards may have changed since the nodes were deployed, or there may be differences in implementations due to non-standard extensions. In such cases, messages originating from a source node may not be accepted by a destination node, even though the source node and the destination node implement the same protocol. In such cases, the dynamic context router may identify the differences in the implementations and change the structure and/or the content of the messages to ensure that the messages will be accepted by the destination node. This embodiment improves network efficiency by providing a protocol agnostic interface between source and destination nodes in a network. Source nodes may communicate with the dynamic context router using any protocol supported by the dynamic context router, and do not need to be informed of the protocols supported by the destination nodes. New instances of any destination node may be added to the network without informing the source nodes of the existence of the new destination node or of the protocols associated with the new node. Likewise, new instances of the source nodes may be added to the network without requiring the new source nodes to be informed of the other nodes in the network, their protocols, or the other intimate details of the network.

[0051] In an embodiment, the dynamic context router may perform protocol translation operations when the first protocol is completely independent of the second protocol. For example, the dynamic context router may receive hypertext transfer protocol (HTTP) messages and convert the messages into Diameter messages.

[0052] The dynamic context router may provide a protocol agnostic interface between source and destination nodes in a network which may serve to provide topology hiding and allow inter-protocol communication within a network. In an embodiment, the dynamic context router may operate as both a server and a client to further facilitate topology hiding. As mentioned above, the dynamic context router may receive messages from source nodes in a first protocol and send messages to a destination node in a second protocol. In an embodiment, the dynamic context router may remove all network specific information for each of the messages that it relays such that the source and destination nodes cannot determine the network topology through which the messages where routed. In an embodiment, the dynamic context router may perform physical topology hiding operations by removing all addressing information that may identify the location of the source nodes to the destination nodes, and the destination nodes to the source nodes.

[0053] The various embodiments provide scalable, distributed, highly available dynamic context router (DCR) systems capable of fast and efficient expansion. As discussed above, operator networks are expanding at an unprecedented rate. As these operator networks expand, so will the amount of signaling traffic that must be processed by each dynamic context router. To support this anticipated increase in workload, the various embodiments provide highly-available, highly-scalable dynamic context router systems that can support the addition of resources (e.g., additional cores, memories, servers, etc.), while maintaining high-availability.

[0054] The various embodiments provide dynamic context router systems configured to manage component failures. The dynamic context router may manage component failures by performing failover operations that automatically switch over to a redundant component (e.g., blade, server, DCR core, memory, network node, etc.) upon the failure or abnormal termination of a component. As new resources are introduced into the network and the dynamic context router systems, the probability of one or more components (e.g., server, processor, hard drive, DCR core, memory, etc.) failing increases. Various embodiments provide dynamic context router systems configured to perform multi-level and multi-tier failover operations that ensure continued dynamic context router operations in the event of multiple component failures. In an embodiment, the dynamic context router system

may be deployed in redundant pairs configured in a distributed array architecture with work load balancing schemes which, in combination, ensure continued dynamic context router operations in the event of failures.

[0055] As mentioned above, for reasons of availability and scalability it is common for multiple instances of particular network elements to be deployed within the same operator network. The deployment of multiple instances of the same component within a single network gives rise to both functionality and configuration overhead. Further, in cases where peer relationships traverse administrative boundaries, the network topology may be exposed across that boundary. Telecommunication system operator networks are particularly exposed in this regard, especially with the emergence of inter-operator Diameter applications, such as S9 and S6a. To meet these and other concerns, the various embodiments provide an extensive and flexible routing logic engine that may be configured to act as a network edge termination point or landing zone for roaming partners wishing to participate in these types of (e.g., Diameter) relationships.

[0056] In an embodiment, the dynamic context router (DCR) may perform application-level topology hiding operations. Certain protocols (e.g., Diameter) have application-level addresses. For example, each Diameter message includes a Diameter address (e.g., Origin-Host address) built into the structure of the messages that cannot be removed. In various embodiments, the dynamic context router may receive messages from source nodes, decode the message contents and store them in a memory, terminate the message, and create a new message that includes all of the stored contents, but not the address information of the source node.

[0057] In an embodiment, the dynamic context router may operate as a software appliance (i.e., may run on commodity hardware) that is capable of routing and load balancing network traffic using both static and context based routing rules.

[0058] The various embodiments may be implemented within a variety of communication systems, an example of which is illustrated in FIG. 1. Wireless devices 102 may be configured to send and receive voice, data and control signals to and from a service network 36 (and ultimately the Internet) using a variety of communication systems/technologies (e.g., GPRS, UMTS, LTE, cdmaOne, CDMA2000TM). For example, general packet radio service (GPRS) data transmitted from a wireless device 102 is received by a base transceiver station (BTS) 12 and sent to a base station controller (BSC) and/or packet control unit (PCU) component (BSC/PCU) 18. Code division multiple access (CDMA) data transmitted from a wireless device 102 is received by a base transceiver station 12 and sent to a base station controller (BSC) and/or point coordination function (PCF) component (BSC/PCF) 22. Universal mobile telecommunications system (UMTS) data transmitted from a wireless device 102 is received by a NodeB 14 and sent to a radio network controller (RNC) 20. Long term evolution (LTE) data transmitted from a wireless device 102 is received by an eNodeB 16 and sent directly to a serving gateway (SGW) 28 located within the EPC 40.

[0059] The BSC/PCU 18, RNC 20 and BSC/PCF 22 components process the GPRS, UMTS and CDMS data, respectively, and send the processed data to a node within the EPC 40. More specifically, the BSC/PCU 18 and RNC 20 units send the processed data to a serving GPRS support node (SGSN) 24 and the BSC/PCF 22 sends the processed data to a packet data serving node (PDSN) and/or high rate packet data serving gateway (HSGW) component (PDSN/HSGW) 30. The PDSN/HSGW 30 may act as a connection point between the radio access network and the IP based PCEF/PGW 32. The SGSN 24 is responsible for routing the data within a particular geographical service area and may send signaling (control plane) information (e.g., information pertaining to call set-up, security, authentication, etc.) to a mobility management entity (MME) 26. The MME may request user and subscription information from a home subscriber server (HSS) 42, perform various administrative tasks (e.g., user authentication, enforcement of roaming restrictions, etc.), select a SGW 28, and send administrative and/or authorization information to the SGSN 24.

[0060] Upon receiving the authorization information from the MME 26 (e.g., an authentication complete indication, an identifier of a selected SGW, etc.), the SGSN 24 sends the GPRS/UMTS data to a selected SGW 28. The SGW 28 stores information about the data (e.g., parameters of the IP bearer service, network internal routing information, etc.) and forwards user data packets to a policy control enforcement function (PCEF) and/or packet data network gateway (PGW) 32. The PCEF/PGW 32 sends signaling information (control plane) to a policy control rules function (PCRF) 34. The PCRF 34 accesses subscriber databases, creates a set of policy rules and performs other specialized functions (e.g., interacts with online/offline charging systems, application functions, etc.) and sends the intelligent policy rules to the PCEF/PGW 32 for enforcement. The PCEF/PGW 32 implements the policy rules to control the bandwidth, the quality of service (QoS), and the characteristics of the data, and services being communicated between the service network 36 and the end users.

[0061] FIG. 2 illustrates various logical components in an example communication system 100 suitable for implementing the various embodiments. Wireless devices 102 may be configured to communicate via a cellular telephone network, a radio access network (e.g., UTRAN, RAN, etc.), WiFi network, WiMAX network, and/or other well known technologies (e.g., GPRS, UMTS, LTE, cdmaOne, CDMA2000TM). FIG. 2 illustrates that wireless devices 102 may be configured to transmit and receive voice, data, and control signals to and from a base station (e.g., base transceiver station, NodeB, eNodeB, etc.) 104. The base station may be coupled to a controller (e.g., cellular base station, radio network controller, service gateway, etc.) operable to com-

municate the voice, data, and control signals between mobile devices and to other network destinations. In the illustrated example of FIG. 2, the base station 104 communicates with an access gateway 110, which serves as the primary point of entry and exit of wireless device traffic and connects the wireless devices 102 to their immediate service provider and/or packet data networks (PDNs). The access gateway 110 may include one or more of a controller, a gateway, a serving gateway (SGW), a packet data network gateway (PGW), an evolved packet data gateway (ePDG), a packet data serving node (PDSN), a serving general packet radio service support node (SGSN), or any combination of the features/functions provided thereof. Since these structures are well known, certain details have been omitted in order to focus the descriptions on the most relevant features.

[0062] The access gateway 110 forwards the voice, data, and control signals to other network components as user data packets, provides connectivity to external packet data networks, manages and stores contexts (e.g. network internal routing information, etc.), and acts as an anchor between different technologies (e.g., 3GPP and non-3GPP systems). The access gateway 110 may coordinate the transmission and reception of data to and from the Internet 107, as well as the transmission and reception of voice, data and control information to and from an external service network 120 connected to the Internet 107, to other base stations 104 and to wireless devices 102. The access gateway 110 may also route control information to a policy and charging control (PCC) network 112, which may be a part of an implementation of an evolved packet core (EPC)/long term evolution (LTE) architecture. In the various embodiments, the access gateway 110 may be a part of the policy and charging control network 112, and the functions described may be implemented in a single computing device or in many computing devices coupled in a local area network or wide area network using any of the above mentioned telecommunication technologies (e.g., 3G, 4G, GPRS, UMTS, LTE, etc.).

[0063] Returning to FIG. 2, as mentioned above, the access gateway 110 routes control/signaling information (e.g., call setup, security, authentication, charging, enforcement of policy rules, etc.) to the policy and charging control (PCC) network 112, which is an example of a telecommunications signaling network. The PCC network 112 provides policy and service control rules, controls charging functionalities, and provides quality of service (QoS) authorizations, as discussed in further detail below. The PCC network 112 may include one or more components for a policy and charging enforcement function (PCEF) 114, a policy charging rules function (PCRF) 116, an off-line charging system (OFCS) 118, an on-line charging system (OCS) 120, a subscriber profile repository (SPR) 122, and an application function (AF) 124. Components in the PCC network 112 (e.g., PCEF, PCRF, OFCS, OCS, SPR, AF) may communicate using a standardized protocol, such as the Diameter protocol, remote authentication dial in user service (RADIUS) protocol, session initiation protocol (SIP), or any other protocol.

[0064] To focus the discussion on the relevant features and functionalities, the various embodiments are described with reference to the Diameter protocol. However, it is to be understood that the various embodiments are protocol agnostic and should not be limited to the Diameter protocol unless expressly recited in the claims.

[0065] FIG. 3 is an architectural diagram illustrating communications between the various logical components in a PCC network 112. The PCC network 112 may include a policy and charging enforcement function (PCEF) component 114 that serves as the primary enforcement point, gateway and a routing mechanism between the Internet and the radio infrastructure/radio access network. As discussed above, the PCEF component 114 may be a part of, or perform operations typically associated with, a gateway GPRS support node (GGSN), a packet data network gateway (PGW), or other similar components. Detailed information about policy and charging enforcement function operations may be found in "3rd Generation Partnership Project Technical Specification Group Services and System Aspects, Policy and Charging Control Architecture," TS 23.203 (updated June 12, 2011), the entire contents of which are incorporated herein by reference.

[0066] The PCEF 114 may receive signaling messages from a gateway (e.g., Access Gateway 110 illustrated in FIG. 2) and use information contained within the signaling messages to select an optimal route and a quality of service (QoS) for a particular type of services, as well as to enforce various policies on those services. The enforcement of policies may include querying, coordinating, removing, revoking and/or adjusting various resources (e.g., network resources, subscriber resources, etc.) based on a set of policy rules.

[0067] The PCEF 114 enforces policies by implementing a set of policy rules. Each policy rule may govern the services, QoS, and/or bandwidth that are to be made available to a particular subscriber. The policy rules may also govern the times when certain services are made accessible to the subscriber (e.g. weekdays from 9AM to 5PM, etc.) and how long the subscriber may access those services (e.g., 15 minutes at a time, a total of two hours, etc.)

[0068] The PCRF 116 is responsible for identifying the appropriate policy rules for a given communication session of a given subscriber or terminal device, and sending the identified policy rules to the PCEF 114 for enforcement. Specifically, the PCRF 116 is responsible for generating, compiling, and selecting a set of business and technology rules that define the policies that are to be enforced for particular call sessions. The PCRF 116 may make rule decisions on a per-subscriber, per-session and/or per-service basis. For example, the PCRF 116 may use subscriber information (e.g., subscriber's city of residence), the current usage parameters (e.g., day of

week, time of day, peak hours, etc.), the subscriber's service level (e.g., Gold, Bronze, etc.), and other information related to the subscriber, session, or service to generate and/or select one or more rules or a rule group. The selected rules or rule group may be communicated to the PCEF 116 (e.g., via the Gx interface) as a profile that defines the policies to be enforced. The PCRF 116 may include one or more databases for storing default rules, maintaining generated rules and keeping track of session information.

[0069] The PCRF 116 may request subscriber profile information from the subscriber profile repository (SPR) 122, which maintains subscriber profiles (e.g., customer IDs, preferences, subscription levels, balances, etc.) in one or more data stores.

[0070] An application function (AF) 124 represents a node involved in the delivery of an application or service (e.g., voice-over-IP, voice and video call, video-on-demand, etc.) that may be used by a subscriber or that may have dealings with the subscriber. The AF 124 may communicate with the PCRF 116 to ensure that the generated rules are sufficient to provide subscribers with a quality of service (QoS) commensurate with the requirements of their requested services/flows. For example, if a current policy is being enforced based on rules for receiving a particular service (e.g., a voice-over-IP call) and the subscriber requests an additional amount of a given service, or another service (e.g., a voice and video call), the application function 124 component may push a new set of rules to the PCRF 116 reflecting the service changes (e.g., QoS, etc.) required for the additional services. The application function may also store information unique to each subscriber, service, session, and/or application.

[0071] In addition to receiving rules from the PCRF 116, the PCEF 114 component may also communicate with an on-line charging system (OCS) 120 and an offline charging system (OFCS) 118 to identify the policies that are to be enforced and/or to ensure proper charging. For example, the PCEF 114 may periodically inform the OFCS 118 of the amount of wireless data that is being used by a subscriber. The OFCS 118 may use this information to monitor the aggregate amount of data/service used by each subscriber, and to generate a record that may be collected, processed, formatted, correlated, aggregated, filtered, and/or sent to an external billing system for processing into a billing statement. In order to monitor the data/service usage of each subscriber, the OFCS 118 may store information related to each subscriber, session, and/or service.

[0072] The PCEF 114 may also periodically inform the OCS 120 of services requested by a subscriber. The OCS 120 is generally responsible for determining if the subscriber has sufficient funds/credits/access units to receive a requested service. In various embodiments, the OCS 120 may also perform other operations related to charging, balance management and real time rating. The OCS 120 may grant or deny access based on the amount of fund/credits/access units available. In an embodiment, the OCS 120 may manage pre-pay services. In an embodiment, the OCS 120 may manage a combination of pre-pay and post-pay services in which some (or a portion) of the services require a pre-paid balance and some (or a portion) of the services may be billed to the client. In any case, the PCEF 114 may issue requests for service authorization to the OCS 120, and the OCS 120 may respond with a message granting or denying authorization. As part of its operations, the OCS 120 may store information unique to each subscriber, session, and/or service.

[0073] FIG. 4 is an architectural diagram illustrating the use of Diameter applications for communications between the various logical components in an example policy and charging control (PCC) network 400. As mentioned above, the logical components may communicate using a protocol, such as RADIUS, SIP or Diameter. Diameter is a protocol standardized by the Internet Engineering Task Force (IETF) and adopted by the Third Generation Partnership Project (3GPP). Diameter is an extensible protocol that provides a general mechanism for two or more nodes in a network to communicate signaling information (e.g., communications involving call setup, security, authentication, charging, enforcement of policy rules). Diameter also includes numerous access control features that make it highly useful in authentication, authorization, and accounting (AAA) systems as well as in the policy and charging control network 112. Detailed information about the Diameter protocol may be found in "Network Working Group Request for Comments: 3588; Diameter Base Protocol," the entire contents of which are hereby incorporated by reference for purposes of disclosing the protocol details.

[0074] The Diameter protocol provides a base protocol (i.e., "Diameter base protocol") and a framework for defining custom extensions (i.e., "Diameter applications") to the base protocol. The base protocol defines a set of generic messages useful for low-level operations (e.g., establishing connectivity, hand-shaking, etc.) and the framework allows application-developers to develop Diameter applications (i.e., extensions of the Diameter base protocol) that define custom messages for more specialized operations. By extending the Diameter base protocol, Diameter applications may use all of the features provided by the Diameter base protocol, as well as any custom protocol extensions they define. For example, a Diameter application may use Diameter base protocol components to define exactly how messages are to be communicated and define custom extensions that describe the content of the messages being communicated.

[0075] As mentioned above, logical components (e.g., PCEF 114, PCRF 116, AF 124, SPR 122, OCS 120, OFCS 118) in the PCC network 400 may use the Diameter protocol to communicate with each other. Components that use the Diameter protocol may support various standardized Diameter applications (e.g., Gx, Gy, Gz, Rx, Sy, etc.) that are especially well suited for their spe-

cialized operations.

[0076] The logical components (e.g., PCEF 114, PCRF 116, AF 124, SPR 122, OCS 120, OFCS 118) in the PCC network 400 may also communicate with resources outside of the provider network. For example, the PCRF 116 in a home provider network may need to communicate with a PCRF 410 in another provider network, such as while a subscriber's cell phone roams in the other provider's network. The external PCRF 410 may communicate with the appropriate logical components (e.g., PCRF 116, OCS 1201, etc.) in the home provider network to ensure proper charging, QoS, charging, etc. In the illustrated example, the external PCRF 410 communicates with PCRF 116 through the S9 interface.

[0077] To focus the discussion on the relevant features, various logical components (e.g., PCEF, PCRF, AF, SPR, OFCS, OCS, etc.) are described as using specific Diameter protocols. However, it should be understood that any protocol may be used (e.g., RADIUS, SIP, etc.) and nothing in the claims should be limited to a particular interface, protocol or application, unless expressly recited in the claims.

[0078] FIG. 5 illustrates the message structure of an example Diameter message 502 suitable for encoding signaling information. Diameter messages 502 have a fixed structure that includes a message header portion 504 and a message payload/body portion 506. The message header 504 contains general information about the message, such as version information 512, bit flags 514, message length 516, a command code 518, an application ID 520, a hop-by-hop identifier 522, and an end-to-end identifier 524. The version information 512 field identifies a Diameter protocol version. The bit flags 514 provide administrative information that may be used to process the message. For example, the first bit ("R") may indicate if the message is a request or an answer, the second bit ("P") may indicate if the messages must be processed locally or is proxiable (e.g., may be proxied, relayed, or redirected), the third bit ("E") may indicate if the message is a standard message or an error message, the fourth bit ("T") may indicate if the messaging is being sent for the first time or if there is a probability that the message is being re-transmitted, etc. The application ID 520 identifies a type of application (authentication, accounting, vendor specific, etc.) to which the message is related. The hop-by-hop identifier 522 is a unique ID that may be used to match requests to answers and send answer messages back to the requesting component. The end-to-end identifier 524 is a time-limited ID generated by the originator of a request message that should not be changed by intermediate network nodes or by the responder to the message. It is used for correlating responses with requests and for detecting duplicate messages.

[0079] The command code 518 identifies a message type of the Diameter message 502. There are several standard Diameter message types (e.g., Accounting-Request, Device-Watchdog-Answer, etc.) defined by the Diameter base protocol. Network components may quickly identify the type of information carried by a particular Diameter message 502 by examining the command code message header 504. For example, a node receiving an "Accounting-Request" message needs only examine the command code (e.g., "271") in the message header 504 to identify the message as an accounting message.

[0080] The Diameter message body 506 contains the actual data/signaling information that is being communicated. The signaling information may be stored in one or more attribute-value-pairs (AVPs) 508, which may nest other attribute value pairs (nested AVPs) 510. Attribute-value-pairs 508, 510 are extendable data-structures that include a header portion 526 and a data portion 528. The header portion 526 may include general information about the attribute-value-pair, such as an AVP code 530, message length 532, an optional vendor ID 534, and various bit flags 536. The data portion 528 may store simple data (e.g., integer, unsigned, float, etc.) or complex data (e.g., other AVPs), in an encoded format. The data portion 528 may encapsulate protocol-specific data (e.g., routing information) as well as authentication, authorization, or accounting information.

[0081] The AVP code 530 field may identify an AVP type. The Diameter base protocol defines a number of standard AVP types (i.e., attributes). Diameter applications extending the base protocol inherit all of the AVP types defined by the base protocol and may define new AVP types unique to each application. AVP codes may be combined with the optional vendor-ID 534 field to uniquely identify an attribute.

[0082] FIG. 6 illustrates an expanded policy and charging control (PCC) network 600 having more than one instances of each of the PCEF (114a-c), PCRF (116a-c), AF (124a-c), OCS (120a-c) and/or OFCS (118a-c) components, as well as a connection to an external PCRF 410. As operator networks expand to meet increased traffic and user demands, multiple instances of the same component may be implemented within a single policy and charging control network 600. Each instance may be uniquely addressable and store information relevant to a particular service, application, session or subscriber in a local memory or database. For example, the first time a destination component (e.g., PCRF 116a) receives a Diameter message from a source component (e.g., PCEF 114a) for a particular subscriber, the destination component (PCRF 116a) may store session information related to that subscriber in a local session database. Subsequent Diameter messages may require access to the session information stored by that particular instance of the destination component (e.g., PCRF 116a). Before the introduction of the DRA there was no method for identifying the desired instances of components within the policy and charging control network 600, and each component was required to discover the correct instance by trial and error. As the operator networks continue to grow, managing communications between the various instances of the various components in a PCC network in a se-

cure and efficient manner is becoming ever more important.

[0083] FIG. 7A illustrates the role of a Diameter routing agent (DRA) 702 in an expanded policy and charging control (PCC) network 700. A Diameter routing agent is a concept introduced by 3GPP in its specifications for facilitating Gx, Gxx, S9, and Rx communications with a particular instance of a PCRF (e.g., 116) when multiple and separately addressable PCRFs (e.g., 116a-c) are deployed in the same Diameter realm. Source components can send messages to a Diameter routing agent (as opposed to the destination node) and rely on the Diameter routing agent to forward the message to the appropriate node. This allows the routing logic required to identify and locate a destination node to be decoupled from the source nodes and included in a specialized component (i.e., the Diameter routing agent).

[0084] However, the 3GPP specifications only identify the general role of a Diameter routing agent (DRA) in a Diameter network, which is to provide a proxy, relay or redirect services in networks having multiple PCRFs. For example, in a PCC network 700, the role of a Diameter routing agent (e.g., DRA 702) may be to manage PCEF 114a communications (e.g., Gx-1, Gx-2) with various instances of the PCRF (116a, 116b) by receiving Gx messages and relaying the Gx messages to the correct instance of the PCRF 116. The Diameter routing agent (e.g., DRA 702) may also manage communications (e.g., Rx-1, Rx-2) between the various instances of the PCRF 116 and AF 124 by performing simple proxy, relay or redirect operations.

[0085] While the Diameter routing agents (e.g., DRA 702) may simplify routing operations in a policy and charging control (PCC) network, they are primarily focused on routing messages involving policy control rules functions (PCRFs). In particular, Diameter routing agents only support specific interfaces (e.g., Gx, Gxx, S9 and Rx); do not perform intelligent routing operations, are unaware of the context of the messages; cannot augment messages; do not support dynamic operations; do not have built-in support for future protocols/ Diameter applications; cannot hide the network topology; cannot perform true translation operations; cannot covert messages into different protocols, and are not resilient in the event of failover.

[0086] FIG. 7B illustrates an expanded policy and charging control (PCC) network 700 that includes a dynamic context router (DCR) 706 in accordance with the various embodiments. A dynamic context router 706 is flexible, protocol agnostic, application-level router and load balancer that may be used to manage communications between the various instances of the various components in a network to ensure that the correct messages are sent to the correct instances. Some of the application layer functions performed by the dynamic context router 706 may include identifying communication partners, and determining resource availability. The identification of communication partners may include determining the identity and availability of communication partners for an application requesting a communication session to transmit data.

[0087] The dynamic context router 706 allows the routing logic required to identify and locate a destination node to be decoupled from the source nodes. Source nodes may communicate with the dynamic context router 706 using any Diameter application (e.g., Gx, Gy, Gz, Rx, Sy, etc.) and do not need to know the protocol requirements and Diameter applications of the destination nodes. In this manner, new instances of any destination node may be added without having to inform the source nodes of the existence of the new destination node or of the protocols associated with the new node. Likewise, new instances of the source nodes may be added to the PCC network 700 without informing the new nodes of the other nodes (and vice versa), their protocols, or other intimate details of the PCC network 700.

[0088] The dynamic context router 706 may make routing and load-balancing decisions dynamically for each instance of an application/message based on the context and content of the data being communicated. The dynamic context router 706 may look inside the messages being communicated and make intelligent decisions based on the content of the messages. The dynamic context router 706 may make calls (e.g., function calls, etc.) to external systems to request additional information for a specific message being communicated. The dynamic context router 706 may receive additional information from external systems and use the information to augment the message, to aid in message routing, and/or to accomplish load balancing operations. The dynamic context router 706 may store information specific to a particular network node, protocol, application, message or message type in an internal memory, and reference the internal memories for message processing. As internal/external data changes, the dynamic context router 706 may update the routing and load balancing decision-making logic to reflect the changes in internal/external data.

[0089] In an embodiment, the dynamic context router may enable node upgrades without interrupting service. For example, a first PCEF in communication with a single PCRF (e.g., using Gx) may require upgrades or may need to be replaced without interrupting the service. The dynamic context router allows a second PCRF to be introduced into the network without any interruption of service by routing old messages (e.g., all existing Gx session messages) to the first PCRF, and all new message (e.g., new Gx session messages) to the second PCRF. The dynamic context router may indicate when all of the old sessions have terminated, indentifying when the old PCRF can be safely removed. In an embodiment, a dynamic context router may be removed from the network after the new PCRF is introduced without interrupting operations. In an embodiment, a dynamic context router may be introduced into the network along with, or immediately prior to, the second PCRF and removed from the network after the new PCRF is introduced.

[0090] In an embodiment, the dynamic context router may use contextual information obtained from response messages to influence future routing decisions. This contextual information may be either intentionally placed within the response message for use by the dynamic context router, or it may normally be there. For example, a dynamic context router that is load balancing between five equal PCRFs may initially use a round-robin algorithm. However, some requests may require more processing than others, and the PCRF loads may differ. In an embodiment, each PCRF may include an additional proprietary parameter in the response messages indicating its current work load, which may be used as contextual information by the dynamic context router when making future load balancing routing decisions.

[0091] In an embodiment, the dynamic context router may utilize a PCRF that is highly optimized for a very limited set of functionality (e.g., a "Voice over LTE" optimized PCRF). For example, when the dynamic context router is routing a message to a PCRF it may use contextual information to choose the right type of DCR. As another example, the dynamic context router may be configured to host simple application logic such that if a certain type of service is not permitted in the network (regardless of all other criteria such as user details) the DCR can respond to the request message directly without needing to send the request message to a PCRF. Thus, in an embodiment, the dynamic context router may shield the PCRFs from additional and unnecessary communications and work.

[0092] FIG. 8 illustrates logical components and communication links of an example dynamic context router system 800. The dynamic context router system 800 may include a dynamic context router core (DCR core) 814 module, a plurality of internal resources 816, and communication links 832, 834. The communication links 832, 834 may link the dynamic context router system 800 to various external resources, such a dictionary server 840, an OracleTM server 808, a lightweight directory access protocol (LDAP) server 810, as well as other external resources 812 (e.g., a subscriber profile repository, an online charging system, etc.). The internal resources 816 may include in-memory database technologies such as a reference database 802, as well as a plurality of session stores 804 and a cache memory 806. The internal resources 816 may be on the same chip, on the same computing device, within the same realm, or in the same network as the DCR core 814. The session stores database 804 may include a DCR-specific session store, a general session store and a session store for each message/session/node/Diameter application serviced by the dynamic context router.

[0093] The reference database 802 may store any type of information that will aid DCR core 814 operations, such as message formats, message processing rules, validation rules, node IDs, etc. The reference database 802 may be populated by data from external sources 830. In such cases the data may either be pulled by the reference database 802 from the external sources 830, or pushed to the reference database 802 by the external sources 830. As discussed below, the session stores 804 may store session information, which may be used to establish "session stickiness" and/or maintain session states. The cache memory 806 may be populated by the DCR core 814, which may periodically cache data in response to on-going dynamic context router operations. For example, the DCR core 814 may cache information received from external sources useful for processing future messages. In an embodiment, the DCR core 814 may perform cache-optimizing operations to identify the most expensive information requests (e.g., requests made to external systems having slow response times) and store information associated with the most expensive information requests in the cache memory 806. In an embodiment, the DCR core 814 may first seek information from the cache memory 806 before attempting to access external resources. In an embodiment, the dynamic context router may periodically expire or remove information from the cache memory 806. In an embodiment, the dynamic context router may perform cache-optimization operations to determine an optimal cache-expiration rate and expire/remove information at the optimal rate.

[0094] The dynamic context router (DCR) may use the communication links 834 to access one or more dictionary servers 840, which may include one or more dictionaries. Each dictionary may define information specific to a particular protocol, application, node or message type. For example, a dictionary may include file definitions, a list of available commands (e.g., "deduct balance," "refund balance," etc.), a list of mandatory message types, a list of optional message types, a list of unsupported message types, field/message descriptions, and message decoding rules. The list of available commands may include a list of specific message types, each of which may be associated with a specific validation rule. A dictionary may also define message requirements, such as rules for storing certain message fields (e.g., session ID must be at the end of the message, session ID cannot be in the middle of the message, etc.) for a given node, protocol, or application.

[0095] The dictionary servers 840 enable the dynamic context router to support any current or future Diameter applications and/or message formats through dictionary updates. For example, if a vendor develops a new Diameter application "Z", the vendor may add a new Diameter dictionary (dictionary entries) that defines the rules/requirements of the new application. In an embodiment, the DCR core 814 may dynamically generate and/or update the dictionary definitions, without requiring any of the dictionaries to be taken offline.

[0096] FIG. 9 illustrates example signaling flows in a network 900 in which a dynamic context router 920 has been deployed. The network 900 may include a plurality of nodes (902a-c, 904a-b, 906a-d) that provide specific functions and/or implement specific protocols (A, C, E). Multiple nodes in the network 900 may provide the same

function and/or implement the same protocol. Nodes that provide the same functions/implement the same protocol may be different instances of the same node (e.g., Node A, Node C, Node E). In an embodiment, the network 900 may be a policy and charging control network, each of A, C and E may be any of the logical components described above (e.g., PCEF, PCRF, OFCS, OCS, SPR, and/or AF) and each of nodes 902a-c, 904a-b and 906a-d may be an instance of one of the logical components.

[0097] Returning to FIG. 9, a source node (e.g., 902a-c, 904a-b) may send a request message (e.g., a connection request) to the dynamic context router 920, which receives the request message and establishes a connection (e.g., 910a-c, 912a-b) with the requesting source node. In an embodiment, the connection may be a physical link layer communication line. Source nodes (902a-c, 904a-b) may send signaling messages that encode signaling data to the dynamic context router 920 over the established connections 910a-c, 912a-b. The signaling messages may encode the signaling data in one or more Diameter messages. Each Diameter message may include a base Diameter message portion and an application specific Diameter message portion. The dynamic context router 920 may receive the signaling messages and examine the base Diameter message portion of the message to determine if the message may processed by performing realm-based routing table look-up operations. If so, the dynamic context router DCR 920 may perform proxy, relay, or redirect operations, which may include performing load balancing operations.

[0098] If the message cannot be processed by performing message-based routing (e.g., realm-based routing) table look-up operations, the dynamic context router 920 may perform application-level routing and load balancing operations to identify a suitable destination node (e.g., 906a-d) to which a corresponding signaling message is to be sent. The dynamic context router 920 may determine if a message may be sent to any destination node offering a particular service (e.g., any "E" node) or if the message requires a particular instance (e.g., 906c) of the destination node. If the message may be sent to any destination node offering the service (906a-d), the dynamic context router 920 may perform load-balancing operations to identify a suitable instance (e.g., 906c), establish a connection/association (e.g., connection 916c) to the identified instance (e.g., 906c), encode the signaling information into a message, and transmit the signaling message to the identified instance.

[0099] If the dynamic context router 920 determines that the messages should be sent to a particular instance of the destination node (e.g., 906a), the dynamic context router 920 may decode the message, examine the contents of the message, perform application-level routing operations to identify the correct instance (e.g., 906a), establish a connection/association (e.g., connection 916a) to the identified instance (e.g., 906a), re-encode the decoded contents into a new message, encode the signaling information into a message, and transmit the signaling message to the identified instance (e.g., 906a).

[0100] FIG. 10A illustrates an example dynamic context router method (DCR method) 1000 for receiving signaling messages from a source node and sending corresponding signaling messages to a destination node. As mentioned above, the dynamic context router may receive a connection/association request from a source node and establish a connection with the requesting source node. In step 1006, the dynamic context router may receive one or more Diameter messages over such connection. In step 1008, dynamic context router may decode a base portion of the Diameter message. In determination step 1010, dynamic context router may perform message-based (e.g., realm-based) routing table look-up operations to determine if an entry corresponding the Diameter message exists in the routing table (i.e., the Diameter message matches a routing table entry). If the dynamic context router determines the Diameter message matches a routing table entry (i.e., determination step 1010 = "Yes"), in determination step 1012, the dynamic context router may determine if a "realm routing action" is a proxy operation. If it is determined that the realm routing action is a proxy operation (i.e., determination step 1012 = "Yes"), in step 1016, the dynamic context router may perform operations to fully decode the message, and in step 1018, begin routing operations. If the realm routing action is not a proxy operation (i.e., determination step 1012 = "No"), in step 1018, the dynamic context router may begin routing operations.

[0101] If in determination step 1010 the dynamic context router determines the Diameter message does not match a routing table entry (i.e., determination step 1010 = "No"), in determination step 1014, the dynamic context router may determine if a Diameter application associated with the Diameter message is supported. If the Diameter application associated with the Diameter message is supported (i.e., determination step 1014 = "Yes"), in step 1016, the dynamic context router may perform operations to fully decode the message. If the Diameter application is not supported (i.e., determination step 1014 = "No"), in step 1018, the dynamic context router may begin routing operations.

[0102] In determination step 1020, the dynamic context router determines if the destination-host is specified in the Diameter message. If the destination-host is specified in the Diameter message (i.e., determination step 1020 = "Yes"), in step 1026, the dynamic context router performs operations to modify the contents of the message (e.g., augments the message) and sends the modified message to the destination node. If the destination-host is not specified in the Diameter message (i.e., determination step 1020 = "No"), in step 1022 the dynamic context router performs context routing operations to select a destination domain. In step 1024, the dynamic context router performs load balancing operations to choose a specific instance of the selected destination domain. In an embodiment, the dynamic context router may match message parameters against internal or external refer-

ence data to identify a suitable instance of the destination node. In various embodiments, the dynamic context router may identify and select the first available instance of the destination node, the most available instance of the destination node, or the most under-utilized instance of the destination node, all of which may be performed with the assistance of dynamic information obtained in real-time from external systems (e.g., external resources 812 illustrated in FIG. 8). In an embodiment, the dynamic context router may identify and select an instance of the destination node, such that the processing workload is distributed across the nodes, the communication traffic is minimized, the network resources are optimally utilized, network throughput is maximized, and/or response time is minimized.

[0103] As mentioned above, in step 1026, the dynamic context router performs message modification operations (e.g., augments the message) and sends the modified message to the selected instance of the destination node.

[0104] FIG. 10B illustrates an example dynamic context router method 1050 for determining if a specific instance of a destination node is required. In step 1052, the dynamic context router may determine if session stickiness has been configured for a particular Diameter message. The dynamic context router may determine if a session exists by, for example, comparing message information to a session identifier stored in a session store. If session stickiness has not been configured (i.e., determination step 1052 = "No"), in step 1054, the dynamic context router may perform routing and load balancing operations to choose a destination node.

[0105] By establishing session stickiness the DCR may select the instance of the destination node to which a previous message related to that session was sent and send all future signaling messages associated with that session to the same instance of the destination node. In this manner, signaling messages belonging to the same session, but originating in different source nodes (e.g., Nodes A and C illustrated in FIG. 9), may be directed to the same instance of the destination node (e.g., 906a-d illustrated in FIG. 9). If the dynamic context router determines that session stickiness has been configured (i.e., determination step 1052 = "Yes"), in step 1056, the dynamic context router may perform a session look up. In determination step 1058, the dynamic context router may determine if the session exists by, for example, comparing session information extracted from the Diameter message to session identifier information stored in a session store. If the session is found (i.e., determination step 1058 = "Yes"), the dynamic context router may, in step 1064, route the message to a specific destination associated with the identified session. If the session is not found (i.e., determination step 1058 = "No"), in step 1060, the dynamic context router may perform routing and load balancing operation to choose a destination node. In step 1062, the dynamic context router may update the session store with the chosen destination node.

[0106] As mentioned above, in the various embodiments, as part of the application-level routing operations, the dynamic context router may determine that a specific instance of a destination node is required. For example, the dynamic context router may determine that a Diameter message must always be sent to a specific node due to a context based routing operation requiring all mobile subscriber integrated services digital network numbers (MSISDNs) matching a certain pattern go to a specific node, or due to a context based routing operation requiring that all messages in the session go to the same destination node.

[0107] FIG. 11 illustrates logical components and information flows 1100 of an example dynamic context router system (DCR system) 1150 configured to receive messages from multiple instances (e.g., 902a-904b) of multiple source nodes (e.g., Nodes A, C) and send corresponding signaling messages to destination nodes (e.g., Node E, 906a-d). The DCR system 1150 may include a dynamic context router core (DCR Core) 1114 module, a plurality of internal resources 1116 and communication links to various external resources, such as a dictionary server 1140a, an Oracle database 1108, a Lightweight Directory Access Protocol (LDAP) database 1110, etc. The internal resources 1116 may include a reference database 1102, session stores 1104 and a cache memory 1106.

[0108] FIG. 11 illustrates that the DCR core 1114 may receive signaling messages from one or more source nodes (902a-904b). Each signaling message may encapsulate signaling information (e.g., charging rules, authentication information, enforcement of policy rules, etc.). Signaling messages, such as Diameter messages, may be sent to the DCR core 1114 using interface 1120. Each Diameter message may have encoded base protocol portions and encoded application-specific portions. The base protocol portions may be decoded by any Diameter application/node and/or relayed or proxied accordingly. The application-specific portions may only be decoded if all of the application-specific decoding rules are known by the receiving node.

[0109] Thus, in an embodiment, the dynamic context router may receive a Diameter message, decode the base Diameter portions of the Diameter message into base parameters/AVPs, decode the application-specific portions of the Diameter message into application parameters/AVPs, use the decoded parameters/AVPs to identify a proper destination node, re-encode the base and application parameters/AVPs into a new Diameter message, and send the Diameter message to the identified destination node.

[0110] As mentioned above, the network nodes generally can only decode the application-specific portions of Diameter messages if all of the application-specific decoding rules are known to the network node. FIG. 11 illustrates that the dynamic context router communicates with a dictionary database 1140a, and may request these application-specific decoding rules from the dictionary

database 1140a. For example, the DCR core 1114 may send a request message identifying a protocol, node, or message to a dictionary server (not illustrated), which receives the request, queries the dictionary database 1140a for the correct set of rules and sends the rules to the DCR core 1114. The DCR core 1114 may then use these rules to decode the application-specific portions of the messages. However, access to the external resources, such as the dictionary database 1140a, is generally an expensive and time consuming process. In addition, once the DCR core 1114 receives the decoding rules, it must spend considerable processing resources to perform the actual decoding operations.

[0111] To improve efficiency and reduce latency, in an embodiment, the DCR core 1114 may access partial dictionaries 1140b and/or perform the decoding operations in two phases. Partial dictionaries 1140b are dictionaries that do not contain a complete set of rules for a particular protocol, message, node or application. In an embodiment, partial dictionaries 1140b may be created out of necessity when the information stored in the complete dictionary cannot fully describe both a newer and an older standard, both of which may exist simultaneously in the network. In an embodiment, partial dictionaries 1140b may contain only the minimum amount of rules required to successfully communicate with a given protocol. Since partial dictionaries may contain less information than complete dictionaries, in an embodiment, the DCR core 1114 may utilize partial dictionaries to receive and process the messages much faster when a partial dictionary is available.

[0112] In an embodiment, the DCR core 1114 may perform decoding operations in two or more phases. This multi-phase decoding allows the dynamic context router to decode a small portion of the message and, if necessary, perform addition decoding operations in small targeted increments until a suitable destination node is identified or it is determined that a suitable destination node cannot be determined from additional decoding operations. For example, the DCR core 1114 may incrementally decode additional portions of the base and/or message body until: a suitable destination node can be identified; the entire message is decoded; or the DCR core otherwise determines that a suitable destination node cannot be determined from further decoding of the message.

[0113] In an embodiment, the DCR core 1114 may perform protocol translation operations. Protocol translations may be performed at several different levels, and multiple translations may be performed together. For example, FIG. 11 illustrates that the DCR core 1114 may receive a Diameter message 1134 from a particular instance of a source node (e.g., 902a). The message 1134 may be implemented in a first protocol (e.g., SOAP) and require transmission to a destination node (e.g., 906a) that requires a second protocol (e.g., Diameter). Since the first and second protocols differ, the destination node will not be able to receive the message. In an embodiment, the DCR core 1114 converts the message from the first protocol into the second protocol. For example, the DCR core 1114 may receive the SOAP message 1134, decode the message, perform operations to identify the destination node, perform operations to identify the protocol supported by the destination node (e.g., Diameter), access the dictionary databases 1140a-b for the message requirements of the second protocol (e.g., Diameter), re-encode the decoded message to implement the second protocol and send the re-encoded message to the destination node.

[0114] In various embodiments, the first protocol may be the same as the second protocol, a subset of the second protocol, a superset of the second protocol, compatible with the second protocol, or completely independent of the second protocol.

[0115] In an embodiment, the DCR core 1114 may perform protocol translation operations even when the first and second protocols are compatible or the same. Often, nodes/logical components (e.g., 902a-906d) vary in their implementation of the same set of standards, especially when the nodes/logical components (e.g., 902a-906d) are manufactured by different vendors. For example, a vendor's implementation of a standard may be less than compliant to the standards, outdated, contain proprietary extensions to the standard, or the standards may have changed since the nodes were deployed. In such cases, messages originating from a source node may not be accepted by a destination node, even though both the source node and the destination node implement the same protocol. In an embodiment, the DCR core 1114 changes the values of the Diameter message. In doing so, the DCR core 1114 may perform operations of: receiving and decoding a Diameter message; decoding the AVPs contained therein; examining the contents of the AVPs; identifying a destination node; identifying the values/fields that need to be added, removed, and/or changed in order for the message to be accepted by the identified destination node; requesting information from the internal and/or external resources; augmenting the message by adding, removing, or changing the identified values/fields; re-encoding the AVPs into a Diameter message that conforms to the standards; and sending the message to the destination node.

[0116] As mentioned above, the dynamic context router may perform routing operations, e.g. proxy, relay, and redirect operations. In order to perform these routing operations, the DCR core 1114 may determine if the message to be routed contains information identifying a specific destination host. If the message identifies a specific destination host, then the DCR core 1114 may forward the message to the specified destination host (e.g., 906a). If the message does not identify a specific destination host, then the DCR core 1114 may analyze the message to determine if the message contains information identifying a specific destination realm to which the message is to be sent. If the message identifies a specific destination realm, the DCR core 1114 may perform one

or more routing/load balancing operations to identify a suitable destination host, supplement the message with additional information (e.g., augment the message), and send the message to the identified destination host.

[0117] As part of the context routing operations, the DCR core 1114 may communicate with external resources (e.g. 1108, 1110, etc.) to receive the additional information that may be used to augment the messages and/or aid the context routing decisions. For example, the DCR core 1114 may generate one or more keys based on values/fields of the decoded messages and send the generated keys to the external resources (e.g., 1108, 1110, etc.). The external resources (e.g., 1108, 1110, etc.) may use the keys to locate (e.g., lookup, pull, etc.) supplementary information that may be used to aid the routing/load balancing operations and send the supplementary data to the DCR core 1114. The DCR core 1114 may receive the supplementary information, identify the proper destination host, add the information to the message, and send the augmented message to the proper destination host.

[0118] As mentioned above, the DCR may send and receive messages to and from any Diameter application, as well as other similar protocols (e.g., SOAP, RADIUS, HTTP, etc.). Also as mentioned above, the DCR may send and receive messages from network nodes (e.g., a subscriber profile repository, an online charging system, etc.) and may route messages to and from such nodes. In an embodiment, the DCR core 1114 communicates with a subscriber profile repository (e.g., SPR 122 discussed above with reference to FIG. 7B) and uses the information contained therein (e.g., subscriber information) to augment the messages and/or identify a destination node. In an embodiment, the DCR core 1114 communicates with an online charging system (e.g., OCS 120a-c discussed above with reference to FIG. 7B) and uses the information contained therein (e.g., charging information) to augment the messages and/or identify a destination node. In an embodiment, the DCR core 1114 accesses an off-line charging system (e.g., OFCS 118a-c discussed above with reference to FIG. 7B) and uses subscriber billing/charging information to augment the messages and/or identify a destination node.

[0119] As previously discussed, nodes/logical components (e.g., 902a-906d) may vary in their implementation of the same set of standards, especially when they are manufactured by a number of different vendors. In some cases, different instances of the same component may vary in their implementation of the same standard even when manufactured by the same vendor. For example, vendors typically upgrade their components piecemeal, as opposed to all-at-once, and it may take the vendors a number of years to fully upgrade all of their components. During this time, the upgraded components may use a newer, updated, or modified version of the standards (e.g., updated message structure, rules, etc.) compared to the yet-to-be upgraded components (i.e., the unimproved components). Since the newer/upgraded components use a different version of the standards than the older/unimproved components, during the upgrade period, the vendor may reduce complete dictionaries to partial dictionaries. In such cases, the partial dictionary is created out of necessity because the information stored in the complete dictionary cannot fully describe both the newer standards and the older standards, both of which exist simultaneously in the network. The various embodiments may address such situations by performing protocol translation operations to cause the different versions to interoperate, by utilizing peer specific dictionaries, by performing partial decoding operations and/or by performing tolerant decoding operations. The partial decoding operations may include using a partial dictionary and/or only decoding parts of the message, as discussed in more detail above.

[0120] In an embodiment, the dynamic context router may operate in an opaque proxy mode that supports piecemeal upgrades. The opaque proxy mode may be logically situated between the relay and proxy modes. The dynamic context router may operate in an opaque proxy mode when the dictionary information is insufficient and/or when the dynamic context router system seeks to improve performance (e.g., intentional partial dictionary).

[0121] The dynamic context router may perform tolerant decoding operations, which may be performed as part of the opaque proxy operations. The tolerant decoding operations may include decoding the complete message while allowing errors to exist (e.g., tolerating errors). For example, the rules specified in the complete dictionary may be relaxed to allow messages with missing mandatory AVPs (or messages with AVPs in the wrong position) to be processed as if they do not include errors.

[0122] As discussed above, the dynamic context router may decode only a portion of the Diameter messages. When dynamic context router operates in the opaque proxy mode (i.e., as an opaque proxy agent), the dynamic context router may access a partial Diameter dictionary and decode only those fields available to it (e.g., inadvertent partial dictionary) or only those fields required by the destination node (e.g., intentional partial dictionary). For example, if a partial dictionary provides only five (5) out of ten (10) total definitions, instead of sending an error message to the source node, the dynamic context router may decode the message using the available definitions and leave the rest of the message in the original format (e.g., binary wire format). The dynamic context router may then re-encode the decoded portions, couple them to the un-encoded portions to create an opaque message, and send the opaque message to a destination node. If, in response to sending the opaque message, the dynamic context router receives an error message from the destination node, the dynamic context router may re-process the message by accessing a complete dictionary and perform a full decoding operation (e.g., in the case of intentional partial dictionary), or send an error message to the source (e.g., in the case of an inadvertent

partial dictionary).

[0123] In an embodiment, the dynamic context router system may perform routing/load balancing operations by hierarchy. For example, the dynamic context router system may organize the network topology into a logical structure that facilitates load balancing and high availability. The logical structure may define the nodes/resources available to the dynamic context router system and enable the dynamic context router system to quickly and efficiently locate nodes/resources. The logical structure may also identify available alternatives to each node/resource for fail-over operations, support the intelligent placing of new assets in peer groups, allow for dynamic addition/removal of nodes/resources to the dynamic context router network, and support intelligent routing between dynamic peers. In an embodiment, the logical structure may be a topology tree stored in memory.

[0124] FIG. 12 illustrates an example DCR topology tree 1200 that may be used by the dynamic context router for performing routing/load balancing operations by hierarchy. FIG. 12 also illustrates example DCR logical components 1250 for performing operations on the DCR topology tree 1200. The DCR logical components 1250 may include a business logic module 1202, a peer group-level module 1204 and a peer module 1206.

[0125] It should be noted that the DCR topology tree 1200 may be implemented using a wide variety of data structures, including arrays, trees, linked-lists, maps, vectors, and graphs. The DCR topology tree 1200 may be configured to support root nodes, internal nodes and terminal nodes. The DCR topology tree 1200 may be configured to allow each node to have more than one parent. The DCR topology tree 1200 may be configured to allow multiple root nodes. Thus, in various embodiments, the DCR topology tree 1200 may be implemented using a wide variety of data structures (e.g., arrays, trees, graphs, etc.) and is not limited to a tree structure.

[0126] In an embodiment, the DCR topology tree 1200 may include domains as root nodes, at least one peer-group as an internal node for each of the one or more domains, and at least one peer as a terminal node for the at least one peer-group. In an embodiment, the dynamic context router may perform application level routing operations to identify a root node in the topology tree and identify a terminal node destination component using the identified root node and hierarchical groups of the topology tree. In an embodiment, identifying a terminal node destination component using the identified root node and the hierarchical groups of the topology tree includes identifying and selecting the root node by performing business rule operations, identifying and selecting internal nodes by performing at least one of partitioning operations and availability operations and identifying and selecting the terminal node based on load balancing requirements.

[0127] Returning to FIG. 12, the DCR topology tree 1200 may be arranged such that peer nodes (e.g., peers 1-8) are grouped into peer groups (e.g., peer groups 1-4), and peer groups are grouped into domains (e.g., domain 1, domain 2) 1208, 1210. The peer nodes may be grouped such that each peer node belonging to a particular peer group is capable of performing the same functions as every other peer node belonging to the same peer group. Sine all of the nodes may be equivalent, this grouping enables the performance of efficient load balancing operations. Domains within the DCR topology tree may be defined according to business rules, e.g. domains can represent geographical areas, datacenters, subscriber ranges, and/or other any other logical group. Each peer may represent a destination node 1208-1222 and/or contain a reference to a destination node 1208-1222. In an embodiment, each peer group may belong to more than one domain, and each peer may belong to more than one peer group. In an embodiment, peer groups may belong to other peer groups, which may facilitate embodiments having multiple layers of internal nodes.

[0128] Each peer group may advertize itself as being in either an available state or in a not-available state. Each peer group may define the number peer nodes that need to be available before the peer group changes its state from not-available to available. Thus, Peer groups may be defined up front; pre-configured peers may be added up front; and non pre-configured peers may be added to peer-groups at run time via regular expression matching.

[0129] The business logic module 1202 may select a domain 1208, 1210 by performing business-level operations by defining a set of rules, regular expressions and/or patterns. In an embodiment, the peer group-level module 1204 may select a peer group by availability (e.g., first available in a chosen domain). Within the selected peer group, a specific peer node may be chosen according to a configured load balancing algorithm.

[0130] In an embodiment, the topology tree may be created such that peers are explicitly configured to belong to peer groups when the peers are added. In an embodiment, the topology tree may be created such that peers may be assigned to peer groups based on the regular expression method. In an embodiment, the rules, regular expressions and/or patterns for the intelligent placing of new assets in peer groups may be defined in a configuration file accessible to the operator network.

[0131] Peer nodes may be pre-configured such that the nodes are placed into a particular peer group as they are added to the topology tree. For example, a peer node may define a specific host and realm, which may be used by the dynamic context router to place the node within a particular peer group in the topology tree. Peer nodes that connect to the dynamic context router system without having been pre-configured to be placed explicitly in a specific peer group may be inserted into the topology tree by matching their host and realm information to a peer group using a regular expression template. The dynamic context router may add each type of peer node (e.g., pre-configured, dynamically defined, etc.) in a manner that allows both types of peer nodes to exist within

in the topology tree.

[0132] In certain situations, a Diameter message may be routed to a peer node that fails before a response is received by the dynamic context router. In such situations, the dynamic context router may coordinate failover operations by re-traversing the topology tree to find an appropriate alternative peer to which to resend the message. For example, if a selected peer node fails, the dynamic context router may traverse up the DCR topology tree 1200 to identify the peer group to which the failing peer node belongs, identify another available peer node within that peer group. If no peers are available in the peer group, the dynamic context router may traverse another level of the hierarchy tree to identify the first available peer group within the same domain, and traverse down the tree to a peer node within the identified peer group.

[0133] In an embodiment, the DCR topology tree 1200 may be generated or updated as part of the dynamic context router performing general processing and routing operations. For example, the dynamic context router may annotate peer destinations as they are processed to create one or more logical overlay networks, which may be represented by the DCR topology tree 1200. The logical overlay networks may lend themselves to simpler routing configurations by allowing routing logic to refer to an entire logical network, instead of having to refer to each constituent destination. For example, if it is determined that a certain geographical area is under heavy load, the dynamic context router may change one or more global context settings for that geographical area to allow multiple applications and routes to be updated in the DCR topology tree 1200, thereby avoiding the congested area (i.e., the geographical area under heavy load).

[0134] In an embodiment, the dynamic context router may prioritize the peers within a peer group. In an embodiment, the dynamic context router may give each of the peers within a peer group equal priority, while in other embodiments peers may be prioritized in a flexible manner. In an embodiment, the dynamic context router may create logical sub groupings of the peer nodes. For example, the dynamic context router may group peer nodes at various locations around the topology by annotating them as belonging to a group (e.g., "New York," "Data Center X," etc.). In this manner, the dynamic context router can control a large number of independent peers and control the execution of many different routing rules through a single command (e.g., "avoid New York").

[0135] As discussed above, the business logic module 1202 may select a domain 1208, 1210 by performing business-level operations, which may be defined by configuration. Allowing the business-level operations to be based on the configuration provides a flexible method of grouping destinations so that the routing operations may select a suitable destination node based on a number of factors. For example, the DCR system may be configured to define the domains 1208, 1210 to represent a subscriber range (e.g., subscriber range A, subscriber range B), in which case, geography only comes into play at the peer group-level module 1204. In this manner, the DCR system may be configured to provide geo-redundancy, load balancing and/or failover capabilities within a single datacenter, as required.

[0136] In an embodiment, the dynamic context router may perform message destination address hunting operations within a network when that information is not ascertainable from the message itself. As discussed above with reference to FIG. 9, every instance of a node (e.g., destination nodes 906a-d) may maintain data that is unique to each node/subscriber/session, and some messages must be routed to a specific instance to access this data. However, on some occasions, the correct instance of the destination node cannot be ascertained from the information included within the message or otherwise available to the dynamic context router. If the decoded message does not include information identifying a specific realm or destination node, and information retrieved from the external and internal resources (e.g., reference databases, session stores, etc.) is not sufficient to identify a proper destination node, the dynamic context router may perform one or more hunting operations to locate the proper instance of the destination node.

[0137] FIG. 13 illustrates a dynamic context router (DCR method 1300 for receiving and sending Diameter messages in accordance with an embodiment. In step 1302, the dynamic context router may receive and decode a Diameter message. In determination step 1304, the dynamic context router may determine if the decoded message identifies a destination realm. If the decoded message does not identify a destination realm (i.e., determination step 1304 = "No"), in step 1340, the dynamic context router may send an error response message to the network node from which the message was received. If, on the other hand, the decoded message does identify a destination realm (i.e., determination step 1304 = "Yes"), in determination step 1306, the dynamic context router may determine if the decoded message identifies a destination host. If the decoded message identifies a destination host (i.e., determination step 1306 = "Yes"), in step 1320 the dynamic context router may re-encode the message into a proper format and/or send the re-encoded message to the identified destination host. If the decoded message does not identify a suitable destination host (i.e., determination step 1306 = "No"), in step 1308, the dynamic context router may request/receive information from internal resources if needed. In step 1310 the dynamic context router may request/receive information from external resources if needed. In step 1312, the dynamic context router may use all of the information available (e.g., information from the message, internal memories, external resources, etc.) to perform application-level routing operations as discussed above.

[0138] In determination step 1314, the dynamic context router may determine if the above-mentioned routing operations identify a suitable destination domain. If the routing operations identify a suitable destination domain

(i.e., determination step 1314 = "Yes"), in step 1316, the dynamic context router may perform load balancing operations to choose a destination host (e.g., a specific instance of a network node). If the routing operation does not identify a suitable destination domain (i.e., determination step 1314 = "No"), in step 1318, the dynamic context router may perform message destination hunting operations to identify a destination host (if configured to do so), and in step 1320, re-encode and send the message to the destination node identified from such hunting operations.

[0139] The node-selection operations may include selecting a node from the hierarchy tree, selecting a node based on heuristics, selecting the first available node, selecting a random node, performing a routing operation, performing a randomization operation, and/or performing a learning operation. Using one of these methods, the dynamic context router may select a node, encode the message into a suitable format/protocol, send the message to the selected destination node, and wait for a response from the destination node. In determination step 1322, the dynamic context router may determine whether it a negative response from the selected destination node, such as the selected destination node rejects the message. If the dynamic context router receives a message acknowledgement or otherwise does not receive a negative response from the selected destination node (i.e., determination step 1322 = "No"), which indicates that the correct destination node has been identified, the dynamic context router may store information correlating the subscriber and/or session to the correct destination node in a cache memory (e.g., cache memory 1016) in step 1324 so that all future messages associated with that subscriber and/or session may be sent to that same node.

[0140] However, if the dynamic context router receives a negative response from the selected destination node (i.e., determination step 1322 = "Yes"), the dynamic context router may add the selected node to a "do-not-use" list in memory, and update the node-selection algorithm in step 1326. In an embodiment, the "do-not-use" list may be a list of destination nodes known not to be correlated to certain subscribers/sessions, which the dynamic context router may reference to exclude certain nodes for future consideration. In an embodiment, adding the selected node to a "do-not-use" list in memory may include performing operations for updating a topology tree stored in memory to include or exclude the selected node. After receiving a negative response and updating the memory/algorithms in step 1326, the dynamic context router may un-select the node and repeat the above-mentioned process with the updated memory/algorithms by returning to determination step 1314 or step 1318. This process may continue until a correct destination node has been identified, as indicated by the message being accepted (i.e., determination step 1322 = "No"). Again, the dynamic context router may store information correlating the subscriber and/or session to the correct destination node in a cache memory (e.g., cache memory 806) in step 1324 so that all future messages associated with that subscriber and/or session may be sent to that same node.

[0141] Message destination hunting operations may include checking (e.g., via customer routing logic) a user defined cache (e.g., user defined caches 2024 illustrated in FIG. 20) to determine if a destination for a particular subscriber being routed is already known. FIG. 14 illustrates in more detail a dynamic context router (DCR) method 1400 for performing message destination hunting operations. In step 1402, the dynamic context router may select a destination node. In step 1404, the dynamic context router may encode the Diameter message into the correct format/protocol and send the message to the selected node. In determination step 1406, the dynamic context router may determine if a reply has been received from the selected node. If a positive reply has been received from the selected node (i.e., determination step 1406 = "No"), in step 1414, the dynamic context router may store (e.g., in an internal memory or resource) information correlating subscriber and/or session information to the selected destination node, and terminate further destination hunting operations for the received message. If, on the other hand, either a negative reply has been received or no reply has been received from the selected node (i.e., determination step 1406 = "Yes"), in step 1408, the DCR may remove the selected node from a list of available nodes, which may be stored in an internal memory. In step 1410, the dynamic context router may unselect the selected node. In step 1412, the dynamic context router may update its node selection algorithms and parameters and re-initiate the node-selection operations (step 1402).

[0142] In an embodiment of message destination hunting operations, the dynamic context router may generate a list of possible destinations and route the message to the first destination on the list in steps 1402 and 1404. In this embodiment, the dynamic context router may issue a request to the Diameter library to store the rest of the list in an outstanding transactions queue. In determination step 1406, the dynamic context router system may examine (e.g., via custom logic in the response handling module/pipeline described below) response messages received in response to routing the message to the first destination. If a response message indicates "success" (i.e., determination step = "No"), the dynamic context router system may terminate further hunting operations and update the user defined cache in step 1414. If, on the other hand, the responses indicate that the message was not successfully transmitted to an appropriate destination node (i.e., determination step = "Yes"), the dynamic context router system may determine if there are more destinations in the generated list, select the next destination from the list, and send the message to the selected destination as part of re-performing step 1402. This process of steps 1402 through 1412 may be repeated until a "successful" response message is received (i.e., an appropriate destination node is discovered) or

until all of the destinations in the list have been attempted (e.g., list is empty). If there are no more destinations, then the dynamic context router system may deem the hunting operations as unsuccessful and send an error to the originating node.

[0143] In an embodiment, as part of performing the message destination hunting operations, the dynamic context router may perform operations that implement a randomization algorithm. The randomization algorithm may use parameters (e.g., uniformly random parameters, concentration parameters, etc.) to guide the dynamic context router's node-selection behavior. The randomization parameters may be selected/updated such that the average-case node-selection performance is greater than selecting the nodes at random.

[0144] In an embodiment, the hunting operations may include identifying and selecting nodes based on network latency, node performance, speed, capacity, workload and/or availability. In this manner, if the selected node is not the correct destination, the dynamic context router may quickly receive the rejection response and update the memories/algorithms accordingly.

[0145] In an embodiment, the hunting operations may continue for a predetermined amount of time or until the correct instance is identified. In an embodiment, the message destination hunting operations may implement one or more learning algorithms. In an embodiment, the hunting operations may be based on heuristics.

[0146] In various embodiments, the message destination hunting operations may be performed to locate information for a particular subscriber or a session. For example, if subscriber related information is partitioned across multiple data nodes and messages need to be routed to a particular node based on the location of the subscriber information, subscriber-based hunting algorithms may be applied to avoid provisioning all nodes with information about the employed partitioning scheme. Likewise, if an ephemeral session state is maintained in a particular network node and other network nodes need to either query or update that session state, the node location may be unpredictable (e.g., due to a non-deterministic routing during session set-up). In such cases, session hunting algorithms may be performed to locate a node storing the pertinent session information.

[0147] In an embodiment, the caching operations may be integrated with message destination hunting operations.

[0148] As discussed above, telecommunications operator networks are expanding. As these networks expand and new resources are introduced, it is more likely that a component (server, processor, hard drive, DCR core, memory, etc.) in the system will fail. The various embodiments enable management of component failure by configuring dynamic context routers to perform failover operations that automatically switch over to a redundant component (e.g., blade, server, DCR core, memory, network node, etc.) upon the failure or abnormal termination of a component. The dynamic context router may be configured to perform multi-level and multi-tier failover operations to ensure continued operations in the event of multiple component failures. Moreover, the various embodiments provide scalable, distributed, highly available dynamic context router systems capable of fast and efficient expansion by supporting the addition of resources (e.g., additional cores, memories), while maintaining high-availability.

[0149] FIGs. 15A-17C illustrate example logical components and information flows in embodiment DCR systems that perform failover operations and maintain session state information in the event of a component failover. FIG. 15A illustrates example logical components in a DCR system 1500 configured to maintain session state information in the event of a failover. The DCR system 1500 may include one or more pairs of servers/DCRs, each pair including a first DCR 1502 having a first DCR core 1504 and a first memory 1506 and a second DCR 1508 having a second DCR core 1510 and a second memory 1512. The first and second memories 1506, 1512 may be any internal resource (e.g., reference database 1102, session stores 1104, cache 1106 discussed above with reference to FIG. 11) for storing information.

[0150] The DCR system 1500 may also include a communication link 1514 connecting the first and second DCRs 1502, 1508. The second memory 1512 may store a replica of the information stored by the first memory 1506, which may be initiated by the DCR system. In an embodiment, the communication link 1514 may connect the first and second memories 1506, 1512 on the first and second DCRs 1502, 1508 such that any information added to the first memory 1506 is automatically added to the second memory 1512. Likewise, any information removed/expired from the first memory 1506 may be automatically removed/expired from the second memory 1512.

[0151] Session information may be stored in the first and second memories 1506, 1512 using a structure (e.g., associative array, hashtable, tree, etc.) that allows the sessions to be quickly located and retrieved from the memories. In an embodiment, the first and second memories 1506, 1512 may store information so that the same decision logic locates the stored information in each physical memory. In this manner, the logic used to locate the session states in memory is the same for both memories, despite the session state information being physically stored in separate memories (e.g., first and second memories 1506, 1512).

[0152] FIG. 15B illustrates example information flows in an example DCR system 1550 configured to maintain session state information in the event of a failover. Specifically, FIG. 15B illustrates that a source node 902a may send a signaling message to the first DCR core 1504 over a primary communications link 1530 and maintain a reference to a secondary communication link 1532 to the second DCR core 1510. The first DCR core 1504 may receive the message, identify a proper destination node (e.g., 906a) and/or perform other DCR operations

on the message. The first DCR core 1504 may also establish session stickiness by storing session information (e.g., session 1) in the first memory 1506, which is automatically replicated in the second memory 1512 via the communication link 1514.

[0153] If the first DCR core 1504 fails or does not respond to the source node 902a in a predetermined amount of time, the source node 902a may fail over to the second DCR core 1510 by sending the signaling message over the secondary communication link 1532. Since the second memory is a replicate of the first memory 1506, the second DCR core 1510 may retrieve the session information from the second memory 1512 and perform any and all operations originally requested from the first DCR core 1504, including sending the message to the destination node 906a. In this manner, session state is maintained and the DCR system is resilient to the failure event.

[0154] It should be understood that the DCR systems discussed herein may operate in both an active-hot standby configuration, as well as in an active-active configuration, and that each of the DCR cores may simultaneously serve as both a primary DCR core and a secondary DCR core.

[0155] FIG. 15C illustrates example information flows in an embodiment DCR system 1570 configured to provide failover support on two layers. Similar to the system described above, the source node 902a sends a signaling message to the first DCR core 1504 over the primary communications link 1530 and maintains a reference to the secondary communication link 1532 to the second DCR core 1510. The first DCR core 1504 receives the message and performs DCR operations, which may include identifying suitable destination nodes and storing session information (e.g., session 1) in the first memory 1506, which is automatically replicated in the second memory 1512 via communication link 1514. The first and second memories 1506, 1512 and the primary and secondary communication links 1530, 1532 provide a first layer of failover support.

[0156] In the illustrated example of FIG. 15C, the DCR core sends messages to destination node 906a using DCR-1 Primary. When destination node 906a becomes unresponsive, the DCR may select destination node 906z (using the topology tree) and start sending future messages to it using DCR-1 Secondary. In other words, destination node 906z may not be chosen before destination node 906a fails.

[0157] In the various embodiments, dynamic context routers may be grouped into pairs (DCR Pairs) such that each dynamic context router system includes an even number of DCR cores. This allows the session stores to be deployed in an active-hot standby configuration while the DCR cores operate in an active-active configuration. That is, each DCR core within the DCR Pair may remain active (i.e., may receive and process network traffic) while one session store within the DCR pair remains active and a second session store within the DCR pair remains on active standby.

[0158] FIG. 16 illustrates logical components and informational flows in another example DCR system 1600 configured to maintain session state information in the event of a failover. The DCR system 1600 may include a DCR pair 1602 having a first DCR 1604 and a second DCR 1606. Similar to the DCR system 1500 described above, the first DCR1604 may include a first DCR core 1608 and a first memory 1610, the second DCR 1606 includes a second DCR core 1612 and a second memory 1614, and a communication link 1616 connects the first DCR1604 to the second DCR 1606, and information may be transferred such that the second memory 1614 contains a replica of the session information stored by the first memory 1610. The DCR system 1600 also includes primary communications links (DCR-1 Primary) 1618, (DCR-2 Primary) 1620 connecting the first and second DCR cores 1608, 1612 to the first memory 1610. Likewise, secondary communications links (DCR-1 Secondary) 1622, (DCR-2 Secondary) 1624 connect the first and second DCR cores 1608, 1612 to the second memory 1614. Each of the first and second DCR cores 1608, 1612 may remain active (e.g., receives and processes Diameter messages), while one of the first and second memories 1610, 1614 remains active. The non-active memory (e.g., 1610 or 1614) may remain in a standby mode.

[0159] A source node 902a may send a signaling message to the first DCR core 1608 over a primary communication link and maintain a secondary communication link to the second DCR core 1612. If the first DCR core 1608 fails or does not respond to the source node in a predetermined amount of time, the source node 902a may fail over to the second DCR core 1612 and send the signaling message using the secondary communication link. Likewise, both the first and second DCR cores 1608, 1612 may read and write information to the first memory 1610 (e.g., via the primarily communications links 1618, 1620). If the first memory fails, both the first and second DCR cores 1608, 1612 may fail over to the second memory 1614 to access the replicated data. In this manner, DCR system 1600 is resilient to the database/memories 1610, 1614 failing, the DCR cores 1608, 1612 failing, and the DCRs 1604, 1606 failing. In addition, the failure of any one component does not affect the availability of the other components.

[0160] FIGs. 17A-17C illustrate example information flows and logical components in an example DCR system 1700 configured to provide failover support and maintain session state information across partitions (e.g., partitions 1730 and 1732). As discussed above, operator networks must expand to meet the increase in user demand, support the array of new services and provide fast, reliable communications. As the operator networks grow, more DCR components must be deployed in each DCR system. To support scalability, the various embodiments provide scalable DCR systems capable of partitioning resources (e.g., logically grouping resources physically located on different DCRs and/or included in different

DCR pairs) and storing information across the network. In an embodiment, the partitioning of resources may include performing partitioning or domaining operations.

[0161] FIG. 17A illustrates example logical components that may be included in a scalable DCR system 1700 configured to maintain session state information across partitions. The DCR system 1700 may include a first DCR pair 1702 and a second DCR pair 1704. Each DCR pair 1702, 1704 may be similar to the DCR pair 1602 described above with reference to FIG. 16. For example, each DCR pair 1702, 1704 may include two DCRs (e.g., DCRs 1-2, 3-4) 1706, 1708, 1710, 1712, each DCR having a DCR core 1714, 1716, 1718, 1720 and a memory 1722, 1724, 1726, 1728. Each of the DCRs 1706, 1708, 1710, 1712 within the first and second DCR pairs 1702, 1704 may also be connected to each other by a communications link 1721, 1725 and the DCR cores 1714, 1716, 1718, 1720 may be configured to replicate the information stored in the primary memory (e.g., first memory 1722, third memory 1726) to the secondary memory (e.g., second memory 1724, fourth memory 1728). The first DCR pair 1702 may be connected to the second DCR pair 1704 via a communications link 1750. The first and second memories 1722, 1724 may be logically grouped together into a first memory group (i.e., the first partition 1730), and the third and fourth memories 1726, 1728 may be grouped together into a second memory group (i.e., the second partition 1732).

[0162] This architecture enables a greater level of redundancy and enables graceful failover operations in the event of failure of any one component. This is revealed by the information flows illustrated in FIGs. 17B and 17C.

[0163] FIG. 17B illustrates example DCR information flows in the DCR system 1700 in receiving messages from a source node 902a. Source node 902a may be configured to communicate with a particular DCR core as the primary DCR, and configured with a backup address to a secondary DCR core. Under normal circumstances, each source node will communicate with its primary DCR core. However, in the event that the primary DCR core is unavailable or does not respond to messages, the source node may begin communicating with its secondary DCR core. This is illustrated in FIG. 17 B by the source node 902a sending a signaling message to the first DCR core (DCR-1 Core) 1714 (illustrated with the solid arrow) while maintaining an address for a secondary DCR core (DCR-2 Core) 1716 (illustrated with the dotted arrow). While FIG. 17 B shows the secondary DCR core being positioned within the same DCR pair 1702, the primary and secondary DCR cores for any particular source node need not be within the same DCR pair, and may be located in other pairs (e.g., the secondary DCR core could be located in DCR pair 2 1704). Provisioning source nodes with primary and secondary DCR addresses is similar to the configurations discussed above with reference to FIGs. 15B, 15C and 16. In processing messages received from the source node 902a and performing DCR operations, the first DCR core 1714 storing session information within a primary memory, which may not be in the same DCR pair. Further, each DCR core may store session data in any one of the primary or secondary memories within the server. This may be implemented in a manner that spreads session data from all of the DCR cores among all of the primary memories in a semi-random manner. By distributing DCR core assignment and primary and secondary memory correlations across several DCR pairs within a given server installation may improve reliability and guard against systematic failures.

[0164] In an embodiment, the first DCR core 1714 may determine the particular primary memory or memory group for saving session data associated with a particular source node or even for a particular session by performing an address assignment operation. Thus, in the illustrated example of messages being received from source node 902a, the primary DCR core 1714 may perform an assignment operation on an address or session identifier portion of the received message to determine that associated session data should be stored in the second memory partition 1732. Using this addressing information, the primary DCR core 1714 stores the session information in the primary memory 1726 of the second memory partition 1732. As discussed above, the session data may be stored within the memory partition in the primary memory 1726, which may then be replicated in the secondary memory 1728. While not shown in this figure, when the primary DCR core 1714 receives messages associated with a different session, performing the address assignment operation may result in the session data being stored in memory partition 1 1730.

[0165] The address assignment function implemented on the primary DCR core 1714 may also be implemented on the secondary DCR core 1716, or on all the DCR cores within the network. This enables another DCR core (e.g., the secondary core 1716) to access session data (e.g., data stored in memory 1726) in the event that the source node 902a begins sending it messages related to a session originally managed by the primary DCR core 1714. This also enables another DCR core (e.g., the secondary core 1716) to access session data (e.g., data stored in memory 1726) in the event that a different source node references the same session as source node 902a begins sending it messages. Thus, by applying the same function to information contained in a portion of messages received from the source node 902a, the secondary DCR core 1716 may obtain the memory partition storing the associated session data without requiring any communication of memory addressing from the primary DCR core beforehand. This functionality enables the DCR core to resolve the Rx-Gx correlation problem that can arise when the source notes are the AF and the PCEF, for example.

[0166] FIG. 17C illustrates a message flow that may occur in the event that the primary memory 1726 within the second partition 1732 fails. As discussed above, the memory contents of the primary memory 1726 may be

replicated to the secondary memory 1728 of the same partition. Thus, in an embodiment, memory accesses and storage communications from the primary DCR core 1714 directed to the memory partition 1732 may be serviced by the secondary memory 1728.

[0167] It should be appreciated that secondary DCR core assignments need not be fully redundant. Instead, each DCR core may serve as a primary DCR for a number of source nodes and as the secondary DCR for another group of source nodes. By distributing session data among memory partitions based upon an addressing function which uses information from received messages as the input, load-balancing and memory allocation can be accomplished autonomously in a manner which can avoid systematic failure while eliminating the need to share addressing information among the various DCR cores.

[0168] In the various embodiments, the DCR may be configured to divide (or "fork") a single request message (e.g., create a full or partial duplicate of the message, create child messages, etc.) that is destined for a single destination into multiple messages addressed to multiple destinations. As part of this message forking process, the dynamic context router may generate one or more child messages from the original message being forked (i.e., the parent message). Each resulting message (i.e., child message) may be equal to the original message, a subset of the original message, or contain additional information not contained by the original message.

[0169] FIG. 18 illustrates example logical components and data flows in a dynamic context router system 1800 configured to enable a single "request" message, as well as a corresponding "response" message, to be forked at the application level and distributed to one or more additional nodes in accordance with an embodiment. In the illustrated example, the dynamic context router 1804 communicates with a source peer 1802, a destination peer 1806, a first network node (Node 1) 1808, and a second network node (Node 2) 1810, each of which may be any of logical network components described above (e.g., PCEF, PCRF, OFCS, OCS, SPR, AF, etc.). The dynamic context router 1804 may receive (e.g., via data flow 1812) a request message from the source peer 1802 and perform operations to identify an appropriate destination peer 1806 to which the message is to be sent. The dynamic context router 1804 may send the request message (e.g., via data flow 1814a) to the identified destination peer 1806, send a duplicate of the request message (e.g., via data flow 1814b) to the first network node 1808, and send (e.g., via data flow 1814c) a new message containing values from the request message to the second network node 1810. The dynamic context router 1804 may receive (e.g., via data flow 1816) a response message from the destination peer 1806 and determine the appropriate source node to which the response message is to be sent (e.g., source peer 1802). The dynamic context router may send the response message (e.g., via data flow 1818a) to the identified source node (i.e., source peer 1802) and send a duplicate of the response message (e.g., via data flow 1818b) to the first network node 1808.

[0170] In an embodiment, the dynamic context router may be configured to discard responses to forked messages. For example, in such configurations, if the first network node (Node 1) 1808 generates a response to a request message sent via data flow 1814b, the dynamic context router may choose to not to send this message back to the source peer. In an embodiment, the dynamic context router may use information from the message (e.g., to update a cache that may be later utilized to make future routing decisions) before the message is discarded. In this manner, the first network node 1808 may be an existing network node that does not need to be informed that it has received a forked message (as opposed to a standard message). In an embodiment, such configurations may be used to perform operations for "hunting in parallel," in which a request may be sent to three candidate nodes, for example, and the first node to respond is used for further requests, while the two slower responses may be discarded.

[0171] When a parent message is forked into one or more child messages, each child message may be generated via any protocol/application/format supported by the dynamic context router. Each child message may be in the same format/protocol as the parent message, or in a different format/protocol than the parent. Multiple child messages may be generated from each parent. Each message may be sent to multiple destinations independent of the destinations of the other child or parent messages. Application level information from within received messages and/or contextual information (which may be obtained from one or more of the methods described above) may be used to determine which messages should be forked and which destination the forked messages are to be sent.

[0172] By forking request messages (as well as corresponding response messages) at the application level for distribution to additional nodes, the dynamic context router functions not only as an application-level router, but also as a source node capable of generating messages based on the content of the messages being routed. The forked messages (i.e., child messages) may be used, for example, by other network components to collect information about the type and content of messages being communicated. The dynamic context router's ability to generate new messages (via forking) in addition performing application-level routing operations allows the DCR system to provide operator networks with a level of functionality not typically provided by, or expected from, intermediate network nodes (e.g., application-level routers).

[0173] FIG. 19 illustrates a fork-routing method 1900 that may be performed by the dynamic context router in accordance with an embodiment. In step 1902, the dynamic context router may receive a first message from the source component. In step 1904, the dynamic context

router may use application-level information obtained from the message to determine which messages should be forked, and to which destination network components each of the messages are to be sent. In step 1906, the dynamic context router may use contextual information to further determine which messages should be forked and to further identify destination network components to which the messages are to be sent. In step 1908, the dynamic context router may fork or duplicate a single message destined for a single destination into multiple forked messages based on the application level and/or contextual information. In step 1910, the dynamic context router may send the original message to the appropriate identified destination. In step 1912, the dynamic context router may send each of the forked messages to their respective identified destinations.

[0174] In an embodiment, the dynamic context router may support the communication of messages between network components implementing different flavors of the same application/protocol/message format by adding extra attribute-value pairs (AVPs) into received messages, dropping AVPs from received messages, or both. In an embodiment, the dynamic context router may maintain references to specific dictionary databases for applications supported by each of the network components with which the dynamic context router communicates. The dynamic context router may communicate with the referenced dictionaries to determine which AVPs are to be added into the message and/or which AVP are to be removed from the message. In this manner, the dynamic context router may support multiple flavors of the same application/protocol/message format even when the specific flavors cannot be ascertained from the type or contents of the message being communicated (e.g., the message being communicated is a Diameter message, which does not include such information).

[0175] In an embodiment, the dynamic context router may modify messages such that they can be received and processed by the receiving network component and/or without causing the receiving network component to send an error message. In an embodiment, the dynamic context router may convert the messages into the specific flavors required by network components with which it communicates.

[0176] FIG. 20 illustrates logical components and interfaces in an example dynamic context router system (DCR system) 2000 configured to facilitate the communication of signaling messages between Diameter peers 2004. The DCR system 2000 may include a DCR core 2002 having a Diameter protocol library module 2006, a dynamic context router dispatcher module 2008 and a message handler module 2010. The message handler module 2010 may include a request handler module 2012, a response module 2014, and a failover handler module 2016, each of which may be a pipeline, which are discussed in more detail further below.

[0177] In the illustrated example of FIG. 20, the DCR core 2002 includes a number of interfaces 1-11 that facilitate communications between the modules (e.g., library module 2006, dispatcher module 2008, message handler module 2010, etc.) and with external resources, such as session stores 2020, external lookup databases 2022, user defined caches 2024, routing configuration data-stores 2026, databases storing peer topology, realm routing and application information 2028, and peer configuration data-stores 2030. For example, the DCR core 2002 may receive DCR Diameter configuration information over interface 8, initialize a Diameter protocol library by specifying application support over interface 5, and register any call-backs required for the Diameter protocol library to DCR notification interface (i.e., interface 2). Each of the interfaces 1-11 are discussed in more detail below.

[0178] The DCR core 2002 interacts with the Diameter Peers 2004 over interface 1, which may be used to perform base protocol interactions (e.g., performing capabilities exchanges, watchdog exchanges, etc.); maintain state information for each configured peer; send and receive Diameter application messages to and from each peer; maintain a transaction queue of unanswered messages sent to each peer; match responses received with entries in the transaction queues; handle redirect responses received from peers; maintain redirect caches; and perform other similar operations.

[0179] The Diameter protocol library module 2006 may communicate with the DCR dispatcher module 2008 and the message handler module 2010 over interface 2, which may be used to pass Diameter messages (requests or responses) to the DCR message handler module 2010 for processing; pass notifications of any peer transport failures to the DCR dispatcher module 2008; pass all outstanding messages for a failed peer to the DCR dispatcher module 2008 in Diameter failover situations (so that an alternative destination can be chosen); periodically pass information on the sizes of peer transaction queues to the DCR dispatcher module 2008 to enable it to make informed load balancing decisions; and perform other similar operations. In an embodiment, the DCR dispatcher module 2008 may receive notifications about the state of the Diameter peers 2004 from the Diameter protocol library module 2006 over interface 2, and manage such notifications accordingly. In an embodiment, the management of notifications may include storing state information in a local peer topology configuration data-store.

[0180] The DCR dispatcher module 2008 may send communications to message handling modules/pipelines (e.g., request handler pipeline 2012, etc.) over interface 3. For example, the DCR dispatcher module 2008 may dispatch messages (both requests and responses) received from the Diameter library module 2006 to the request handler pipeline module 2012 over interface 3.

[0181] The DCR dispatcher module 2008 may receive messages from the message handler module 2010 over interface 4 and perform operations that assist in the identification of a suitable Diameter peer destination for the

received messages. These operations may include: converting non-specific domain destinations populated by routing logic into specific destination hosts using the DCR dispatcher's 2008 knowledge of the peer topology (which may be loaded from interface 8) and each peer's availability; and selecting a specific destination based on failover and load balancing configuration information embedded in the peer topology definition.

[0182] The DCR dispatcher module 2008 may communicate with the Diameter protocol library module 2006 over interface 5, which may be used to: forward a Diameter message to a nominated destination-host; generate a Diameter response to the originating diameter node (e.g., instead of forwarding to another Diameter node); generate a redirect response to the originating diameter node; and perform other similar operations. Interface 5 may also be used by the DCR core 2002 to initialize a Diameter protocol library (e.g., by specifying application support).

[0183] The Diameter protocol library 2006 may include system libraries (e.g., libdbprotocol.so, libdbparser.so, etc.) as well other information that may be used to implement base diameter protocol functionality. Information retrieved from the Diameter protocol library 2006 may also be used to: perform capabilities exchanges with each configured peer (which may be loaded via interface 9); maintain connectivity using device watchdogs; provide an application programming interface (API) that allows the DCR core 2002 to send and receive messages from other Diameter nodes; and provide a notification interface so that the DCR core 2002 can be made aware of important Diameter events.

[0184] The message handler modules 2010 and the DCR dispatcher module 2008 may communicate with a session store 2020 via interface 6. The DCR core 2002 may receive routing configuration information over interface 7.

[0185] The DCR core 2002 may receive DCR Diameter configuration information over interface 8. The DCR Diameter configuration information may include a DCR realm based routing table and a topology tree that organizes the Diameter peers 2004 into a topology that may be used to derive load balancing and failover rules.

[0186] In an embodiment, the routing configuration information and logic may be decoupled from other aspects related to Diameter connectivity. This allows the DCR core 2002 to support failover and load balancing operations across all of the configured peers, while at the same time, not cluttering the routing logic with all of the peer and connectivity knowledge.

[0187] In an embodiment, the DCR routing configuration information may only include information for choosing an appropriate destination domain. For example, the DCR may be configured such that a telecommunications operator with a requirement to route messages to one of two data centers according to some business rules can define domains representing the possible destinations.

[0188] The DCR core 2002 may receive peer configuration information over interface 9, which may be used to load configured peers. The DCR core 2002 may send data requests to user defined caches via interface 10, and to external lookup engines/databases via interface 11.

[0189] As mentioned above, the DCR system may arrange network elements into a logical tree topology. The base Diameter library (on top of which messages processed by the DCR system may be built) maintains the peer configuration as a simple unstructured list. In an embodiment, the DCR system may, through configuration, arrange the elements of the base Diameter library's peer configuration list into a logical tree topology reflecting: at the top level, the high level routing domains (e.g., destinations chosen by routing logic); within a domain, a prioritized list of peer groups for availability purposes; and within a peer group, an unordered list of peers for load balancing purposes. This topology arrangement enables the DCR dispatcher 2008 to be given a high level destination domain and to route messages to specific peers by applying failover and load balancing rules. This also enables components which load the topology configuration at run time to be informed of peer availability.

[0190] In an embodiment, the topology arrangement may include at least one domain in a DCR deployment, at least one peer-group per domain, and at least one peer per peer-group. Peer groups within a domain may be prioritized, such that routing within a domain may be directed to the highest priority peer group that is available. Peer groups may specify how many peer failures can be tolerated before the peer group is to be considered unavailable. Peer groups may also specify the load balancing algorithms (e.g., round robin, weighted round robin, least outstanding messages, etc.) that are to be used when routing messages to the peer group's constituent peers.

[0191] In an embodiment, the DCR system may be configured to filter messages based on user defined criteria. This filtering may be performed at the beginning, middle, or end of the request processing operations. In an embodiment, filtering may be performed after the request processing operations to maximize the data available for use by the filtering operations. In an embodiment, the outcome from the filter process may be a Boolean value, which may be made available to the DCR dispatcher 2008, which may generate either an error response (if the message is to be filtered) or route the message to the destination node (message is not filtered).

[0192] In an embodiment, the dynamic context router system may be configured to append information, such as domain failover information, to the messages in the transaction queue. This enables the dynamic context router to subsequently take actions using this additional information which would otherwise not be possible. The DCR system may also store a destination domain in the transaction queue. In an embodiment, if a failover is later initiated, the DCR system may choose an alternative destination host based on the originally chosen destination

domain.

[0193] In an embodiment, the DCR system may be configured to process messages by decoding a received message into an internal representation of the message (e.g., a structured message format proprietary to the DCR system), and passing it to a routing logic module/pipeline responsible for performing the routing operations. In an embodiment, the internal representation may be an AVS.

[0194] In an embodiment, the DCR system may implement a fixed pipeline model (e.g., a model in which each module includes a number of optional steps for performing a specific set of tasks) to control the processing of the message. For example, Diameter request messages received by the DCR system may be processed by a request pipeline, which may make routing decisions and/or manipulate the message using a discrete number of configurable steps.

[0195] As discussed above with reference to FIG. 20, each of the message handling modules (e.g., request handler module 2012, response module 2014, failover handler module 2016, etc.) may be a pipeline, and the various DCR message handling operations may be managed by a separate pipeline depending on the type of message or type of operation (e.g., requests, responses, failovers, etc.). For example, messages originating from the Diameter protocol library module 2006 may be passed (e.g., via the DCR dispatcher module 2008, etc.) to the appropriate pipelines/modules within the message handling module 2010 responsible for processing the message. Each pipeline may be configured in accordance with user preferences, network requirements, deployment environment and/or user requirements. Each pipeline may also be configured on a "per message type" and/or "per application" bases.

[0196] In the various embodiments, each pipeline may be minimally configured or extensively configured. For example, a pipeline may be minimally configured to handle situations where the Diameter realm based routing table provides all of the information necessary to route a message, or extensively configured to handle situations requiring custom processing involving lookups and routing logic.

[0197] Each of the message handling pipelines/modules may include a number of sub-modules (steps) that provide a set of highly customizable functions. For example, each module/step may be configured to perform a specific set of operations such as:

interacting with the default session store (e.g., when session state only needs to store a destination choice); interacting with a user defined session store (e.g., for more complex session store operations); augmenting the incoming message by performing external and
internal lookups (e.g., via interfaces 10 and 11 of FIG. 20) using keys from the incoming message or from the results of other lookups; examining the contents of augmented message to choose one or more destination domains or to perform message destination hunting operations; preparing message to be routed by modifying, adding or removing AVPs from one or more messages; filtering messages via a user defined white-list or
black-list (e.g., refusing to route the message), etc. Each sub-module (step) may have a specific set of permissions that limit the allowable operations available to that step, which may be based on a number of configurable factors (e.g., type of module requesting the operation, deployment environment, network conditions, etc.).

[0198] In an embodiment, each pipeline may be a fixed message handling pipeline that aids the management of routing decisions and/or message manipulation operations.

[0199] In an embodiment, each pipeline may be configured at an application command level granularity. For example, each pipeline may be configured for Gx-based credit control requests.

[0200] In an embodiment, the DCR system may be configured to detect the existence of an empty pipeline (e.g., a pipeline that is not configured, is configured to exclude all steps, etc.) and perform routing operations using the routing functionality of the base Diameter protocol.

[0201] In the various embodiments, the DCR system may include one or more of a request handling pipeline, a response handling pipeline, and a failover handling pipeline.

[0202] FIG. 21 illustrates a request pipeline 2102 for processing Diameter request messages. The request pipeline 2102 may be a part of the DCR core, which may utilize the request pipeline 2102 to make routing decisions (e.g., locating a destination node, determining that the message cannot be routed, etc.) and/or to manipulate messages. The routing logic used to process the messages may be specific to the received message or message type. In an embodiment, the routing logic may be dynamic and/or attached to each pipeline stage via a proprietary DCR scripting language.

[0203] In an embodiment, each incoming request message may be passed to the request pipeline 2102, which is then identified by application and command. An empty routing ticket may be constructed upon entry to the pipeline process, which is then populated with a decoded internal representation of the received request message.

[0204] The request pipeline 2102 may include a number of discrete steps, stages, or modules (herein steps which may be performed in sequence as a message passes through the pipeline 2102), with each step performing a distinct DCR operation. Each step of the pipeline may populate different portions of the routing ticket, which may include portions for: the decoded request message (AVS type structure); raw data (e.g., message data not decoded); a request action; lookup results;

session state; destination domain(s); a filter decision; and redirect AVPs. In the example illustrated in FIG. 21, the request pipeline 2102 includes a realm routing lookup step 2110, a session lookup step 2112, a gather data step 2114, a routing core step 2116, a prepare AVS step 2118, a filter step 2120, a dispatcher step 2122, and a session update step 2124.

[0205] In the realm routing lookup step 2110, the request pipeline may perform a lookup on a configured realm based routing table. The realm based routing table may have the same or similar characteristics as a standard Diameter routing table (as described in Diameter standards RFC 3588), or may be a modified version of a standard Diameter routing table.

[0206] In an embodiment, the realm based routing table may include the following modifications over a standard Diameter routing table: a configuration column containing an "Override Destination" flag, which may express whether the destination read from a row in the table can be overridden; a configuration column containing an "Override Action" flag, which may express whether the action read from this row in the table can be overridden; a "Redirect host usage" column and a "Redirect max cache time" column, which may be used when the action is redirect and the redirect response message should populate correspondingly named AVPs; a server column renamed to domain, which may contain the name of a DCR configured domain rather than a specific host (as would be the case under Diameter standards RFC3588).

[0207] As mentioned above, the DCR system may be configured to perform decoding operations in multiple phases. In such configurations, the incoming request message may be partially decoded during the realm routing lookup step 2110 (e.g., only the header and base protocol routing AVPs may be extracted). The entire message may or may not be fully decoded (at a later stage) depending on an outcome of the lookup operations. For example, if there is no match resulting from the table look, or if the action is proxy and the destination domain is assigned, the message may be fully decoded. On the other hand, the message may be partially decoded if the action is relay or redirect, and the destination domain is assigned. The DCR system may also be configured to cause the message to be handled (e.g., routing the message, rejecting the message, etc.) at a later stage/step when there is no match on the table lookup by fully decoding the message but not setting a destination domain. In an embodiment, the outcome of the realm routing lookup step 2110 may be overridden depending on the value of the override flags in a matched table row.

[0208] The session lookup step 2112 may be performed as part of establishing session stickiness. In the session lookup step 2112, the DCR system may determine if the message belongs to a known and previously routed session. If so, the destination host and destination domain may be set in the routing ticket. In an embodiment, the session lookup step 2112 may be minimally configured for applications that do not need to maintain session state other than the routing destination. In an embodiment, the session lookup step 2112 may be more extensively configured (e.g., via a proprietary DCR language) to perform custom operations and/or to include a custom session store.

[0209] In the gather data step 2114, the DCR system may gather data upon which routing decisions may depend (e.g., via cache lookups, external lookups, reference data lookups, etc.), configure the execution of the required lookups, reference the predefined lookup definitions and/or provide keys from any data available in the routing ticket. In an embodiment, the DCR system may populate a lookup results section of the routing ticket with the results of lookups performed as part of the gather data step 2114.

[0210] In the routing core step 2116, the DCR system may make routing decisions based on any of the information available in the routing ticket. As part of the routing core step 2116, the DCR system may also populate the destination domain in the routing ticket (assuming it was not already set by previous stages or it is allowed to override a previously set value) and/or override request actions (e.g., proxy, relay, redirect, unset, etc.) populated in the realm table (e.g., via the realm table lookup step 2110 discussed above). In an embodiment, when the request action is "unset," as part of the routing core step 2116, the DCR system may choose a method of delivery (e.g., proxy, relay or redirect) in addition to making a routing decision. In an embodiment, routing decisions made in the routing core step 2116 may be configured via a proprietary DCR language to perform custom logic/operations.

[0211] In the prepare AVS step 2118, the DCR system may make modifications to the message before it is sent. These modifications may include the addition of new AVPs, the modification of existing AVPs or the removal of AVPs. In an embodiment, the prepare AVS step 2118 may be limited to modifying the message within the routing ticket. In an embodiment, details of how the messages are modified in the prepare AVS step 2118 may be configured via a proprietary DCR language.

[0212] In the filter step 2120, the DCR system may filter messages based on user defined criteria. In an embodiment, the user-defined criteria may be specified via a proprietary DCR language.

[0213] In the dispatcher step 2122, the DCR system may choose a specific host. If a destination host and a destination domain are not specified by earlier stages in the pipeline 2102 (i.e., no host, no domain), an error response message may be sent to the network node originating the message (e.g., the source node). If a destination host is provided but there is no destination domain (i.e., provided host, no domain), the message may be routed to the specified destination host, and an error response may be sent to the originator of the message if the host is unavailable. If a destination host and a destination domain are both provided (i.e., provided host, provided domain), the message may be routed to the pro-

vided destination host, and an alternative destination host may be attempted if the specified one is unavailable. If no destination host is provided (i.e., no host, provided domain), an appropriate destination host may be chosen from the specified destination domain (e.g., via performing failover and load balancing operations), and an error response may be sent to the originator of the message if there are no available hosts within the domain.

[0214] As discussed above, messages handling operations may be facilitated by passing a routing ticket along various stages of a message handling pipeline. The dispatcher step 2122 may receive the routing ticket populated with: an action (e.g., Proxy, Relay, Redirect, etc.); a non-specific list of destination domains or a specific destination-host (if the message arrived at the DCR with this already set); the message to be sent (which may be a modified message); redirect related AVPs (which may be specified if the action is redirect); and/or a decision (e.g., yes, no) from the filter stage of the request pipeline.

[0215] In an embodiment, in the dispatcher step 2122, the DCR system may examine the routing ticket and perform operations (e.g., make calls to the Diameter protocol library) based on the contents of the examined message.

[0216] In an embodiment, in the dispatcher step 2122, the DCR system may generate a response message to be sent back to the originating peer with the Result-Code AVP set to "DIAMETER_UNABLE_TO_COMPLY" if the message filtering flag is set.

[0217] In an embodiment, in the dispatcher step 2122, the DCR system may select a peer from the specified domain if the action is proxy or relay, the destination-host is not specified and the destination-domain is specified. The highest priority available peer group from the domain may be chosen and a peer from within the chosen peer group may be chosen by performing a load balancing algorithm. If there are no available peer groups, an error response may be generated with Result-Code set to "DIAMETER_UNABLE_TO DELIVER".

[0218] In an embodiment, in the dispatcher step 2122, the DCR system may route the message to a specified destination-host if the action is proxy or relay, the destination-host is specified and the Destination-Domain is not specified (e.g., when the destination-host is provided by the incoming message or else populated by session stickiness processing). A message may be sent to a peer regardless of the state of its containing peer group (e.g., when a parent peer group is unavailable but the required child peer is available). If the specified peer is unavailable then an error may be returned to the originator specifying a Result-Code set to "DIAMETER_UNABLE_TO DELIVER".

[0219] In an embodiment, in the dispatcher step 2122, the DCR system may send a message to a specified destination-host if the action is proxy or relay, the destination-host is specified, and the destination-realm is specified. If the destination-host it is not available, the dispatcher may choose an alternative destination-host from the nominated destination-realm.

[0220] In an embodiment, in the dispatcher step 2122, the DCR system may send a redirect response to the originating node specifying the accompanying redirect related AVPs, Redirect-Cache-Usage and Redirect-Max-Cache-Time if the if the action is Redirect.

[0221] In an embodiment, in the dispatcher step 2122, the DCR system may perform message manipulation operations (e.g., changing the end-to-end-id, Route-Record and Origin-Host AVPs) if the message is to be routed onward and the topology hiding option is configured for the message.

[0222] The dispatcher step 2122 may receive multiple possible destination domains as part of hunting operations. When the dispatcher is required to route a message and it detects that destination domain is actually a list of possible destinations, the dispatcher may strip the first destination from the list and use it as the destination domain. The rest of the list may be stored in the transaction queue of the Diameter protocol library module and used by the response handling pipeline to determine the next destination that is to be tried if a response message indicates a failure.

[0223] In an embodiment, if a destination host and a destination domain are not specified by earlier stages in the pipeline 2102 (i.e., no host, no domain), an error response message may be sent to the network node originating the message (e.g., the source node). If a destination host is provided but there is no destination domain (i.e., provided host, no domain), the message may be routed to the specified destination host, and an error response may be sent to the originator of the message if the host is unavailable. If a destination host and a destination domain are both provided (i.e., provided host, provided domain), the message may be routed to the provided destination host, and an alternative destination host may be attempted if the specified one is unavailable. If no destination host is provided (i.e., no host, provided domain), an appropriate destination host may be chosen from the specified destination domain (e.g., via performing failover and load balancing operations), and an error response may be sent to the originator of the message if there are no available hosts within the domain.

[0224] In the session update step 2124, the DCR system may update one or more session stores by inserting new session entries, updating existing sessions and/or deleting session entries.

[0225] In an embodiment, the DCR system may be configured to process Diameter response messages via a response pipeline 2202, an example of which is illustrated in FIG. 22. The response pipeline 2202 may be a part of the DCR core. The response pipeline 2202 may include a number of discrete steps, stages, or modules (herein steps), each step performing a distinct DCR operation.

[0226] The DCR system may construct an empty routing ticket at an entry to the pipeline and populate the empty routing ticket with a decoded internal representation of the Diameter response message, as well as with

data stored with the matching original request. Each step of the pipeline may populate different portions of the routing ticket, which may include portions for: the decoded response message (AVS type structure); raw data (e.g., message data not decoded); the originally decoded request message (AVS type structure); any data that was stored with the request in the transaction queue; destination domain list; lookup results; and a response action (e.g., Send, Send-Next, Respond, Redirect).

[0227] In an embodiment, the response pipeline 2202 may be a subset of the request pipeline and/or include steps that perform operations similar to those performed by the request pipeline steps. In the illustrated example of FIG. 22, the response pipeline 2202 includes a gather data step 2210, a routing core step 2212, a prepare AVS step 2214 and a dispatcher step 2216. In the gather data step 2210, the DCR system may gather data upon which routing decisions may depend (e.g., via cache lookups, external lookups, reference data lookups, etc.). The DCR system may also configure the execution of the required lookups, reference the predefined lookup definitions and provide keys from any data available in the routing ticket. In the routing core step 2212, the DCR system may make routing decisions based on any of the information available in the routing ticket. In the prepare AVS step 2214, the DCR system may make modifications to the message before it is sent (e.g., adding new AVPs, modifying existing AVPs or removing AVPs). In the dispatcher step 2216, the DCR system may choose a specific host.

[0228] In an embodiment, the DCR system may be configured to accommodate component, system node and partial network failures, as well as discrete message delivery failures, in failover operations using a failover pipeline 2302, an example of which is illustrated in FIG. 23. The failover pipeline 2302 may be a part of the DCR core. The failover pipeline 2302 may include a number of discrete steps, stages, or modules (herein steps), each step performing a distinct DCR operation. In the illustrated example of FIG. 23, the failover pipeline 2302 includes a dispatcher step 2310 and a session update step 2312.

[0229] For example, in an embodiment, the DCR system may detect a transport failure and initiate Diameter failover procedures by sending the outstanding messages destined for the failed peer to the DCR failover pipeline 2302 for reprocessing. The DCR failover pipeline 2302 may choose an alternative destination for the message (e.g., based on the original destination host and/or original destination domain) in the dispatcher step 2310, and update the session store with the updated destination in session update step 2312. If the DCR system determines that the message cannot be re-routed, the DCR system may generate a response message to be sent to the requesting node. If the DCR system determines that the message can be re-routed, the message is re-routed to the alternative destination determined in the dispatcher step 2310. In the session update step 2312, the session store may be updated with new destination information.

[0230] In an embodiment, the DCR system (e.g., in the DCR failover pipeline 2302) may be configured to determine when it is not possible to route to an alternative destination by determining if the message was originally sent to a fixed destination to which no alternative destination is acceptable (e.g., the message requires a specific destination node) and/or by determining if all acceptable alternative peers are unavailable.

[0231] In an embodiment, the DCR system may perform application level operations in response to receiving a redirect message. As discussed above, the DCR system may receive redirect response messages from network peers, which may be processed without performing application-level operations in response to receiving the message. In an embodiment, the DCR system may be configured to perform application-level operations (e.g., update an application level cache in order to avoid unnecessary or incorrect routing of future messages) in response to receiving a redirect message. The DCR system may be configured to perform the application level redirect operations using a redirect pipeline 2402, an example of which is illustrated in FIG. 24. The redirect pipeline 2402 may be a part of the DCR core. The redirect pipeline 2402 may include a number of discrete steps, stages, or modules (herein steps), each step performing a distinct DCR operation. For example, the redirect pipeline may include a redirect step 2410 and a dispatcher step 2412.

[0232] In the various embodiments, the DCR system may create a cache with an identity, a configured key and an AVS for storage.

[0233] In the various embodiments, reference data may be configured by: defining a named reference data lookup by configuring the structure of the stored data; populating the reference data by importing a structured file, such as a file containing comma separated values; and/or allowing incremental updates to the reference data by importing file updates. Reference data may be non-volatile and persist across restarts.

[0234] As mentioned above, the DCR system may perform operations to establish session stickiness. For example, each time a session initialization message is routed though the DCR, the DCR system may make a determination as to whether session stickiness is required, and add session information to a session store if it is determined that session stickiness is required. Likewise, when the DCR system receives a session update message or a terminate message, the DCR system may update or remove entries from the session stores, respectively. In an embodiment, the various session sticky behaviors may be implemented in two separate parts of the DCR request processing pipeline. In an embodiment, the DCR system include a session store that uses known AVPs as keys and stores only routing information.

[0235] In an embodiment, the DCR system may perform topology hiding operations. Since Diameter is an end to end protocol, when Diameter client applications interact with server applications, the clients, through inspection of base routing AVPs, can learn about the mul-

tiplicity and addresses of server nodes, as well as the hops involved in reaching those servers. In some cases (e.g., where inter-PLMN routing of Diameter messages is performed) it is desirable to hide the server locations from client applications. In an embodiment, the DCR system may operate as a joint server and client Diameter node. In this manner, intermediate nodes cannot determine the true destination of a Diameter message because the information contained within the message will list the DCR system as the source/destination.

[0236] In an embodiment, the DCR system may perform topology hiding operations via AVP manipulation in order to make messages being routed by the DCR appear to originate from the DCR. In an embodiment, the manipulation of the AVPs for topology hiding may be performed within a dispatcher module or step (e.g., dispatcher step 2122) in a message processing pipeline. The dispatcher's topology configuration may include the ability to indicate if topology hiding should be applied on a per domain basis. For example, in a request processing pipeline (e.g., request pipeline 2102) the dispatcher (e.g., dispatcher step 2122) may receive a routing ticket with a destination domain(s) and a destination-host. If a selected destination domain requires topology hiding, then the dispatcher may modify the relevant AVPs such as the Origin-Host AVP and the Route-Record AVP to contain the DCR Diameter identity, and modify the End-to-End-Id AVP for the onward hop. In this case, the dispatcher (e.g., dispatcher step 2216) in the response processing pipeline (e.g., response pipeline 2202) may subsequently need to make equivalent topology hiding modifications. Topology hiding may also be applied in the same manner if it is required by the origin domain.

[0237] As discussed above, each of the request handling pipeline 2102, response handling pipeline 2202, failover handling pipeline 2302, and redirect pipeline 2402 may include a dispatcher step or module (herein dispatcher) responsible for mapping the destination domain decisions to specific destination hosts (with reference to the peer topology). In an embodiment, the dispatcher may map messages arriving from Diameter peers to the correct message handler, and handle notifications from the Diameter library about peer state changes and transaction queue sizes, such that the DCR system can make informed routing decisions.

[0238] In an embodiment, the DCR system may be configured to notify the dispatcher of peer state changes (e.g., via the Diameter library), which may be used by the dispatcher to make informed routing decisions by combining the peer topology and peer state.

[0239] In an embodiment, the dispatcher may translate a non-specific domain destination into a specific peer for routing by choosing the highest priority available peer group in the specified domain, and choosing a peer from the chosen peer group based on the configured load balancing algorithm

[0240] The various embodiments may be implemented on any of a variety of commercially available server devices, such as the server 2500 illustrated in FIG. 25. Such a server 2500 typically includes a processor 2501 coupled to volatile memory 2502 and a large capacity non-volatile memory, such as a disk drive 2503. The server 2500 may also include a floppy disc drive, compact disc (CD) or DVD disc drive 2506 coupled to the processor 2501. The server 2500 may also include network access ports 2504 coupled to the processor 2501 for establishing data connections with a network 2505, such as a local area network coupled to other operator network computers and servers.

[0241] The processor 2501 may be any programmable microprocessor, microcomputer or multiple processor chip or chips that can be configured by software instructions (applications) to perform a variety of functions, including the functions of the various embodiments described below. Multiple processors 2501 may be provided, such as one processor dedicated to wireless communication functions and one processor dedicated to running other applications. Typically, software applications may be stored in the internal memory 2502, 2503 before they are accessed and loaded into the processor 2501. The processor 2501 may include internal memory sufficient to store the application software instructions.

[0242] The foregoing method descriptions and the process flow diagrams are provided merely as illustrative examples and are not intended to require or imply that the steps of the various embodiments must be performed in the order presented. As will be appreciated by one of skill in the art the order of steps in the foregoing embodiments may be performed in any order. Words such as "thereafter," "then," "next," etc. are not intended to limit the order of the steps; these words are simply used to guide the reader through the description of the methods. Further, any reference to claim elements in the singular, for example, using the articles "a," "an" or "the" is not to be construed as limiting the element to the singular.

[0243] The various illustrative logical blocks, modules, circuits, and algorithm steps described in connection with the embodiments disclosed herein may be implemented as electronic hardware, computer software, or combinations of both. To clearly illustrate this interchangeability of hardware and software, various illustrative components, blocks, modules, circuits, and steps have been described above generally in terms of their functionality. Whether such functionality is implemented as hardware or software depends upon the particular application and design constraints imposed on the overall system. Skilled artisans may implement the described functionality in varying ways for each particular application, but such implementation decisions should not be interpreted as causing a departure from the scope of the present invention.

[0244] The hardware used to implement the various illustrative logics, logical blocks, modules, and circuits described in connection with the aspects disclosed herein may be implemented or performed with a general purpose processor, a digital signal processor (DSP), an ap-

plication specific integrated circuit (ASIC), a field programmable gate array (FPGA) or other programmable logic device, discrete gate or transistor logic, discrete hardware components, or any combination thereof designed to perform the functions described herein. A general-purpose processor may be a microprocessor, but, in the alternative, the processor may be any conventional processor, controller, microcontroller, or state machine. A processor may also be implemented as a combination of computing devices, e.g., a combination of a DSP and a microprocessor, a plurality of microprocessors, one or more microprocessors in conjunction with a DSP core, or any other such configuration. Alternatively, some steps or methods may be performed by circuitry that is specific to a given function.

[0245] In one or more exemplary aspects, the functions described may be implemented in hardware, software, firmware, or any combination thereof. If implemented in software, the functions may be stored on or transmitted over as one or more instructions or code on a computer-readable medium. The steps of a method or algorithm disclosed herein may be embodied in a processor-executable software module which may reside on a tangible, non-transitory computer-readable storage medium. Tangible, non-transitory computer-readable storage media may be any available media that may be accessed by a computer. By way of example, and not limitation, such as, non-transitory computer-readable media may comprise RAM, ROM, EEPROM, CD-ROM or other optical disk storage, magnetic disk storage or other magnetic storage devices, or any other medium that may be used to store desired program code in the form of instructions or data structures and that may be accessed by a computer. Disk and disc, as used herein, includes compact disc (CD), laser disc, optical disc, digital versatile disc (DVD), floppy disk, and blu-ray disc where disks usually reproduce data magnetically, while discs reproduce data optically with lasers. Combinations of the above should also be included within the scope of non-transitory computer-readable media. Additionally, the operations of a method or algorithm may reside as one or any combination or set of codes and/or instructions on a tangible, non-transitory machine readable medium and/or computer-readable medium, which may be incorporated into a computer program product.

[0246] The preceding description of the disclosed embodiments is provided to enable any person skilled in the art to make or use the present invention. Various modifications to these embodiments will be readily apparent to those skilled in the art, and the generic principles defined herein may be applied to other embodiments. Thus, the present invention is not intended to be limited to the embodiments shown herein but is to be accorded the widest scope consistent with the following claims and the principles and novel features disclosed herein.

Claims

1. A method of communicating signaling information in a telecommunications signaling network, comprising:

   receiving, in a first processor, a first message encoding signaling information from a source component;
   decoding the received first message into an internal representation;
   processing the internal representation of the message via a pipeline having a plurality of stages, each stage containing one or more procedures for performing a specific set of tasks;
   performing application level routing operations using contextual information derived from the internal representation to identify a destination component;
   encoding the signaling information contained in the internal representation into a second message; and
   sending the second message encoding the signaling information to the identified destination component.

2. The method of claim 1, wherein performing application level routing operations using contextual information derived from the internal representation to identify a destination component comprises using at least one pipeline stage to make a routing decision using a discrete number of configurable procedures.

3. The method of claim 1, wherein the pipeline type is one of a request handler pipeline, a response handler pipeline, a failover handler pipeline, or a redirect handler pipeline.

4. The method of claim 1, wherein the pipeline type and instance is selected on a per message type or on a per application basis.

5. The method of claim 1, wherein the pipeline has a plurality of stages that include at least one stage from the group consisting of a realm routing lookup stage, a session lookup stage, a gather data stage, a routing core stage, a prepare attribute value stream (AVS) stage, a filter stage, a dispatcher stage, a session update stage, and a redirect stage.

6. A server configured for use in a telecommunications signaling network, comprising:

   a processor configured with processor-executable instructions to perform operations comprising:

   receiving a first message encoding signal-

ing information from a source component;
decoding the received first message into an internal representation;
processing the internal representation of the message via a pipeline having a plurality of stages, each stage containing one or more procedures for performing a specific set of tasks;
performing application level routing operations using contextual information derived from the internal representation to identify a destination component;
encoding the signaling information contained in the internal representation into a second message; and
sending the second message encoding the signaling information to the identified destination component.

7. The server of claim 1, wherein the processor is configured with processor-executable instructions to perform operations such that performing application level routing operations using contextual information derived from the internal representation to identify a destination component comprises using at least one pipeline stage to make a routing decision using a discrete number of configurable procedures.

8. The server of claim 1, wherein the processor is configured with processor-executable instructions to perform operations such that the pipeline type is one of a request handler pipeline, a response handler pipeline, a failover handler pipeline, or a redirect handler pipeline.

9. The server of claim 1, wherein the processor is configured with processor-executable instructions to perform operations such that the pipeline type and instance is selected on a per message type or on a per application basis.

10. The server of claim 1, wherein the processor is configured with processor-executable instructions to perform operations such that the pipeline has a plurality of stages that include at least one stage from the group consisting of a realm routing lookup stage, a session lookup stage, a gather data stage, a routing core stage, a prepare attribute value stream (AVS) stage, a filter stage, a dispatcher stage, a session update stage, and a redirect stage.

11. A non-transitory server-readable storage medium having stored thereon server-executable instructions configured to cause a server to perform operations comprising:

receiving a first message encoding signaling information from a source component;
decoding the received first message into an internal representation of the message;
processing the internal representation of the message via a pipeline having a plurality of stages, each stage containing one or more procedures for performing a specific set of tasks;
performing application level routing operations using contextual information derived from the internal representation to identify a destination component;
encoding the signaling information contained in the internal representation into a second message; and
sending the second message encoding the signaling information to the identified destination component.

12. The non-transitory server-readable storage medium of claim 1, wherein the stored server-executable instructions are configured to cause a server to perform operations such that performing application level routing operations using contextual information derived from the internal representation to identify a destination component comprises using at least one pipeline stage to make a routing decision using a discrete number of configurable procedures.

13. The non-transitory server-readable storage medium of claim 1, wherein the stored server-executable instructions are configured to cause a server to perform operations such that the pipeline type is one of a request handler pipeline, a response handler pipeline, a failover handler pipeline, or a redirect handler pipeline.

14. The non-transitory server-readable storage medium of claim 1, wherein the processor is configured with processor-executable instructions to perform operations such that the pipeline type and instance is selected on a per message type or on a per application basis.

15. The non-transitory server-readable storage medium of claim 1, wherein the stored server-executable instructions are configured to cause a server to perform operations such that the pipeline has a plurality of stages that include at least one stage from the group consisting of a realm routing lookup stage, a session lookup stage, a gather data stage, a routing core stage, a prepare attribute value stream, AVS, stage, a filter stage, a dispatcher stage, a session update stage, and a redirect stage.

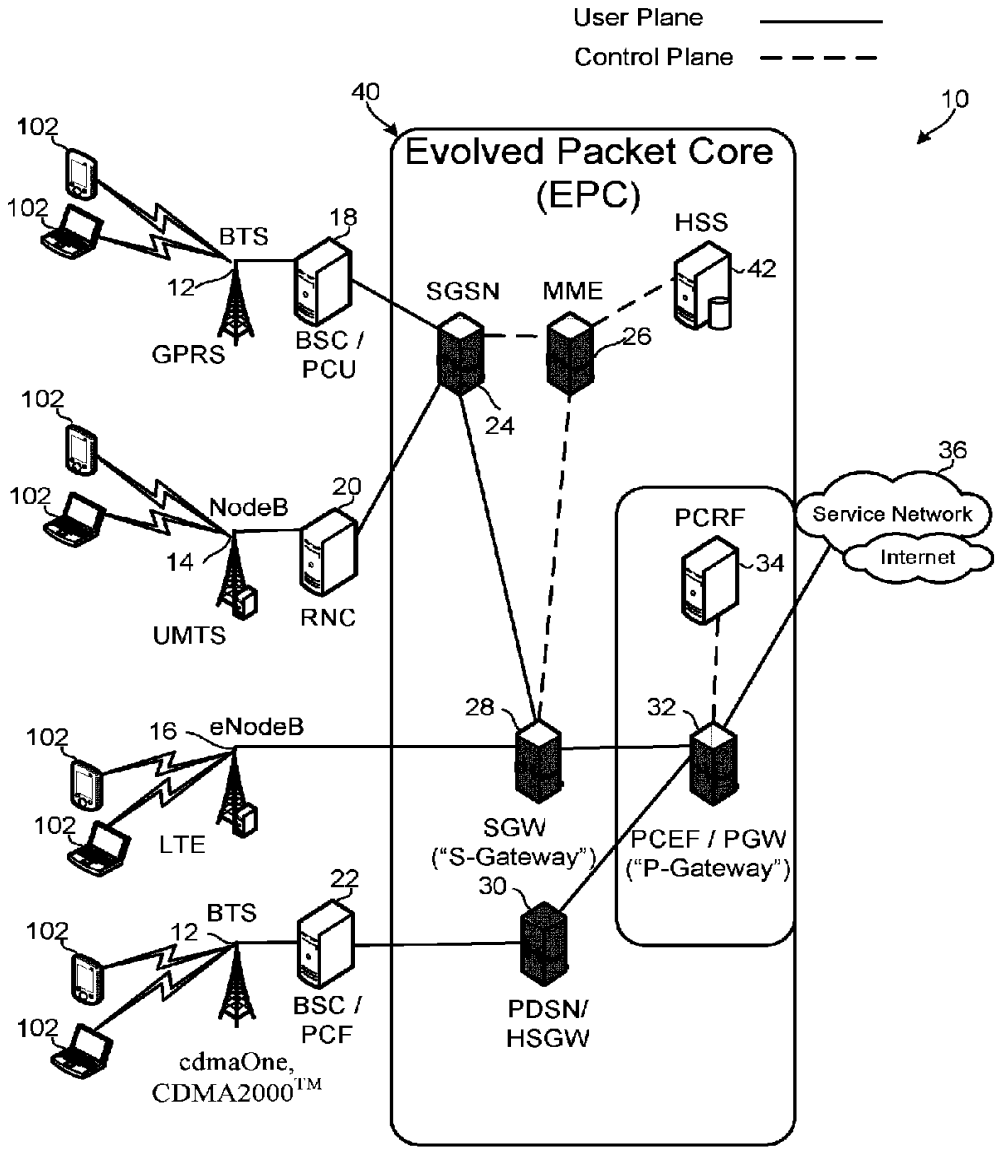

User Plane
Control Plane
40
10
Evolved Packet Core
(EPC)
102
102
BTS
18
12
GPRS
BSC /
PCU
SGSN
MME
HSS
42
26
24
102
102
NodeB
20
14
UMTS
RNC
36
Service Network
Internet
PCRF
34
28
32
102
16
eNodeB
102
LTE
SGW
("S-Gateway")
PCEF / PGW
("P-Gateway")
30
22
102
BTS
12
102
BSC /
PCF
cdmaOne,
CDMA2000™
PDSN/
HSGW

FIG. 1

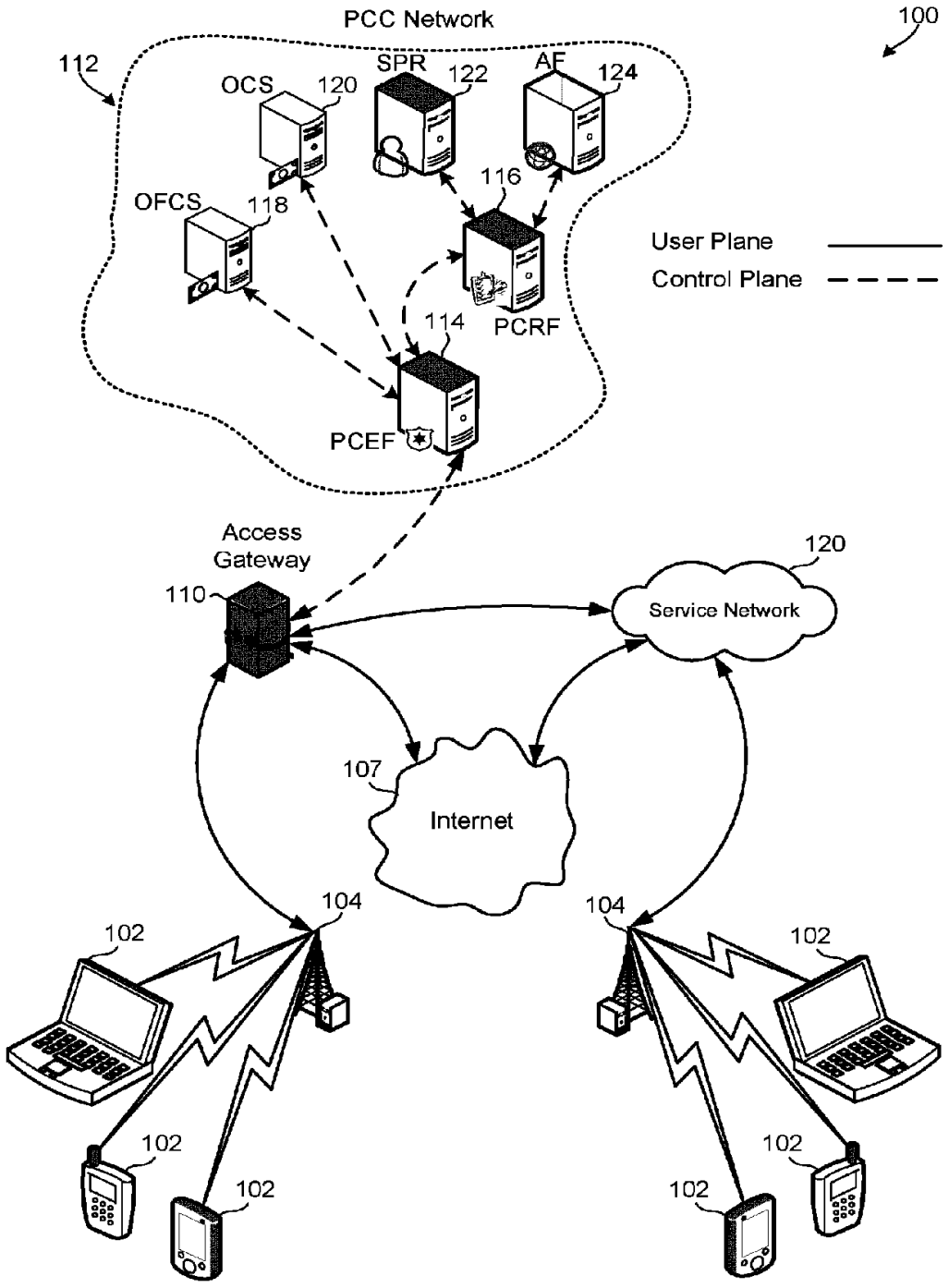

PCC Network
100
112
OCS
120
SPR
122
AF
124
116
OFCS
118
User Plane
Control Plane
114
PCRF
PCEF
Access
Gateway
110
120
Service Network
107
Internet
104
104
102
102
102
102
102
102

FIG. 2

Policy and Charging Control (PCC) Architecture

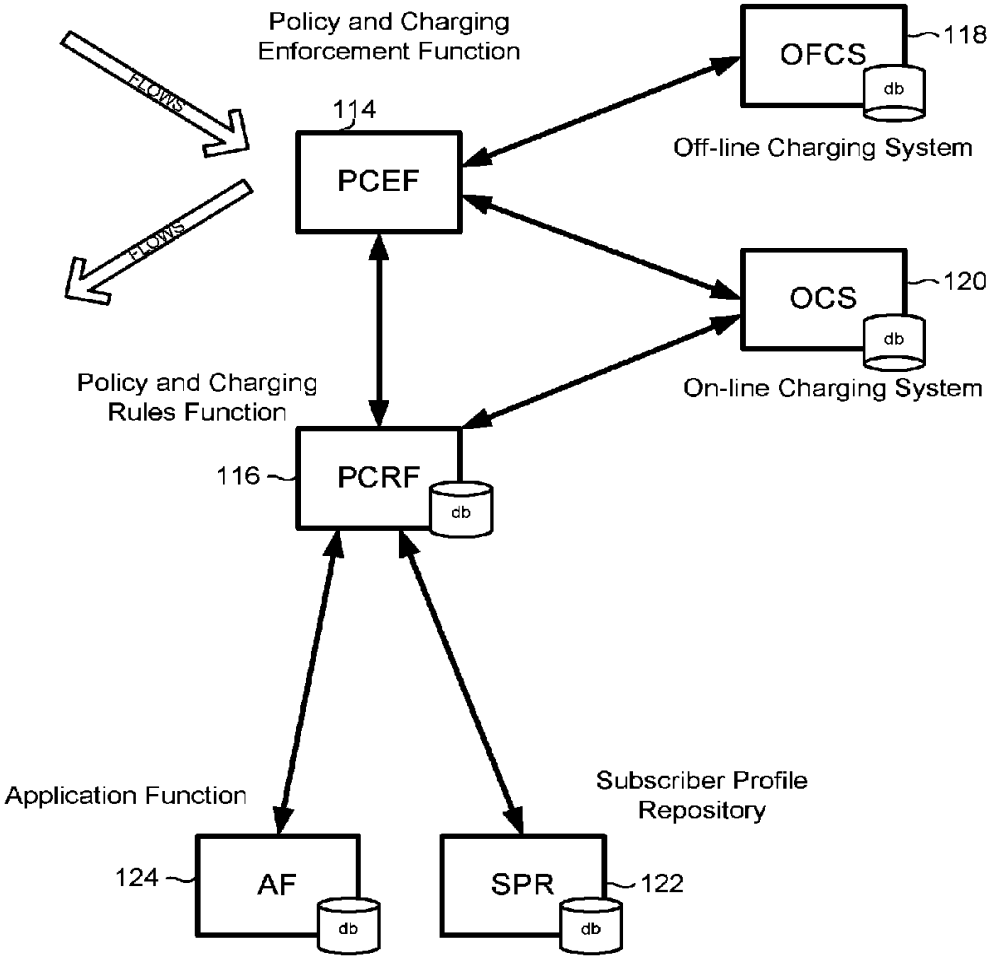


FIG. 3

Communication Interfaces/Protocols

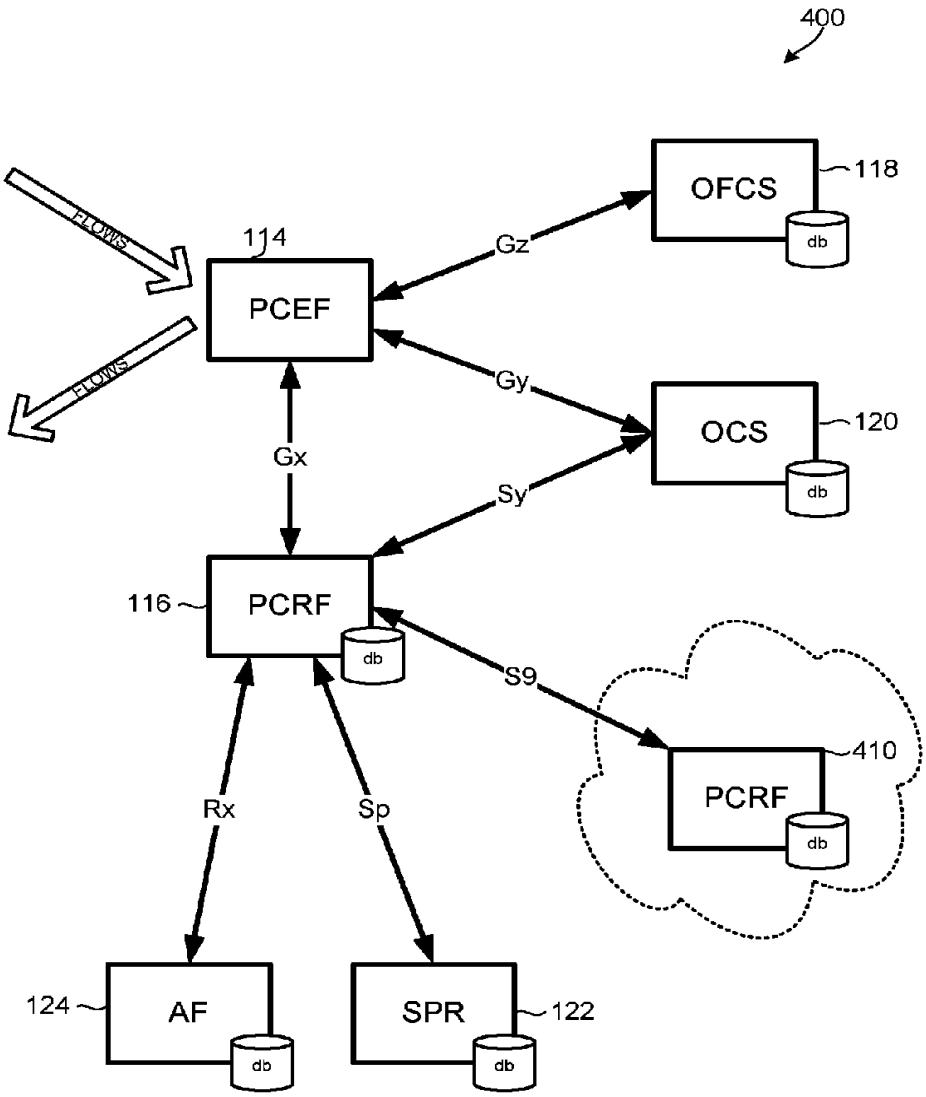


FIG. 4

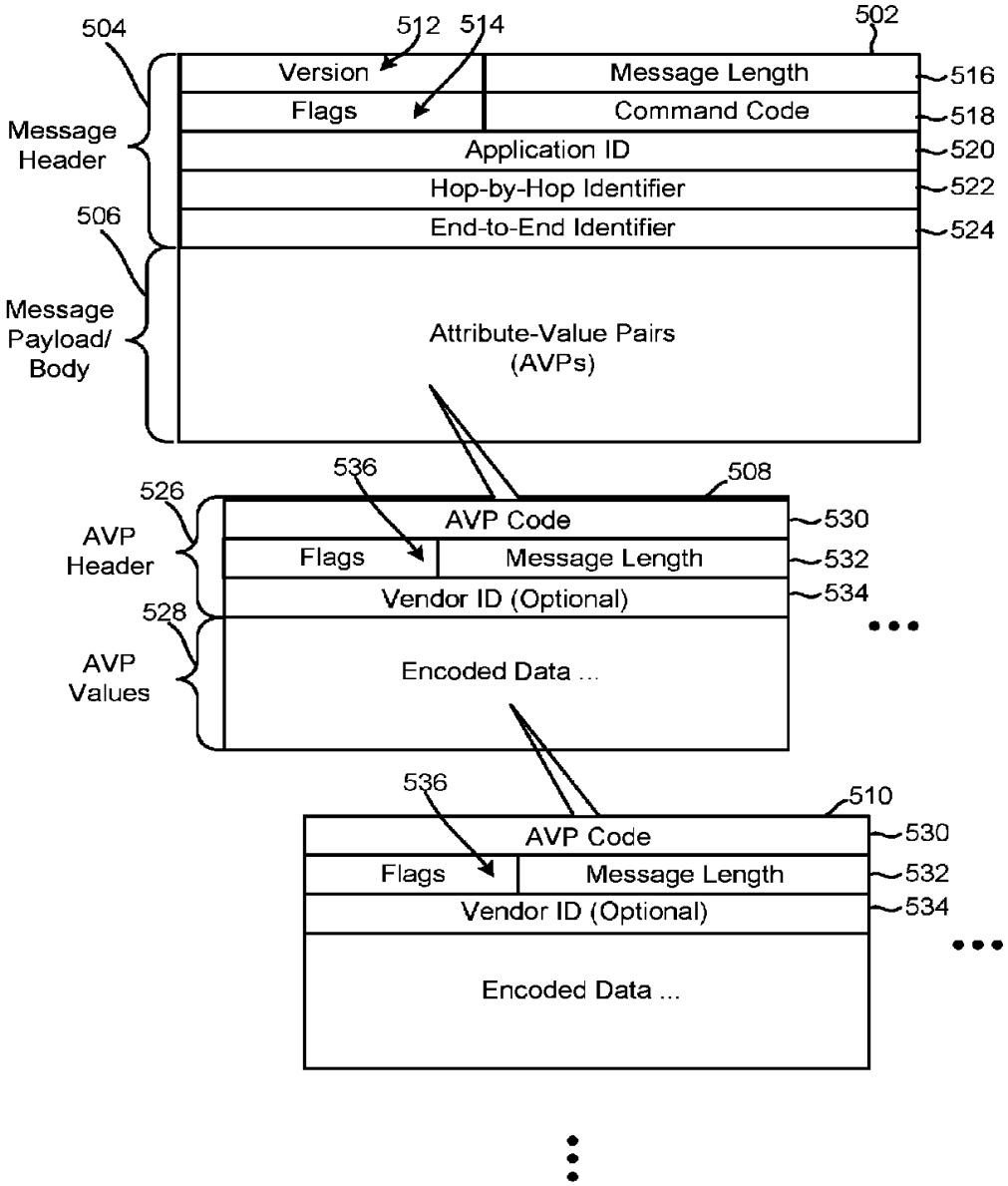

504
512
514
502
Version
Message Length
516
Flags
Command Code
518
Message Header
Application ID
520
Hop-by-Hop Identifier
522
506
End-to-End Identifier
524
Message Payload/ Body
Attribute-Value Pairs (AVPs)
536
508
526
AVP Code
530
AVP Header
Flags
Message Length
532
Vendor ID (Optional)
534
528
AVP Values
Encoded Data ...
536
510
AVP Code
530
Flags
Message Length
532
Vendor ID (Optional)
534
Encoded Data ...

FIG. 5

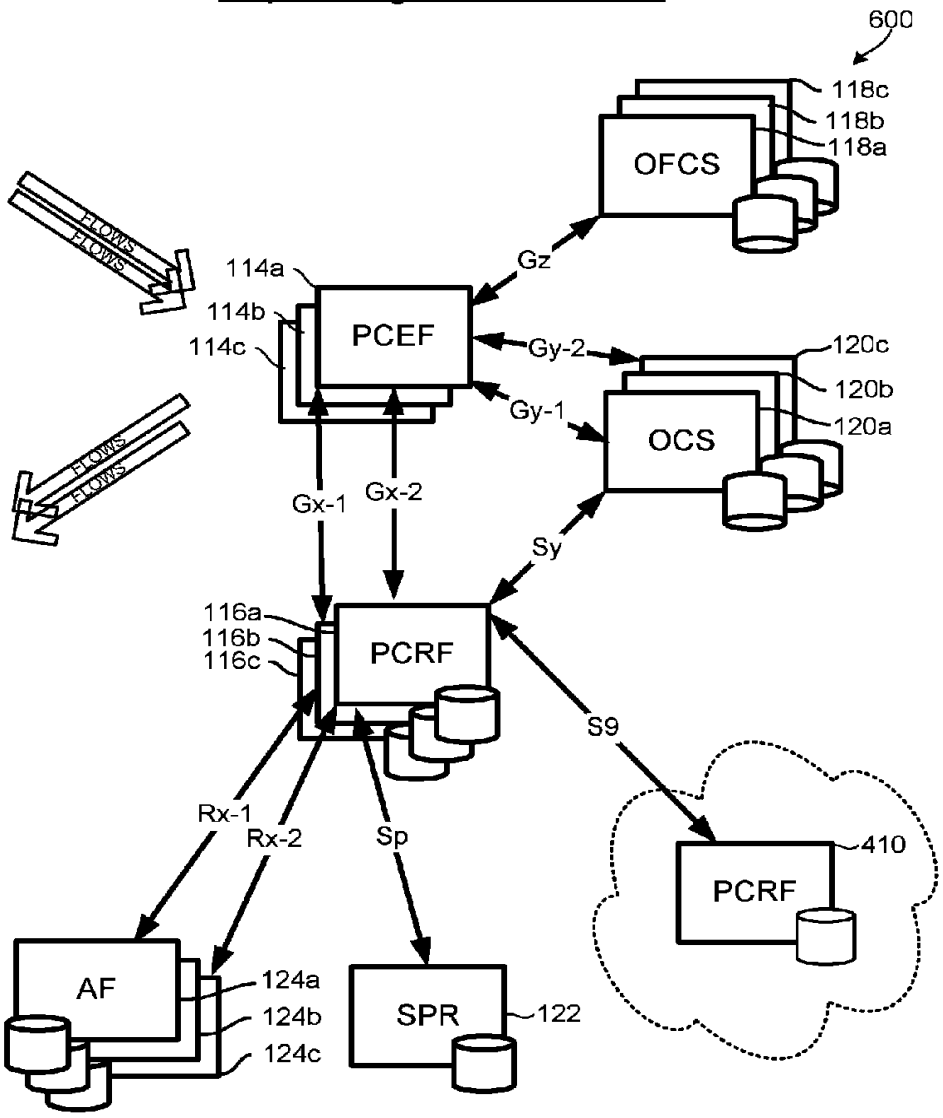

Expanding PCC Network
600
118c
118b
118a
OFCS
Gz
114a
114b
114c
PCEF
Gy-2
120c
120b
120a
Gy-1
OCS
FLOWS
FLOWS
FLOWS
FLOWS
Gx-1
Gx-2
Sy
116a
116b
116c
PCRF
S9
Rx-1
Rx-2
Sp
410
PCRF
AF
124a
124b
124c
SPR
122

FIG. 6

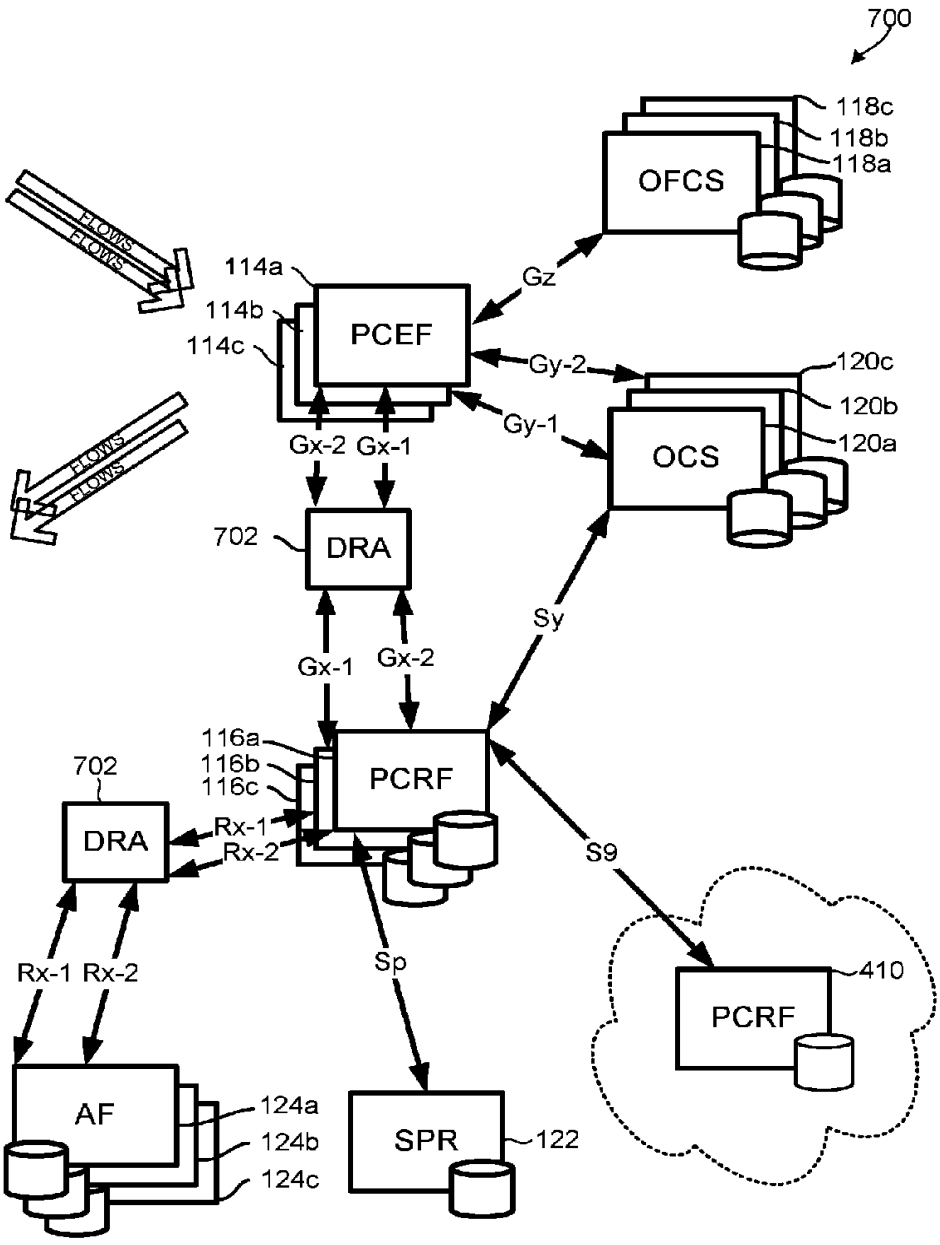

PCC Architecture -- DRA
700
118c
118b
118a
OFCS
FLOWS
FLOWS
114a
114b
114c
PCEF
Gz
Gy-2
Gy-1
120c
120b
120a
OCS
Gx-2
Gx-1
FLOWS
FLOWS
702
DRA
Sy
Gx-1
Gx-2
116a
116b
116c
PCRF
702
DRA
Rx-1
Rx-2
S9
Rx-1
Rx-2
Sp
410
PCRF
AF
124a
124b
124c
SPR
122

FIG. 7A

PCC Architecture -- DCR

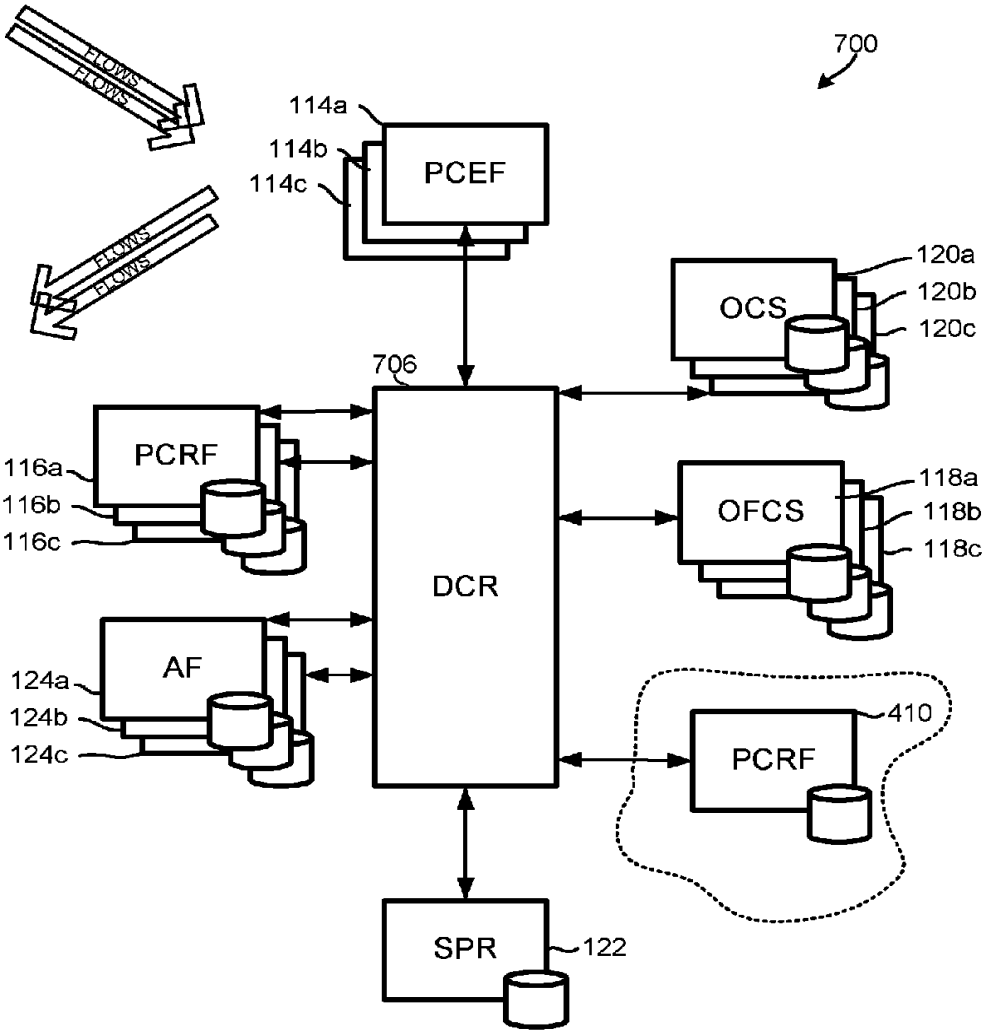


FIG. 7B

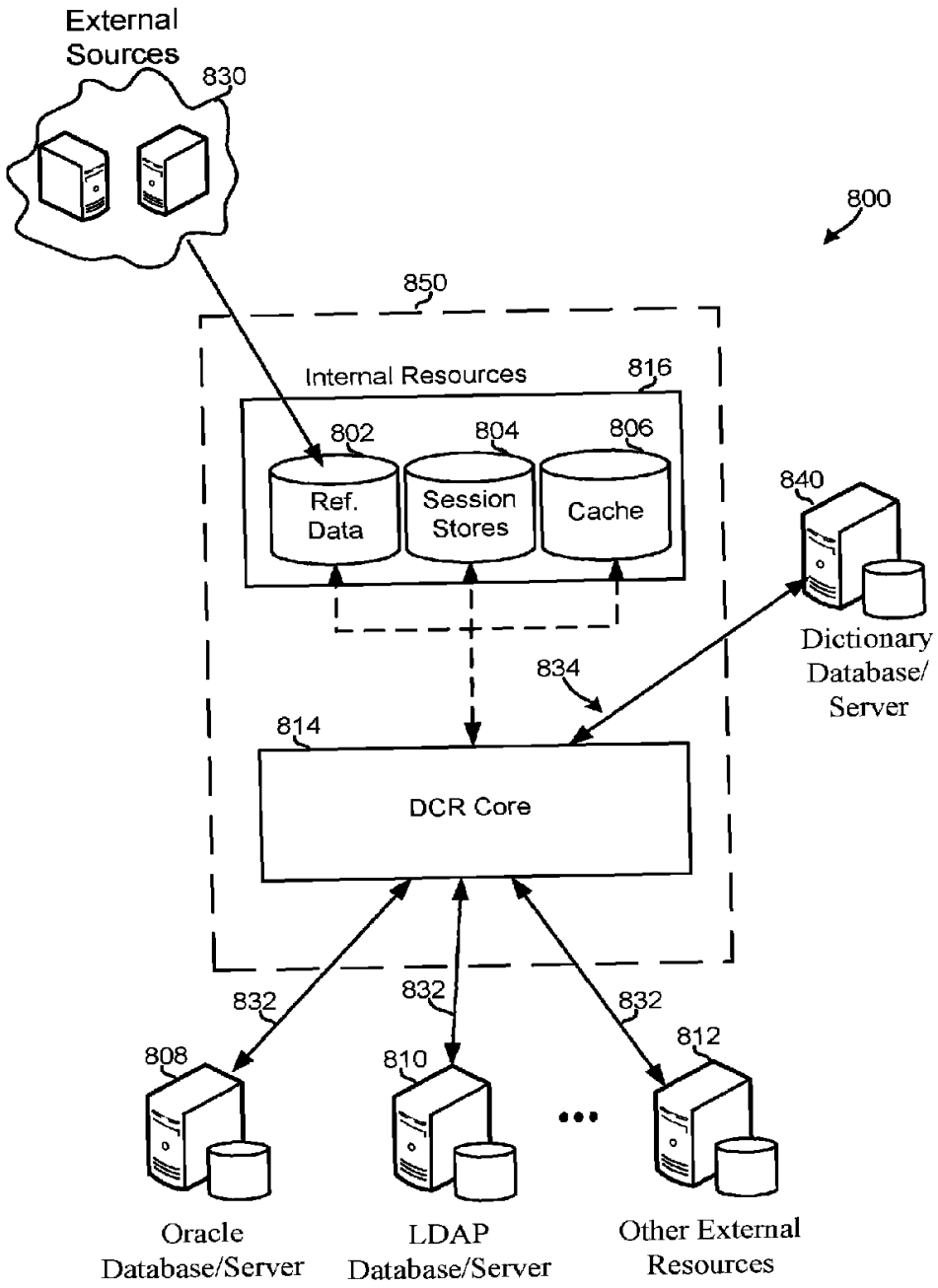

External Sources
830
800
850
Internal Resources
816
802
804
806
Ref. Data
Session Stores
Cache
840
Dictionary Database/ Server
834
814
DCR Core
832
832
832
808
810
812
Oracle Database/Server
LDAP Database/Server
Other External Resources

FIG. 8

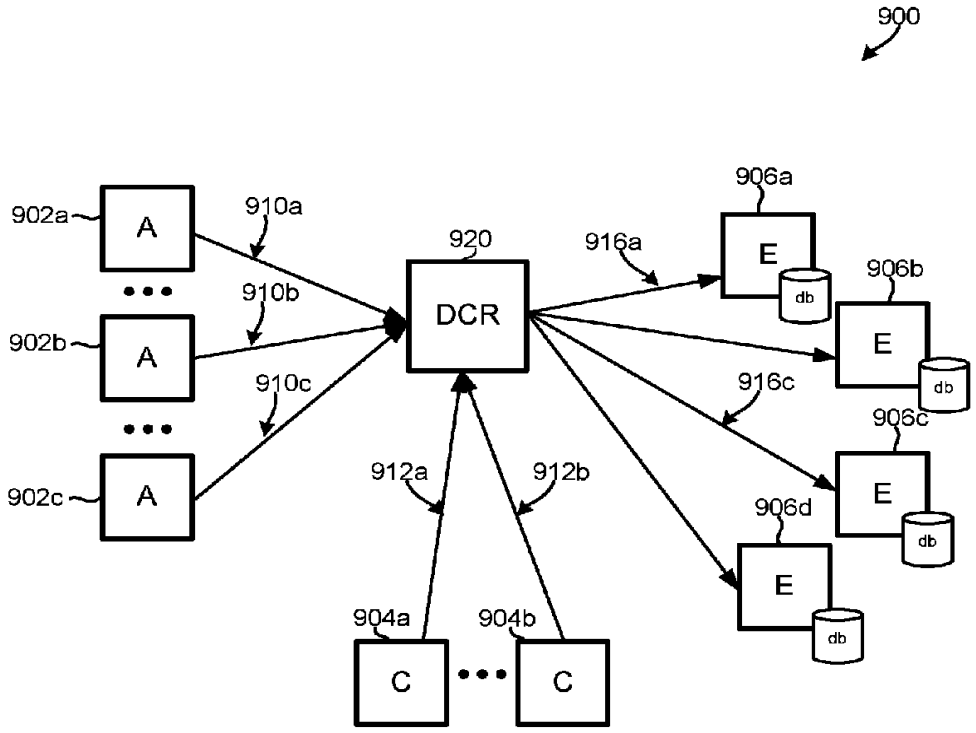

900
902a
A
910a
920
916a
906a
E
db
906b
910b
DCR
902b
A
E
db
916c
910c
906c
912a
912b
E
db
902c
A
906d
E
db
904a
904b
C
C

FIG. 9

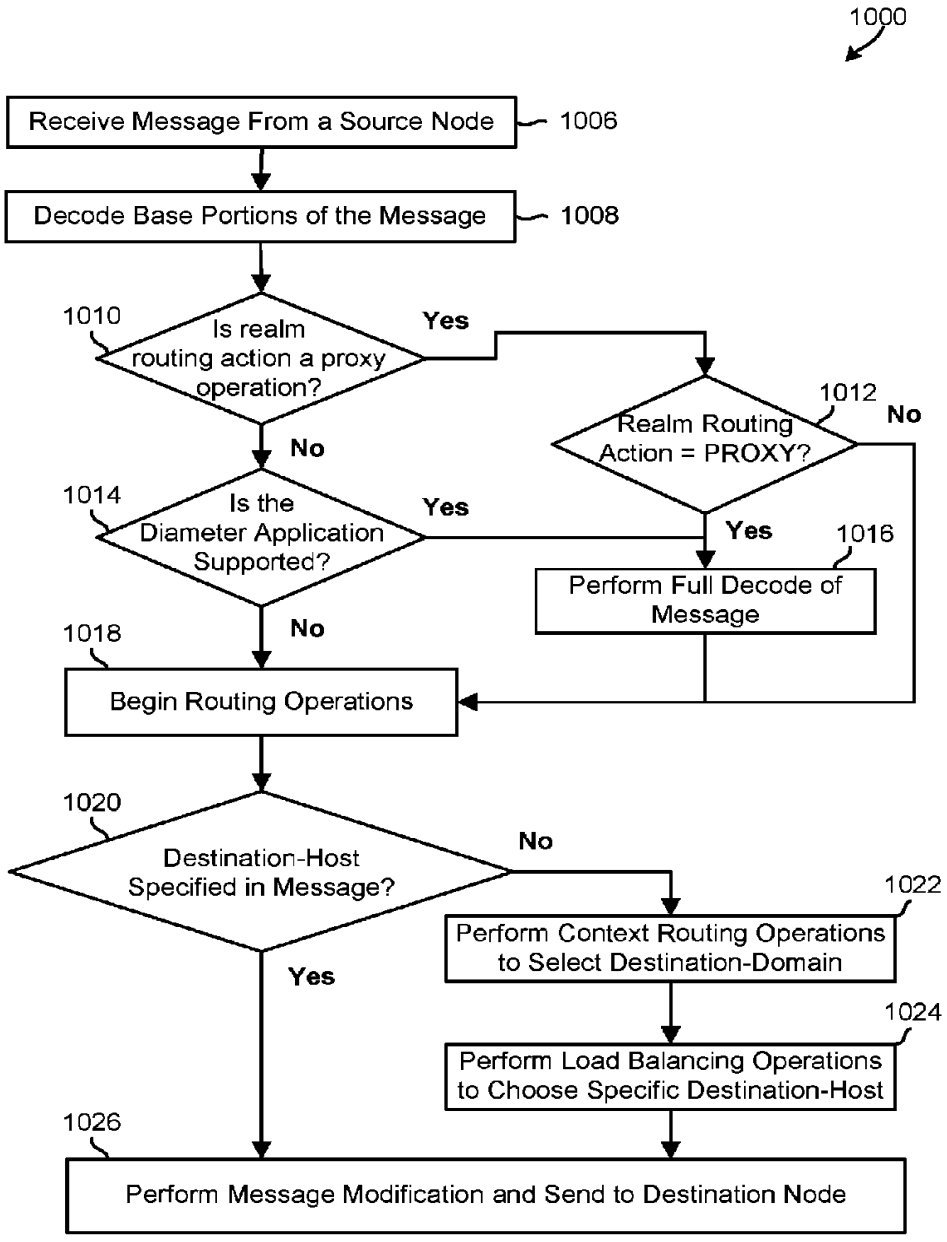

1000
Receive Message From a Source Node
1006
Decode Base Portions of the Message
1008
1010
Is realm routing action a proxy operation?
Yes
No
1012
Realm Routing Action = PROXY?
No
Yes
1014
Is the Diameter Application Supported?
Yes
No
1016
Perform Full Decode of Message
1018
Begin Routing Operations
1020
Destination-Host Specified in Message?
No
Yes
1022
Perform Context Routing Operations to Select Destination-Domain
1024
Perform Load Balancing Operations to Choose Specific Destination-Host
1026
Perform Message Modification and Send to Destination Node

FIG. 10A

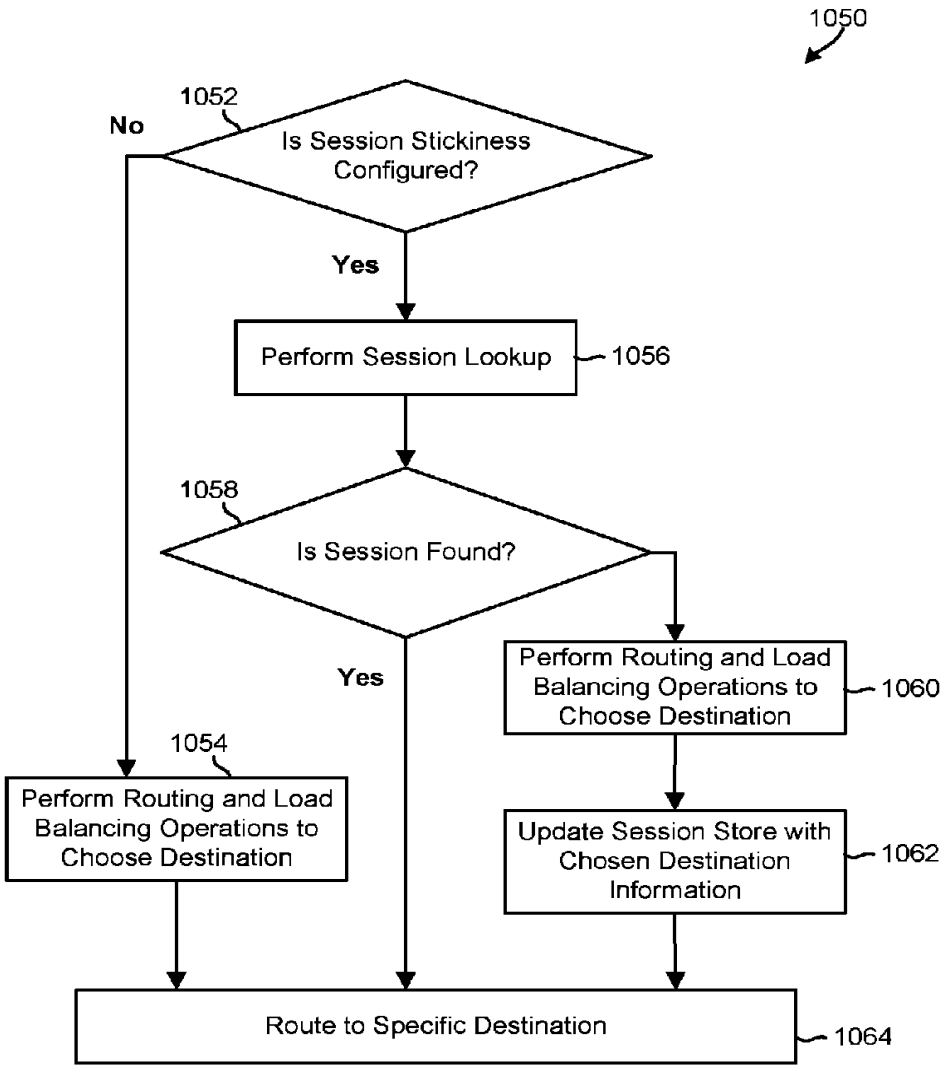

1050
1052
No
Is Session Stickiness Configured?
Yes
Perform Session Lookup
1056
1058
Is Session Found?
Yes
Perform Routing and Load Balancing Operations to Choose Destination
1060
1054
Perform Routing and Load Balancing Operations to Choose Destination
Update Session Store with Chosen Destination Information
1062
Route to Specific Destination
1064

FIG. 10B

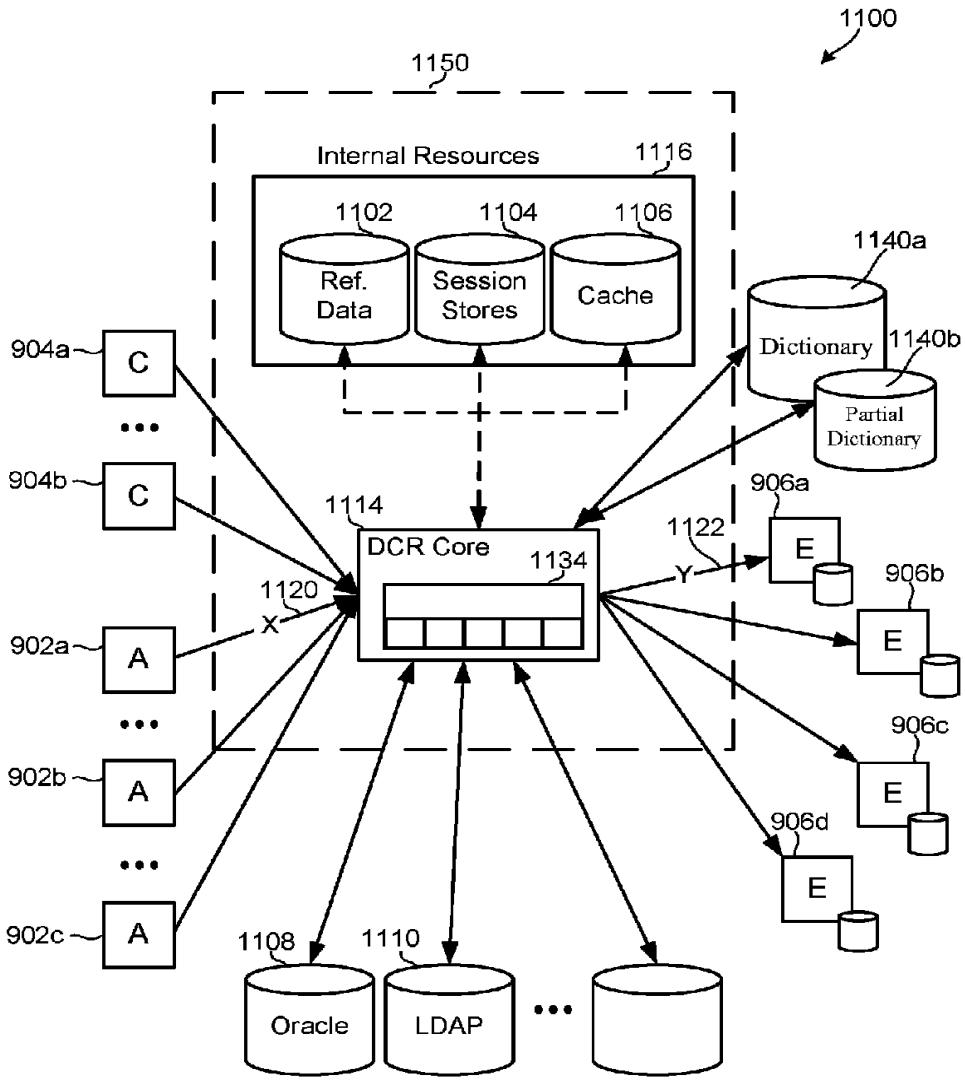

1100
1150
Internal Resources
1116
1102
1104
1106
Ref. Data
Session Stores
Cache
1140a
Dictionary
1140b
Partial Dictionary
904a
C
904b
C
1114
DCR Core
1134
1120
X
1122
Y
906a
E
906b
E
906c
E
906d
E
902a
A
902b
A
902c
A
1108
1110
Oracle
LDAP

FIG. 11

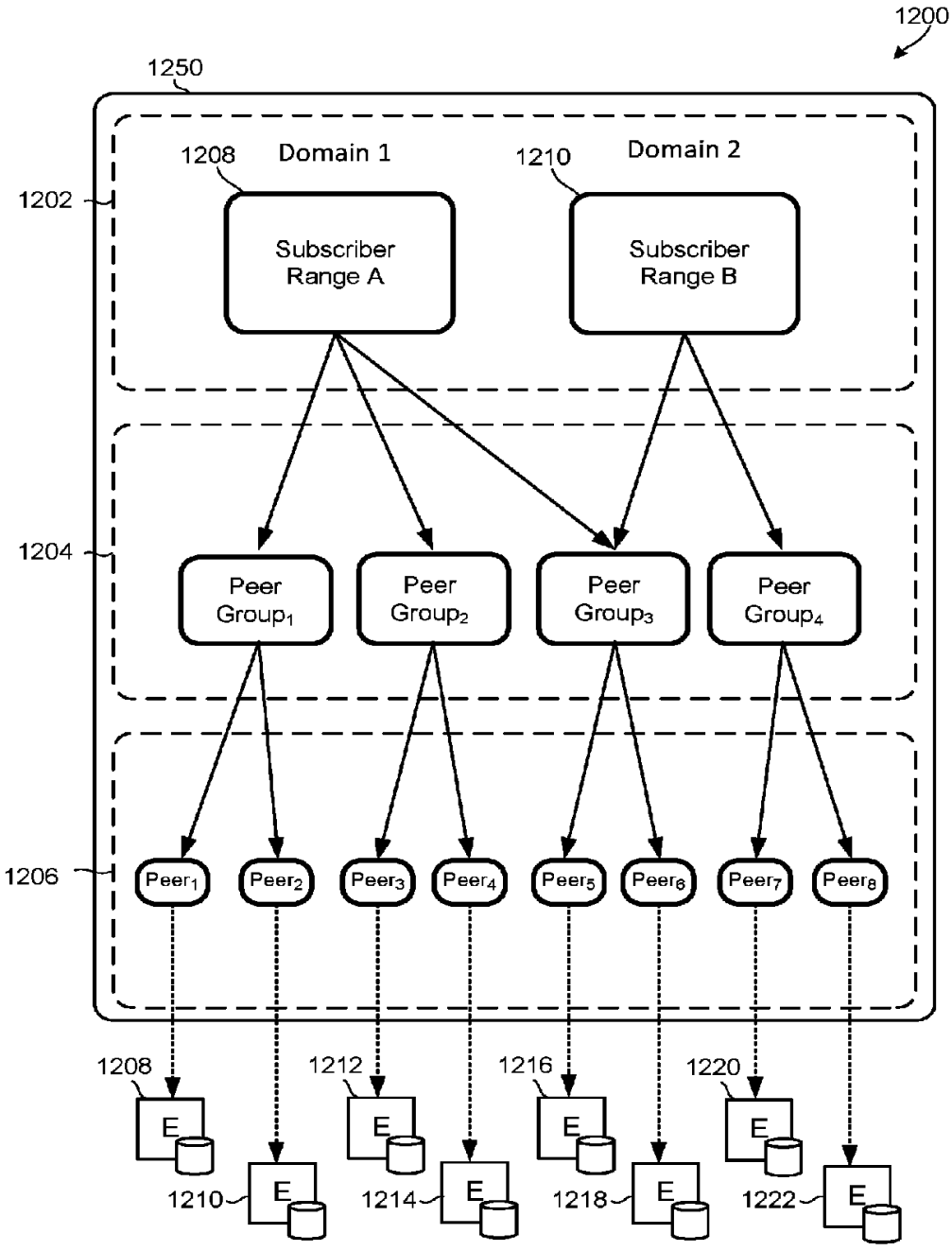

1200
1250
1208
Domain 1
1210
Domain 2
1202
Subscriber Range A
Subscriber Range B
1204
Peer Group1
Peer Group2
Peer Group3
Peer Group4
1206
Peer1
Peer2
Peer3
Peer4
Peer5
Peer6
Peer7
Peer8
1208
1212
1216
1220
E
1210
1214
1218
1222

FIG. 12

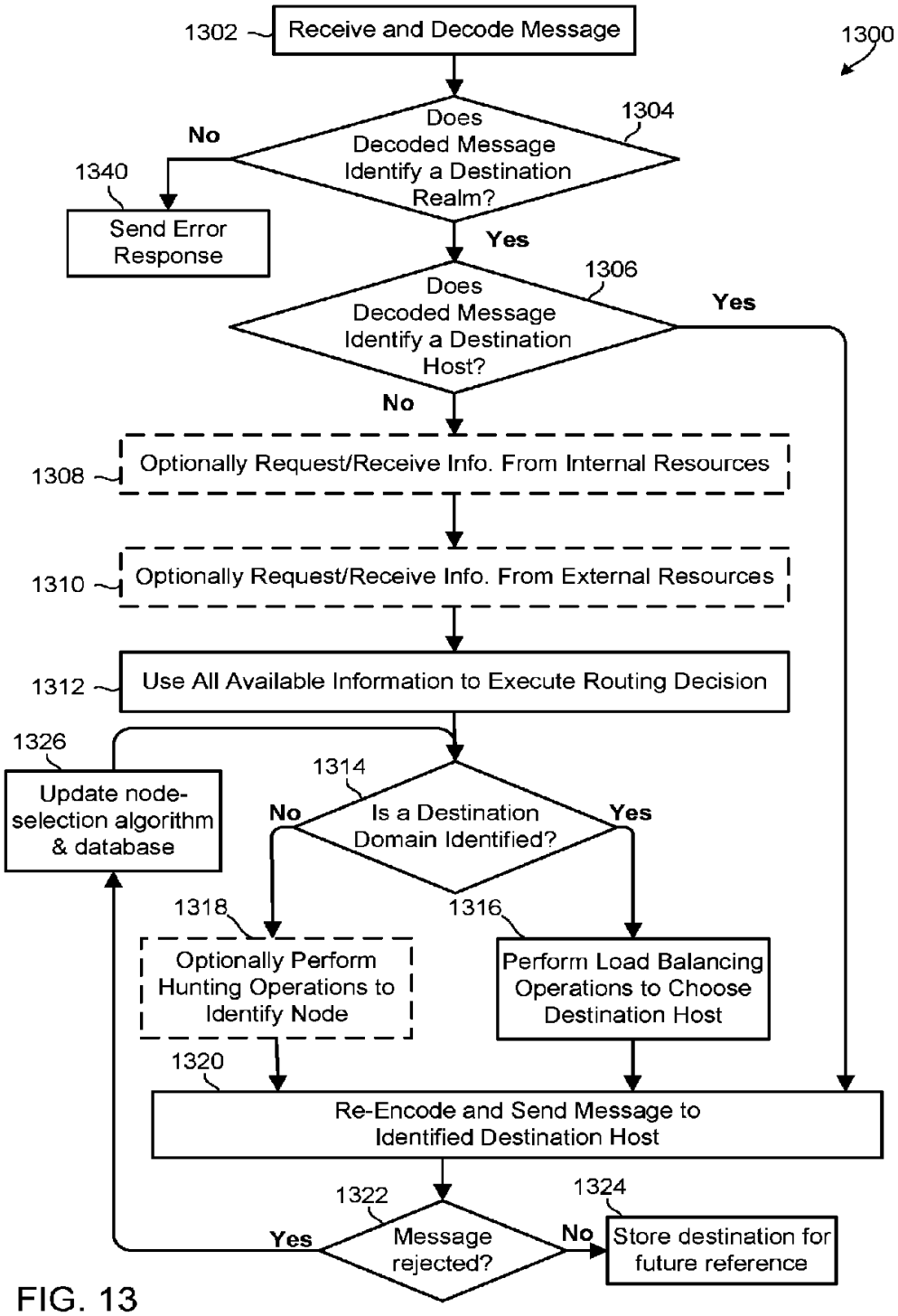

1300
1302
Receive and Decode Message
1304
Does Decoded Message Identify a Destination Realm?
No
1340
Send Error Response
Yes
1306
Does Decoded Message Identify a Destination Host?
Yes
No
1308
Optionally Request/Receive Info. From Internal Resources
1310
Optionally Request/Receive Info. From External Resources
1312
Use All Available Information to Execute Routing Decision
1326
Update node-selection algorithm & database
1314
Is a Destination Domain Identified?
No
Yes
1318
Optionally Perform Hunting Operations to Identify Node
1316
Perform Load Balancing Operations to Choose Destination Host
1320
Re-Encode and Send Message to Identified Destination Host
1322
Message rejected?
Yes
No
1324
Store destination for future reference

FIG. 13

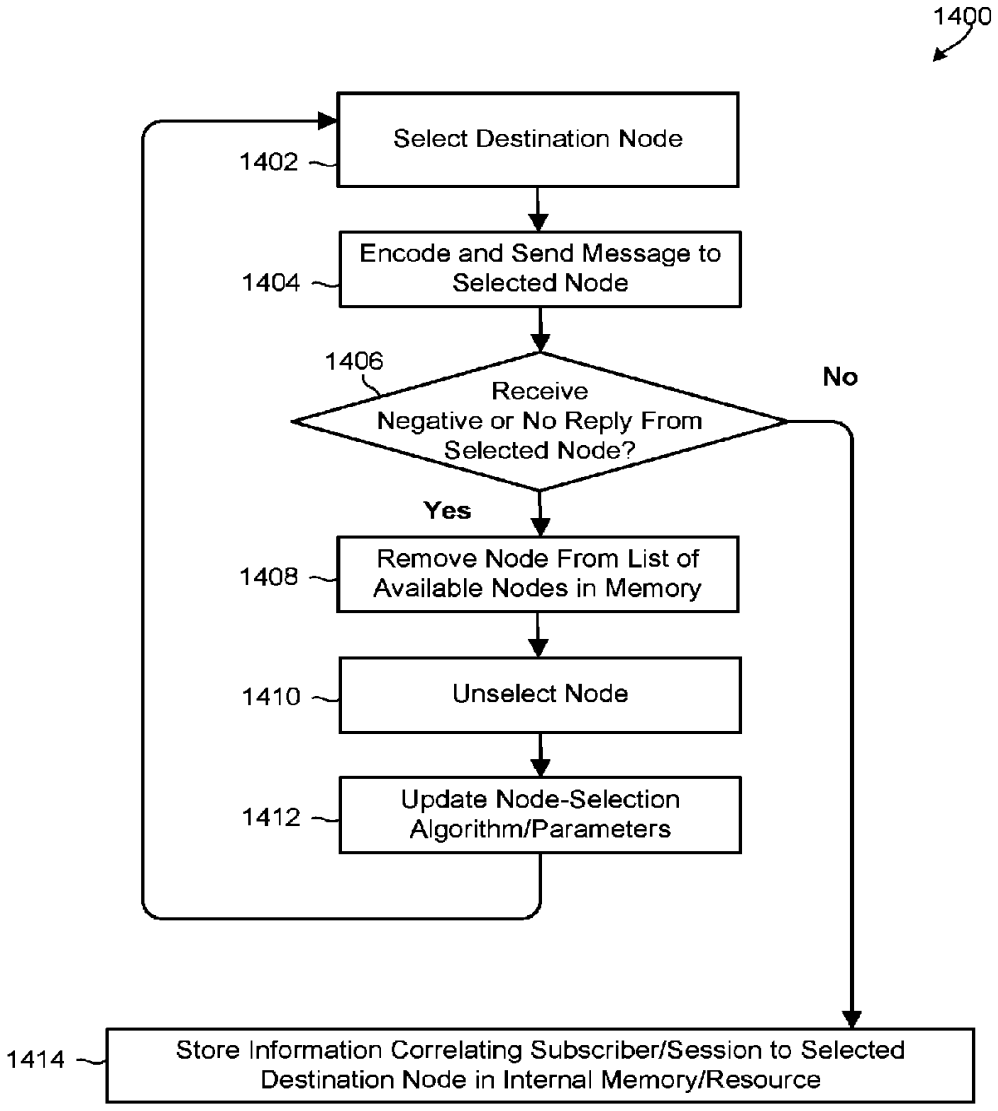

1400
Select Destination Node
1402
Encode and Send Message to Selected Node
1404
1406
Receive Negative or No Reply From Selected Node?
No
Yes
Remove Node From List of Available Nodes in Memory
1408
Unselect Node
1410
Update Node-Selection Algorithm/Parameters
1412
Store Information Correlating Subscriber/Session to Selected Destination Node in Internal Memory/Resource
1414

FIG. 14

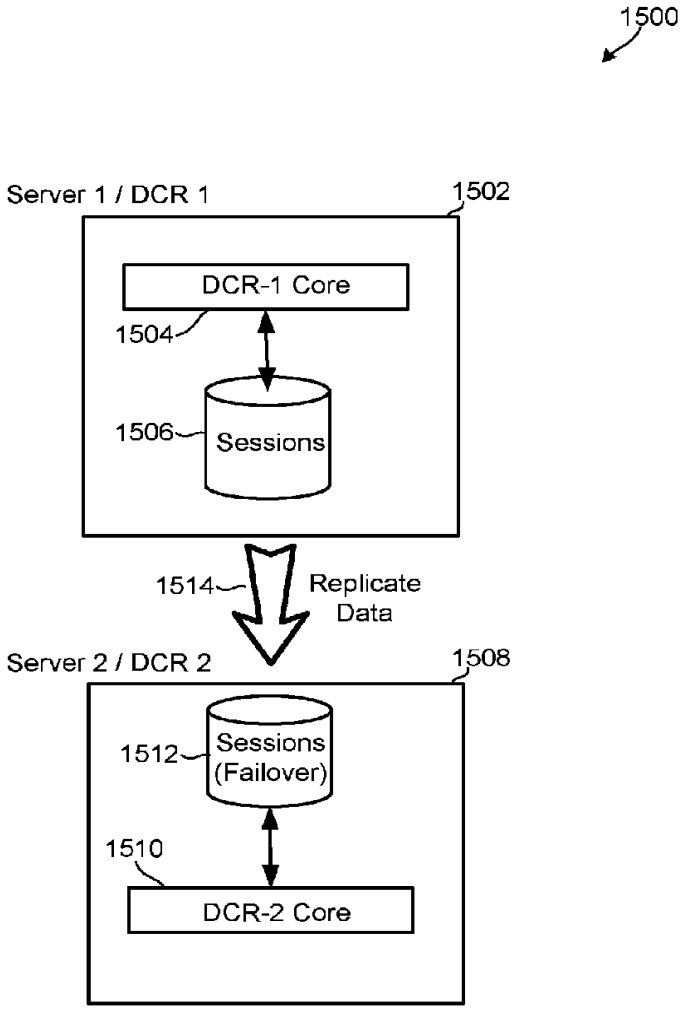

1500
Server 1 / DCR 1
1502
DCR-1 Core
1504
1506
Sessions
1514
Replicate
Data
Server 2 / DCR 2
1508
1512
Sessions
(Failover)
1510
DCR-2 Core

FIG. 15A

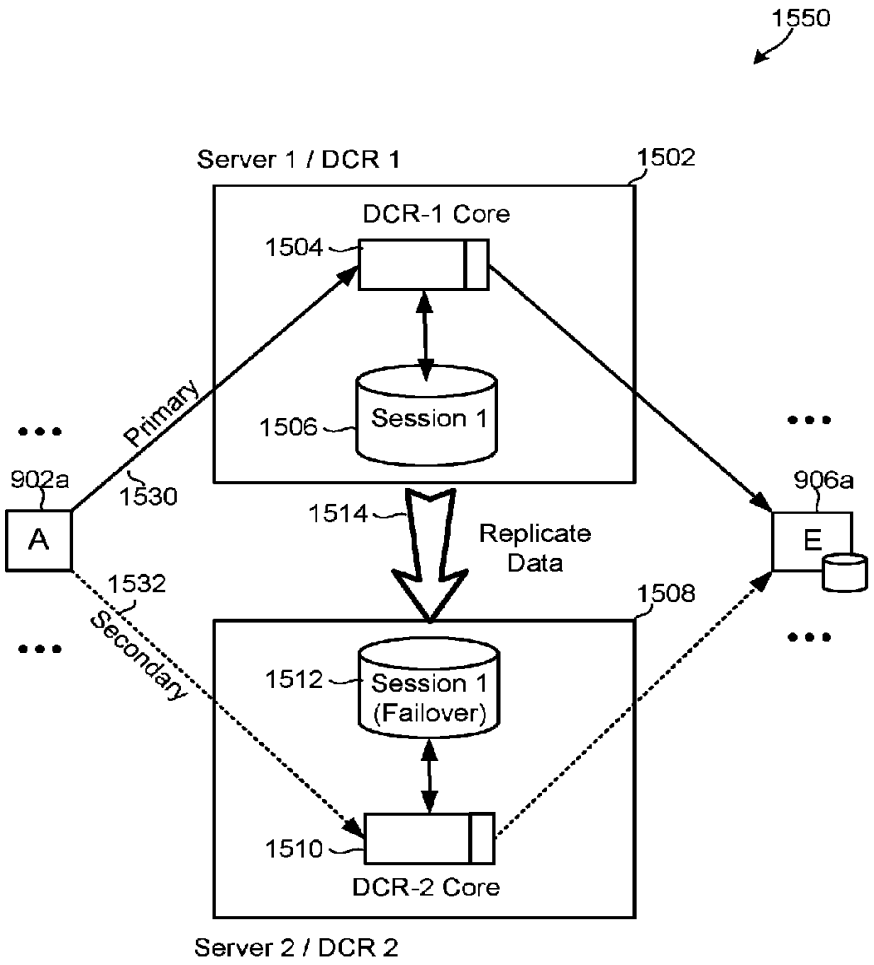

1550
Server 1 / DCR 1
1502
DCR-1 Core
1504
1506
Session 1
Primary
902a
1530
A
1514
Replicate
Data
906a
E
1532
Secondary
1508
1512
Session 1
(Failover)
1510
DCR-2 Core
Server 2 / DCR 2

FIG. 15B

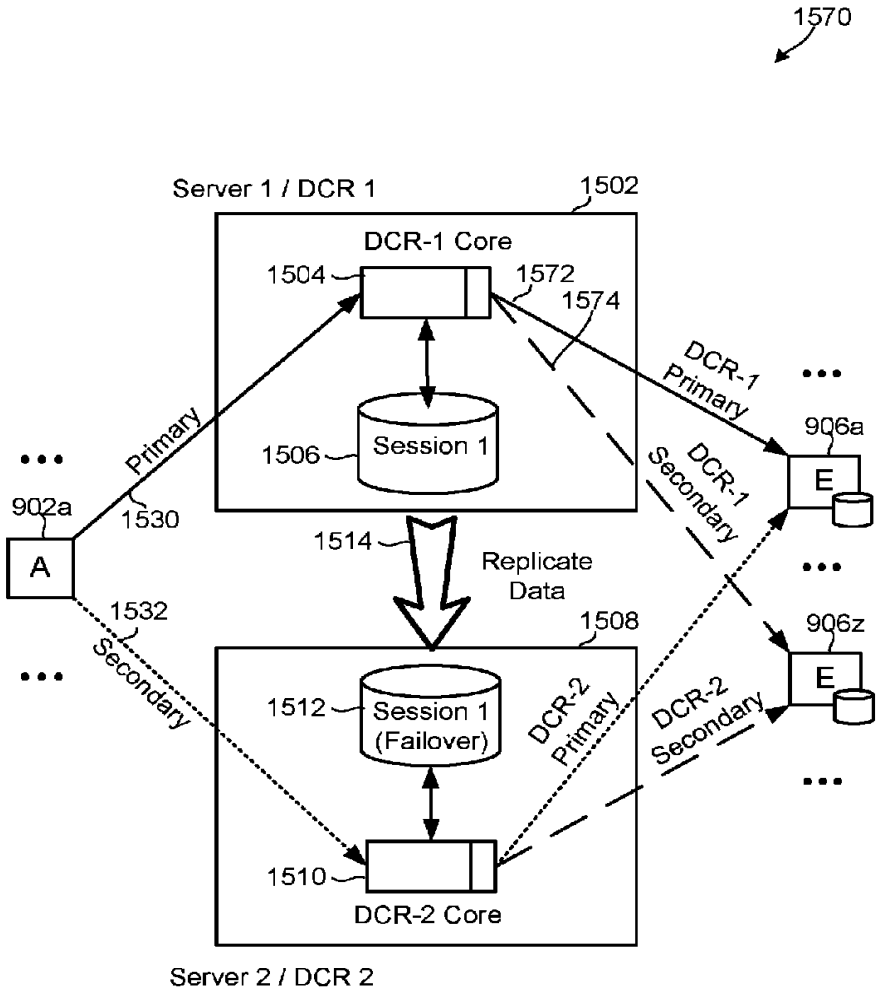

1570
Server 1 / DCR 1
1502
DCR-1 Core
1504
1572
1574
1506
Session 1
DCR-1
Primary
906a
E
Primary
902a
1530
A
1514
Replicate
Data
DCR-1
Secondary
1532
Secondary
1508
906z
E
1512
Session 1
(Failover)
DCR-2
Primary
DCR-2
Secondary
1510
DCR-2 Core
Server 2 / DCR 2

FIG. 15C

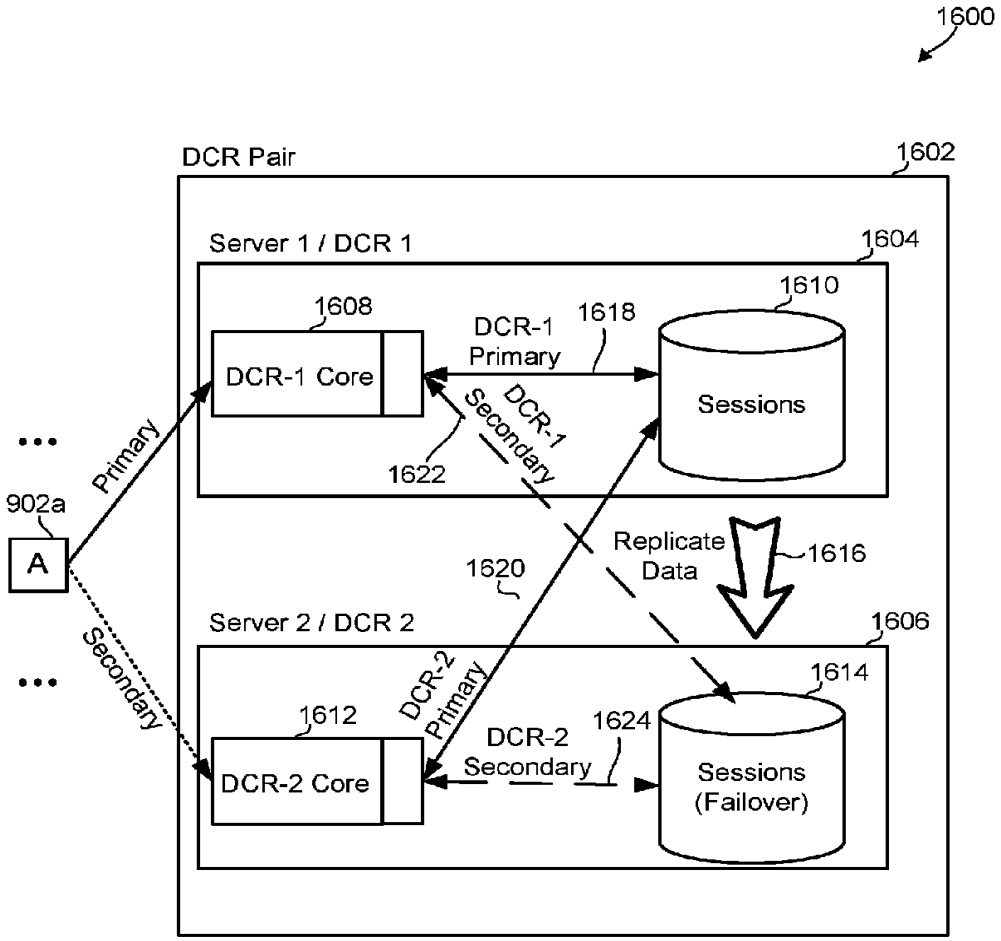

1600
DCR Pair
1602
Server 1 / DCR 1
1604
1608
DCR-1 Core
DCR-1
Primary
1618
1610
Sessions
DCR-1
Secondary
1622
902a
A
Primary
Secondary
1620
Replicate
Data
1616
Server 2 / DCR 2
1606
1614
1612
DCR-2 Core
DCR-2
Primary
DCR-2
Secondary
1624
Sessions
(Failover)

FIG. 16

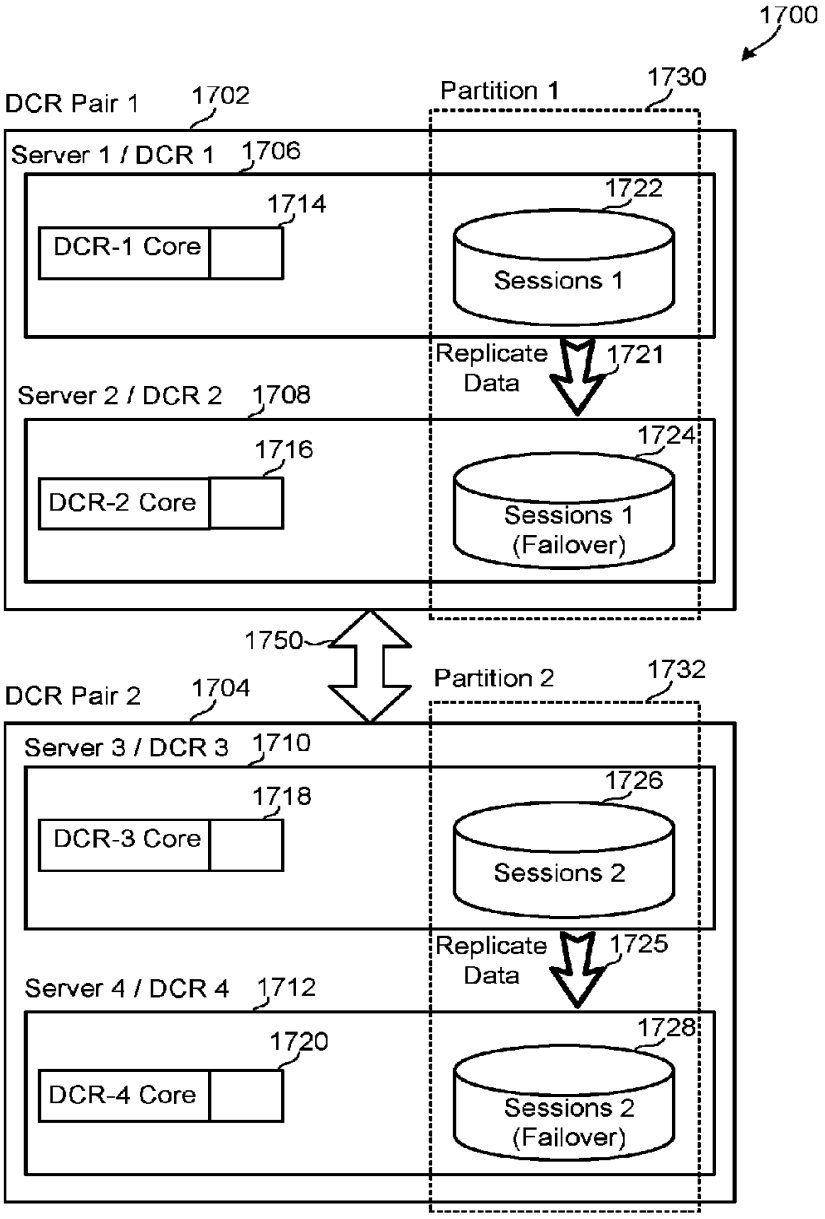

1700
DCR Pair 1
1702
Partition 1
1730
Server 1 / DCR 1
1706
1714
DCR-1 Core
1722
Sessions 1
Replicate Data
1721
Server 2 / DCR 2
1708
1716
DCR-2 Core
1724
Sessions 1 (Failover)
1750
DCR Pair 2
1704
Partition 2
1732
Server 3 / DCR 3
1710
1718
DCR-3 Core
1726
Sessions 2
Replicate Data
1725
Server 4 / DCR 4
1712
1720
DCR-4 Core
1728
Sessions 2 (Failover)

FIG. 17A

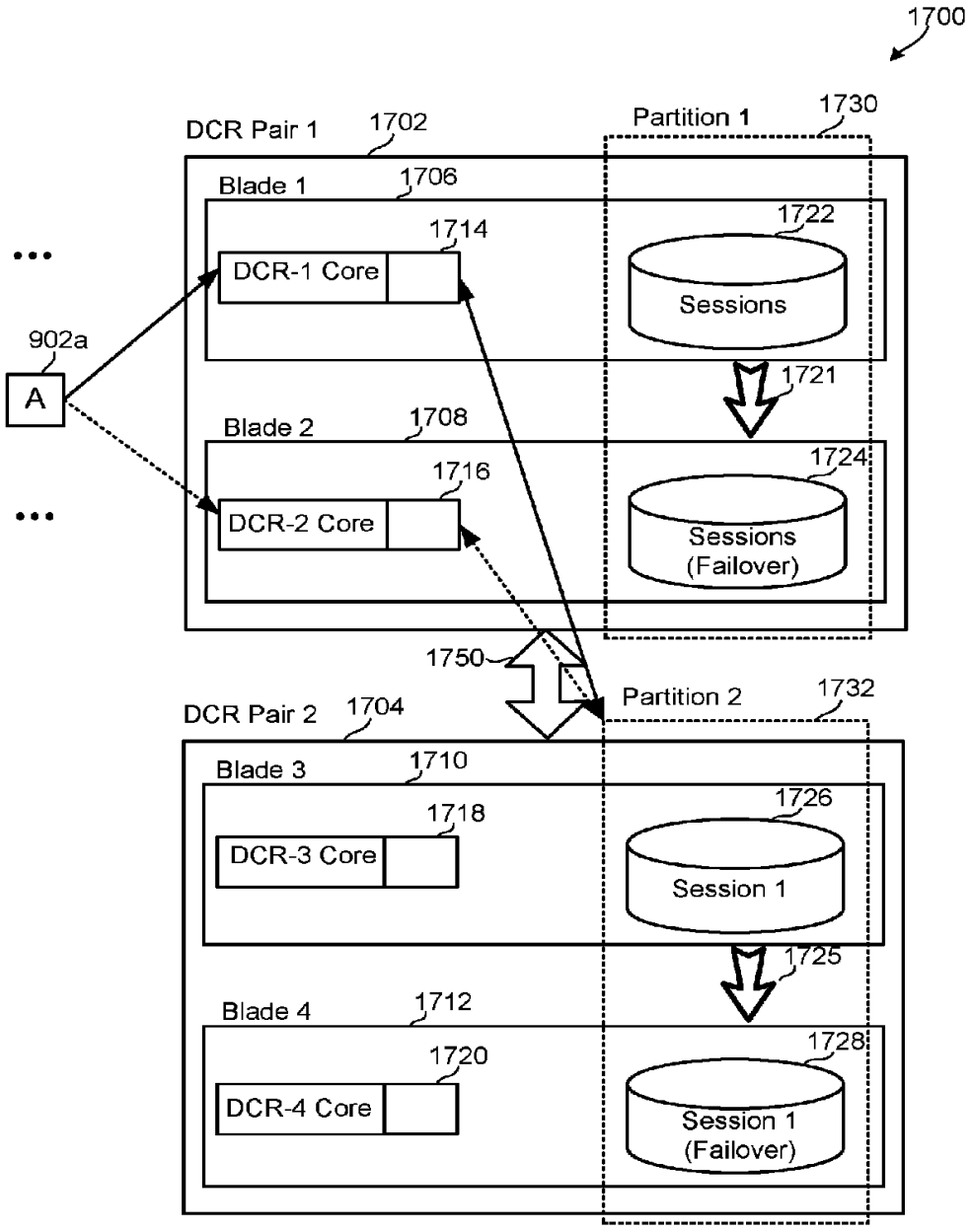

1700
DCR Pair 1
1702
Partition 1
1730
Blade 1
1706
1722
1714
DCR-1 Core
Sessions
902a
A
1721
Blade 2
1708
1724
1716
DCR-2 Core
Sessions
(Failover)
1750
Partition 2
1732
DCR Pair 2
1704
Blade 3
1710
1726
1718
DCR-3 Core
Session 1
1725
Blade 4
1712
1728
1720
DCR-4 Core
Session 1
(Failover)

FIG. 17B

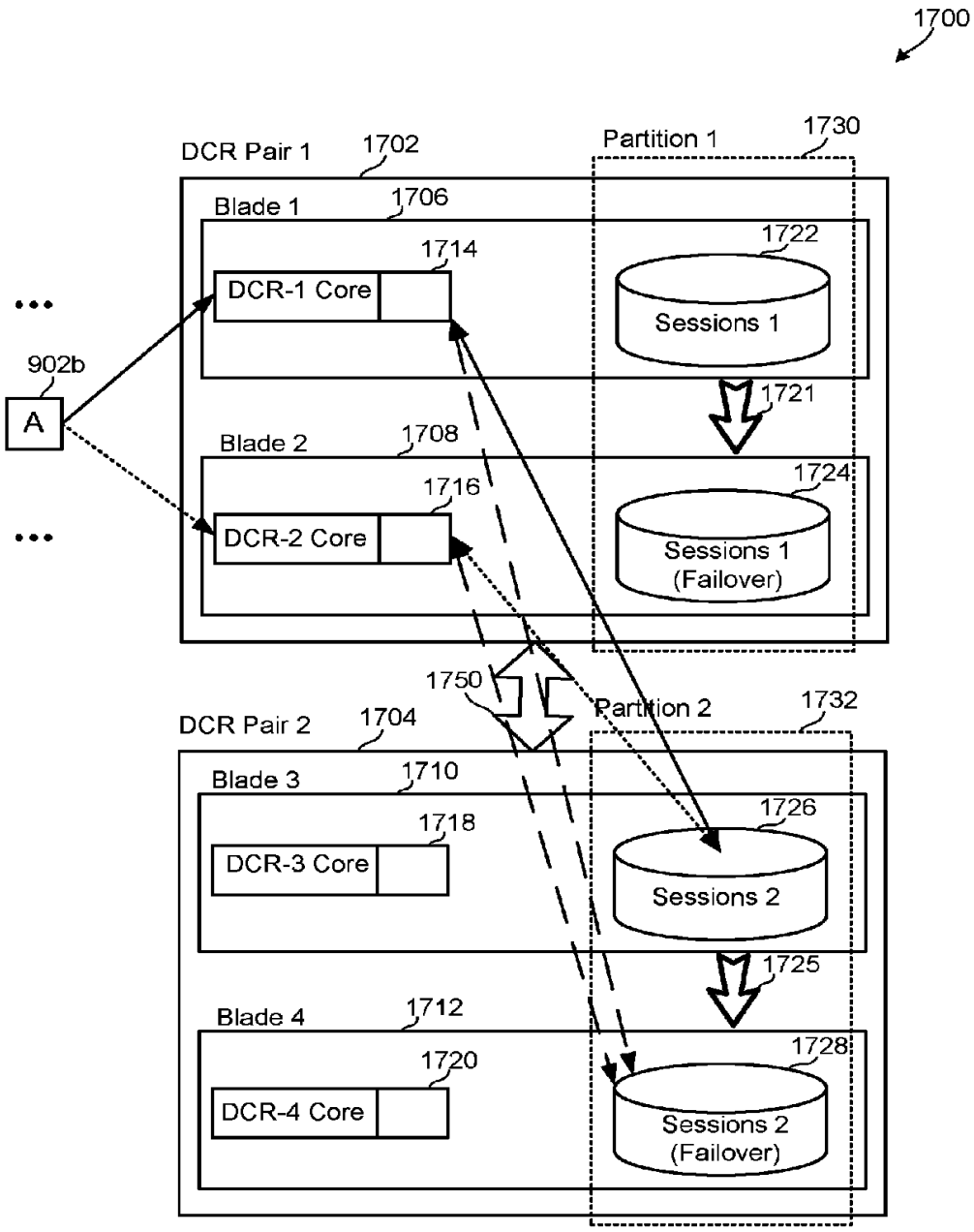

1700
DCR Pair 1
1702
Partition 1
1730
Blade 1
1706
1722
1714
DCR-1 Core
Sessions 1
1721
902b
A
Blade 2
1708
1724
1716
DCR-2 Core
Sessions 1
(Failover)
1750
DCR Pair 2
1704
Partition 2
1732
Blade 3
1710
1726
1718
DCR-3 Core
Sessions 2
1725
Blade 4
1712
1728
1720
DCR-4 Core
Sessions 2
(Failover)

FIG. 17C

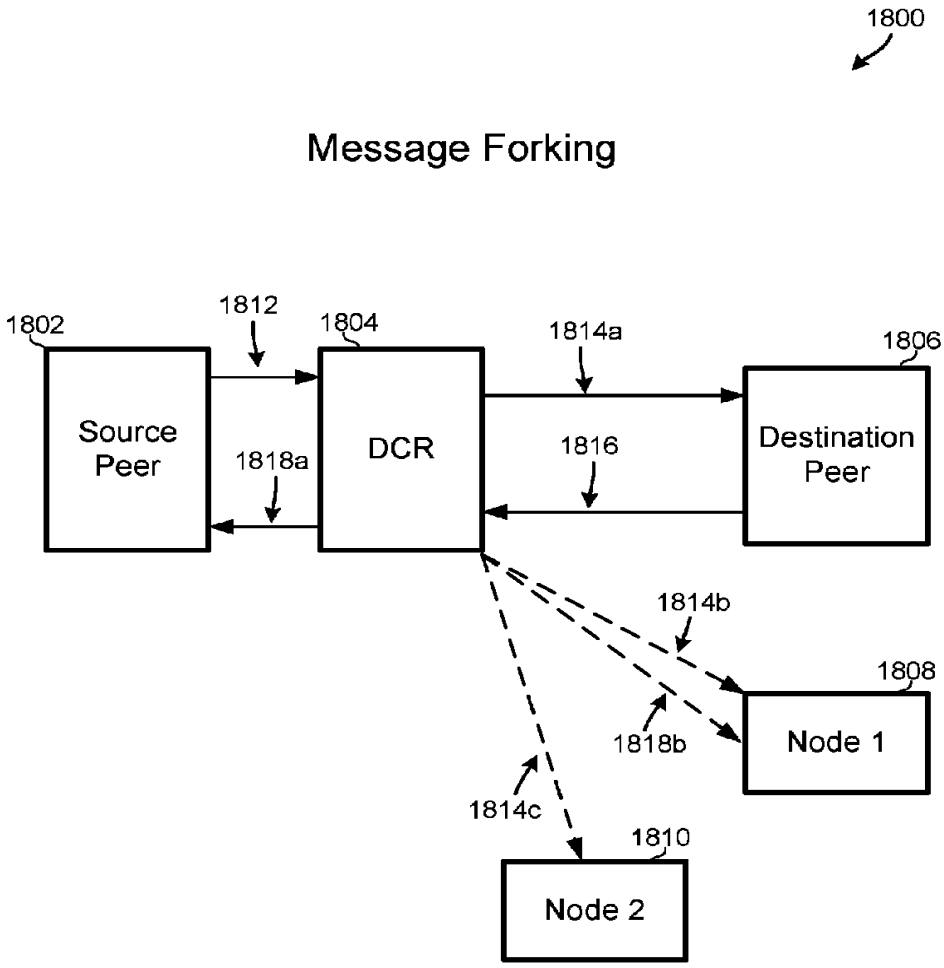

1800
Message Forking
1802
1812
1804
1814a
1806
Source Peer
DCR
Destination Peer
1818a
1816
1814b
1808
Node 1
1818b
1814c
1810
Node 2

FIG. 18

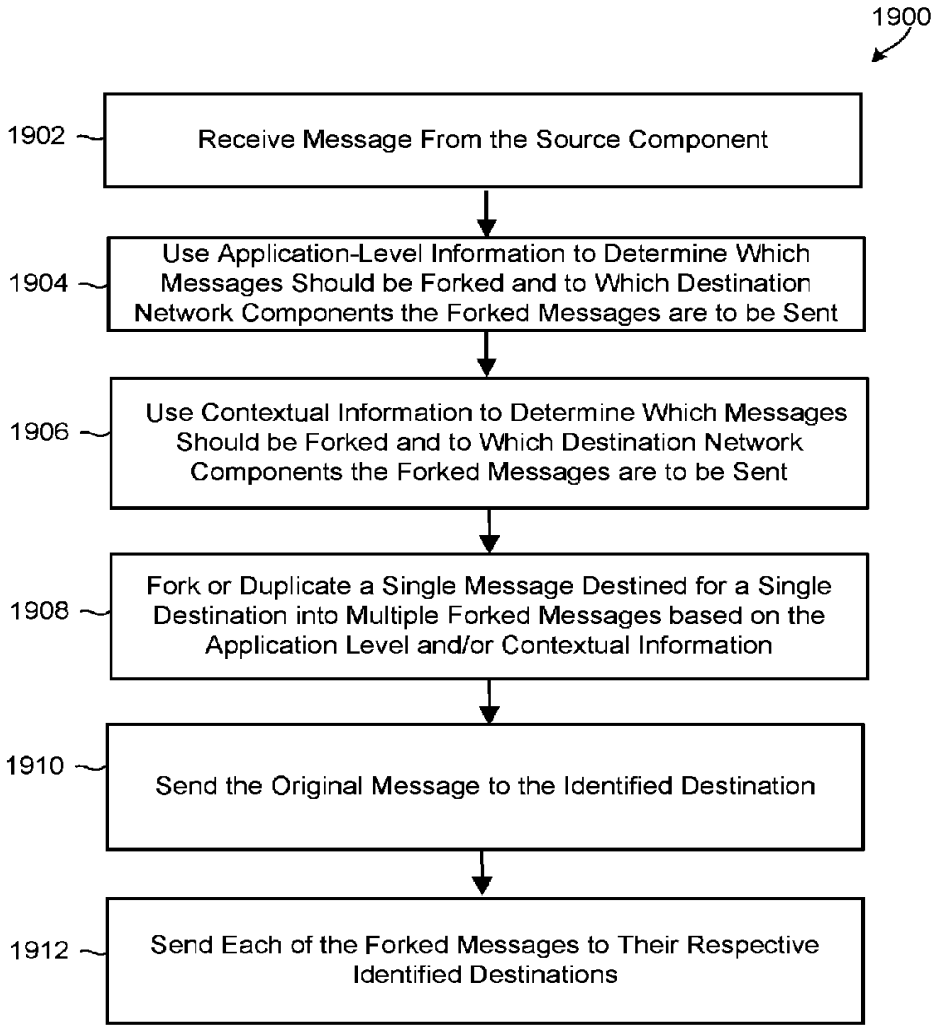

1900
1902
Receive Message From the Source Component
1904
Use Application-Level Information to Determine Which Messages Should be Forked and to Which Destination Network Components the Forked Messages are to be Sent
1906
Use Contextual Information to Determine Which Messages Should be Forked and to Which Destination Network Components the Forked Messages are to be Sent
1908
Fork or Duplicate a Single Message Destined for a Single Destination into Multiple Forked Messages based on the Application Level and/or Contextual Information
1910
Send the Original Message to the Identified Destination
1912
Send Each of the Forked Messages to Their Respective Identified Destinations

FIG. 19

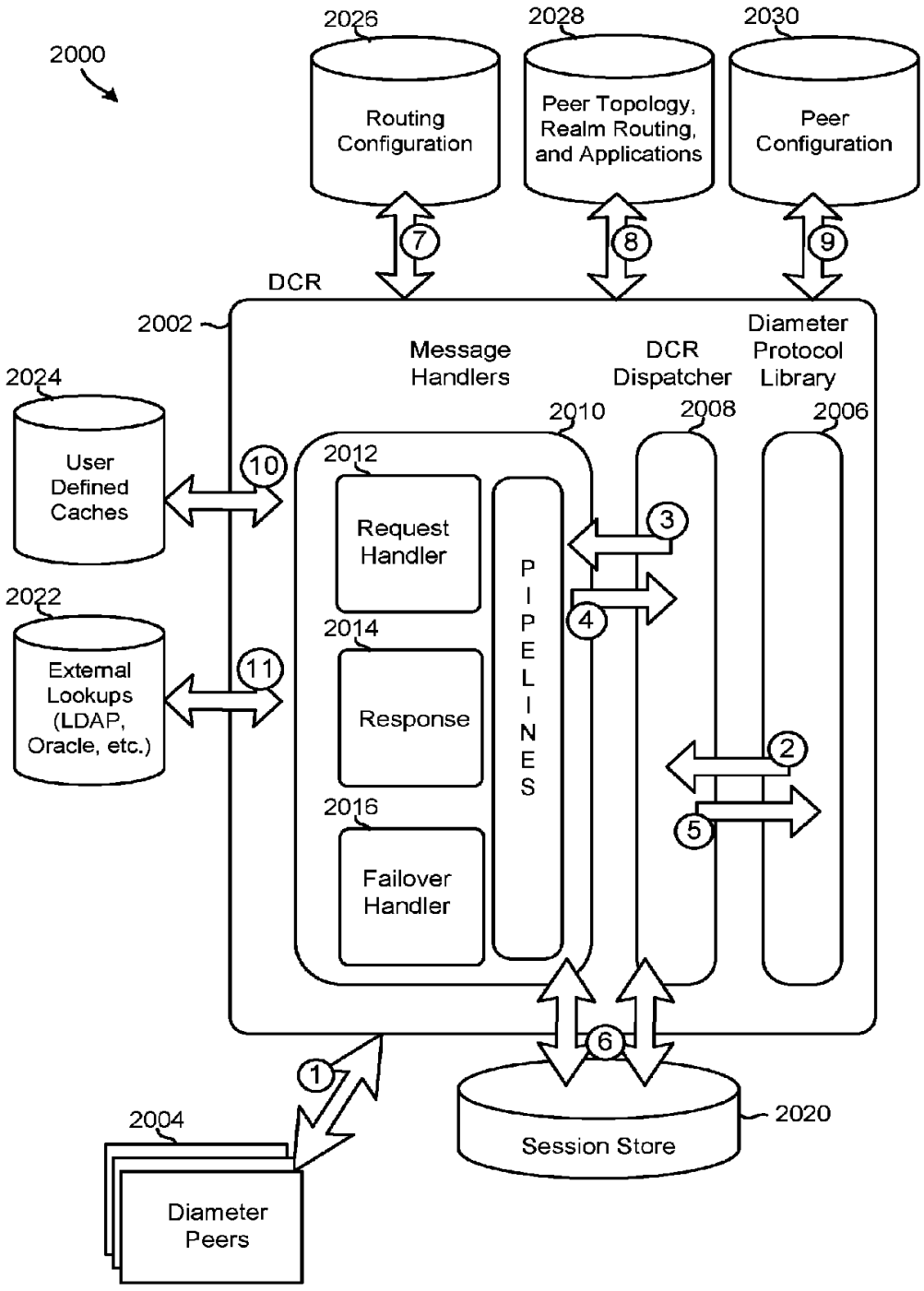

2000
2026
Routing Configuration
2028
Peer Topology, Realm Routing, and Applications
2030
Peer Configuration
7
8
9
DCR
2002
Message Handlers
DCR Dispatcher
Diameter Protocol Library
2024
User Defined Caches
2010
2008
2006
10
2012
Request Handler
3
4
2022
External Lookups (LDAP, Oracle, etc.)
11
2014
Response
PIPELINES
2
5
2016
Failover Handler
6
1
2004
Diameter Peers
Session Store
2020

FIG. 20

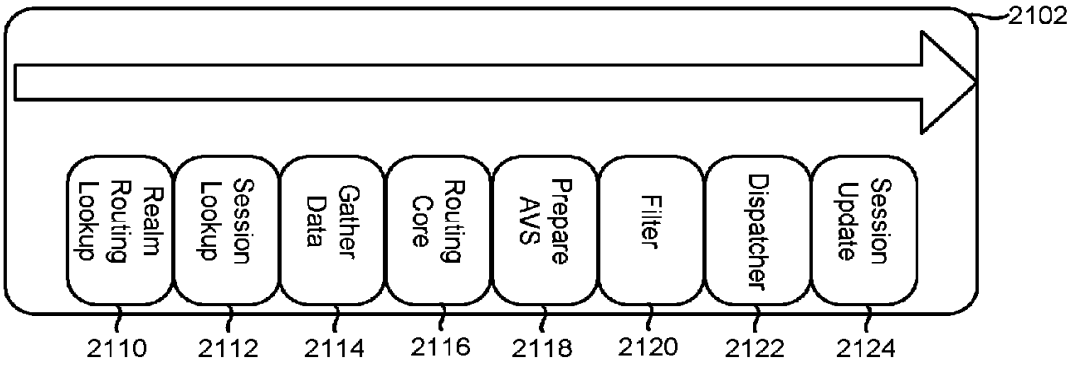


FIG. 21

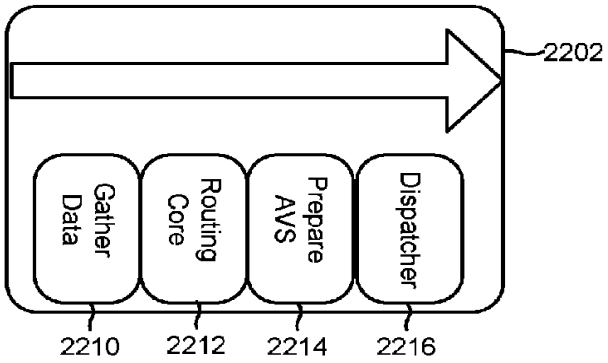


FIG. 22

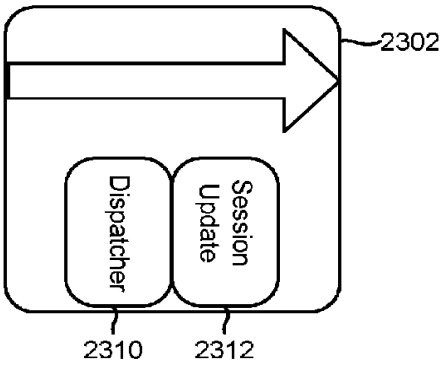


FIG. 23

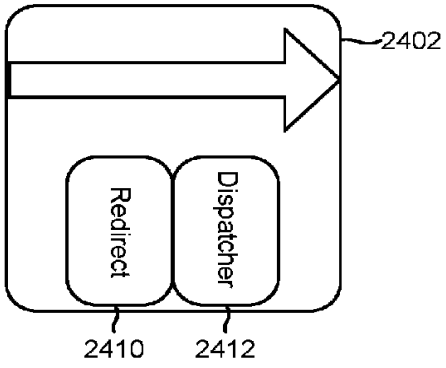


FIG. 24

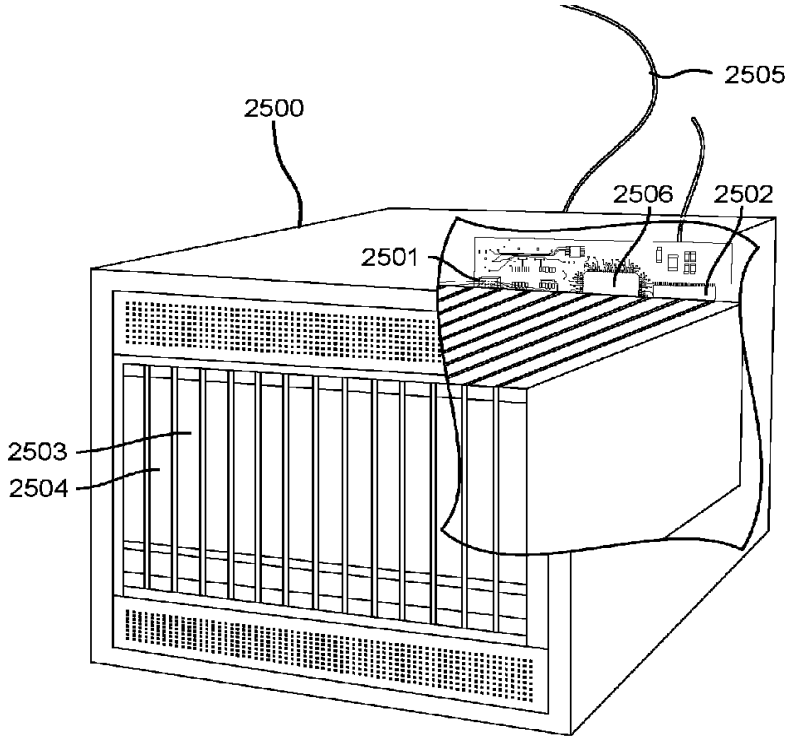


FIG. 25

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 11 19 3499

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X Y	EP 2 262 199 A1 (HUAWEI TECH CO LTD [CN]) 15 December 2010 (2010-12-15) * paragraphs [0020], [0022], [0023] * * paragraphs [0037] - [0039] * * paragraphs [0092] - [0095] * * figures 2,4,6 * -----	1,3,5,6, 8,10,11, 13,15 2,4,7,9, 12,14	INV. H04L12/56 H04L29/08 H04L29/06
X	J. Korhonen, M. Jones, L. Morand, T. Tsou: "Clarifications on the Routing of Diameter Requests Based on the Username and the Realm", , 31 December 2009 (2009-12-31), XP002671488, Retrieved from the Internet: URL:http://tools.ietf.org/html/rfc5729 [retrieved on 2012-03-14] * paragraph [04.4] * -----	1,5,6, 10,11,15	
Y	WOOD J ET AL: "A Web Services Architecture for Visualization", ESCIENCE, 2008. ESCIENCE '08. IEEE FOURTH INTERNATIONAL CONFERENCE ON, IEEE, PISCATAWAY, NJ, USA, 7 December 2008 (2008-12-07), pages 1-7, XP031399597, ISBN: 978-1-4244-3380-3 * pages 2-4; figures 1,2 * -----	2,7,12	TECHNICAL FIELDS SEARCHED (IPC) H04L
Y	US 6 427 173 B1 (BOUCHER LAURENCE B [US] ET AL) 30 July 2002 (2002-07-30) * paragraphs [0068] - [0070] * * paragraphs [0119] - [0128] * * paragraphs [0082], [0083] * * figures 3,6 * -----	4,9,14	

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	14 March 2012	Kesting, Christiane

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 11 19 3499

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

14-03-2012

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 2262199 A1	15-12-2010	CN 101547189 A	30-09-2009
		EP 2262199 A1	15-12-2010
		US 2011023071 A1	27-01-2011
		WO 2009117919 A1	01-10-2009
US 6427173 B1	30-07-2002	NONE	

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Non-patent literature cited in the description

- *3rd Generation Partnership Project Technical Specification Group Services and System Aspects, Policy and Charging Control Architecture*, 12 June 2011 **[0065]**

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : **H04Q 7/22, H04M 15/00**	**A1**	**(11) International Publication Number:** **WO 99/27723** **(43) International Publication Date:** 3 June 1999 (03.06.99)

(21) International Application Number: PCT/SE98/02111

(22) International Filing Date: 20 November 1998 (20.11.98)

(30) Priority Data:
08/977,455 24 November 1997 (24.11.97) US

(71) Applicant: TELEFONAKTIEBOLAGET LM ERICSSON (publ) [SE/SE]; S–126 25 Stockholm (SE).

(72) Inventors: NGUYEN, Binh; 275 St. Aubin, St. Laurent, Quebec H4M 231 (CA). MURRAY, James; 1445 Panama, Brossard, Quebec J4W 2G3 (CA). POULIN, Andre; 2332 Devigeois, Laval, Quebec H7K 3R1 (CA). IOCULANO, Angelo; 2/95 The Boulevard, Thomastown, Melbourne, VIC 8074 (AU). STROUD, John; 39 Versailles Street, Karori, Wellington 6004 (NZ).

(74) Agent: ERICSSON RADIO SYSTEMS AB; Common Patent Dept., S–164 80 Stockholm (SE).

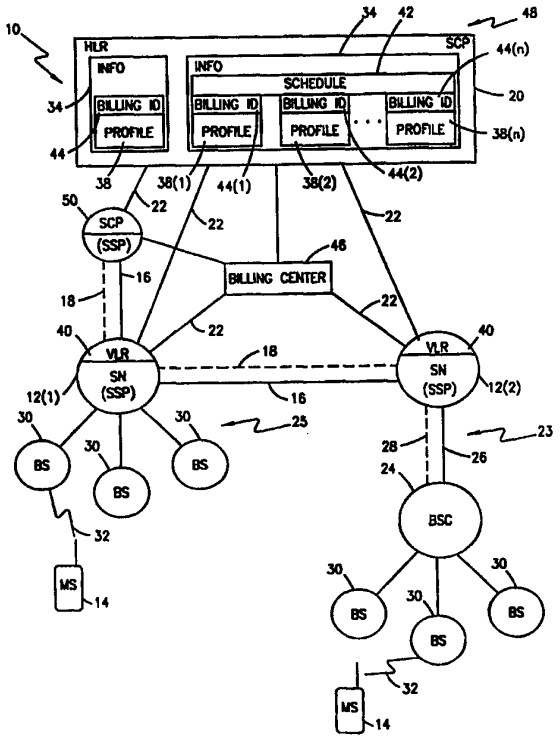
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: MULTIPLE SUBSCRIBER SERVICE PROFILES PER MOBILE STATION IN A CELLULAR COMMUNICATIONS SYSTEM

(57) Abstract

The conventional one–to–one relationship between a mobile station (14) and its associated service profile (38) is broken to allow for plural service profiles to be selectively activated for use in connection with a single mobile station. These plural service profiles are stored in the home location register HLR (20) of the cellular network (10). A separate billing identification (44) is maintained for each service profile in order to allow for segregated billing of service charges incurred with respect to use of the mobile station. Selection of a certain one of the plural service profiles to be active for a mobile station is made through, for example, a default choice, a user selected choice, a feature code selected choice, or a schedule driven selected choice. The active one of the plural service profiles is down–loaded from the home location register, and applied in connection with both in–coming and out–going calls.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

MULTIPLE SUBSCRIBER SERVICE PROFILES PER MOBILE STATION IN A CELLULAR COMMUNICATIONS SYSTEM

BACKGROUND OF THE INVENTION

Technical Field of the Invention

The present invention relates to cellular communications systems and, in particular, to the maintaining of multiple subscriber service profiles for a given mobile station operating within a cellular communications system.

Description of Related Art

In a conventional cellular communications system, a one-to-one relationship is typically maintained between the mobile station and the subscription for that mobile station. In this regard, the "subscription" refers to the contract entered into by a user (also referred to as the "subscriber") with a cellular service provider. The subscription defines not only to whom billing for cellular services should be charged, but also sets forth the particular types of cellular calling services and features that are to be provided to the subscriber. Once the subscripted to cellular calling services and features have been defined, this data is collected in a subscriber service profile that is stored and maintained in a database. The service profile is linked in that database to an identification of the mobile station for the subscriber. Thus, the conventional system also maintains a one-to-one relationship between each mobile station and the service profile that defines the cellular services and features provided to that mobile station.

In most cases, there are no difficulties experienced with maintaining this one-to-one relationship between a mobile station and its associated subscription/service profile. However, situations do arise where the provision of a single subscription/service profile presents a problem. For example, many individual subscribers utilize their mobile stations for both business and personal calls. Often times the charges incurred by the subscriber for business cellular calls may be reimbursed by their employer. As only one bill is generated for the associated subscription, the subscriber must carefully review each billing statement, excise out the charges for business related calls, and submit those charges for employer reimbursement. In an analogous situation, a corporate subscriber may maintain a cellular telephone for employee use during business hours for business purposes. At the same time, however, the corporate subscriber may desire to give the using employee the privilege of access to cellular service for personal calls. Again, as only one bill is generated, some segregation of cellular service charges

must be made, and a corresponding deduction from employee pay applied for the cost of personal calls.

There is a need then for a technique that would not only enable a mobile station user to differentiate between business and personal calls, but also separately account for such calls in service billings.

SUMMARY OF THE INVENTION

To address the foregoing needs, a subscription for cellular service is associated with plural service profiles. Thus, a one-to-many relationship is established between a mobile station and its associated subscription/service profiles. Different billing statements for use of the same mobile station are then generated for each service profile to allow for segregated billing of service charges incurred for mobile station use.

The home location register (HLR) of the cellular network stores plural service profiles for such subscripted mobile stations. Each of the service profiles is associated with a different billing identification to allow service charges incurred for use of the single mobile station to be properly allocated between the different profiles. The user selects in the mobile station (MS) a particular one of the profiles to be active. At each registration, an identification of this selected service profile is sent to the serving cellular network, and the selected service profile is down-loaded from the home location register. Alternatively, the user selects the active service profile to be down-loaded from the home location register by sending a feature code to the cellular network. Furthermore, selection of the active service profile for down-loading may be made by the network in accordance with a stored schedule maintained by the home location register.

Charging on a per service profile basis is made for both in-coming and out-going calls. In each case, appropriate toll tickets are generated by the network. These toll tickets identify not only the subscription for the mobile station involved in the call, but also the particular active one of the plural service profiles for that mobile station to which the service charges should be applied. By processing these toll tickets, a billing center may segregate the billing of service charges incurred for mobile station use against each of the plural service profiles.

BRIEF DESCRIPTION OF THE DRAWINGS

A more complete understanding of the method and apparatus of the present invention may be acquired by reference to the following Detailed Description when taken in conjunction with the accompanying Drawings wherein:

FIGURE 1 is a schematic diagram of a cellular telephone network of the present invention;

FIGURE 2 is a node operation and signal flow diagram illustrating selection at mobile station registration between plural available service profiles;

FIGURE 3 is a node operation and signal flow diagram illustrating selection using a feature code transmission between plural available service profiles;

FIGURE 4 is a node operation and signal flow diagram illustrating selection according to a schedule between plural available service profiles;

FIGURE 5 is a node operation and signal flow diagram illustrating a first embodiment for effectuating a call set up and delivery;

FIGURE 6 is a node operation and signal flow diagram illustrating a second embodiment for effectuating a call set up and delivery;

FIGURE 7 is a flow diagram illustrating handling of an outgoing call from a mobile station associated with plural service profiles; and

FIGURE 8 is a flow diagram illustrating handling of an incoming call to a mobile station associated with plural service profiles.

DETAILED DESCRIPTION OF THE DRAWINGS

Reference is now made to FIGURE 1 wherein there is shown a schematic diagram of a cellular telephone network 10 including a plurality of interconnected switching nodes (SN) 12. Although only two switching nodes 12 are shown, it will be understood that the network 10 likely includes many more interconnected nodes. The first and second switching nodes 12(1) and 12(2) may comprise any one of a number of known telecommunications switching devices, including those commonly used and known in the art for providing either digital or analog cellular telephone service to a plurality of mobile stations (MS) 14. The switching nodes 12 are interconnected with each other for communication via both voice trunks 18 (illustrated with broken lines) and signaling links 16 (illustrated with solid lines) providing a known ISUP (or R1 or R2) type connection. The voice trunks 18 provide voice and data communications paths used to carry subscriber communications between the switching nodes 12. The signaling links 16 carry command signals between the switching nodes 12. These signals may be used, for example, in setting up and tearing down voice and data communications links over the voice trunks 18 and controlling the provision of calling services to the mobile stations 14.

The switching nodes 12 are also connected to a home location register (HLR) 20 through their associated visitor location register (VLR) 40 by means of

signaling links 22 providing a known Mobile Application Part (MAP) or IS-41 type connection. The home location register 20 stores information relating to the mobile stations 14 and their subscriptions comprising location information and service profile information. In connection with the present invention, as will be described in more detail below, the home location register 20 in particular stores plural service profiles for at least one of the mobile stations.

In one cellular system implementation, illustrated generally at 23, the switching node 12 is further connected to at least one associated base station controller (BSC) 24 via both a signaling link 26 and a voice trunk 28. Only one base station controller 24 is shown connected to switching node 12(2) in order to simplify the illustration. The voice trunk 28 provides a voice and data communications path used to carry subscriber communications between the second switching node 12(2) and its base station controller 24. The signaling link 26 carries command signals between the node 12 and its associated base station controller 24. The signaling link 26 and trunk 28 are collectively commonly referred to in the art as the "A interface". The base station controller 24 is then connected to a plurality of base stations (BS) 30 which operate to effectuate radio frequency communications with proximately located mobile stations 14 over an air interface 32. The base station controller 24 functions in a well known manner to control this radio frequency communications operation.

In another cellular system implementation, illustrated generally at 25, the switching node 12(1) is further connected to a plurality of base stations (BS) 30 which operate to effectuate radio frequency communications with proximately located mobile stations 14 over the air interface 32. In this implementation, the functionality provided by the base station controller 24 (see, generally at 23) is instead provided by the switching node 12(1).

Although direct communications links (signaling and/or trunk) are illustrated in FIGURE 1, it is understood by those skilled in the art that the links are not necessarily direct between the illustrated nodes, and may instead pass through many other communications nodes (not shown) of the mobile network, and perhaps even utilize other communications networks (such as the public switched telephone network - PSTN). Illustration of the links in a "virtual" manner as shown in FIGURE 1 is therefore by way of simplification of the drawing and the communications relationship between the various included nodes within the network 10.

For each cellular service subscription associated with a served mobile station 14, the home location register 20 stores service profile information 34

relating to cellular services and features subscripted to by the subscriber for that served mobile station. If conventional service is provided to a mobile station 14, the service profile information 34 associated with that mobile station subscription comprises a single service profile 36 per subscription. Conversely, and in accordance with the present invention, plural service profiles 38(n), where n>1, may comprise the service profile information 34 associated with a single mobile station 14. For mobile stations 14 having subscriptions that support plural service profiles 38(n), any one of those plural profiles may be selected, either by the system or by the subscriber (with some restrictions), for use at a specific time or in connection with a specific call.

When a mobile station 14 makes an initial registration with the system through a particular switching node 12, that switching node requests a subscriber service profile 36 or 38(n) relating to that mobile station, and its corresponding subscription, from the home location register 20. This subscriber service profile 36 or 38(n) information is downloaded from the home location register 20 for storage in a visitor location register (VLR) 40 associated with the switching node 12. Service for both in-coming and out-going calls is then provided to the mobile station 14 by the serving switching node 12 in accordance with the downloaded service profile 36 or 38(n).

In accordance with one embodiment of the present invention, the subscriber enters a service profile selection code into the mobile station 14, and this selection information is conveyed by the serving switching node 12 to the home location register 20 at each registration. The home location register 20 processes the selection information to identify the proper one of the n available service profiles 38(n) for the mobile station 14. This profile is then downloaded to the visitor location register 40.

In another embodiment of the present invention, the subscriber sends a feature code through the mobile station 14. This feature code is indicative of the activation of a certain one of the n available service profiles 38(n) for the mobile station 14. Responsive to receipt of the feature code, the proper service profile 38(n) is identified by the home location register 20 and downloaded to the visitor location register 40. That particular service profile 38(n) is further marked as being active by the home location register 20. In response to any subsequent registration of the mobile station, the home location register 20 automatically retrieves the active one of the service profiles 38(n) for a visitor location register 40 download. Deactivation of the currently activated service profile occurs when the mobile station powers-off or when the mobile station has been idle for longer than a

predetermined time period. Alternatively, the selected service profile 38(n) continues to remain active until such time as a new selection is made through feature code entry.

In yet another embodiment of the present invention, the activation of a certain one of the n available service profiles 38(n) depends on a subscriber or service provider defined schedule 42 for the mobile station 14. This schedule may, for example, designate that a business related one of the service profiles 38(n) be active during weekday business hours, while a personal related one of the service profiles be active at all other times. As another application, the schedule may designate that a first employee related service profile 38(n) be active during a first weekday time shift, a second employee related service profile be active during a second weekday time shift, a third employee related service profile be active during a third weekday time shift, and that no service profile be active on weekends. No matter what the particular schedule that is established, in response to a registration, the home location register 20 identifies (based on the schedule 42) the proper active one of the n available service profiles 38(n) for the mobile station 14. This profile is then downloaded to the visitor location register 40.

In each case, a different billing identification 44(n) is provided for each of the n available service profiles 38(n) for the mobile station 14. A billing center 46 for the service provider receives toll tickets (TTs) relating to calling charges, processes the toll tickets with respect to the mobile station and particular active service profile thereof, and then accordingly generates a separate billing statement for each identification 44(n) effectively allocating cellular service costs properly among various usages and subscribers. Taking, for example, the previous scenario where a business service profile 38(n) and personal service profile are provided for a single mobile station 14, one business billing statement and one personal billing statement are generated by the billing center 46. This allows the subscriber to account between business and personal calling expenses. Similarly, for the previous multi-shift related service profiles 38(n), one billing statement is generated for each weekday time shift. This allows an employer to allocate business calling expenses by shift and/or the assigned personnel. In order to generate this billing information, properly allocated to the plural service profiles, each toll ticket generated by the network 10 during a call and communicated to the billing center 46 must included information identifying the mobile station/subscription at issue, and further include information identifying, or allowing the billing center to identify, the particular one of the service profiles 38(n) that is active for the call.

Furthermore, if needed or desired, each of the plural service profiles 38(n) may be associated with a different directory number. Thus, not only is a single mobile station associated with different service profiles, but it may also be accessed by a caller through the dialing of any one of a number of different directory numbers. This allows each one of a number of potential users of the mobile station to have a unique telephone directory number for in-coming calls. In connection with the handling of such calls, a number of billing options are available. First, an in-coming call dialed to a certain directory number may be delivered to the mobile station regardless of whether the service profile associated with that number is currently active. Billing is made either to the service profile for the called number, or the service profile that is currently active. Second, the alternative holds true: no call delivery occurs unless the service profile associated with the dialed number is currently active. Billing is made to the active service profile of the called number.

Reference is now made to FIGURE 2 wherein there is shown a node operation and signal flow diagram illustrating selection at mobile station registration between plural available service profiles. The subscriber selects (action 200) a particular one of plural available service profiles 38(n) for use by making an appropriate entry into the mobile station 14. This selection is stored (action 202) by the mobile station. The mobile station 14 then makes a registration with the cellular telephone network by transmitting a registration message 204 to the serving switching node 12 through the serving base station 30 (and perhaps the serving base station controller 24). This registration message 204 includes information, perhaps stored in an included parameter, identifying the subscriber selected one of plural available service profiles 38(n). Responsive thereto, the switching node 12 sends a registration notification message 206 to the home location register 20 through the visitor location register 40 requesting the selected one of the service profiles 38(n) associated with the registering mobile station 14. The home location register 20 retrieves the selected one of the service profiles 38(n), and sends that information in message 208 back for storage (action 210) in the visitor location register 40 associated with the requesting switching node 12. In-coming and out-going calling service is thereafter provided to the mobile station in accordance with the down-loaded service profile. If desired, the selected 200 service profile remains active until the mobile station has been idle for longer than a predetermined time period (action 212).

Reference is now made to FIGURE 3 wherein there is shown a node operation and signal flow diagram illustrating selection using a feature code transmission between plural available service profiles. A feature request is dialed

(action 220) by a subscriber into their mobile station 14. This feature request (perhaps in the form of an appropriately formatted star code) identifies a subscriber selected one of plural available service profiles 38(n) for activation, and may further present a personal identification number (PIN) indicating authorization for the selection. A feature origination message 222 is then sent by the mobile station 14 (over the air interface and through the base station) to the switching node 12. In response thereto, the switching node 12 sends a feature request message 224, including the dialed feature code, to the home location register 20. The home location register 20 then processes the message 224 to determine whether the subscriber is authorized to use the feature (action 226), and if so, what actions need to be taken in response to the request (action 228) and what instructions, if any, need to be presented to the mobile switching center to effectuate the feature (action 230). In particular, with respect to the actions 228 taken, the home location register 20 marks the subscriber selected one of plural available service profiles 38(n) as being active. A feature request return result message 232, confirming activation of the selected service profile 38(n), is then sent by the home location register 20 back to the mobile station 14 through the switching node 12. The home location register 20 also retrieves the selected one of the service profiles 38(n), and sends that information in message 234 back for storage (action 236) in the visitor location register 40 associated with the switching node 12. In-coming and out-going calling service is thereafter provided to the mobile station in accordance with the down-loaded service profile.

Once a subscriber selected one of plural available service profiles 38(n) has been marked as being active, it remains active until the mobile station powers-off (action 238), the mobile station has been idle for longer than a predetermined time period (action 240), or a new selection is made by the subscriber through feature code entry (action 220). The feature code entry (action 220) may alternatively simply de-activate the currently active service profile (taken in actions 228), with activation of a service profile requiring the entry of another feature code.

Once a service profile 38(n) is activated, it is made available at each time the mobile station 14 registers. The mobile station 14 makes a registration with the cellular telephone network by transmitting a registration message 242 to the serving switching node 12 through the serving base station 30 (and perhaps the serving base station controller 24). Responsive thereto, the switching node 12 sends a registration notification message 244 to the home location register 20 through the visitor location register 40 requesting the currently active one of the service profiles 38(n) associated with the registering mobile station 14. The home location register

20 retrieves the active one of the service profiles 38(n), and sends that information in message 246 back for storage (action 248) in the visitor location register 40 associated with the requesting switching node 12. In the event that none of the service profiles 38(n) is currently active, the home location register 20 returns a registration denied message 250 back the switching node 12. If possible, the reason for denial is conveyed to the mobile station in message 252. This prompts the subscriber to activate one of the plural service profiles 38(n) through feature code entry (action 220), resulting in a down-loading of the selected one of the service profiles 38(n) in message 234 for storage (action 236) in the visitor location register 40 associated with the switching node 12.

Reference is now made to FIGURE 4 wherein there is shown a node operation and signal flow diagram illustrating selection according to a schedule between plural available service profiles. A schedule 42 designating the activation periods for each of plural available service profiles 38(n) of a mobile station 14 is stored (action 260) in the home location register 20. The schedule 42 may be either service provider or subscriber defined. The mobile station 14 subsequently makes a registration with the cellular telephone network by transmitting a registration message 262 to the serving switching node 12 through the serving base station 30 (and perhaps the serving base station controller 24). Responsive thereto, the switching node 12 sends a registration notification message 264 to the home location register 20 through the visitor location register 40 requesting the schedule 42 defined active one of the service profiles 38(n) associated with the registering mobile station 14. The home location register 20 retrieves the service profile 38(n) identified by the schedule as being active, and sends that information in message 266 back for storage (action 268) in the visitor location register 40 associated with the requesting switching node 12. In-coming and out-going calling service is thereafter provided to the mobile station in accordance with the down-loaded service profile.

Reference is now once again made to FIGURE 1. Although not necessarily a requirement, the cellular telephone network 10 is preferably implemented as a wireless intelligent network (IN) and thus further includes at least one service control point (SCP) 48. The switching nodes 12 (also referred to as service switching points (SSPs) in this configuration) are connected to the service control point 48 by means of the signaling links 22 which utilize protocols such as Mobile Application Part (MAP), IS-41, Intelligent Network Application Part (INAP), or Transaction Capability Application Part (TCAP). The home location register 20 is preferably implemented in conjunction with the service control point 48. The

service control point 48 provides a centralized processing platform for implementing the "intelligence" of the network 10. In the context of the present invention, this intelligence comprises the administration over the plural service profiles 38(n) available to certain ones of the mobile stations 14. This administration primarily involves the operations described herein for selecting which one of the service profiles 38(n) is to be active at any one time (either in response to subscriber selection, feature code selection, or scheduling selection). Alternatively, a separate combined service switching point/service control point (SSP/SCP or SSCP) 50 is provided for handling of calls implicating multiple service profile 38(n) selection. This combined service switching point/service control point 50 is connected to the switching nodes 12 via both voice trunks 18 (illustrated with broken lines) and signaling links 16 (illustrated with solid lines) providing a known ISUP (or R1 or R2) type connection, and is connected to the home location register by means of the signaling links 22 which utilize protocols such as Mobile Application Part (MAP), IS-41, Intelligent Network Application Part (INAP), or Transaction Capability Application Part (TCAP). Although not specifically illustrated, it is understood that the intelligent network further includes intelligent peripherals (IPs) and other nodes as needed to implement in a known manner any desired intelligent network services.

Reference is now made to FIGURE 5 wherein there is shown a node operation and signal flow diagram illustrating a first embodiment for effectuating a call set up and delivery. A call 300 dialed to the directory number (B-number) of a mobile station 14 originates from another cellular subscriber or the public switched telephone network (PSTN), and is received at a first (originating or gateway) switching node 12(1). The originating switching node 12(1) determines whether the calling party is entitled to receive any intelligent network services (action 302). One such service may comprise the plural service profile 38(n) service of the present invention. If so, the originating switching node 12(1) sends an originating access message 304 to the home location register 20 (service control point 48). This message 304 requests an identification of each intelligent network service to which either the calling party is entitled. The list of such services (including, for example, the plural service profile 38(n) service) is returned to the originating switching node 12(1) in message 306. The identified services in the returned list are then evaluated and organized (action 308) for implementation in connection with the call 300.

With respect to call handling in the context of the plural service profile 38(n) service of the present invention, the call is routed 310 to the particular

combined service switching point/service control point 50 supporting that service (assuming the home location register 20 cannot provide all necessary support, including billing). In this regard, the combined service switching point/service control point 50 has knowledge (perhaps down-loaded from, or accessed from the home location register 20) of the plural service profiles 38(n) associated with the calling/called party. The active one of the plural service profiles 38(n) is then implemented (action 312) in connection with the call, and a toll ticket for billing is generated 314 specifically identifying the active profile of a given subscription be charged. The call is then routed 316 back to the originating switching node 12(1). As a further refinement of the call handling process, the call leg routings 310 and 316 may be dropped (if desired), as generally indicated with "X" markings, from the call 300 once generation 314 of the toll ticket associating the call with the proper service profile is completed. Another toll ticket for billing is then generated 318 by the originating switching node 12(1) identifying that the given subscription be charged. These toll tickets are processed by the billing center 46 to generate a charge for the call, with that charge being assessed against the currently active one of the service profiles 38(n) of the calling party subscription. As another refinement, the billing information relating to the active service profile 38(n) is sent to the originating switching node 12(1) to be included in its generated 318 toll ticket, thus obviating the need for a separate toll ticket generated 314 by the service switching point/service control point 50.

Now that the appropriate one of the plural service profiles 38(n) has been associated with the call, and following the actuation of any other appropriate intelligent network services in connection with the call, the originating switching node 12(1) interrogates the home location register 20 with a location request (send routing) message 320. The location request (send routing) message 320 is processed by the home location register 20 to determine the location (i.e., second or serving switching node 12(2)) within the cellular network 10 of the called mobile station 14. Responsive to this interrogation, the home location register 20 messages the serving switching node 12(2) for the called mobile station 14 with a routing request (provide roaming) message 322 to prepare for the call. The serving switching node 12(2) then determines in action 324, to some selected degree of granularity, the location (for example, location area) of the called mobile station 14. This location may be identified, for example, based on information resulting from a most recent registration (not shown) of the called mobile station 14 as stored in the visitor location register (not shown) associated with the serving switching node 12(2). Alternatively, the serving switching node 12(2) may page (not shown) the

called mobile station 14, and process the page response (not shown) to make a more precise location determination. In accordance with this determined location, the serving switching node 12(2) selects in action 326 an appropriate routing number (for example, a temporary location directory number (TLDN) or a roaming number) for that location. In this instance, the routing number is selected from a plurality of such numbers associated with the serving switching node 12(2). The selected routing number is then returned 328 to the originating switching node 12(1) via the home location register 20. The incoming call is then delivered (through connected) 330 to the serving switching node 12(2) using the routing number for attempted completion to the called mobile station 14. Completion of the call involves further routing 332 the incoming call to the currently serving base station 30 (perhaps through the base station controller 24), and then to the called mobile station 14 over the air interface 32. The serving switching node 12(2) handles the call in accordance with the down-loaded, visitor location register stored, service profile of the called mobile station. It is recognized that this down-loaded service profile may comprise one of a number of service profiles 38(n) assigned to the called mobile station 14 subscriber and currently designated as active (see, FIGURES 2, 3 and 4). A toll ticket (TT) is accordingly generated (action 334) against the active one of the service profiles for the called mobile station. Toll ticket processing enables the billing center 46 to properly generate a charge for the call, with that charge being assessed against the currently active one of the service profiles 38(n) of the called party subscription.

Reference is now made to FIGURE 6 wherein there is shown a node operation and signal flow diagram illustrating a second embodiment for effectuating a call set up and delivery. A call 300 dialed to the directory number (B-number) of a mobile station 14 originates from another cellular subscriber or the public switched telephone network (PSTN), and is received at a first (originating or gateway) switching node 12(1). The originating switching node 12(1) determines whether the calling party is entitled to receive any intelligent network services (action 302). One such service may comprise the plural service profile 38(n) service of the present invention. If so, the originating switching node 12(1) sends an originating access message 304 to the home location register 20 (service control point 48). This message 304 requests an identification of each intelligent network service to which either the calling party is entitled. The list of such services (including, for example, the plural service profile 38(n) service) is returned to the originating switching node 12(1) in message 306. The identified services in

the returned list are then evaluated and organized (action 308) for implementation in connection with the call 300.

Routing of the call to a service switching point/service control point 50 is not required in this embodiment as the home location register 20 (service control point 48) support all aspects (including billing) for the plural service profile 38(n) service of the present invention. Thus, responsive to the originating access message 304, the active one of the plural service profiles 38(n) is then implemented (action 312') in connection with the call, and a toll ticket for billing is generated 314' specifically identifying that the specific active profile of a subscription be charged. Another toll ticket for billing is then generated 318 by the originating switching node 12(1) identifying that the subscription be charged. These toll tickets are processed by the billing center 46 to generate a charge for the call, with that charge being assessed against the currently active one of the service profiles 38(n) of the identified calling party subscription. As a refinement to the process, the billing information relating to the active service profile 38(n) is sent to the originating switching node 12(1) to be included in its generated 318 toll ticket, thus obviating the need for a separate toll ticket generated 314' by the home location register 20.

Now that the appropriate one of the plural service profiles 38(n) has been associated with the call, and following the actuation of any other appropriate intelligent network services in connection with the call, the originating switching node 12(1) interrogates the home location register 20 with a location request (send routing) message 320. The location request (send routing) message 320 is processed by the home location register 20 to determine the location (i.e., second or serving switching node 12(2)) within the cellular network 10 of the called mobile station 14. Responsive to this interrogation, the home location register 20 messages the serving switching node 12(2) for the called mobile station 14 with a routing request (provide roaming) message 322 to prepare for the call. The serving switching node 12(2) then determines in action 324, to some selected degree of granularity, the location (for example, location area) of the called mobile station 14. This location may be identified, for example, based on information resulting from a most recent registration (not shown) of the called mobile station 14 as stored in the visitor location register (not shown) associated with the serving switching node 12(2). Alternatively, the serving switching node 12(2) may page (not shown) the called mobile station 14, and process the page response (not shown) to make a more precise location determination. In accordance with this determined location, the serving switching node 12(2) selects in action 326 an appropriate routing number

(for example, a temporary location directory number (TLDN) or a roaming number) for that location. In this instance, the routing number is selected from a plurality of such numbers associated with the serving switching node 12(2). The selected routing number is then returned 328 to the originating switching node 12(1) via the home location register 20. The incoming call is then delivered (through connected) 330 to the serving switching node 12(2) using the routing number for attempted completion to the called mobile station 14. Completion of the call involves further routing 332 the incoming call to the currently serving base station 30 (perhaps through the base station controller 24), and then to the called mobile station 14 over the air interface 32. The serving switching node 12(2) handles the call in accordance with the down-loaded, visitor location register stored, service profile of the called mobile station. It is recognized that this down-loaded service profile may comprise one of a number of service profiles 38(n) assigned to the called mobile station 14 subscriber and currently designated as active (see, the process of FIGURES 2, 3 and 4). A toll ticket (TT) is accordingly generated (action 334) against the active one of the service profiles for the called mobile station. Toll ticket processing enables the billing center 46 to properly generate a charge for the call, with that charge being assessed against the currently active one of the service profiles 38(n) of the called party subscription.

Reference is now made to FIGURE 7 wherein there is shown a flow diagram illustrating handling of an outgoing call from a mobile station associated with plural service profiles. In step 100, a call origination is received by the process. This received call origination 100 includes an identification of digits dialed for an outgoing call and/or code dialings. A determination is then made in step 102 as to whether the received call concerns a user designated and transmitted activation (feature) code. If yes, an appropriate action is taken in step 104 in response to the code. For example, the sent code may identify a subscriber selected one of plural available service profiles 38(n) for activation (see, FIGURE 3). Other actions relevant to the plural service profile 38(n) service of the present invention and involving a feature code selection are presented below. It should further be noted that a specific feature code may be recognized that would prevent unauthorized entry of feature codes to specify certain actions and changes. An appropriate confirming announcement with respect to the action (such as confirming the selection of a certain service profile) is then sent back to the mobile station in step 106, and the call is terminated. If no, a determination is then made in step 108 as to whether the received call concerns a user designated and transmitted escape code. This escape code signals the process to switch between

available service profiles 38(n) for a current call only. This differs from the activation code of step 102 where a semi-permanent switch of service profiles may be made. Accordingly, if yes, a toggle is set in step 110. Thereafter, or if no in step 108, a determination is made in step 114 as to whether a scheduling feature (42, FIGURE 1) for the user is currently enabled. The scheduling feature enables the user (or the subscriber, if different) to select based on time of day, and day of week parameters, which of the plural service profiles 38(n) is to be active. If the scheduling feature is enabled, then the appropriate one of the service profiles based on the schedule is selected in step 116 to be implemented in connection with the call. Through the use of an appropriate activation (feature) code (step 102), the user may selectively choose not to have an established schedule be activated and followed. In the event the schedule designates the current time of day and day of week are black-out periods for user originated calls, an appropriate confirming announcement with respect to the black-out is then sent back to the mobile station in step 106, and the call is terminated. If no (in step 114), the default one of the plural service profiles 38(n) for the user, or the user activated one of the plural service profiles (step 104), is selected in step 118 to be implemented in connection with the call. Following selection of a service profile (116 or 118), a determination is made in step 120 as to whether the toggle was previously set in step 110. If yes, the service profile effective for the call is switched in step 122 from that selected in steps 116 or 118, to one of the other service profiles for the duration of the current call only. Thereafter, or if no in step 120, the call is screened in step 124 according to the active service profile in order to determine if call completion is permitted. In this regard, there are two kinds of screening lists that are implemented for each of the service profiles. The first is an outgoing allowed list. If the dialed digits (step 100) meet the parameters of the allowed list, call completion is permitted. Charging for the call is then made against the active service profile in step 126 and the call is completed 128. The second is an outgoing restricted list. If the dialed digits (step 100) meet the parameters of the restricted list, call completion is rejected in step 130. An appropriate confirming announcement with respect to the restriction is then sent back to the mobile station in step 106, and the call is terminated.

Reference is now made to FIGURE 8 wherein there is shown a flow diagram illustrating handling of an incoming call to a mobile station associated with plural service profiles. In step 200, an incoming call is received dialed to a particular directory number (i.e., the B number). A determination is then made in step 202 as to which of a number of available profiles is currently in effect. This

determination may be made by having a different profile 38 associated with each B number, and thus selecting the profile for the dialed B number. In accordance with the present invention, the determination is made by having multiple profiles 38(n) associated with each individual B number, and then selecting that profile which is either currently selected by the called subscriber as being active or is active based on a schedule. The process then selects the proper profile 38(n) in step 204.

Once the proper profile 38(n) has been determined and selected, the process next screens against the calling party telephone number (i.e., the A number) in step 206. This screening process is performed against a list of A number from which it is permissible for the called mobile station to receive an incoming call. The list can be as specific as including particular numbers, or a general as including broad source indications (like prefixes and area codes). If the A number is not authorized by the list, the incoming call is rejected in step 208. If the A number is on the list, the incoming call is next processed through a diversion selection function in step 210.

With respect to the diversion selection function, the process may implement location based diversion in step 212. In accordance with location base diversion, the incoming call is diverted for call delivery based on called mobile station location. A number of different diversion options are available contingent on mobile station roaming status. The subscriber may, for example, specify delivery of the call to the mobile station, or alternatively delivery to a forwarding directory number (C number). The selection of one delivery option over another option depends upon the current roaming status (public or private network) of the mobile station in combination with the options specifically assigned by the subscriber for that status.

The process of diversion selection may further implement a mobile status based diversion in step 214. In accordance with mobile status based diversion, the incoming call is diverted for call delivery based on called mobile station operational status. A number of different diversion options are available contingent on mobile station operational status. The subscriber may, for example, designate the mobile station itself as the first point of contact as long as the mobile station is currently in active operational mode. If the mobile station is currently in inactive operational mode, however, the incoming call is instead routed in accordance with a diversion routing in step 216. Furthermore, if the mobile station is currently active, but is busy or there is no answer to the incoming call alert, the incoming call is again instead routed in accordance with the diversion routing of step 216.

The diversion routing of step 216 specifies the manner with which call delivery is be accomplished. As a general rule, this manner of accomplishing call delivery is specified by the subscriber based on the currently effective operation status of the called mobile station at the time of delivery. For example, if the current status of the mobile station is either inactive, busy or no answer, diversion routing may specify forwarding of the incoming call to a certain directory number (perhaps, comprising a voice mail box for the subscriber or other selected C number). Optionally, other delivery mechanisms may be employed. Examples of these mechanisms include sequential paging, sequential time based paging, or called party controlled completion (CPCC) services. Sequential paging refers to a delivery mechanism where a list of forwarding numbers to be sequentially tried is maintained to handling step 216 diversion routing instances. If one of the numbers on the list is busy, the call is routed to an identified end of list destination (typically comprising a voice mail box). If the last number on the list is reached without completing a successful call set-up, then the call is also routed to an identified end of list destination. Furthermore, if a time out occurs without making a successful call set-up, then the call is also routed to an identified end of list destination. Sequential time based paging refers to a delivery mechanism use of certain one or more of the numbers on the list is restricted in time. For example, a business hours dialing list and a non-business hours dialing list may be maintained. Thus, certain numbers are effective only at certain times of the day (or perhaps day of the week), and those effective numbers are sequentially tried during step 216 diversion routing. Called party controlled completion refers to a delivery mechanism where the called party exercises control over how an incoming call is to be handled (such as, for example, transfer to voice mail, forward to alternate number, and the like).

Once A number screening and diversion function have been performed, the process moves to charge for the incoming call against the active service profile in step 218 and the call is completed 220. It is recognized that in some instances completion of the call will not occur, the process accordingly returns (also dotted path 222) back to the diversion function 210 for further handling. Such handling may, for example, comprise retrieving a different forward to number in the case of the sequential call delivery mechanism.

Although preferred embodiments of the method and apparatus of the present invention have been illustrated in the accompanying Drawings and described in the foregoing Detailed Description, it will be understood that the invention is not limited to the embodiments disclosed, but is capable of numerous rearrangements,

modifications and substitutions without departing from the spirit of the invention as set forth and defined by the following claims.

WHAT IS CLAIMED IS:

1. A cellular telephone system serving a plurality of mobile stations, comprising:

at least one home location register storing service profile information for each of the served mobile stations, wherein the stored service profile information comprises plural different service profiles maintained for each of certain ones of the mobile stations.

2. The system as in claim 1 wherein each of the plural different service profiles maintained for each of the certain ones of the mobile stations has a billing identification in order to allow for segregated billing by service profile of service charges incurred with respect to use of the certain mobile stations.

3. The system as in claim 1 further comprising means for selecting an active one of the plural different service profiles for application in providing cellular telephone service to the certain mobile station.

4. The system as in claim 3 wherein the means for selecting comprises a schedule that identifies which of the plural different service profiles is to be active at any given time.

5. The system as in claim 3 wherein the means for selecting comprises a feature code selection that identifies which of the plural different service profiles is to be active at any given time.

6. The system as in claim 3 wherein the means for selecting comprises a default selection that identifies which of the plural different service profiles is to be active.

7. A method for providing cellular telephone service to a mobile station, comprising the steps of:

storing for that mobile station a plurality of different service profiles; and

activating a certain one of the plurality of different service profiles for application in providing cellular telephone service to the certain mobile station.

8. The method as in claim 7 wherein the step of storing comprises the step of maintaining a billing identification for each of the plural service profiles in

order to allow for segregated billing by service profile of service charges incurred with respect to use of the mobile station.

9. The method as in claim 7 wherein the step of activating comprises the steps of:

establishing an activation schedule defining times when each of the plural service profiles is to be active for application in providing cellular telephone service to the certain mobile station; and

activating ones of the plural service profiles in accordance with the established schedule.

10. The method as in claim 7 wherein the step of activating comprises the steps of:

selecting by a user of the mobile station of a certain one of the plural service profiles to be active for application in providing cellular telephone service; and

communicating that selection at mobile station registration to activate the certain service profile.

11. The method as in claim 10 wherein the step of activating further comprises the step of maintaining the certain service profile as active until the expiration of a predetermined time period.

12. The method as in claim 7 wherein the step of activating comprises the steps of:

making a feature code selection identifying a certain one of the plural service profiles to be active for application in providing cellular telephone service; and

sending that feature code to activate the certain service profile.

13. The method as in claim 12 wherein the step of activating further comprises the step of maintaining the certain service profile as active until the expiration of a predetermined time period.

14. The method as in claim 7 wherein the step of activating comprises the step of activating a designated default one of the plural service profiles for application in providing cellular telephone service.

15. A method for handling a call origination in a cellular telephone system, comprising the steps of:

determining if a calling party is entitled to utilize a plural service profiles per subscriber service;

if yes, determining which one of the plural service profiles for the calling party is currently active;

applying the currently active one of the plural service profiles to the call origination; and

billing service charges for the call origination against the currently active service profile.

16. The method as in claim 15 wherein the step of determining comprises the step of choosing the one of the plural service profiles selected by the calling party.

17. The method as in claim 15 wherein the step of determining comprises the step of choosing the one of the plural service profiles dictated by a schedule.

18. The method as in claim 17 further including the step of rejecting the call origination if the schedule indicates that a call black-out period is currently in effect.

19. The method as in claim 15 wherein the step of determining comprises the step of choosing a default one of the plural service profiles.

20. The method as in claim 15 wherein the step of billing comprises the step of generating at least one toll ticket for the call origination that identifies not only the calling party but also the active one of the plural service profiles for that calling party.

21. The method as in claim 15 further including the steps of:

screening a called number for the call origination against a screening list associated with the active one of the plural subscriber profiles; and

permitting the call origination if the step of screening is passed.

22. A method for handling a call delivery in a cellular telephone system, comprising the steps of:

determining if a called party is entitled to utilize a plural service profiles per subscriber service;

if yes, determining which one of the plural service profiles for the called party is currently active;

applying the currently active one of the plural service profiles to the call delivery; and

billing service charges for the call delivery against the currently active service profile.

23. The method as in claim 22 wherein the step of determining comprises the step of choosing the one of the plural service profiles selected by the called party.

24. The method as in claim 22 wherein the step of determining comprises the step of choosing the one of the plural service profiles dictated by a schedule.

25. The method as in claim 22 further including the step of applying diversion in connection with delivery of the call to a particular forward to number based on current called mobile station location.

26. The method as in claim 22 further including the step of applying diversion in connection with delivery of the call to a particular forward to number based on called mobile station status.

27. The method as in claim 22 further including the step of completing the call.

28. An intelligent network implementation for a cellular telephone system, comprising:

an originating switching node receiving a call from a calling party, the originating node detecting whether the calling party is subscripted to a plural service profiles per subscriber service; and

a service switching point/service control point (SSCP) through which the call is routed by the originating switching node if the calling party is subscripted

to the plural service profiles per subscriber service, the service switching point/service control point determining which one of the plural service profiles for the calling party is currently active, and generating a toll ticket for the call to be applied against the currently active service profile for the calling party.

29. The system as in claim 28 further including:

a home location register connected to the originating switching node, the home location register storing information concerning the plural service profiles for the calling party;

wherein the originating switching node determines whether the calling party is subscripted by querying the home location register storing the plural service profiles information.

30. The system as in claim 28 further including a billing center for collecting toll tickets for calls and generating segregated billing of service charges incurred with respect to use of each service profile for the calling party.

31. The system as in claim 28 further including a destination switching node serving a called party for the call, wherein the called party is subscripted to the plural service profiles per subscriber service, and the destination switching node serving the called party in accordance with a currently active one of the plural service profiles for the called party, and generating a toll ticket for the call to be applied against the currently active service profile for the called party.

32. The system as in claim 31 further including:

a visitor location register connected to the destination switching node, the visitor location register storing information concerning the currently active one of the plural service profiles for the called party.

33. An intelligent network implementation for a cellular telephone system, comprising:

an originating switching node receiving a call from a calling party, the originating node detecting whether the calling party is subscripted to a plural service profiles per subscriber service; and

a home location register/service control point (HLR/SCP) connected to the originating switching node, the home location register storing information concerning the plural service profiles for the calling party, the home location

register/service control point further being queried by the originating switching node to detect the calling party subscription to the plural service profiles per subscriber service, the home location register/service control point still further determining which one of the plural service profiles for the calling party is currently active, and generating a toll ticket for the call to be applied against the currently active service profile for the calling party.

34. The system as in claim 33 further including a billing center for collecting toll tickets for calls and generating segregated billing of service charges incurred with respect to use of each service profile for the calling party.

35. The system as in claim 33 further including a destination switching node serving a called party for the call, wherein the called party is subscripted to the plural service profiles per subscriber service, and the destination switching node serving the called party in accordance with a currently active one of the plural service profiles for the called party, and generating a toll ticket for the call to be applied against the currently active service profile for the called party.

36. The system as in claim 35 further including:

a visitor location register connected to the destination switching node, the visitor location register storing information concerning the currently active one of the plural service profiles for the called party.

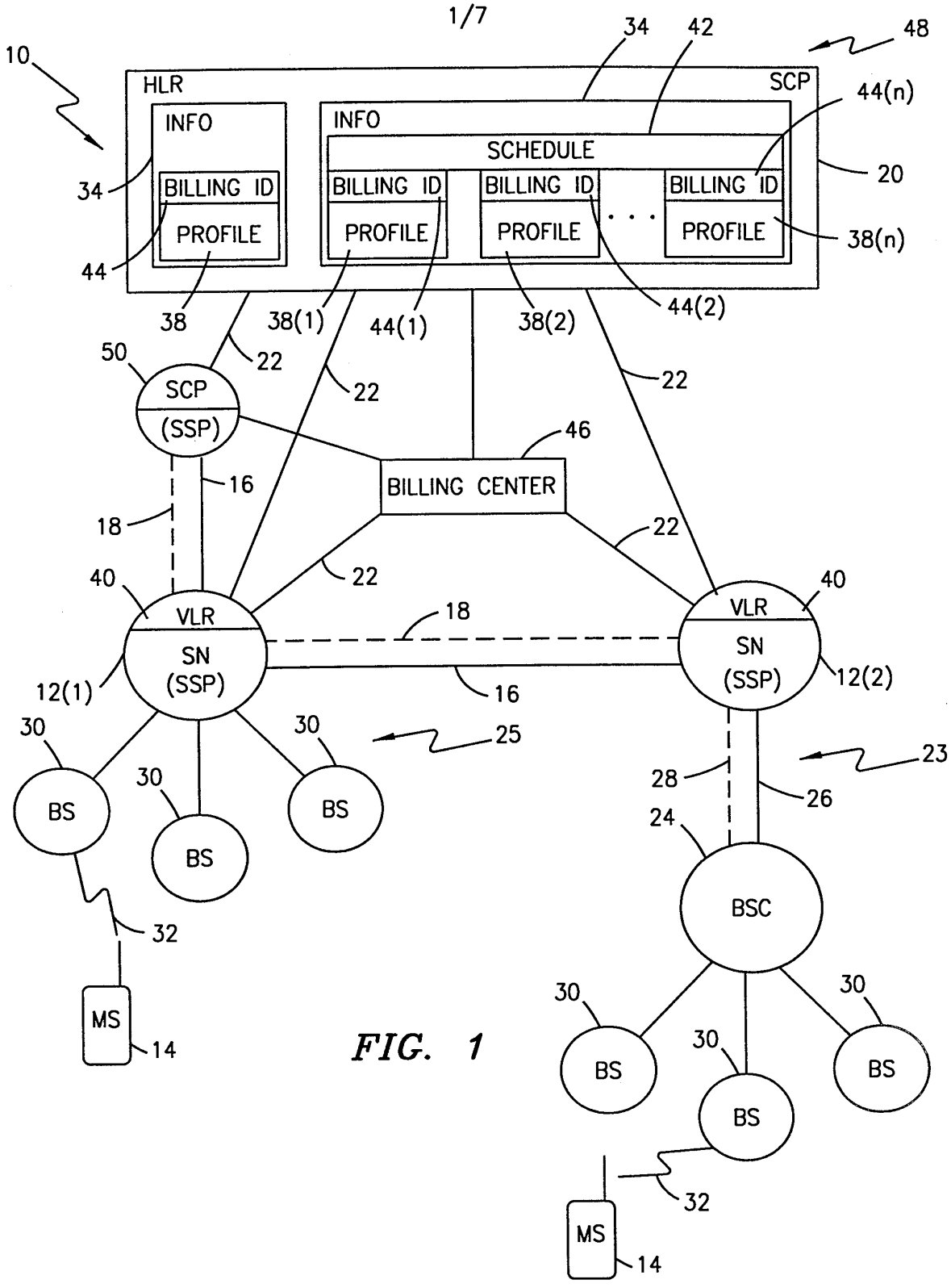

10
HLR
INFO
BILLING ID
PROFILE
34
44
38
SCP
INFO
SCHEDULE
BILLING ID
PROFILE
BILLING ID
PROFILE
BILLING ID
PROFILE
34
42
48
44(n)
20
38(n)
38(1)
44(1)
38(2)
44(2)
22
50
SCP
(SSP)
46
BILLING CENTER
16
18
40
VLR
SN
(SSP)
12(1)
18
40
VLR
SN
(SSP)
12(2)
16
30
BS
30
BS
30
BS
25
23
28
26
24
BSC
32
MS
14
30
BS
30
BS
30
BS
32
MS
14

FIG. 1

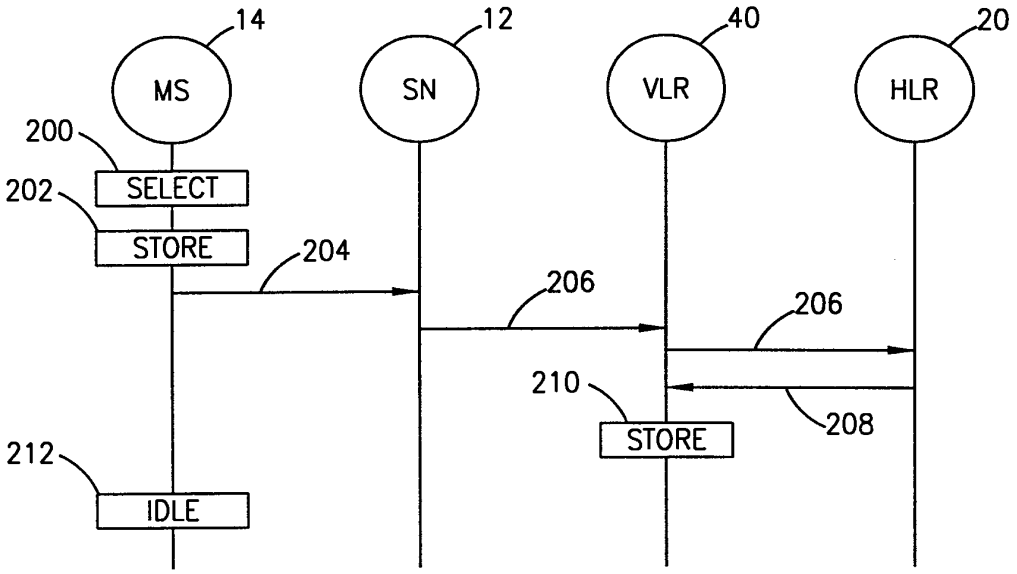

14
12
40
20
MS
SN
VLR
HLR
200
SELECT
202
STORE
204
206
206
210
208
STORE
212
IDLE

FIG. 2

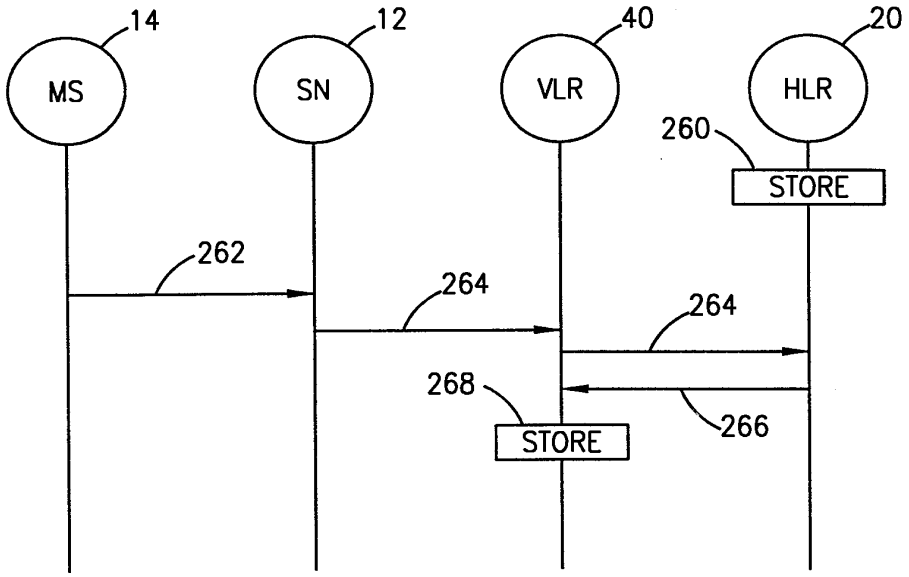

14
12
40
20
MS
SN
VLR
HLR
260
STORE
262
264
264
268
266
STORE

FIG. 4

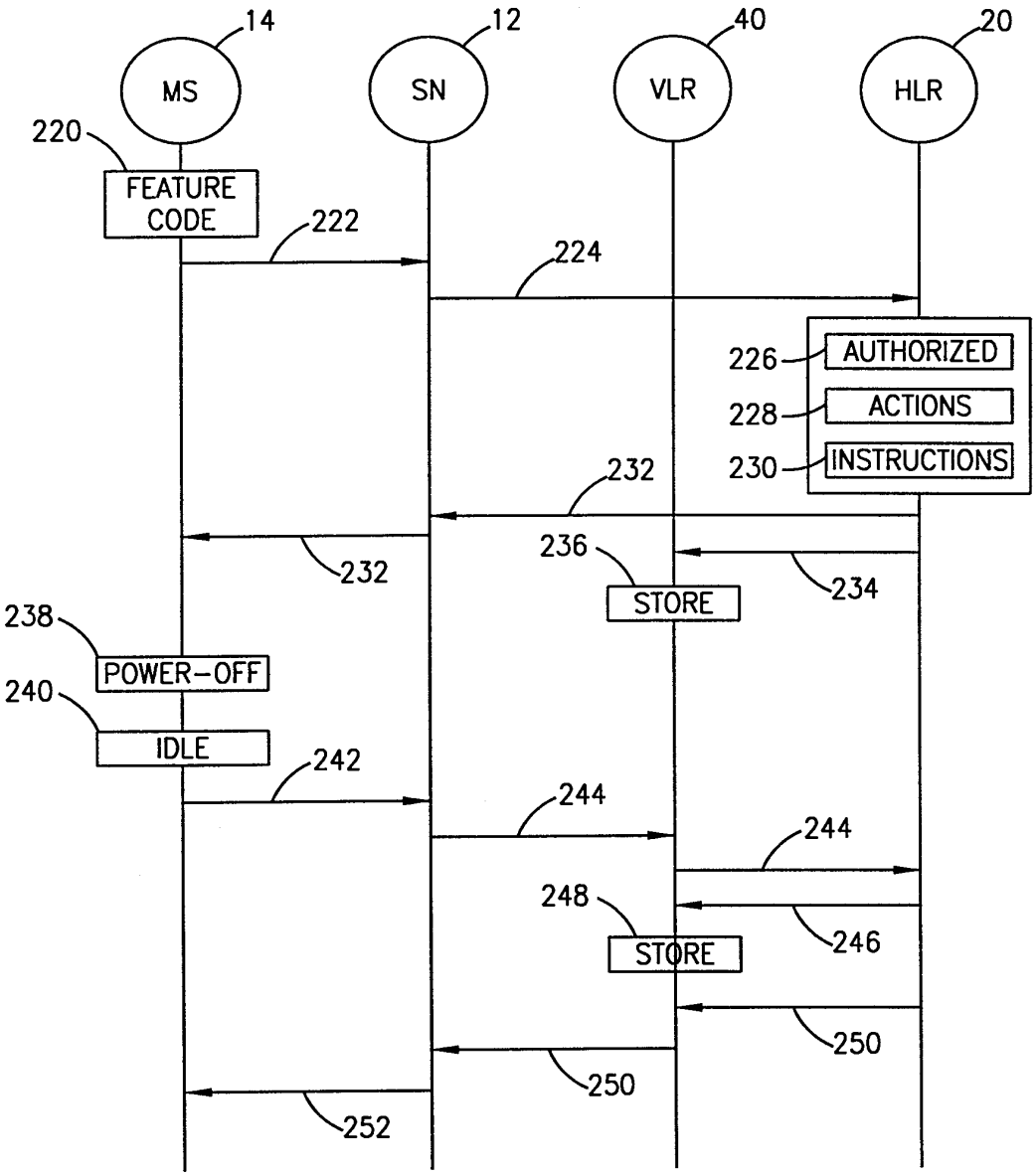

14
MS
12
SN
40
VLR
20
HLR
220
FEATURE CODE
222
224
226
AUTHORIZED
228
ACTIONS
230
INSTRUCTIONS
232
232
236
STORE
234
238
POWER-OFF
240
IDLE
242
244
244
248
STORE
246
250
250
252

FIG. 3

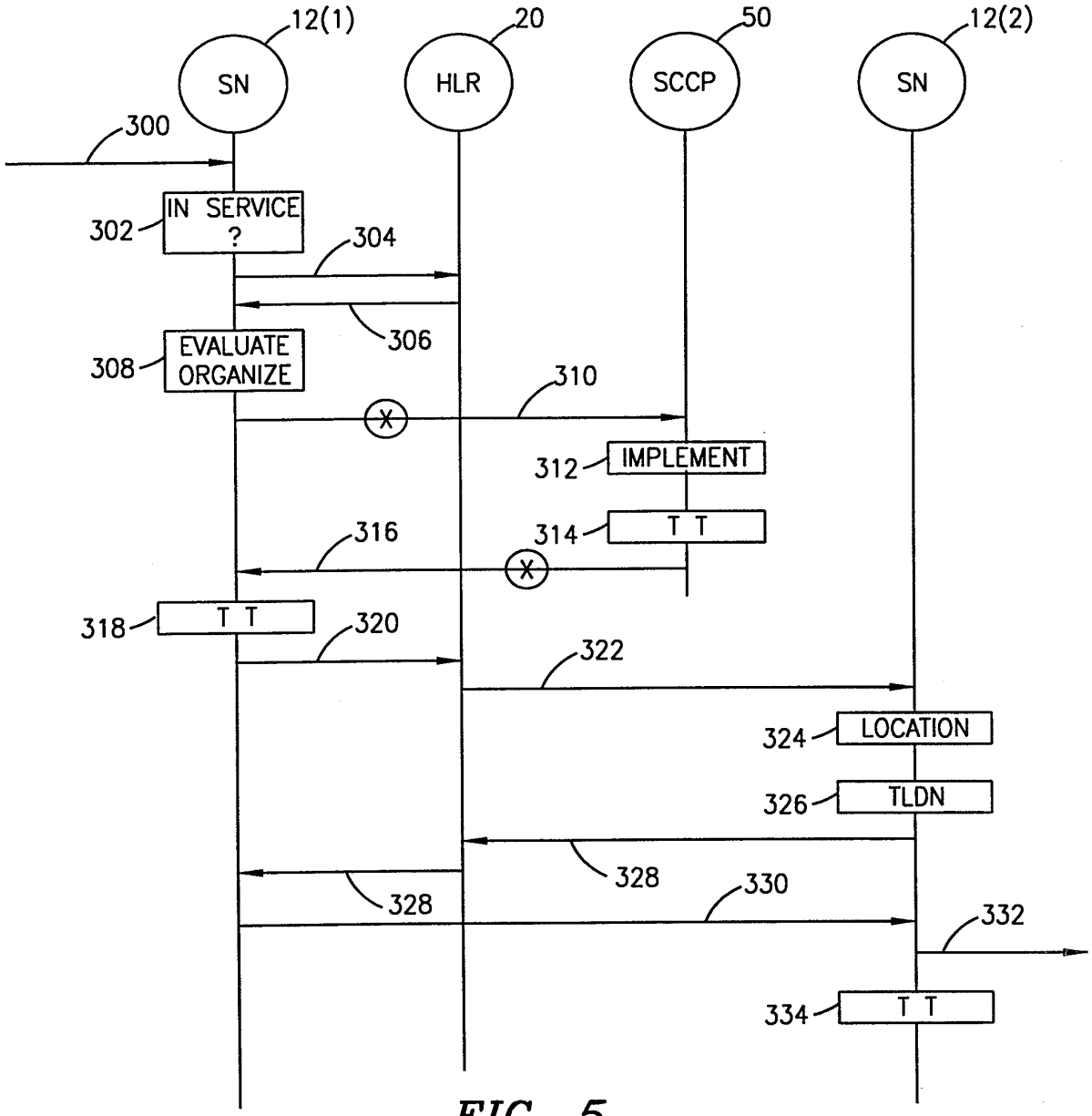

12(1)
SN
20
HLR
50
SCCP
12(2)
SN
300
IN SERVICE ?
302
304
306
EVALUATE ORGANIZE
308
310
IMPLEMENT
312
T T
314
316
T T
318
320
322
LOCATION
324
TLDN
326
328
328
330
332
T T
334

FIG. 5

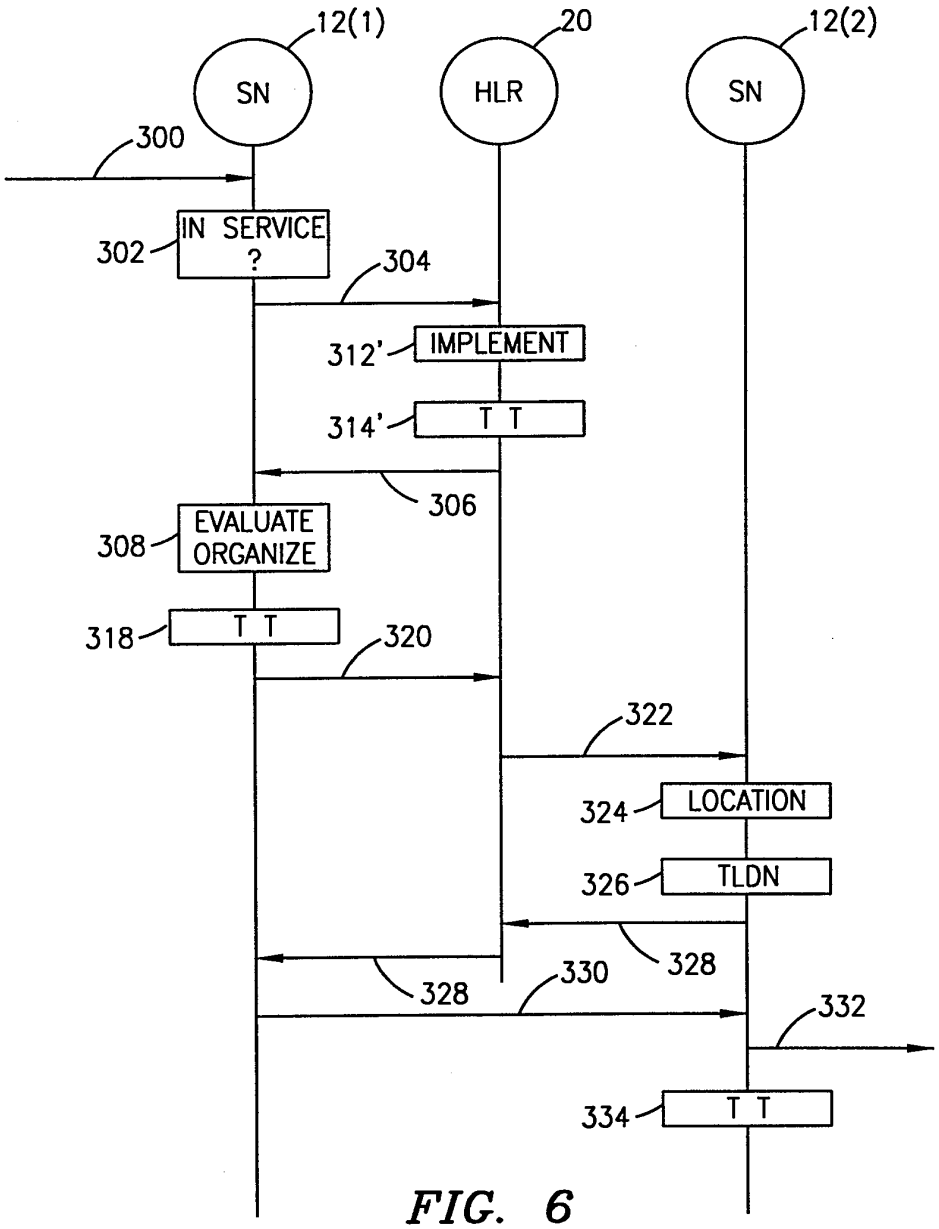

12(1)
SN
20
HLR
12(2)
SN
300
IN SERVICE ?
302
304
312'
IMPLEMENT
314'
T T
306
EVALUATE ORGANIZE
308
318
T T
320
322
324
LOCATION
326
TLDN
328
328
330
332
334
T T

FIG. 6

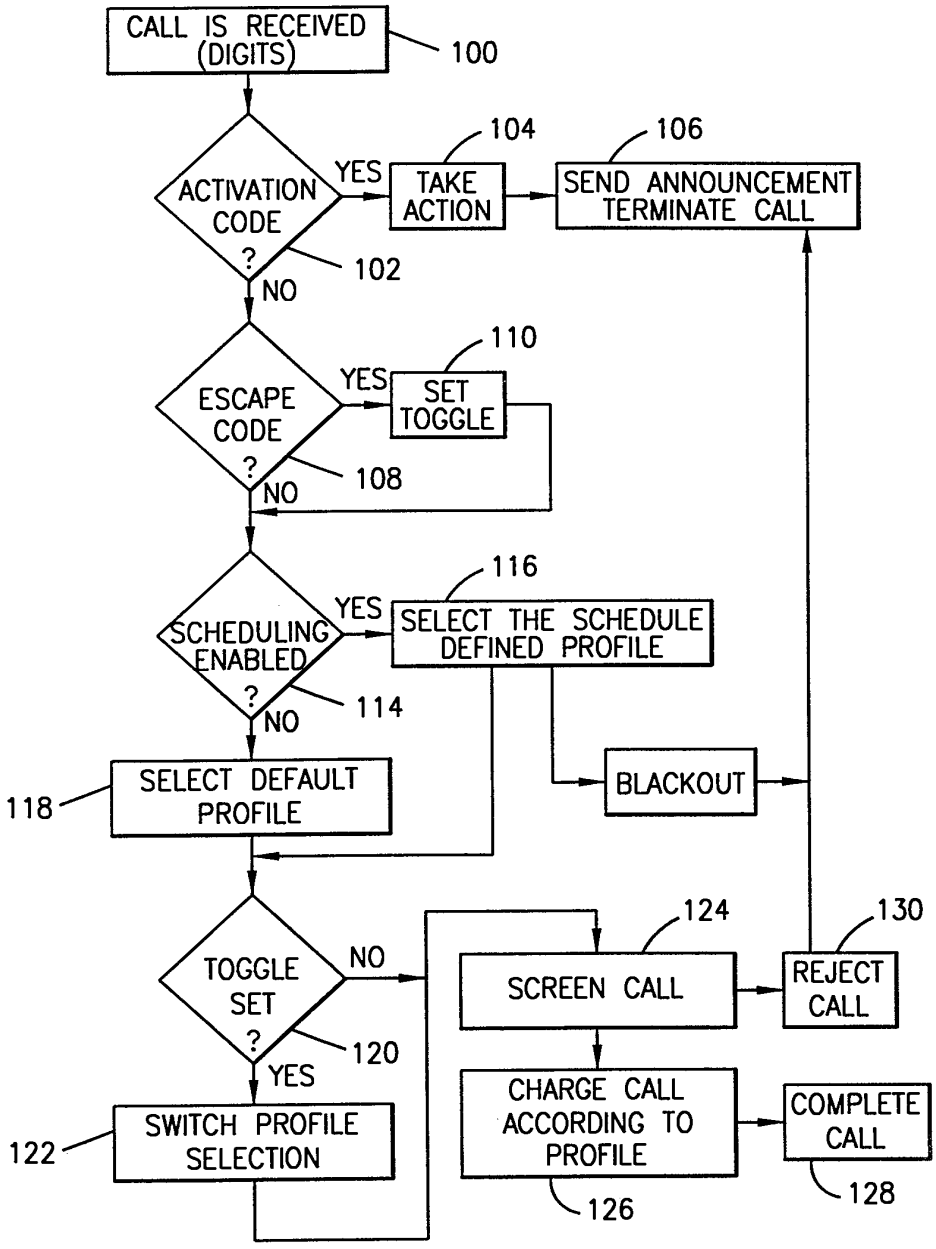

CALL IS RECEIVED (DIGITS)
100
ACTIVATION CODE ?
YES
104
TAKE ACTION
106
SEND ANNOUNCEMENT TERMINATE CALL
102
NO
ESCAPE CODE ?
YES
110
SET TOGGLE
108
NO
SCHEDULING ENABLED ?
YES
116
SELECT THE SCHEDULE DEFINED PROFILE
114
NO
118
SELECT DEFAULT PROFILE
BLACKOUT
TOGGLE SET ?
NO
124
SCREEN CALL
130
REJECT CALL
120
YES
CHARGE CALL ACCORDING TO PROFILE
COMPLETE CALL
122
SWITCH PROFILE SELECTION
126
128

FIG. 7

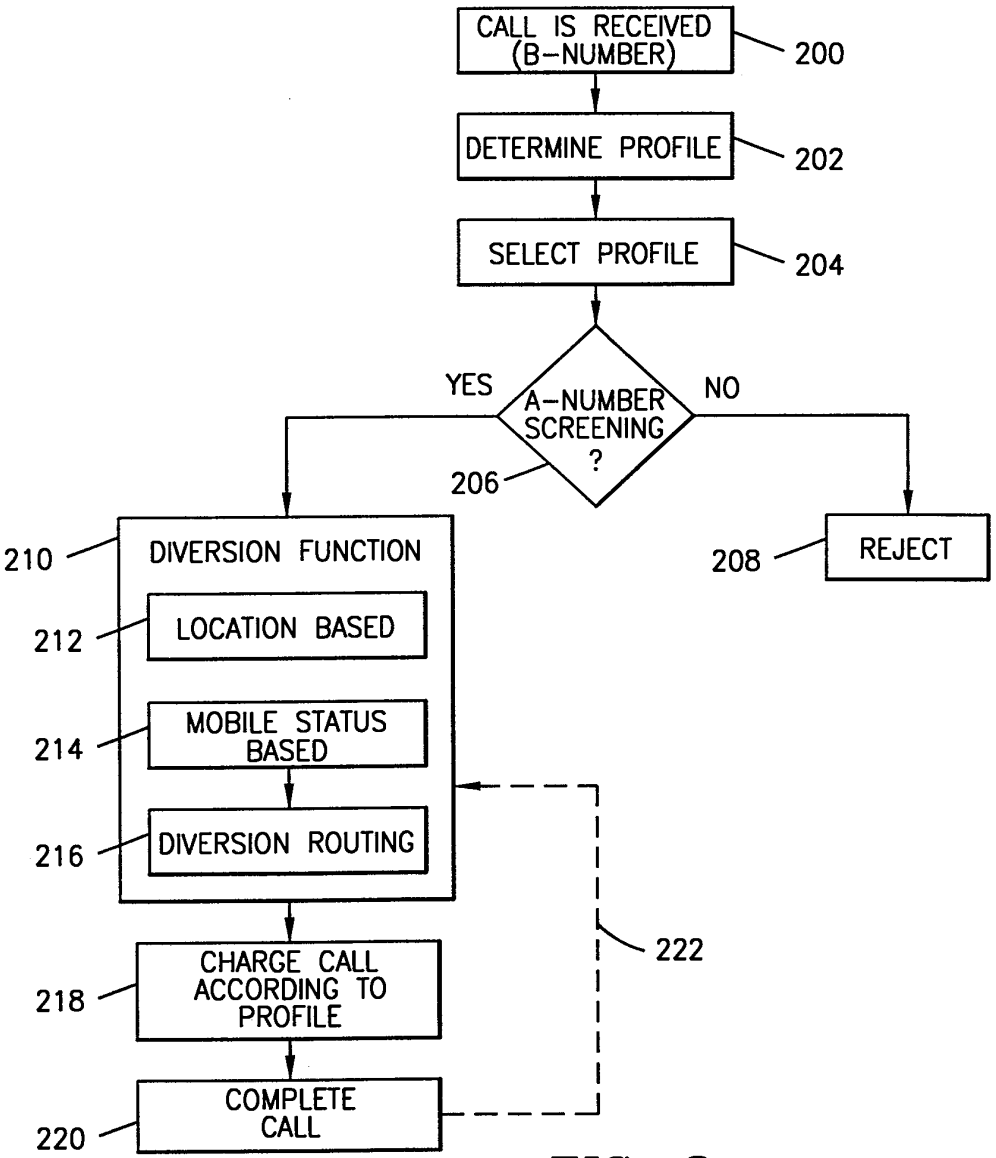

CALL IS RECEIVED (B-NUMBER)
200
DETERMINE PROFILE
202
SELECT PROFILE
204
YES
A-NUMBER SCREENING ?
NO
206
210
DIVERSION FUNCTION
208
REJECT
212
LOCATION BASED
214
MOBILE STATUS BASED
216
DIVERSION ROUTING
222
218
CHARGE CALL ACCORDING TO PROFILE
220
COMPLETE CALL

FIG. 8

INTERNATIONAL SEARCH REPORT

Im tional Application No
PCT/SE 98/02111

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04Q7/22 H04M15/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04Q H04M

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

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5 561 706 A (FENNER PETER R) 1 October 1996	1-3,5,7, 8,12,15, 16, 20-23, 27-36
A	see column 2, line 28 - column 5, line 59	9,10,17, 18

Y	WO 97 30559 A (ERICSSON GE MOBILE INC) 21 August 1997	1-3,5,7, 8,12,15, 16, 20-23, 27-36
A	see page 7, line 14 - page 19, line 4	13,25,26

	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 January 1999	05/02/1999

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

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Int tional Application No
PCT/SE 98/02111

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	SHERBURNE T J ET AL: "TIME ACTIVATED SUBSCRIBER PRIVILEGES" MOTOROLA TECHNICAL DEVELOPMENTS, vol. 25, 1 July 1995, page 59 XP000524341 see the whole document	

1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int ional Application No
PCT/SE 98/02111

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5561706 A	01-10-1996	NONE	
WO 9730559 A	21-08-1997	US 5815808 A	29-09-1998
		AU 2204197 A	02-09-1997
		EP 0882374 A	09-12-1998

Form PCT/ISA/210 (patent family annex) (July 1992)

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 November 2007 (22.11.2007)

PCT

(10) International Publication Number
WO 2007/133844 A2

(51) International Patent Classification:
A61F 15/00 (2006.01)

(21) International Application Number:
PCT/US2007/064164

(22) International Filing Date: 16 March 2007 (16.03.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/783,230 17 March 2006 (17.03.2006) US
60/783,232 17 March 2006 (17.03.2006) US

(71) Applicant *(for all designated States except US)*: **CAMIANT, INC.** [US/US]; 2nd Floor, 200 Nickerson Road, Marlborough, MA 01752 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **RILEY, Yusun, Kim** [US/US]; 630 Hemenway Street, Marlborough, MA 01762 (US).

(74) Agents: **DEMSHER, Ronald, R.** et al.; Wilmer Cutler Pickering Hale and Dorr LLP, 60 State Street, Boston, MA 02109 (US).

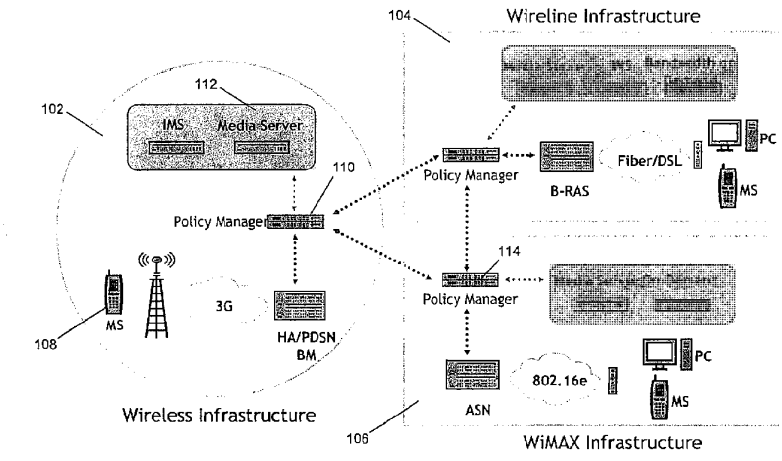
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR,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

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

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: DISTRIBUTED POLICY SERVICES FOR MOBILE AND NOMADIC NETWORKING



(57) Abstract: A method of disseminating topology information related to a subscriber in a system having one or more networks, each network having access devices and policy functions, includes identifying a current location of the subscriber by a serving policy function. The method further includes forwarding information relating to the current location from the serving policy function to an anchor policy function associated with the subscriber. The process of identifying the location of the subscriber and forwarding the information to the anchor policy server is repeated each time the subscriber changes its physical location. The system uses the current location information to route policy information from the anchor policy function to the policy function that is serving the subscriber. The system may use a push model, a pull model, or a combination thereof, to disseminate the topology information.

WO 2007/133844 A2

DISTRIBUTED POLICY SERVICES FOR MOBILE AND NOMADIC NETWORKING

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application claims benefit of the following Patent Applications:
U.S. Provisional Patent Application Serial No. 60/783,232, filed March 17, 2006.
U.S. Provisional Patent Application Serial No. 60/783,230, filed March 17, 2006.

BACKGROUND OF THE INVENTION

[0002] The present invention relates to communication systems and services for distributing digital content, and more particularly, to techniques for properly associating subscribers with appropriate policy servers regardless of the physical location of the subscriber.

[0003] FIG. 1 shows a prior art system 10 for delivering digital content to a number of subscribers. An application function 12 (in this example a P-CSCF; proxy call session control function), provides session setup functions to enable subscribers to make VoIP calls, or can also be a server, which serves digital content such as a video stream to one of several subscribers 14. The subscribers may include any of a number of electronic devices such as telephones or personal computers. These electronic devices may be wireless or they may be connected to a local wired network.

[0004] During a session, the digital content the application server 12 provides to a subscriber 14 may pass through a number of network components. The content passes through enforcement points(s), but the signaling to request policy is signaled between the policy elements in the diagram – the policy router 16 and the policy server 18 as well as the enforcement point.

[0005] The enforcement point 20 is an edge device, such as a cable modem termination system (CMTS), GPRS gateway support node (GGSN), a packet data serving node (PDSN), etc. In general, an enforcement point can be any entity in the network through which packets traverse during the subscriber's session. The enforcement points

20 are not dedicated to any particular application server 12, but instead resources on the enforcement points are allocated to the subscriber's application session by the policy function (e.g., the policy server 18 in this example) in the network.

[0006] "Policy function" is used as the generic term for an entity in the network that is performing policy. The primary purpose of the policy function is providing the appropriate Quality of Service for the session, as well as managing any billing and accounting information associated with the session. The policy function is responsible for conveying or "pushing" a policy decision to the enforcement point 20, and making sure the correct set of policies for the subscriber is set. The policy function thus controls the enforcement point 20 via on behalf of the application server 12.

[0007] The policy router 16 in the above diagram is a policy function that also can route or forward policy requests to a downstream policy function. In the example of FIG. 1, the application server 12 conveys a policy request to the policy server 20 via the policy router 16.

[0008] In general, FIG. 1 shows a service provider policy environment supporting multiple applications, multiple subscribers and multiple subscriber edge devices. The subscriber edge devices 20 function as policy enforcement points for operator policies relating to Quality of Service, Bandwidth Management, and Admission Control.

SUMMARY OF THE INVENTION

[0009] The following are some key goals of the policy environment provided by the described embodiments:

- Applications should not require knowledge of the network topology or technology. The policy servers in the network should take care of the topology abstraction so applications can remain topology unaware.
- The policy environment should scale to countrywide deployments.
- The actual network topology should be dynamic. Network subscribers, policy servers, enforcement points, and their interconnections can be added, changed, or

deleted. Administrative provisioning may be minimized

- Subscribers should be able to access applications from different networks and different service providers. This type of roaming behavior means the enforcement points associated with the subscriber could change over time. Also, a subscriber could potentially access services and applications from different networks and providers, potentially at the same time.
- Network subscribers should be able to access the network from different subscriber edge devices at different times (i.e., the subscribers are nomadic) or move between one subscriber edge device and another during the same session (i.e., the subscribers are mobile).
- Regardless of where the subscriber is attaching from, the subscriber should be provided with the consistent set of policies. Policy governs the following types of attributes of a subscriber's service:
    - the subscribers' entitlements (i.e., what services and content they can and cannot access.
    - the quality of service for a subscriber – how good of a user experience for a service, or how much bandwidth a subscriber is allowed to get for any service
    - what the subscriber should be charged for a particular service or application
- In order for the customer to be provided with a consistent set of policies, there should be a mechanism by which the policy function in the network responsible for controlling the enforcement points (typically, this is referred to as the 'visited' network), be able to communicate with the 'home' policy function, which contains all the information about the subscriber's policies.

[0010] In one aspect, the invention is a method of disseminating topology information related to a subscriber in a system having one or more networks, each network having access devices and policy functions. The method includes identifying a current location of the subscriber by a serving policy function. The method further includes forwarding information relating to the current location from the serving policy

function to an anchor policy function associated with the subscriber.

[0011] One embodiment further includes performing the identifying step and the forwarding step each time the subscriber moves to a different serving policy function. Another embodiment further includes using the information related to the current location of the subscriber to route policy information related to the subscriber from the anchor policy function to the serving policy function.

[0012] One embodiment further includes further includes routing policy information related to the subscriber and requests for the policy information by implementing a push model. Another embodiment further includes routing policy information related to the subscriber and requests for the policy information by implementing a pull model.

[0013] One embodiment further includes maintaining, with the anchor policy function, state information associated with the subscriber, and executing policy rules according to the state information.

[0014] In another embodiment, the serving policy function and the anchor policy function are located in different service provider networks, such that the step of forwarding information relating to the current location further includes conveying the information relating to the current location across at least one service provider network boundaries.

[0015] One embodiment further includes the serving policy function implementing one or more resource level policy rules to limit or control policy decisions associated with the subscriber, based upon resource consumption in the network for which the serving policy server oversees resource control.

[0016] Yet another embodiment further includes decoupling the serving policy function from the anchor policy function. One embodiment further includes disseminating the information relating to the current location of the subscriber to one or more other policy functions in the system.

[0017] Another aspect is a system for disseminating topology information related to a subscriber in a network having one or more sub-networks, each sub-network having access devices and policy functions. The system includes a serving policy function for identifying a current location of the subscriber, and an anchor policy function associated with the subscriber for receiving information relating to the current location from the serving policy function.

[0018] In one embodiment, each time the subscriber moves to a different serving policy function, the different serving policy function identifies the current location of the subscriber and forwards the current location to the anchor policy function.

[0019] In another embodiment, the network routes policy information related to the subscriber from the anchor policy function to the serving policy function using the information related to the current location of the subscriber.

[0020] In one embodiment, the network routes policy information related to the subscriber and requests for the policy information by implementing a push model. In another embodiment, the network routes policy information related to the subscriber and requests for the policy information, by implementing a pull model.

[0021] In one embodiment, the anchor policy function maintains state information associated with the subscriber, and executes policy rules according to the state information. In another embodiment, the serving policy function and the anchor policy function are located in different service provider networks, such that the information relating to the current location is conveyed across at least one service provider network boundaries.

[0022] In another embodiment, the serving policy function implements one or more resource level policy rules to limit or control policy decisions associated with the subscriber, based upon resource consumption in the sub-network for which the serving policy server oversees resource control.

[0023] In one embodiment, the serving policy function is decoupled from the

anchor policy function.

[0024] Another embodiment further includes one or more other policy functions in the network. The information relating to the current location of the subscriber is disseminated to the one or more other policy functions.

BRIEF DESCRIPTION OF DRAWINGS

[0025] FIG. 1 shows a prior art system 10 for delivering digital content to a number of subscribers.

[0026] FIG. 2 shows an exemplary embodiment of a system architecture constructed and arranged according to the invention.

[0027] FIGs. 3 and 4 show the serving PS 150 forwarding registration information to the designated policy router

[0028] FIGs. 5 and 6 illustrate the routing of policy requests from the policy router, to the anchor, then to the serving PS.

[0029] FIG. 7 illustrates an embodiment in which the location of the application function resides in the same network as the anchor PS.

[0030] FIG. 8 is an exemplary message flow for one embodiment of the system shown in FIG. 2.

[0031] FIG. 9 illustrates a 'Pulling' model for disseminating policies.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0032] FIG. 2 shows an exemplary embodiment of a system architecture constructed and arranged according to the invention. The exemplary system shown in FIG. 2 includes a wireless network 102, a wireline network 104 and a WiMAX (i.e., IEEE 802.16) network 106.

[0033] In the wireless network 102, a subscriber 108 uses a mobile device (MS) to

access the wireless network 102. The subscriber 108 subscribes to a particular access provider, for example Sprint®. The subscriber's policy function 110 is located within the Sprint wireless network 102.

[0034] Consider the situation in which the subscriber 108 "roams" to another access provider's network. In this example, the Sprint network 102 is considered the subscriber's "home network." The policy function 110 in the sprint network (a policy manager in this example) is the subscriber's "home policy function" – or the "anchor policy function."

[0035] Suppose the subscriber roams to an access provider that supports a different type of network, for example a WiMAX wireless network 106. Once the subscriber 108 is connected into the WiMAX network, the subscriber may want to access applications 112 that are located in its home network (i.e., the Sprint network 102). To accomplish this, the policies of the subscriber 108 that reside in the home policy function 110 need to ultimately be implemented in the network in which the subscriber is visiting (i.e., the WiMAX network 106).

[0036] However, the home/anchor policy function 110 from the wireless network 102 does not and cannot directly control the WiMAX network 106 (i.e., the network into which the subscriber has roamed). For a variety of security reasons, a network provider typically does not allow an outside entity to directly control its network equipment for policy enforcement. Therefore, the home/anchor policy function must communicate and coordinate with the "visited" policy function, in this example the policy manager 114 in the WiMAX network 106, to allocate the necessary network assets. This visited policy function is also referred to herein as the "serving" policy function, because it is the policy function responsible for serving the subscriber in the visited network.

[0037] The described embodiments include techniques and mechanisms that fulfill the following objectives:

1. Associate a given subscriber with a particular policy server, even when the subscriber accesses the network in a mobile or nomadic fashion. The subscriber can therefore be associated with the appropriate visited policy function, and the

correct home/anchor policy function

2. Free an application from determining which policy server is responsible for determining the policy for accessing a given application, even when the subscriber accesses the network in a mobile or nomadic fashion
3. Allow a policy server to map application addressing (typically the 5-tuple IP source address, IP destination address, source port, destination port, and protocol), as well as other the subscriber identifiers such as MAC addresses or email ID (Invariant Subscriber Identifier or ISI), to the network edge device currently supporting a particular subscriber.

[0038] Each subscriber station in the access network is associated with an invariant subscriber identifier (ISI) dependant on the particular access technologies that the subscriber uses. Examples of an ISI include an Electronic Serial Number, a phone number, a Mobile Station Integrated Services Digital Network number (MS-ISDN), an International Mobile Subscriber Identifier, an Ethernet Media Access Control (MAC) address, among others. Unlike an IP address range that can change each time the subscriber accesses the network from a different access device, the ISI is associated with the subscriber and doesn't change from access to access, or when the subscriber accesses the network via a different subscriber access device. The extent to which (i) the ISI number codes the "typical" location from which the subscriber accesses the network, and (ii) sequential identifiers are likely provisioned from the same location, can make the mapping operation more efficient, but is not specifically required by the embodiments describe herein.

[0039] A Policy Server (hereinafter "PS") can "learn" or be provisioned with information identifying which ISIs they typically serve. In this way a particular PS becomes the "anchor" PS for a given set of subscribers. Being the "anchor" PS means that PS will always be the ultimate policy decision maker for the associated subscriber, regardless of where the subscriber may be currently accessing the network.

STATEFULNESS

[0040] The anchor PS for a particular subscriber is stateful of the subscriber. Being

"stateful" means that whenever the subscriber is on the network, the anchor PS is aware of (i.e., has information regarding) the state of the subscriber, in terms of which applications requiring policy the subscriber has invoked. Even when the subscriber moves across the network, for example to another region of the network that has its own policy server, policy requests ultimately need to interact with the anchor PS for that subscriber. Because the anchor PS is aware of the subscriber, it can make policy decisions based on subscriber-centric parameters (i.e., parameters specific to that subscriber). For example, the anchor PS can execute policy rules that determine what a subscriber may or may not do, based on who he is, what tier or packages of service he has purchased or is entitled to, and how many of such application sessions he may be allowed, among others.

[0041] Although the anchor PS is stateful of the subscriber and its policy parameters, the anchor PS may not have information regarding what network resources the subscriber is utilizing. This is because the anchor PS may not be the serving PS, if the subscriber is roaming, as an example. The anchor PS is in the home network, and if the subscriber is in a location that is being served by another PS (visited PS or serving PS because the subscriber has roamed into another part of the network or to another provider), then it is only the visited or serving PS that is aware of the network resources the subscriber is utilizing. As a result, the serving or visited PS can be in charge of network resource-centric policies (i.e., policies specific to those network resources). The visited or serving PS can execute the policy rules that focus on setting thresholds for resource consumption. Because the serving PS is the one interfacing with the enforcement points, and it is aware of all the sessions that are being admitted over the enforcement points it controls, it is aware of the resources that are being utilized. As a result, the serving PS can enforce policy rules that control the amount of resources (e.g., bandwidth, or number of sessions) that can be admitted over the enforcement points.

[0042] The anchor PS is therefore responsible for executing subscriber-centric policies, and the visited or serving PS is responsible for executing resource-centric policies. An anchor policy server that is stateful of the subscriber's sessions can implement subscriber-aware policy rules to control what a subscriber is entitled to do.

For example, the anchor PS can deny a third session if the subscriber already has two simultaneous sessions running. Or, the anchor PS can deny a request for video if the subscriber currently has a voice application running. For the same scenario, the anchor PS could allow the request for video if the subscriber is in an elite (i.e., "gold") service tier, even when the voice application is already running.

PERCOLATION OF TOPOLOGY THROUGH THE NETWORK

[0043] Each time a subscriber registers onto the network, information about the subscriber's point of attachment (i.e., topology) must be percolated through the relevant policy functions in the network. This ensures that for roaming subscribers, the correct set of policy functions will participate in the policy activity when applications are invoked. The result is that subscriber-centric policies, as well as resource-centric policies, are properly executed and enforced.

[0044] There are several ways in which this topology information can be disseminated. As shown the diagrams of FIGs. 3 and 4, the serving policy server 150 can forward registration information 152 to the designated policy router 154 in the network (this designation information can be provisioned on the serving policy server, or it can be algorithmically derived by the serving policy server).

[0045] The policy router can then be responsible for forwarding the registration information to the anchor PS designated for the subscriber. The policy router can gain information regarding which anchor PS is designated for a particular subscriber in a number of different ways, for example:

- The policy router can be provisioned with the information;
- The policy router can retrieve the information via an external database lookup;
- The policy router can algorithmically derive the information (for example, based on the telephone number of the device the subscriber is using, use the area code to locate the anchor); or,
- The anchor PS can percolate the topology information to the policy router.

[0046] Once the policy router forwards the registration information to the designated anchor PS, both the policy router and the anchor PS know which serving or visited PS is currently associated with the subscriber. If the subscriber physically moves, a new serving PS may be associated with the subscriber. When this happens, the registration process happens all over again and the anchor and the policy router will "discover" or "learn" the new association as described above.

[0047] Alternatively, the serving PS may use similar mechanisms as above to send the topology information to the anchor PS as well. For example, when the subscriber registers, the serving PS can use the realm information in the registration to determine which anchor policy server should receive the registration/topology information.

REGISTRATION AND TOPOLOGY LEARNING

[0048] Subscribers access the network via subscriber access equipment such as a Cable Modem Termination System (CMTS), Packet Data Serving Node (PDSN), Gateway GPRS Serving Node (GGSN) or Broadband Remote Access Server (B-RAS) device that will typically assign a dynamic IP networking address to the subscriber station. A PS provides the Policy Decision Function (PDF – determines the rules for Quality of Service, admission control, and packet processing disciplines, and how the particular session should be charged) for application data streams flowing from network applications to the subscriber through subscriber access equipment.

[0049] Once the subscriber registers onto the network, the subscriber may invoke applications through signaling with the application function. The application function may reside in a centralized location, and the application function is unaware of the physical location of the subscriber with respect to the network.

[0050] When a subscriber initiates a request for a session from an application server, the application function/server issues a request to the PS for a policy decision, which ultimately decides the policies (QoS treatment and the charging rules associated with the particular session as well as potentially entitlements). The PS evaluates the request against the rules that have been provisioned on the PS (rules can be based on information such as subscriber tier, time of day, network usage) and pushes down the

policy decision (QoS policy decision as well as charging) down to the subscriber access equipment, i.e., the enforcement point.

[0051] As the network gets larger, it is usually desirable to partition the PDF across multiple PSs, each signaling a set of subscriber access equipment. A policy router allows applications to have a single point of contact for policy decisions across the network and frees applications from knowledge of the network topology or subscriber location. The policy router maintains the knowledge of which subscriber access device is serving the subscriber and which PSs (serving and anchor) may implement policy decisions related to the subscriber.

[0052] In a mobile network, when a subscriber first accesses the system, the subscriber access equipment signals the network IP address and the ISI to its associated PS. In non-mobile networks, the PS may learn of the subscriber association through other means, including SNMP, or through provisioning. The PS will learn the association of the subscriber to the enforcement point relationship and provide the information to the policy router. The policy router can now use the information to perform its policy routing function – which is when an application issues a request to the policy router, it can now figure out which PS to route the request to based on either the subscriber IP address or the ISI.

[0053] PSs can also be provisioned to be the 'anchor' PS for a particular subscriber, so that no matter where the subscriber is physically located (the subscriber could move between different enforcement points), the policy requests are always routed to the anchor PS. It is then the responsibility of the anchor PS to route the request to the serving PS responsible for serving the particular enforcement point with which the subscriber is now associated. The policy router can use the ISI to route the request to the anchor PS, and the anchor PS can use either the ISI or the subscriber IP address in order to route to the serving PS.

[0054] This anchoring technique is useful when there is a distribution of policy functions in the network due to scalability, as well as when subscribers are roaming between networks or network providers.

[0055] FIGs. 5 and 6 illustrate the routing of policy requests from the policy router, to the anchor, then to the serving PS. Each PS can route appropriately based on the topology information learned during the registration process.

[0056] In one embodiment the application function, and the policy router, reside in a third party network or application provider's domain. In another embodiment, all policy components reside in different networks or provider domains.

[0057] In the scenario described above, the subscriber accesses an application that is located at a centralized part of the network. The application function issues the policy request to its default PS – which in this case is the policy router. The policy router is then responsible for forwarding the policy request to the relevant anchor PS in order for the anchor PS to execute subscriber centric policies. The anchor PS executes its relevant policy rules, and then forwards the request onto the serving PS.

PUSH MODEL

[0058] The policy interactions described so far implement a "push" model for policy distribution; the application function 'pushes' the request to the policy router, the policy router 'pushes' the request onto the anchor PS, and the anchor 'pushes' the request to the serving PS.

[0059] The topology learning process is critical in being able to implement the push model for policy. When a subscriber accesses an application that requires QoS, the application will signal the request to the policy router. The policy router may evaluate certain global or application specific policy rules before looking up the anchor PS for the subscriber and forwarding the QoS request to that anchor PS for evaluation. The policy router and the anchor PS could be in the subscriber's 'home network' domain (e.g., if this is a Sprint subscriber, and the subscriber is accessing a Sprint service from another network, the application, the policy router and the anchor PS involved in the transaction would all be within Sprint's domain).

[0060] The anchor PS evaluates the QoS request with respect to subscriber policy

rules (referred to herein as subscriber-centric rules – e.g., how many sessions the particular subscriber is allowed to have concurrently, or what applications and services is the subscriber entitled to, or has the subscriber exceeded some usage limit, for example). If the QoS request is evaluated as being acceptable, the anchor PS sends the request to the 'serving' PS interfacing to the subscriber access device currently serving the subscriber.

[0061] If required, the anchor PS may also evaluate the QoS request based on administrative policy rules (for example, if the subscriber was roaming in another administrative domain). Ultimately the serving PS will send the QoS directive to the subscriber access equipment to implement the QoS for the subscriber. The serving PS may reside in a visited network. The serving PS will execute policy rules around resource usage – controlling the amount of resources that are consumed on the access network.

[0062] For example, the serving PS can deny a subscriber's request for resources if the total bandwidth consumed on the access network over which the subscriber is receiving service (under the domain of the visited/serving policy server) exceeds some predetermined threshold X. Another example – the serving PS can deny a video request from a subscriber if the bandwidth consumed for all video applications over a particular enforcement point (under the control of the serving/visited policy server) exceeds some predetermined threshold Y. Or, the serving PS can deny the above request for video the total number of voice sessions currently being delivered over a particular enforcement point exceeds another predetermined threshold Z.

[0063] Alternatively, the application function could also reside in the same domain/network as the anchor PS, in which case the application function will signal directly to the anchor PS and treat the anchor as the application function's default PS. The anchor PS performs both the policy routing functions (because it is routing to the serving PS) as well as the PS responsible for executing the subscriber-centric policy rules. The anchor policy server is also directly interfacing to the application function.

[0064] FIG. 7 illustrates an embodiment in which the location of the application function resides in the same network as the anchor PS, and thus using the anchor PS as the application function's default PS.

[0065] In the system shown in FIG. 7, the subscriber's serving PS may be in a visited network (e.g., Telus), but the subscriber is a Verizon customer and his anchor policy server is in the Verizon network, along with the applications the subscriber wishes to access. In some embodiments, networks operated by different commercial entities cooperate through what is referred to herein as "policy peering." Using the roaming information associated with the subscriber, the serving and anchor policy servers can implement policy inter-operator service level agreements (SLAs) and other business agreements.

[0066] An application request can originate from a subscriber physically located in a network or provider different from that in which the anchor PS resides. The policy request is ultimately forwarded onto the serving or visited PS. In this scenario, the visited PS can be used to limit what the third party application can request of the visited network. For example, based on the agreed-to business arrangement between two parties (the access network provider and the content provider) the visited policy server can keep track of what has been admitted into the network for content/applications invoked by the third party content/application provider

[0067] Depending on the scale of the deployment, the logical policy functions (such as routing, anchor, serving, etc.) can be co-located to reduce complexity of the architecture.

[0068] In the wireless world, when the subscriber de-registers from the subscriber access equipment, a de-registration message is sent to the serving PS, which is forwarded to the policy router. FIG. 8 is an exemplary message flow for one embodiment. The policy router forwards the de-registration event to the anchor PS to indicate that the subscriber is no longer accessible on the network or associated with a serving PS. Alternatively, the de-registration message can be directly forwarded from the serving PS to the anchor PS as well.

[0069] Generally a subscriber will be associated with a particular anchor PS, and this relationship should be persistent in most instances. However, there may be cases where the subscriber's anchor PS changes over time. Periodically, based on an

administratively set timer, the policy router and the anchor PS may flush the ISI from the range of served ISI. This may be done in case there is a more efficient PS that could serve the subscriber based on the subscriber access equipment typically used.

PULL MODEL

[0070] Another method of policy distribution is implemented via the 'pull' model. In the pull model, the client/subscriber invokes a policy request directly, instead of the request coming from the application function. The client may use messaging like RSVP to trigger a request from the access equipment (enforcement point). The access equipment may initiate a policy request from its designated serving PS. The serving policy server may need to retrieve the correct set of policies for the subscriber from the anchor PS. Using the same type of mechanisms that were used during the topology discovery/distribution phase, the serving PS could 'pull' for the correct set of policies from the anchor PS. It is likely that in large-scale deployments, both push and pull models are implemented in the network.

[0071] FIG. 9 illustrates a 'Pulling' model for disseminating policies, in which the subscriber triggers a policy request. The Access network equipment could pull for policies from the Serving PS. The serving PS, using the same type of methods that it used for the distribution of topology information, can pull for the policy for the subscriber from the anchor PS. The types of policies that can be pulled include subscriber entitlements (what services/applications is the subscriber entitled to have access to), QoS treatment for any one of the services, how the services should be billed (flat rate billing, or per byte billing, or time based billing, etc).

[0072] When the subscriber first registers onto the network, the serving PS is aware of whether the subscriber is roaming or not. The anchor PS is also aware of the subscriber's roaming status. Roaming information can be inferred from messaging from the access network equipment when the subscriber first attaches to the network. The subscriber's realm information that is present in the initial attachment message can provide information about the subscriber. For example, the subscriber may be a Verizon wireless subscriber roaming into the Telus network. The information from the

subscriber/client will indicate that he is a Verizon wireless subscriber. The serving PS uses this information to determine which anchor PS or policy router should receive the topology information (in a push from the serving PS) and provide policy information (in a pull by the serving PS).

[0073] Various policy servers can also use the subscriber's realm information to execute policy rules against the subscriber. For example, the serving PS in the Telus network may have rules, which provide a different level of treatment if the subscriber is a Verizon subscriber, as opposed to a subscriber of some other service provider. If there are service level agreements or business agreements put in place between Telus and Verizon, the Telus serving PS may be used to implement those business rules, such as providing enhanced QoS for voice, video or data services. In some embodiments, the realm information is also used to provide differential billing, in which a subscriber is billed differently for the various applications as a function of the particular realm.

[0074] The invention may be embodied in other specific forms without departing from the spirit or essential characteristics thereof. The present embodiments are therefore to be considered in respects as illustrative and not restrictive, the scope of the invention being indicated by the appended claims rather than by the foregoing description, and all changes which come within the meaning and range of the equivalency of the claims are therefore intended to be embraced therein.

What is claimed is:

1. A method of disseminating topology information related to a subscriber in a system having one or more networks, each network having access devices and policy functions, comprising:

identifying a current location of the subscriber by a serving policy function; and,

forwarding information relating to the current location from the serving policy function to an anchor policy function associated with the subscriber

2. The method of claim 1, further including performing the identifying step and the forwarding step each time the subscriber moves to a different serving policy function.

3. The method of claim 1, further including using the information related to the current location of the subscriber to route policy information related to the subscriber from the anchor policy function to the serving policy function.

4. The method of claim 1, further including routing policy information related to the subscriber and requests for the policy information by implementing a push model.

5. The method of claim 1, further including routing policy information related to the subscriber and requests for the policy information by implementing a pull model.

6. The method of claim 1, further including maintaining, by the anchor policy function, state information associated with the subscriber, and executing policy rules according to the state information.

7. The method of claim 1, wherein the serving policy function and the anchor policy function are located in different service provider networks, such that the step of forwarding information relating to the current location further includes conveying the information relating to the current location across at least one service provider network boundaries.

8. The method of claim 1, further including the serving policy function implementing one or more resource level policy rules to limit or control policy decisions associated with the subscriber, based upon resource consumption in the network for which the serving policy server oversees resource control.

9. The method of claim 1, further including decoupling the serving policy function from the anchor policy function.

10. The method of claim 1, further including disseminating the information relating to the current location of the subscriber to one or more other policy functions in the system.

11. A system for disseminating topology information related to a subscriber in a network having one or more sub-networks, each sub-network having access devices and policy functions, comprising:

a serving policy function for identifying a current location of the subscriber; and,

an anchor policy function associated with the subscriber for receiving information relating to the current location from the serving policy function.

12. The system of claim 11, wherein each time the subscriber moves to a different serving policy function, the different serving policy function identifies the current location of the subscriber and forwards the current location to the anchor policy function.

13. The system of claim 11, wherein the network routes policy information related to the subscriber from the anchor policy function to the serving policy function using the information related to the current location of the subscriber.

14. The system of claim 11, wherein the network routes policy information related to the subscriber and requests for the policy information, by implementing a push model.

15. The system of claim 11, wherein the network routes policy information related to the subscriber and requests for the policy information, by implementing a pull model.

16. The system of claim 11, wherein the anchor policy function maintains state information associated with the subscriber, and executes policy rules according to the state information.

17. The system of claim 11, wherein the serving policy function and the anchor policy function are located in different service provider networks, such that the information relating to the current location is conveyed across at least one service provider network boundaries.

18. The system of claim 11, wherein the serving policy function implements one or more resource level policy rules to limit or control policy decisions associated with the subscriber, based upon resource consumption in the sub-network for which the serving policy server oversees resource control.

19. The system of claim 11, wherein the serving policy function is decoupled from the anchor policy function.

20. The system of claim 11, further including one or more other policy functions in the network, wherein the information relating to the current location of the subscriber is disseminated to the one or more other policy functions.

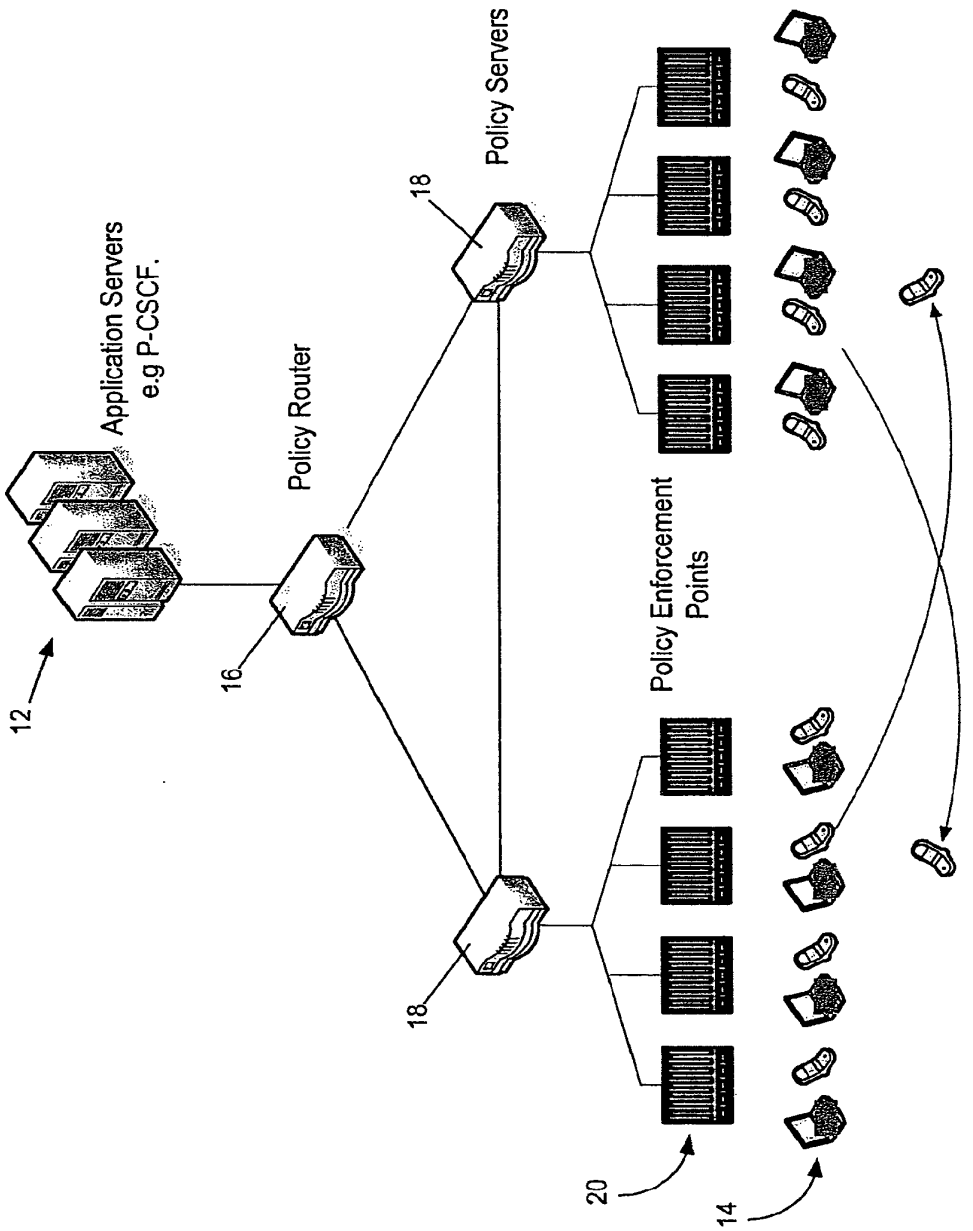

Application Servers
e.g P-CSCF.
Policy Router
Policy Servers
Policy Enforcement
Points
12
16
18
18
20
14

FIG. 1

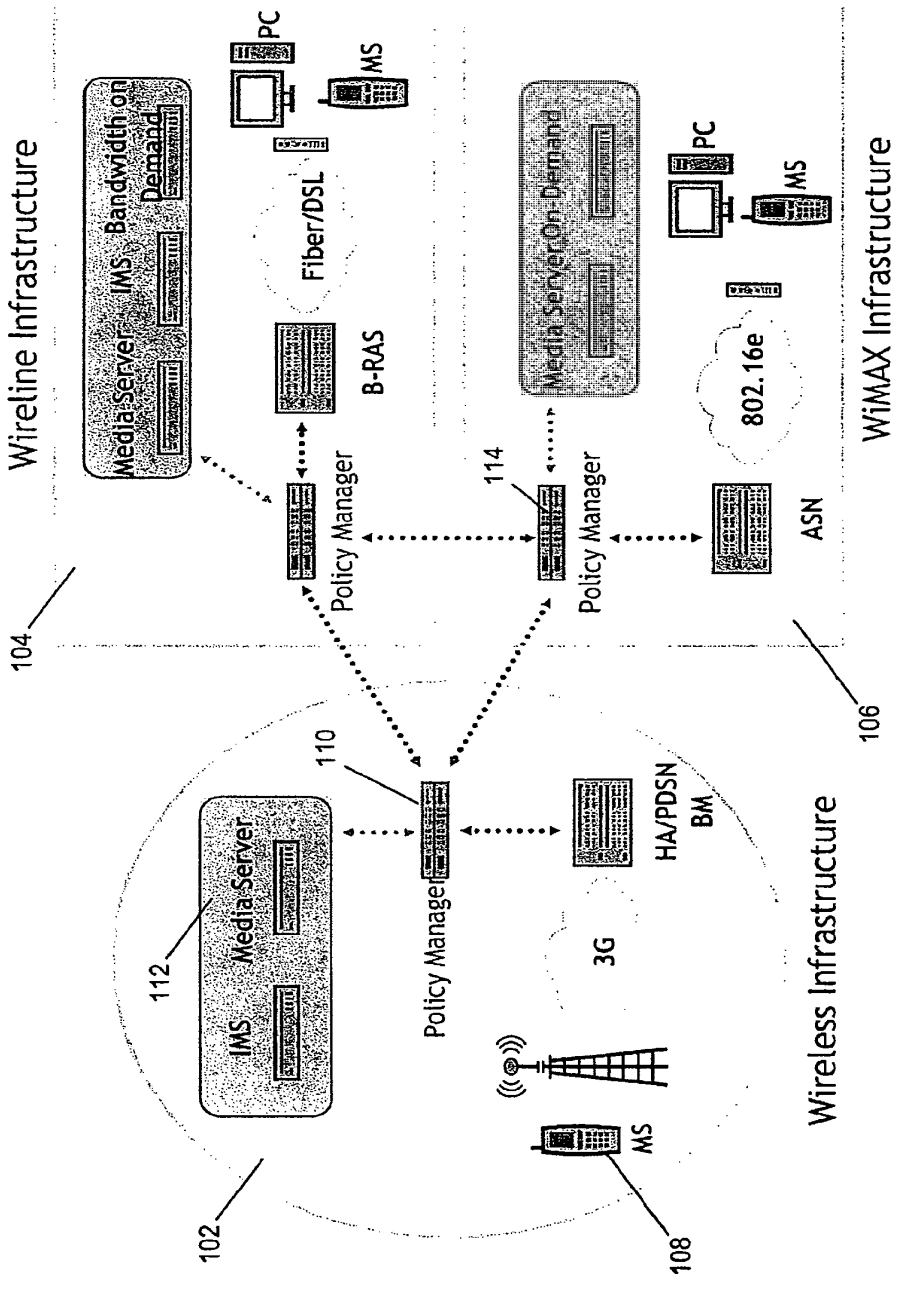

Wireline Infrastructure
Media Server IMS Bandwidth on Demand
PC
MS
Fiber/DSL
B-RAS
Policy Manager
104
Media Server On Demand
PC
MS
802.16e
ASN
WiMAX Infrastructure
114
Policy Manager
106
110
IMS Media Server
112
Policy Manager
HA/PDSN
BM
3G
MS
102
108
Wireless Infrastructure

FIG. 2

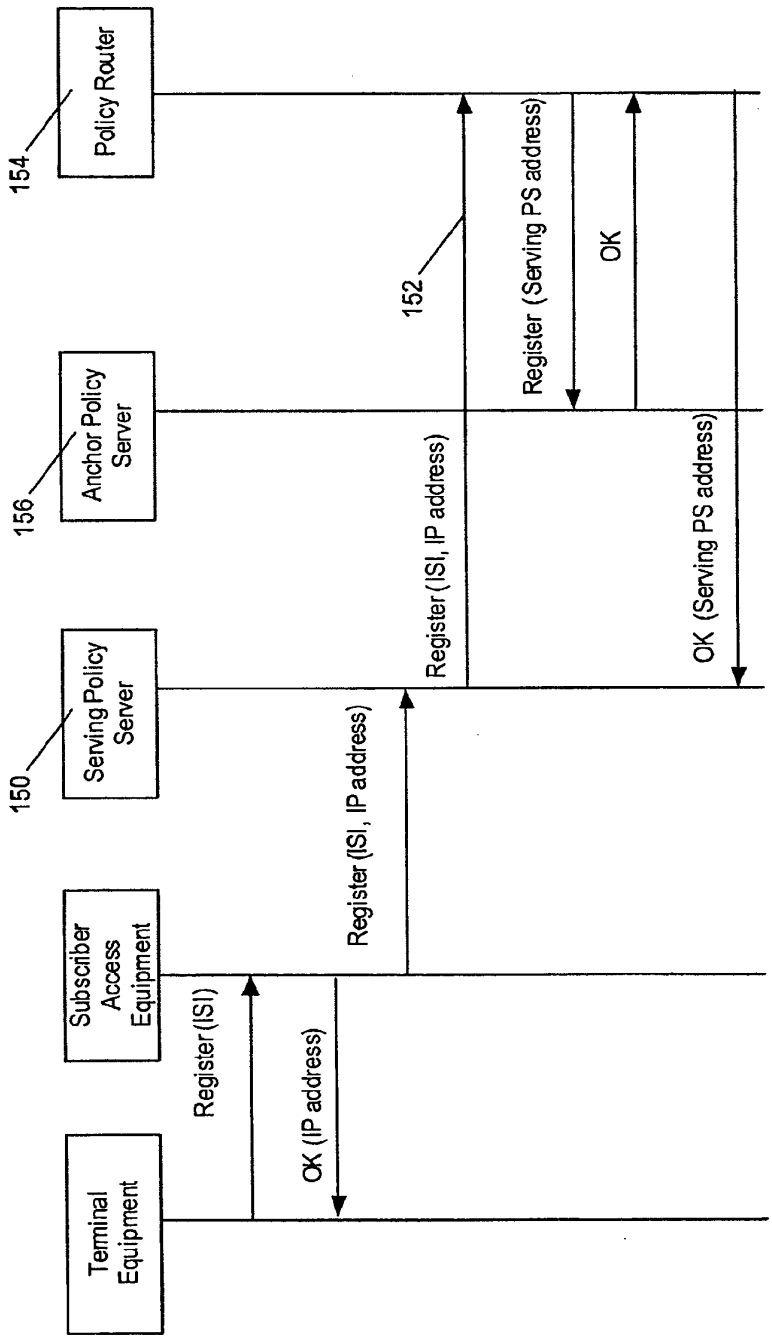

Terminal Equipment
Subscriber Access Equipment
Serving Policy Server
Anchor Policy Server
Policy Router
150
156
154
152
Register (ISI)
OK (IP address)
Register (ISI, IP address)
Register (ISI, IP address)
Register (Serving PS address)
OK
OK (Serving PS address)

FIG. 3

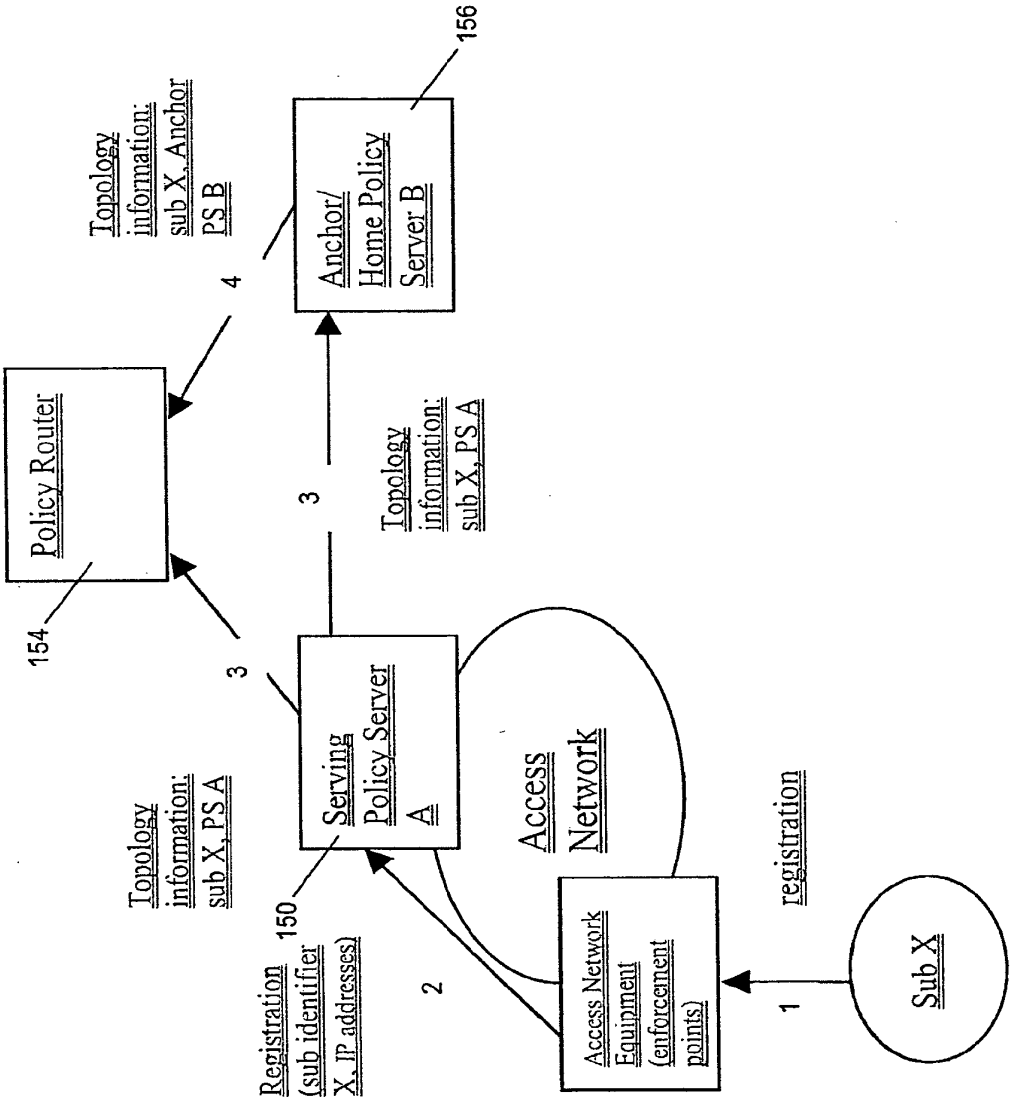

Policy Router
154
Topology information: sub X, Anchor PS B
4
Anchor/ Home Policy Server B
156
3
Topology information: sub X, PS A
3
Topology information: sub X, PS A
Serving Policy Server A
150
Registration (sub identifier X, IP addresses)
2
Access Network
Access Network Equipment (enforcement points)
1
registration
Sub X

FIG. 4

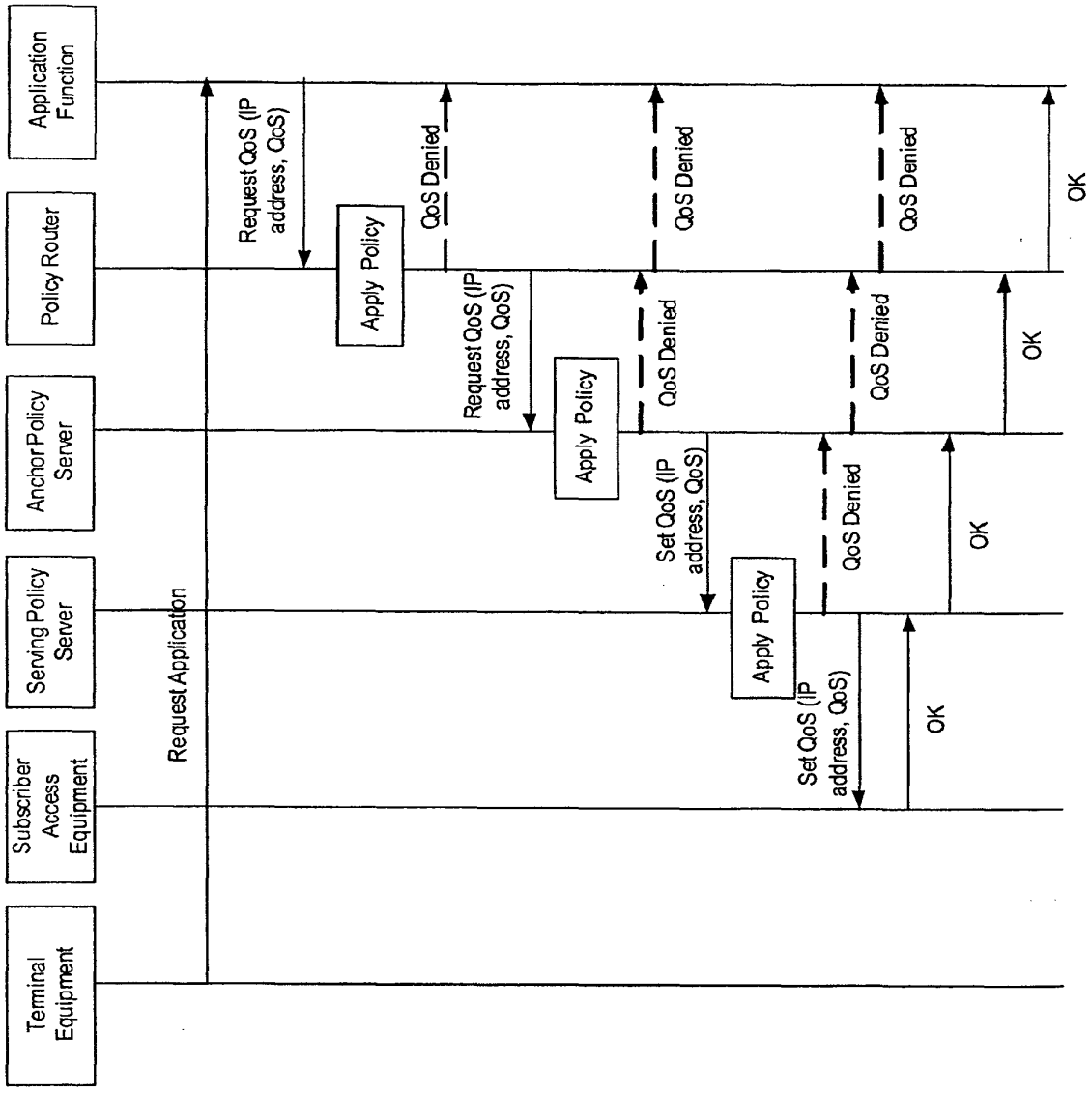

Application Function
Policy Router
Anchor Policy Server
Serving Policy Server
Subscriber Access Equipment
Terminal Equipment
Request Application
Request QoS (IP address, QoS)
Apply Policy
QoS Denied
Request QoS (IP address, QoS)
Apply Policy
QoS Denied
Set QoS (IP address, QoS)
Apply Policy
QoS Denied
Set QoS (IP address, QoS)
QoS Denied
QoS Denied
OK
OK
OK
OK

FIG. 5

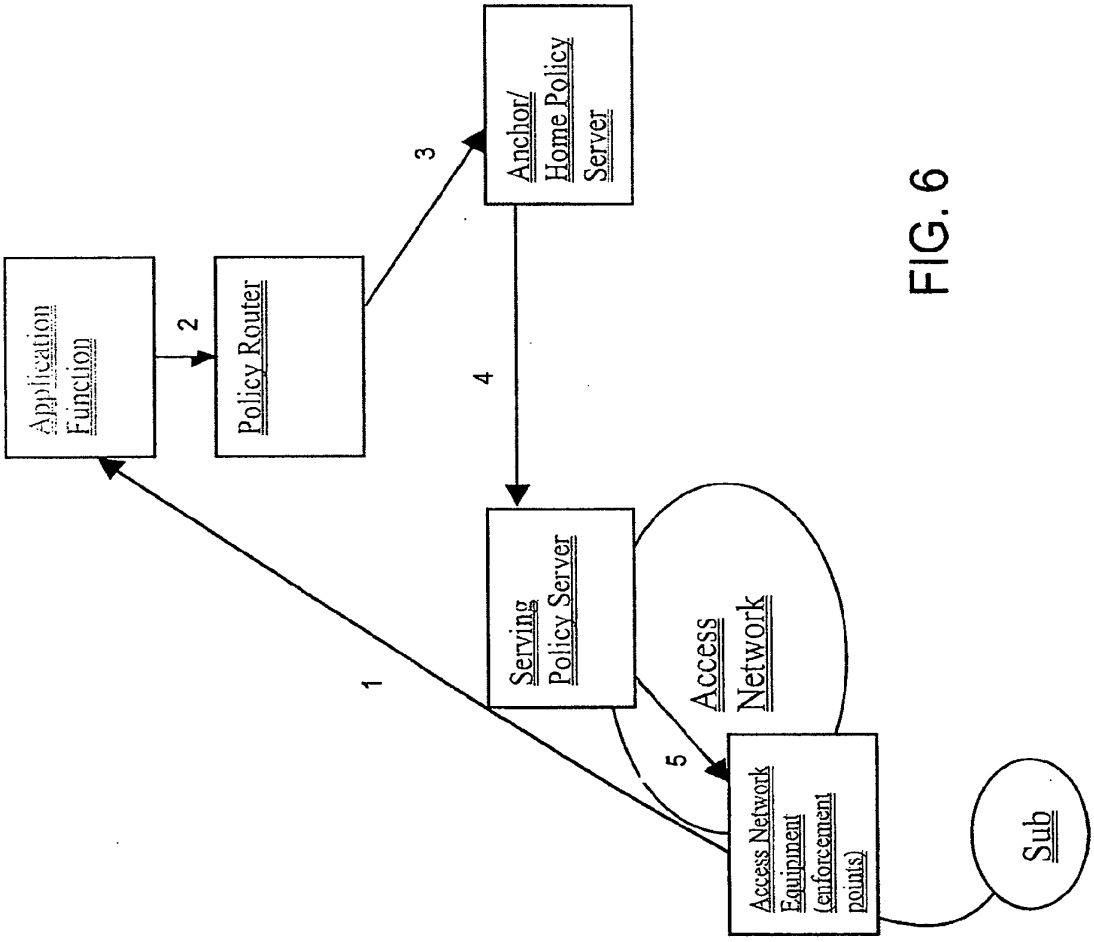

Application Function
Policy Router
Anchor/ Home Policy Server
Serving Policy Server
Access Network
Access Network Equipment (enforcement points)
Sub
1
2
3
4
5

FIG. 6

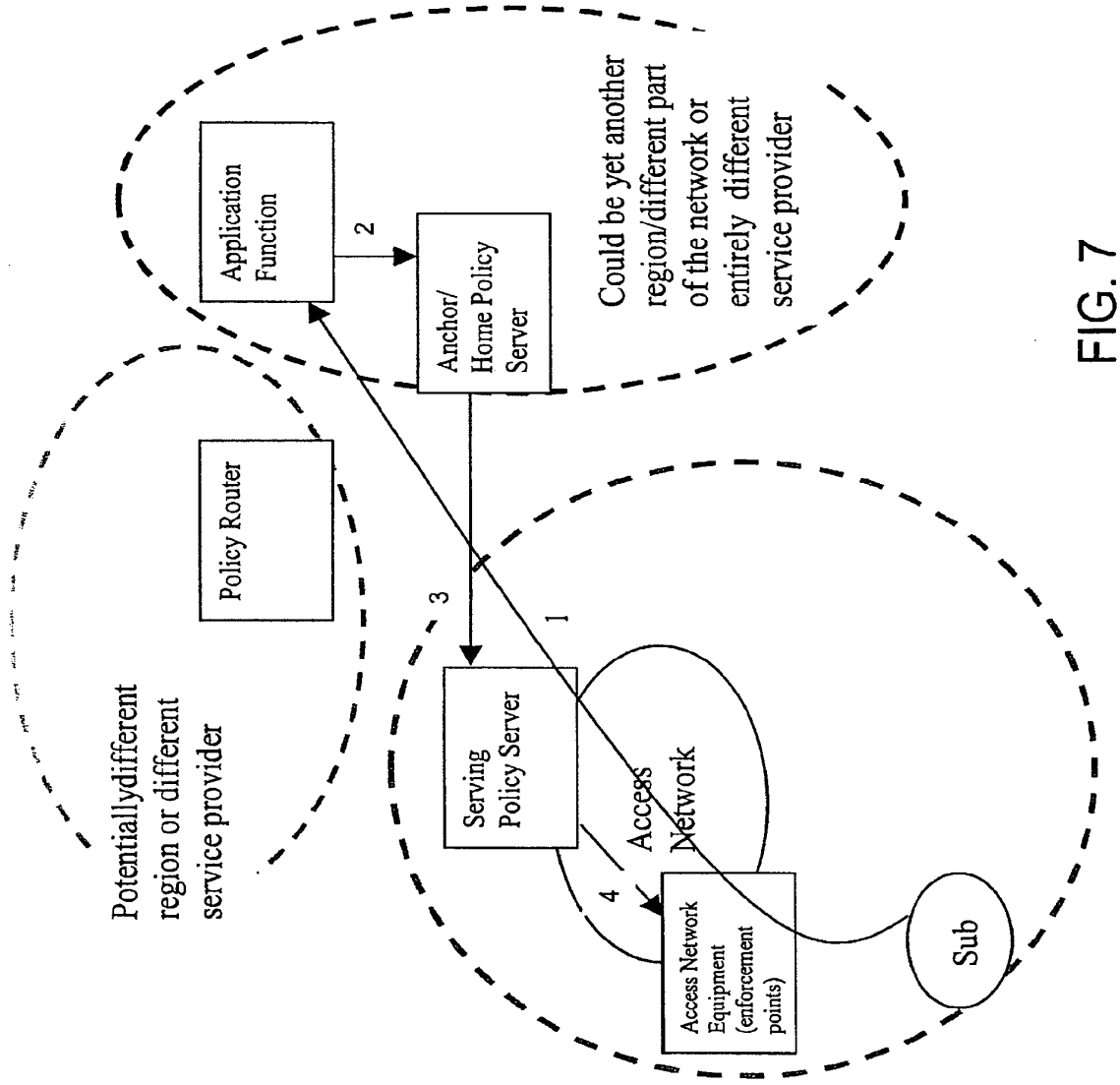

Application Function
2
Anchor/ Home Policy Server
Could be yet another region/different part of the network or entirely different service provider
Policy Router
Potentiallydifferent region or different service provider
3
1
Serving Policy Server
Access Network
4
Access Network Equipment (enforcement points)
Sub

FIG. 7

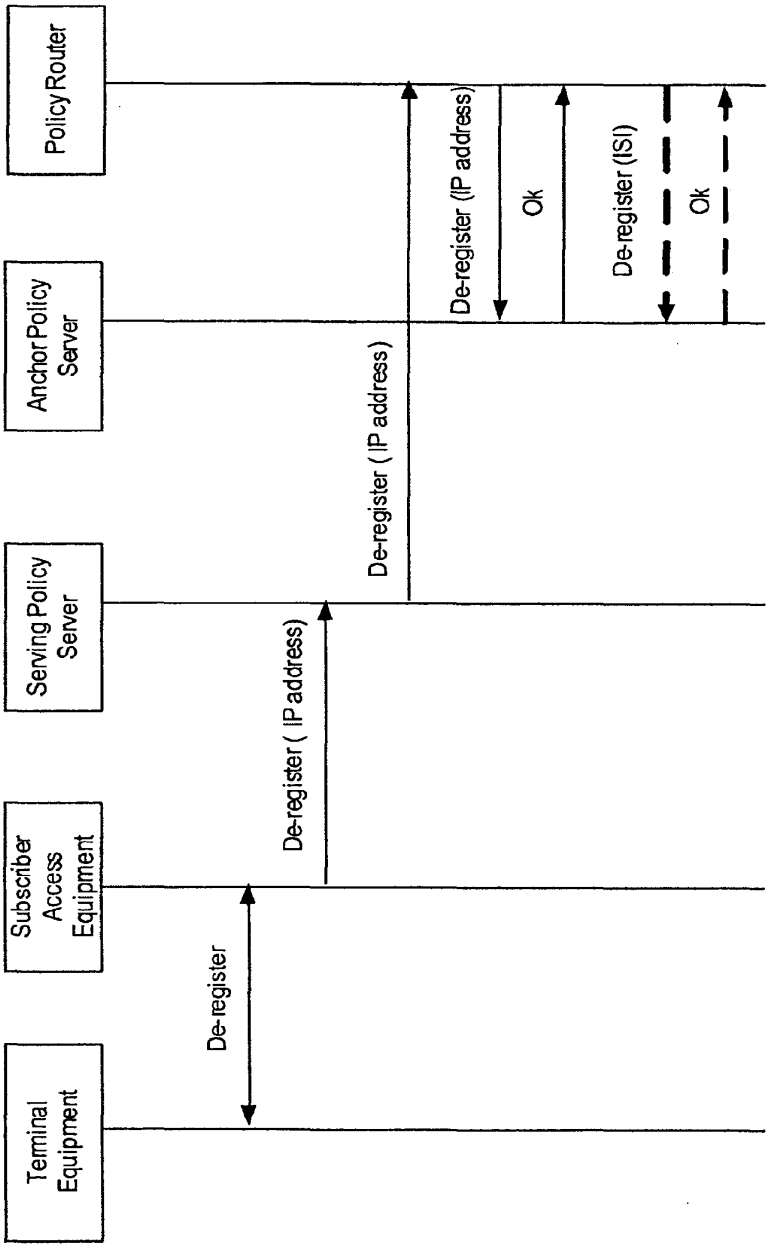

Policy Router
Anchor Policy Server
Serving Policy Server
Subscriber Access Equipment
Terminal Equipment
De-register (IP address)
Ok
De-register (ISI)
Ok
De-register (IP address)
De-register (IP address)
De-register

FIG. 8

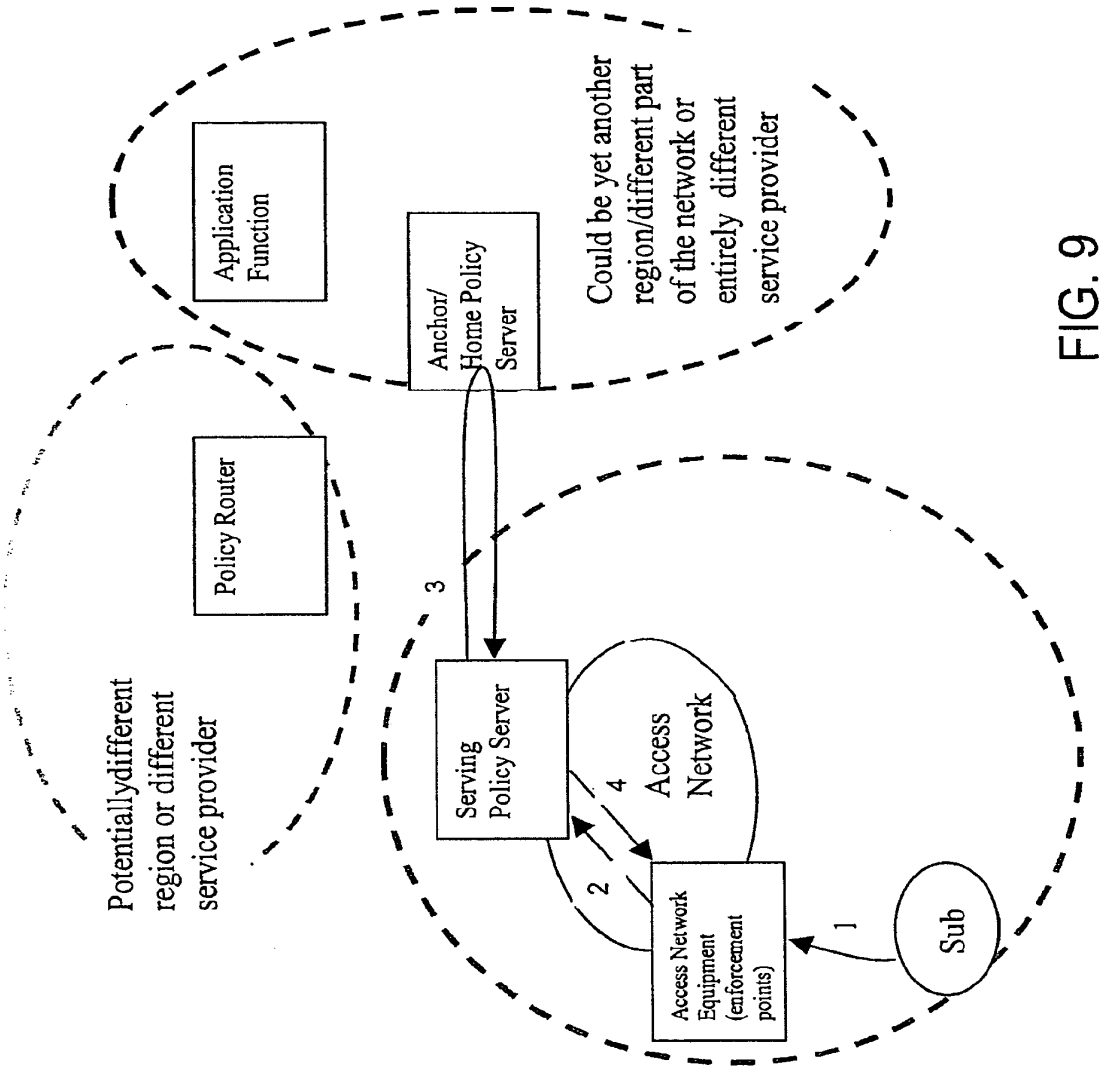

Application Function
Anchor/ Home Policy Server
Could be yet another region/different part of the network or entirely different service provider
Policy Router
Potentiallydifferent region or different service provider
3
Serving Policy Server
4
Access Network
2
Access Network Equipment (enforcement points)
1
Sub

FIG. 9

[19]中华人民共和国国家知识产权局

[51]Int. Cl[7]
G06F 13/14

[12]发明专利申请公开说明书

[21]申请号 00102757.3

[43]公开日 2001年8月29日

[11]公开号 CN 1310401A

[22]申请日 2000.2.22 [21]申请号 00102757.3

[71]申请人 王迪兴
地址 100080 北京市中科院黄庄小区813楼521
[72]发明人 王迪兴

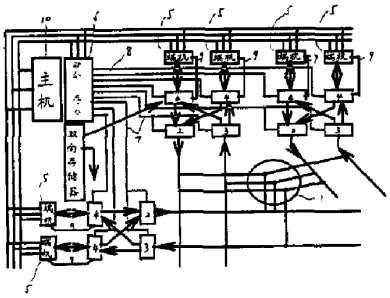
[74]专利代理机构 北京三友专利代理有限责任公司
代理人 王 琦

权利要求书1页 说明书7页 附图页数4页

[54]发明名称 并行运算、交换、控制多用平台

[57]摘要

本发明公开了一种并行运算、交换、控制多用平台，由数据、地址、命令 总线及总线控制、命令寄存器、外设接口和双端口 RAM 及一全互联控制电路组 成，其中，命令寄存器、外设接口及总线控制均挂在所述的总线上，外设接口 与双端口 RAM 的一端口之间有双向入出的数据端口及读写控制相连，一具有三 个双向入出端口的逻辑可逆运算器，其三个双向端口分别与双端口 RAM 的另一 端口相连，命令寄存器全部连到所述的全互联控制电路，另有读写控制分别到 双端口 RAM。



ISSN1008-4274

知识产权出版社出版

权　利　要　求　书

1、一种并行运算、交换、控制多用平台，由数据、地址、命令总线及总线控制、命令寄存器、六个外设接口和双端口 RAM、组成，其特征在于：还进一步包括一全互联控制电路，其中所述的命令寄存器、外设接口及总线控制均挂在所述的总线上，该等外设接口与双端口 RAM 的一端口之间有双向入出的数据端口及读写控制相连；一具有三端口的逻辑可逆运算器，其每个端口各有一输入端口和输出端口，该逻辑可逆运算器的三个输入端口分别通过一二选一电路而与双端口 RAM 的另一端口的输出两两相连，三个输出端口分别通过一一二分配器而与双端口 RAM 的另一端口的输入两两相连；所述的命令寄存器全部连到所述的全互联控制电路，另有读写控制分别到双端口 RAM，有方向选择控制分别到二选一电路、一二分配器。

2、根据权利要求 1 所述的并行运算、交换、控制多用平台，其特征在于：所述的一个逻辑可逆运算器六端口与六个外设接口和六个双端口 RAM 一一对应，以此单元为基础可并行扩展 2、3、4……个单元组，所述命令寄存器的字长亦相应地跟着扩展到 12、18、24 位……。

3、根据权利要求 1、2 所述的并行运算、交换、控制多用平台，并行扩展的单元组之间通过全互联控制电路连通各个单元组的各个端口，每两个端口之间均有一连通控制开关，连通控制开关信号由命令寄存器的存储内容决定。

4、根据权利要求 1 或 2 所述的并行运算、交换、控制多用平台，其特征在于：所述的逻辑可逆运算器由一个加法运算器与两个减法运算器构成。

5、根据权利要求 1 所述的并行运算、交换、控制多用平台，其特征在于：所述的逻辑可逆运算器的位片可多位级联或通过拼接扩展一个位片的进制值域。

6、根据权利要求 1 所述的并行运算、交换、控制多用平台，其特征在于：有一工作模式控制电路连到命令寄存器，及进制设定电路，控制平台的运算或交换工作状态。

说　明　书

并行运算、交换、控制多用平台

本发明属于数据处理技术领域，具体涉及一种可广泛应用于并行控制、并行数据处理、并行通信交换、计算机网络及智能模拟等领域的多用智能平台。

代表数据处理先端技术的计算机自 40 年代问世以来，一直沿袭着冯·诺依曼机的体系结构，其主要特点是：第一，程序内存、串行处理；第二，存储地址与存储内容分开；第三，只能被动执行确定程序。50 多年来尽管计算机技术取得了突飞猛进的发展，但人们也越来越深刻地感受到传统计算机体系结构所带来的限制。例如科学技术的发展对计算机提出了越来越多的要求，某些应用领域甚至需要每秒运算 1 万亿次甚至更快的高性能计算机。诸如新型药物设计、生物分子结构、催化剂和酶的性质、人类基因、新材料性质、湍流、海洋回流、核聚变能源系统设计、核爆炸模拟、量子色动力学、密码学、全球天气预报、灾害性风暴预报、地震预测、石油勘探中的三维地震资料处理等。

而计算机自问世以来一直遵循着循序串行的运算方法。为了提高计算机的速度，人们通过提高时钟频率减少指令的执行时间，但这总要有一个局限。因此开拓了并行运算的研究，使多个向量处理机和一个中央存储器连接在一起，构成了超级计算机。高性能处理器的出现和价格的逐渐降低，使大规模并行处理（MPP）机的体系结构具有一定的发展潜力。但真正使 MPP 的潜力得到充分的发挥，还需在系统设计和应用设计上找到有效驱动大量处理器协同工作的原理与途径。应该说，这一问题的解决，在冯型机框架下有一定的难度，原因在于冯型机是按地址方式工作的，各计算机之间没有内在的联系，即没有自组织性，因而在多机之间，不论是任务分配还是实时通信都是难以解决的问题，它在本质上只面对 1 个信息源。因而必须创造一种机制，使有多少个外设，就允许多少个外设直接面向环境同步接受并处理信息，且保证子系统之间能够实时并行交互作用。

本发明的目的就在于突破串行工作、地址操作及程序化运行方式的框架，

而提供一种以自组织原理为基础，实现读写算同步，可开放性并行读写算，具有子系统透明化功能耦合、且能串并行自适应交互作用的多用智能平台。

本发明的进一步目的是结合具有多值态的逻辑可逆运算器，而提供一种具有多值态的、模数统一的、系统结构与功能可扩展的多功能一体化多用智能平台。

本发明是一种并行运算、并行交换、并行控制，人脑智能模拟多用平台，由数据、地址、命令总线及总线控制、命令寄存器、六个外设接口和双端口RAM、全互联控制电路组成，其中，命令寄存器、外设接口及总线控制均挂在所述的总线上,该等外设接口与双端口 RAM 的一端口之间有双向入出的数据端口及读写控制相连；一具有三端口的逻辑可逆运算器，其每个端口各有一输入端口和输出端口，该逻辑可逆运算器的三个输入端口分别通过一二选一电路而与双端口 RAM 的另一端口的输出两两相连，三个输出端口分别通过一一二分配器而与双端口 RAM 的另一端口的输入两两相连；所述的命令寄存器有读写控制分别到双端口 RAM，有方向选择控制分别到二选一电路、一二分配器。

根据上述技术方案，其中一个逻辑可逆运算器六端口与六个外设接口和六个双端口 RAM 一一对应，以此单元为基础可并行扩展 2、3、4……个单元组，所述命令寄存器的字长亦相应地跟着扩展到 12、18、24 位……。

并行扩展的单元组之间通过全互联控制电路联通各个单元组的各个端口，每两个端口之间均有一联通控制开关，联通控制开关信号由命令寄存器的存储内容决定。

逻辑可逆运算器由一个加法运算器与两个减法运算器构成。

逻辑可逆运算器的位片可多位级联或通过拼接扩展一个位片的进制值域，如由 8 扩展到 16 进制，或由 16 扩展到 32 进制。

进一步可有一工作模式控制电路联到命令寄存器，及进制设定电路，控制平台的工作状态－－运算或交换。

本发明并行运算、交换、控制多用平台用于运算的优点是并行、适应多种

进制代码运算交换，适应连续模拟量运算，具有实时性，可逆向逻辑运算；用于交换的优点是并行、高速、实时双向、自选路由；用于控制的优点是互为因果，实时双向，模数统一，任意一个端机都能做为主机实施全局控制。

发明并行运算、交换、控制多用平台可用于多子系统功能随机耦合，多存储器交互存取及联想读写，可在运算、交换、控制领域，体现其多用性及多功能性，因而适用面广，且具有极强的自开发性－－除上述并行运算、并行交换、并行控制以外，用于人脑智能模拟领域的应用开发。

下面结合附图及具体实施例对本发明再作进一步详细的说明。

图 1 是本发明的电路原理示意图；

图 2 是本发明的并行处理原理示意图；

图 3 是本发明的逻辑可逆运算器的实施例连接示意图；

图 4 是本发明的全互联的控制电路。

首先，请参见图 1，本发明是以逻辑可逆运算器 1 为核心，配合二选一电路 2、一二分配器 3、双端口 RAM 4、命令寄存器 6 及总线控制 10 和外设接口 5 组成。

其中，命令寄存器 6、外设接口 5 及总线控制 10 均挂在由数据、地址、控制线组成的三总线 11 上。外设接口 5 与双端口 RAM 4 的一端口之间通过双向入出的数据端口与读写控制 9 相连，双端口 RAM 4 的另一端口的输出分别两两连接于二选一电路 2 的输入端，其输入亦分别两两连接于一二分配器 3 的输出端。

该逻辑可逆运算器 1 的三个输入端口分别与一二选一电路 2 的输出端相连，三个输出端口分别与一一二分配器 3 的输入端相连。命令寄存器 6 有读写控制 8 与双端口 RAM 4 连接，实现面向运算器的读写控制，有方向选择控制 7 与二选一电路 2、一二分配器 3 相连，实现对二选一电路 2、一二分配器 3 的逻辑控制，将面向逻辑可逆运算器 1 的单向入出转变为面向双端口 RAM 4 的双向入出，使本发明多用智能平台可通过命令寄存器 6，实现串并读写、串

并交换、串并运算、串并控制，及实时双向读写、实时双向交换、实时并行运算、实时双向控制。

参见图 3 所示，逻辑可逆运算器 1 具体可由一加法运算器 A1 + B1 = C1 和二减法运算器 C2 - B2 = A2、C3 - A3 = B3 组成，将其中的输入端口 A1 与 A3 并接、B1 与 B2 并接、C2 与 C3 并接，组成一具有三个输入端口 A1（A3）、B1（B2）、C2（C3），三个输出端口 C1、A2、B3 的运算器，体现了一种 A + B = C、C - A = B、C - B = A 的逻辑可逆运算关系。图中，A1(A3)、A2 为 A 口，B1(B2)、B3 为 B 口，C2(C3)、C1 为 C 口，设 A 与 B 入则 C 出，C 与 A 入则 B 出，C 与 B 入则 A 出，运算器具逻辑可逆性，可双向同步入出、同步加减运算。具体应用时，可三口同时入，三口同时出，可逆向逻辑推理及运算。

逻辑可逆运算器 1 与外设接口 5 及双端口 RAM 4 可呈对应关系的扩展，命令寄存器可相应地扩展字长或增加控制级数，使本发明在命令寄存器的读写控制 8 的控制下，可完成并行运算、交换与控制。

参见图 1 所示，当把外设接口 5 视为端机，总线控制 10 视为主机，主机或端机，对于各口双口 RAM 4 的并行读写，与地址选通，是同一信号，且并行读写信号，是通过命令寄存器 6 以位为单位读写相应的双口 RAM 4（此对应关系是可编程的，当然也可以是固定的）。因并行读写只能对各双口 RAM 的 0 地址操作，所以各双口 RAM，都配有地址发生器，读时向外推出数据，写时向里推入数据。主机与端机、端机与端机的数据交换，则是通过双口 RAM 确定其通讯协议的，且这种协议具有并行性。各双口 RAM 的并行读写，还有一层含义，即各口的双口 RAM，在同时读写时，交换与运算的过程隐含在内，即完成双向读写的同时，亦完成了双向交换及运算，即读写算同步完成。

本发明多用智能平台的各个端机都能通过总线共享命令寄存器 6，并行读写各口的双口 RAM 4，至于哪一个端机能占用命令寄存器，由总线控制 10 按优先申请原则裁决。

命令寄存器 6 中的命令字决定哪些双口 RAM 读或写，各双口 RAM 的读

写及相应的运算、交换、控制功能都通过一条命令在一个时钟周期完成。

如实现运算，并行读 A、B 口，则 A、B 的运算结果写在 C 口，并行读 A、C 口，则 A、C 的运算结果写在 B 口，并行读 B、C 口，则 B、C 的运算结果写在 A 口。

如实现交换或控制，可在 A 口给一设置，由 A、B、C 三口的运算关系决定，B、C 两口可双向同步交换或控制，具体是交换还是控制，由外设确定。如是交换，各外设接口接群入群出设备或主被叫用户；如是控制，各外设接口接传感器或执行器。同样的，在 B 口给一设置，A、C 两口可双向同步交换或控制，在 C 口给一设置，A、B 两口可双向同步交换或控制。

4 个运算器通过全互联控制电路，可在 24 个端口之间实现任意两个端口的交换，及任意两个端口中的任意两个脚的交换，可通过一条指令在一个时钟周期实现 8 个端口之间的双向同步交换（24 个端口中任意组合）。

本发明多用智能平台通过模式切换，运算与交换两种功能模式可选；通过串并行读写控制，交换与运算串行、并行两种模式可选；通过模式切换，固定主机与多主机两种模式可选。另外，主机串行读写、与并行读写两种模式可选，主机参与交换、运算，和不参与而只进行设定控制两种模式可选。其关健在于主机与端机都能共用命令寄存器，并行读写各口的双口 RAM，至于哪一个端机能并行读写，由总线控制 10 来分配解决。

参见图 4 所示，命令寄存器按交换需求接节点控制。命令寄存器的输出命令直接通过与门控制互联节点，通过交换模式控制直接接到设置端口。如 1 与 4 交换 1 与 4 与后控制 2 与 5 节点开关，再通过交换模式控制，使 1 与 4 直接控制设置端 3 与 6。设置端可以是恒高，1 与 4 作为开关控制。

组成本发明的核心运算器—逻辑可逆运算器 1 的加法运算器和减法运算器，更可是具有多值态的加法运算器和减法运算器，此项技术已另案申请，在此不予赘述。

上述的多用智能平台，具有多值运算、交换、多种进制代码选择设定、互

为因果关系控制等功能。具有多值态，适应多种进制代码运算处理及交换，如8、16 以至 32、64……进制代码。具有开放性，可随意以运算器位片为基础级联拼接使用，具体可根据需要在片级，以位为单位多位级联，又可在板级以片为单位多片级联。且不管怎样级联，都不存在进借位累加延迟时间问题。

上述的多用智能平台，具模数统一、储算一体化的特点，可实时非程序化数据处理及控制。具地址与数据口统一、运算与交换功能合一的特点，可实现互为因果关系控制。系统各端口的参量，可动态交互定义及互补定义，因而体现了系统的自组织及互为因果目的性。相对于冯机及其运算器，它解决了多值态、多种进制代码运算问题，解决了系统自组织透明化、及非程序化功能耦合问题，解决了因扩展字长而产生的进借位累加延迟时间问题，解决了系统的自组织及开放性问题，解决了信息处理系统的时空统一、模数统一、逻辑可逆、与不可逆的统一问题。

上述的多用智能平台的核心逻辑可逆运算器，用于交换，一个可实现 6 大口之间的任意交换——（1＋6）×6／2＝21 种交换关系。4 个逻辑可逆运算器通过全互联控制电路、可实现 24 个端口之间的任意交换－（1＋24）×24/2=300 种交换关系。用于运算，一个运算器可实现 3 口并行输入、3 口并行输出，以八进制多值态逻辑可逆运算器位片为例，它可满足八位二进制码的并行运算，满足除 2 进制代码以外，3、4、5、6、7、8 进制代码的一位加减运算，多位片组合即可满足多位、多种进制代码的并行运算，且可和差同时输出。4 个运算器组合可实现 12 个口同时输入，12 个口同时输出，满足 12 个操作数的 12 种加减运算。用于控制，以八进制多值态逻辑可逆运算器位片为例，可实现多值态（2—8）之间的，互为因果关系双向控制。多位片组合，可 16 值或 32 至 64、128 值态……可选，及多口多脚之间的并行控制、互补控制，及互为因果关系控制。

上述多用智能平台的最大特点：一是具有开放性，片级板级都可根据实际需要，随意增加大口的数量，及增加各口管脚的数量或多值状态，还可将主板

做成可随意级联扩展形式的。扩展后各大口与各管脚之间，如上所述同样可以（1＋N）×N／2 的关系，实现全互联双向交换及控制。二是具有并行性，即可通过并行读写各口的双口 RAM，实现全并行运算，又可通过设置某个口，实现并行双向交换，或并行双向控制。三是各端机，均可作为主机，实施全局控制。

说　明　书　附　图

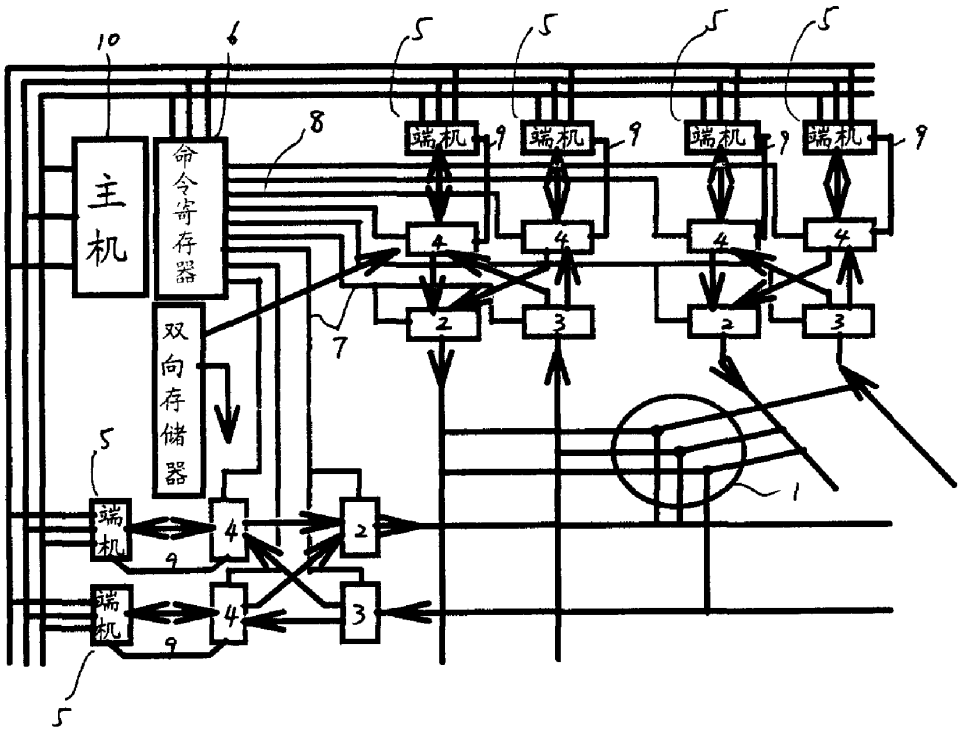


图 1

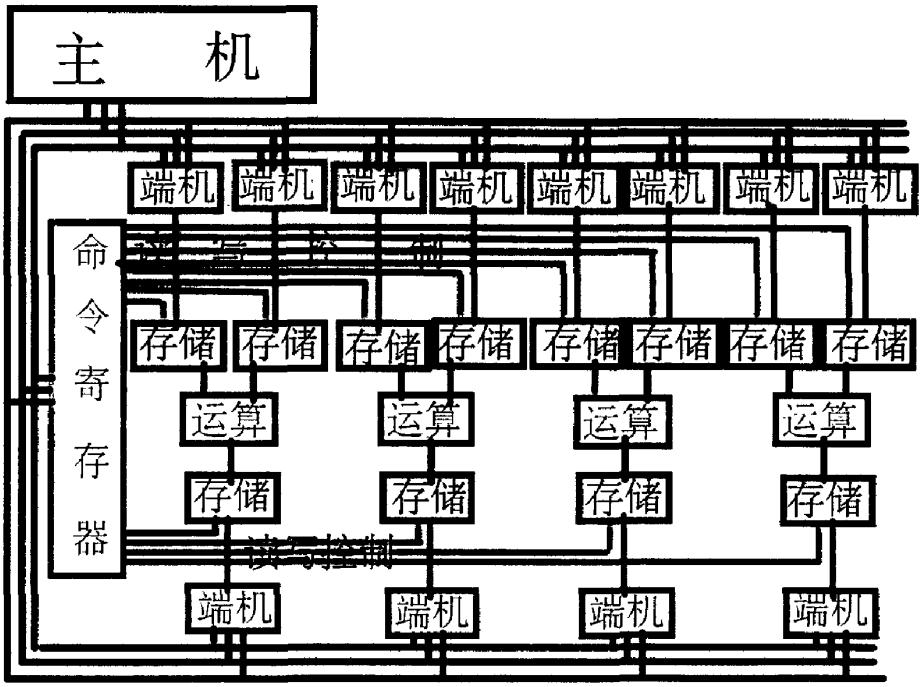

主　机
端机
端机
端机
端机
端机
端机
端机
端机
命令寄存器
存储
存储
存储
存储
存储
存储
存储
存储
运算
运算
运算
运算
存储
存储
存储
存储
端机
端机
端机
端机

图 2

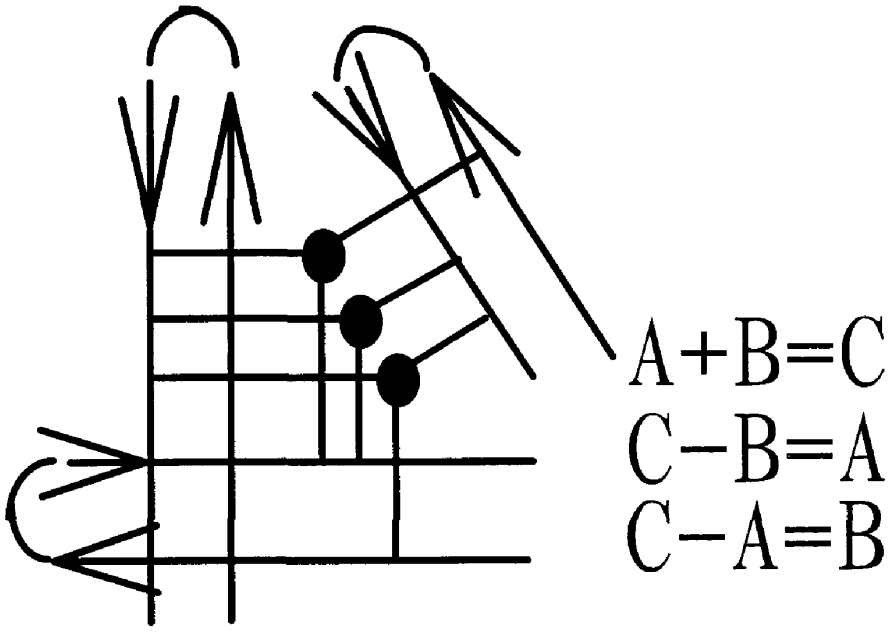


图 3

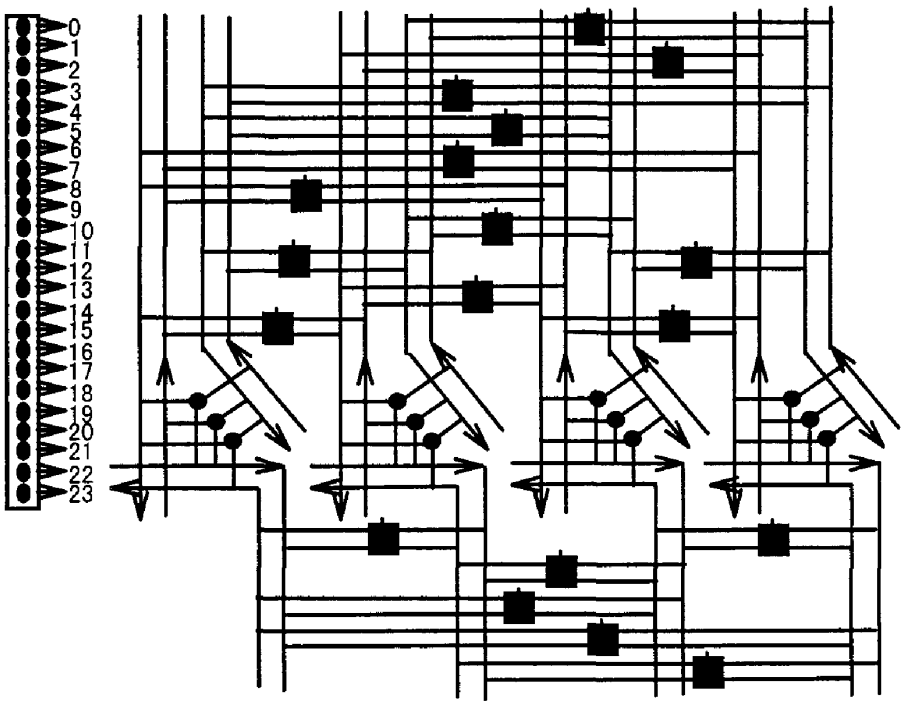


图 4

Electronic Acknowledgement Receipt

EFS ID:	19103390
Application Number:	14082040
International Application Number:	
Confirmation Number:	1015
Title of Invention:	Device-Assisted Services for Protecting Network Capacity
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	Krista Susan Jacobsen
Filer Authorized By:	
Attorney Docket Number:	RALEP032C1
Receipt Date:	22-MAY-2014
Filing Date:	15-NOV-2013
Time Stamp:	14:04:19
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	P032C1IDS.pdf	613368 89e8dbcbacafe1bd37275580165165460c375caa	no	7
Warnings:					
Information:					

2	Foreign Reference	2043_EP2466831A1.pdf	1530373 fcc550ea4f7f61dc3b1fb7695c6b44459cb7cf30	no	63
Warnings:					
Information:					
3	Foreign Reference	2044_WO1999027723A1.pdf	904456 a688012e12d1ad3b8550a0c726a94bd72b28a6fa	no	36
Warnings:					
Information:					
4	Foreign Reference	2045_WO2007133844.pdf	1180849 f4c87541e0759ae271d1a7f67a656801997a5558	no	30
Warnings:					
Information:					
5	Foreign Reference	2046_CN1310401A.pdf	992440 a1b82929f3d1ce8d217485b34de268afea8f7863	no	13
Warnings:					
Information:					
6	Non Patent Literature	3037_EndtoEnd.pdf	1097643 c0f57a22ab875fecfc286cd70be1ebcae7fc806b	no	5
Warnings:					
Information:					
7	Non Patent Literature	3038_ASA.pdf	786693 5580855f6934ae1eab1a3251238ecc9c807ee7a9	no	24
Warnings:					
Information:					
		Total Files Size (in bytes):	7105822		

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

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

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

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/082,040	11/15/2013	Gregory G. Raleigh	RALEP032C1

CONFIRMATION NO. 1015

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

PUBLICATION NOTICE

OC000000067548549

Title: Device-Assisted Services for Protecting Network Capacity

Publication No.US-2014-0095706-A1
Publication Date:04/03/2014

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

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

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

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

Application Number	14082040
Filing Date	2013-11-15
First Named Inventor	Gregory G. Raleigh
Art Unit	2447
Examiner Name	not yet assigned
Attorney Docket Number	RALEP032C1

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	6885997	B1	2005-04-26	Roberts, David T.	
	2	7720464	B2	2010-05-18	Batta, Puneet	
	3	7797060	B2	2010-09-14	Grgic et al.	
	4	7853255	B2	2010-12-14	Karaoguz et al.	
	5	7930327	B2	2011-04-19	Craft David et al.	
	6	8046449	B2	2011-10-25	Yoshiuchi, Hideya	
	7	8095124	B2	2012-01-10	Balia, Hinal K.	
	8	8229394	B2	2012-07-24	Karlberg, Johan	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	9	8264965	B2	2012-09-11	Dolganow et al.	
	10	8442015	B2	2013-05-14	Behzad et al.	
	11	8495700	B2	2013-07-23	Shahbazi, Majid	
	12	8528068	B1	2013-09-03	Weglein et al.	
	13	8548427	B2	2013-10-01	Chow et al.	
	14	8566236	B2	2013-10-22	Busch, James David	
	15	8572117	B2	2013-10-29	Rappaport, Theodore S.	
	16	8589955	B2	2013-11-19	Roundtree et al.	
	17	8601125	B2	2013-12-03	Huang et al.	
	18	8635164	B2	2014-01-21	Rosenhaft et al.	
	19	8660853	B2	2014-02-25	Robb et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20030188006	A	2003-10-02	Bard, Steven R.	
	2	20030188117	A	2003-10-02	Yoshino et al.	
	3	20040255145	A	2004-12-16	Chow, Jerry	
	4	20050055595	A	2005-03-10	Frazer et al.	
	5	20060160536	A	2006-07-20	Chou, Joey	
	6	20060168128	A	2006-07-27	Sistla et al.	
	7	20070259656	A	2007-11-08	Jeong, Jong Woo	
	8	20080263348	A	2008-10-23	Zaltsman et al.	
	9	20080313315	A	2008-12-18	Karaoguz et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	10	20090282127	A	2009-11-12	Leblanc et al.	
	11	20100167696	A	2010-07-01	Smith, Christopher David et al.	
	12	20110019574	A	2011-01-27	Malomsoky et al.	

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	101123553A	CN		2007-09-11	Southeast University		☐
	2	1937511A	CN		2007-03-28	ZTE		☐

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

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		☐

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

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

EFS Web 2.1.17

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

CERTIFICATION STATEMENT

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

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

OR

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

☐ See attached certification statement.

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

☒ None

SIGNATURE

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

Signature	/Krista S. Jacobsen/	Date (YYYY-MM-DD)	2014-03-19
Name/Print	Krista S. Jacobsen	Registration Number	59374

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 12/28 (2006.01)
H04L 12/56 (2006.01)
H04J 13/00 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200710131504.7

[43] 公开日 2008 年 2 月 13 日

[11] 公开号 CN 101123553A

[22] 申请日 2007.9.11
[21] 申请号 200710131504.7
[71] 申请人 东南大学
地址 210096 江苏省南京市四牌楼 2 号
[72] 发明人 宋宇波

[74] 专利代理机构 南京经纬专利商标代理有限公司
代理人 叶连生

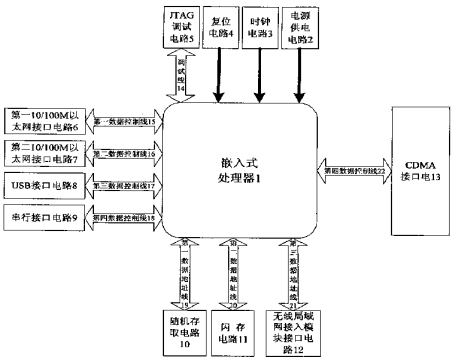
权利要求书 2 页 说明书 9 页 附图 4 页

[54] 发明名称

基于码分多址技术的移动无线局域网接入装置及方法

[57] 摘要

基于码分多址技术的移动无线局域网接入装置及方法涉及一种局域网接入装置及其方法，尤其涉及一种基于码分多址技术(CDMA)的移动无线局域网接入装置及其方法，该装置主要包括三大组成部分：嵌入式硬件平台、多路 CDMA 接口模块电路和无线局域网接入模块电路。嵌入式硬件平台主要由嵌入式微处理器、电源模块电路、时钟模块电路、复位模块电路、JTAG 调试口、以太网接口模块电路、USB 接口模块电路、串口接口模块电路、随机存取模块电路和闪存模块电路组成。多路 CDMA 接口模块电路由串口扩展模块电路，1～4 路 CDMA2000 1X 数据链路组成，每路包含 CDMA 通信模块电路和 R－UIM 智能卡模块电路。无线局域网接入模块电路由 MiniPCI 接口电路和局域网无线接入模块组成。



1、一种基于码分多址技术的移动无线局域网接入装置，其特征在于嵌入式微处理器（1）与电源供电电路（2）、时钟电路（3）、复位电路（4）直接相连；嵌入式微处理器（1）经过调试线（14）与 JTAG 调试电路（5）相连；嵌入式微处理器（1）经过第一数据控制线（15）与第一 10/100M 以太网接口电路（6）相连，经过第二数据控制线（16）与第二 10/100M 以太网接口电路（7）相连，经过第三数据控制线（17）与 USB 接口电路（8）相连，经过第四数据控制线（18）与串行接口电路（9）相连，经过第五数据控制线（22）与 CDMA 接口电路组成（13）相连；经过第一数据地址线（19）与随机存取电路（10）相连，经过第二数据地址线（20）与闪存电路（11）相连，经过第三数据地址线（21）与无线局域网接入模块接口电路（12）相连。

2、根据权利要求 1 所述的基于码分多址技术的移动无线局域网接入装置，其特征是嵌入式微处理器（1）经过第四数据控制线（22）与 CDMA 接口电路（13）相连，具体表现在：嵌入式微处理器（1）的扩展地址总线与译码器 U3 的地址线通过地址线（23）相连；嵌入式微处理器（1）的扩展地址总线与通用异步收发器 U2 的地址线通过地址线（25）相连；嵌入式微处理器（1）的通用 I/O 接口与通用异步收发器 U2 的串口中断通过中断线（26）相连；嵌入式微处理器（1）的扩展数据总线与通用异步收发器 U2 的数据线通过数据线（27）相连；嵌入式微处理器（1）的扩展写数据使能、扩展读数据使能与通用异步收发器 U2 的写使能、读使能相连。

3、根据权利要求 1 所述的基于码分多址技术的移动无线局域网接入装置，其特征是 CDMA 接口电路（13）包括通用异步收发器 U2、译码器 U3、7.3728M 晶体振荡器、第一 CDMA 数据通信模块 U4、第二 CDMA 数据通信模块 U5、第三 CDMA 数据通信模块 U6、第四 CDMA 数据通信模块 U7，第一 R-UIM 智能卡接口 U8、第二 R-UIM 智能卡接口 U9、第三 R-UIM 智能卡接口 U10、第四 R-UIM 智能卡接口 U11 组成；通用异步收发器 U2 的扩展串口 1、扩展串口 2、扩展串口 3、扩展串口 4 和第一 CDMA 数据通信模块 U4、第二 CDMA 数据通信模块 U5、第三 CDMA 数据通信模块 U6、第四 CDMA 数据通信模块 U7 分别通过第一控制数据线（28）、第二控制数据线（29）、第三控制

数据线（30）、第四控制数据线（31）相连；第一 CDMA 数据通信模块 U4、第二 CDMA 数据通信模块 U5、第三 CDMA 数据通信模块 U6、第四 CDMA 数据通信模块 U7 的 R-UIM 接口和第一 R-UIM 智能卡接口 U8、第二 R-UIM 智能卡接口 U9、第三 R-UIM 智能卡接口 U10、第四 R-UIM 智能卡接口 U11 的 UIM 卡数据接口分别通过 UIM 卡数据线相连。

4、根据权利要求 1 所述的基于码分多址技术的移动无线局域网接入装置，其特征是嵌入式微处理器（1）经过第三数据地址线（21）与无线局域网接入模块接口电路（12）相连，具体表现在：嵌入式微处理器（1）的 PCI 控制器地址线、PCI 数据线、通用 I/O 接口、PCI 控制器分别与无线基带处理芯片 U25 的地址线、数据线、中断信号、控制线相连。

5、根据权利要求 1 所述的基于码分多址技术的移动无线局域网接入装置，其特征是无线局域网接入模块接口电路（12）包括无线基带处理芯片 U25，双边带多模式射频芯片 U29，射频输出电路 U30 组成；无线基带处理芯片 U25 的模数转换接口、数模转换接口、射频重启动、时钟接口、数据输入口、数据输出口分别和双边带多模式射频芯片 U29 的射频接收接口、射频发送接口、重启动、数据时钟、数据输出、数据输入相连；无线基带处理芯片 U25 的射频电路控制线与射频输出电路 U30 的控制接口相连；双边带多模式射频芯片 U29 的 2.4G 频率接口、5G 频率接口分别与射频输出电路 U30 的 2.4G 频率接口、5G 频率接口相连。

6、一种基于码分多址技术的移动无线局域网接入装置的接入方法，其特征在于该接入方法具体包括以下步骤：

1.）该装置通过 CDMA 接口电路（13）实现 CDMA 网络接入，并通过认证与因特网连接，

2.）该装置通过无线局域网接入模块接口电路（12）与其他无线局域网设备连接，

3.）该装置同时通过第一 10/100M 以太网接口电路（6）和第二 10/100M 以太网接口电路（7）与有线网络进行连接，

4.）该装置将无线局域网接入模块接口或以太网接口接入的用户数据根据路由策略通过 CDMA 接口进行转发，同时将 CDMA 接口接收的数据根据接收目的地址通过无线局域网模块接口或以太网接口转发。

基于码分多址技术的移动无线局域网接入装置及方法

技术领域

本发明涉及一种局域网接入装置及其方法，尤其涉及一种基于码分多址技术（CDMA）的移动无线局域网接入装置及其方法，本发明属于无线网络通信接口技术领域。

背景技术

无线局域网(WLAN ，Wireless Local Area Network)作为无线通信网络的一个重要组成部分，近几年已经成为一个在通信技术领域取得巨大成功的典范；尤其是基于IEEE 802.11协议族的无线局域网目前已成为无线局域网领域中的主流，取得了广泛的应用，基本上成了无线局域网的代名词。目前无线局域网的应用模式可以分为两大类：一类是企业或个人自建的无线局域网，另一类是电信营运商构建的可运营的公共无线局域网（PWLAN)。PWLAN在机场、车站、酒店、旅馆、超市、剧场、公园、会议场所等人口密集的公共热点地区部署基于无线局域网技术，提供高带宽无线互联网接入服务。当今，随着WLAN市场的快速增长，公共无线局域网逐渐受到网络服务提供商(ISP)和蜂窝运营商（Celluar Operator）的青睐得到大规模的部署。无线局域网有着有线网络无法媲美的优点：可以在特定的环境，特定的时间随意构建网络；无线局域网又不像2G 或3G 那么庞大复杂，它更小巧，更灵活，更廉价，同时提供了更高的接入带宽。另一方面，随着无线局域网带宽的增加，以及视频编解码技术的发展，使无线局域网中的视频传输成为可能，也为无线局域网的视频通信提供了广阔的发展空间。现有的公共无线局域网多由小型的无线网络服务提供商(WISP)架构，缺乏一个有效的面向大众的收费平台。一般说来，虽然WLAN可以提供高速的数据业务，但WLAN却缺少对用户进行鉴权与计费机制，而且无线局域网的覆盖范围较小，一般都在热点地区，用户使用时受到地点限制，除此以外它还具有以

下缺点：1）公共无线局域网架构复杂，部署不便；需要经过专业培训的人员进行架构部署，不方便公共无线局域网的推广。2）现有公共无线局域网还是依托于有线网络的无线扩展，架构中不可避免的需要铺设网线，会对原有建筑装潢造成破坏，这也阻碍了在公共热点地区的推广。3）现有公共无线局域网只能应用向静止、准静止的状态下的人群提供无线宽带数据业务。4） 缺乏有效的收费模式。相比之下CDMA2000 1X网络经过多年的研究和实践，不仅有成熟的鉴权和计费机制，并且具有广覆盖的特点。如果互补两网的优势，将两网结合起来，将为运营商提供良好的发展用户、扩展用户的空间。

发明内容

技术问题：本发明的目的在于克服现有技术中的不足，提供一种基于码分多址技术的移动无线局域网接入装置及方法，通过 CDMA 1X 技术在移动环境和准静止环境下提供高带宽无线互联网接入的无线局域网接入设备。

技术方案：本发明将 WLAN 数据转换成 CDMA1X 数据，通过网络无线转发网络数据到互联网；使得用户通过无线局域网链路与本发明装置相连时可以共享多路 CDMA 带宽。

在电路结构上：嵌入式微处理器与电源供电电路、时钟电路、复位电路直接相连；嵌入式微处理器经过调试线与 JTAG 调试电路相连；嵌入式微处理器经过第一数据控制线与第一 10/100M 以太网接口电路相连，经过第二数据控制线与第二 10/100M 以太网接口电路相连，经过第三数据控制线与 USB 接口电路相连，经过第四数据控制线与串行接口电路相连，经过第五数据控制线与 CDMA 接口电路组成相连；经过第一数据地址线与随机存取电路相连，经过第二数据地址线与闪存电路相连，经过第三数据地址线与无线局域网接入模块接口电路相连。

嵌入式微处理器经过第四数据控制线与 CDMA 接口电路相连，具体表现在：嵌入式微处理器的扩展地址总线与译码器 U3 的地址线通过地址线相连；嵌入式微处理器的扩展地址总线与通用异步收发器 U2 的地址线通过地址线相连；嵌入式微处理器的通用 I/O 接口与通用异步收发器 U2 的串口中断通过中断线相连；嵌入式微处理器的扩展数据总线与通用异步收发器 U2 的数据线通过数据线相连；嵌入式微处理器的扩

展写数据使能、扩展读数据使能与通用异步收发器 U2 的写使能、读使能相连。

CDMA 接口电路包括通用异步收发器 U2、译码器 U3、7.3728M 晶体振荡器、第一 CDMA 数据通信模块 U4、第二 CDMA 数据通信模块 U5、第三 CDMA 数据通信模块 U6、第四 CDMA 数据通信模块 U7，第一 R-UIM 智能卡接口 U8、第二 R-UIM 智能卡接口 U9、第三 R-UIM 智能卡接口 U10、第四 R-UIM 智能卡接口 U11 组成；通用异步收发器 U2 的扩展串口 1、扩展串口 2、扩展串口 3、扩展串口 4 和第一 CDMA 数据通信模块 U4、第二 CDMA 数据通信模块 U5、第三 CDMA 数据通信模块 U6、第四 CDMA 数据通信模块 U7 分别通过第一控制数据线、第二控制数据线、第三控制数据线、第四控制数据线相连；第一 CDMA 数据通信模块 U4、第二 CDMA 数据通信模块 U5、第三 CDMA 数据通信模块 U6、第四 CDMA 数据通信模块 U7 的 R-UIM 接口和第一 R-UIM 智能卡接口 U8、第二 R-UIM 智能卡接口 U9、第三 R-UIM 智能卡接口 U10、第四 R-UIM 智能卡接口 U11 的 UIM 卡数据接口分别通过 UIM 卡数据线相连。

嵌入式微处理器经过第三数据地址线与无线局域网接入模块接口电路相连，具体表现在：嵌入式微处理器的 PCI 控制器地址线、PCI 数据线、通用 I/O 接口、PCI 控制器分别与无线基带处理芯片 U25 的地址线、数据线、中断信号、控制线相连。

无线局域网接入模块接口电路包括无线基带处理芯片 U25，双边带多模式射频芯片 U29，射频输出电路 U30 组成；无线基带处理芯片 U25 的模数转换接口、数模转换接口、射频重启动、时钟接口、数据输入口、数据输出口分别和双边带多模式射频芯片 U29 的射频接收接口、射频发送接口、重启动、数据时钟、数据输出、数据输入相连；无线基带处理芯片 U25 的射频电路控制线与射频输出电路 U30 的控制接口相连；双边带多模式射频芯片 U29 的 2.4G 频率接口、5G 频率接口分别与射频输出电路 U30 的 2.4G 频率接口、5G 频率接口相连。

接入方法具体包括以下步骤：

1.）该装置通过 CDMA 接口电路实现 CDMA 网络接入，并通过认证与因特网连接，

2.）该装置通过无线局域网接入模块接口电路与其他无线局域网设备连接，

3.）该装置同时通过第一 10/100M 以太网接口电路和第二 10/100M 以太网接口电路与有线网络进行连接，

4.）该装置将无线局域网接入模块接口或以太网接口接入的用户数据根据路由

策略通过 CDMA 接口进行转发，同时将 CDMA 接口接收的数据根据接收目的地址通过无线局域网模块接口或以太网接口转发。

有益效果： WLAN 虽然可以提供高速的数据业务，但 WLAN 却缺少对用户进行鉴权与计费机制，而且无线局域网的覆盖范围较小，一般都在热点地区，用户使用时受到地点限制。CDMA2000 1X 网络经过多年的研究和实践，不仅有成熟的鉴权和计费机制，并且具有广覆盖的特点。本发明充分利用两网的优势，将两网结合起来，利用 CDMA2000 1X 和 WLAN 技术提供一个可以部署在移动环境或静止环境的轻量级纯无线网络连接的网络接入系统。该装置部署简单，只需提供电源即可实现无线网络连接，内网提供 802.11b/g 宽带无线接入服务和 10/100M 以太网接入服务，外网接口采用 4 路 CDMA2000 1X 数据链路连接到 CDMA 网，通过 CDMA 运营商现有的网络实现互联网访问。该装置可以方便地组建无线局域网、有线局域网以及两者的混合型网络，并为其中的用户提供便捷的英特网接入服务。将为运营商提供良好的发展用户、扩展用户的空间。

附图说明

图 1 是本发明的电路原理总框图，其中有：嵌入式微处理器 1、电源供电电路 2、时钟电路 3、复位电路 4、JTAG 调试电路 5、10/100M 以太网接口电路 6、10/100M 以太网接口电路 7、通用串行总线（USB）接口电路 8、串行接口电路 9、随机存取电路 10、闪存电路 11、无线局域网接入模块接口电路 12、CDMA 接口电路 13；调试线 14、第一数据控制线 15、第二数据控制线 16、第三数据控制线 17、第四数据控制线 18、第一数据地址线 19、第二数据地址线 20、第三数据地址线 21、第五数据控制线 22。

图 2 是本发明嵌入式微处理器 1 与 CDMA 接口电路 13、复位电路 4 连接的电路原理图。

图 3 是本发明嵌入式微处理器 1 与 10/100M 以太网接口电路 6、10/100M 以太网接口电路 7、通用串行总线（USB）接口电路 8、串行接口电路 9 连接的电路原理图。

图 4 是本发明嵌入式微处理器 1 与时钟电路 3、复位电路 4、JTAG 调试电路 5、闪存电路 11、无线局域网接入模块接口电路 12 连接的电路原理图。

具体实施方式

在电路中：U1 是嵌入式微处理器 Intel IXP425 网络处理器；U2 是串口扩展芯片 ST16C554D 通用异步收发器。U3 是 74138 数据选择器；U4～U7 是 CM800A 作为 CDMA 数据通信模块；U8～U11 是 R-UIM 智能卡接口；U12、U13 是 10/100M 以太网接口。U14 是 USB 接口；U15 是串行通信接口；U16～U17 是以太网电平转换接口；U18～U19 是 DM9161 以太网物理层芯片；U20 是 ISP1161A1 通用串行总线控制器；U21 是 SP3232E 一种 RS-232 通讯器；U22、U23、U26、U27 是 HY57V561620B 存储芯片；U24、U28 是 Intel TE28F128 Flash 芯片；U25 是 5GHz 和 2.4GHz 无线局域网多协议 MAC/基带处理器 AR5212；U29 是支持 IEEE 802.11a/b/g 无线局域网的双边带多模式射频芯片；U30 是射频输出电路和天线整合模块。

以下具体的实施例结合附图对本发明的技术方案作进一步详细描述：本实施例在以本发明技术方案为前提下进行实施，给出了详细的实施方式和具体的操作过程，但本发明的保护范围不限于下述的实施例。

本实施例硬件环境：

嵌入式微处理器 1：具体采用 Intel Xscale 系列网络处理器；

电源供电电路 2：具体采用 LM1084 线性电源芯片以及 1117 系列电源芯片；

时钟电路 3：具体采用 33MHZ 晶体振荡器；

复位电路 4：具体采用 SN74AHC1G04 芯片；

JTAG 调试电路 5：具体采用标准的 JTAG 接口与芯片 JTAG 接口相连；

第一 10/100M 以太网接口电路 6：具体采用 25MHZ 晶体振荡器、DM9161 以太网物理层 TX/FX 收发器芯片和 11F-05 以太网电压转换接口芯片；

第二 10/100M 以太网接口电路 7：具体采用 25MHZ 晶体振荡器、DM9161 以太网物理层 TX/FX 收发器芯片和 11F-05 以太网电压转换接口芯片；

通用串行总线（USB）接口电路 8：具体采用 6MHZ 晶体振荡器、ISP1161A1 通用串行总线控制器芯片；

串行接口电路 9：具体采用 SP3232E TTL 电平转换芯片；

随机存取电路 10：具体采用四片 HY57V561620CT-H 芯片；

闪存电路 11：具体采用两片 Intel TE28F128；

无线局域网接入模块接口电路 12：具体采用 Atheros 公司的 AR5212 芯片作为基带控制模块，采用双边带多模式射频芯片 AR5112 作为射频模块，支持 802.11 b/g 两种模式。

CDMA 接口电路 13：具体采用 7.3728MHZ 晶体振荡器、74138 译码器芯片、ST16C554D 串口扩展芯片和韩国 GIGA 公司的 CM800A 模块。

嵌入式微处理器 1 与电源供电电路 2、时钟电路 3、复位电路 4 直接相连；嵌入式微处理器 1 经过调试线 14 与 JTAG 调试电路 5 相连；嵌入式微处理器 1 经过第一数据控制线 15 与第一 10/100M 以太网接口电路 6 相连，经过第二数据控制线 16 与第二 10/100M 以太网接口电路 7 相连，经过第三数据控制线 17 与 USB 接口电路 8 相连，经过第四数据控制线 18 与串行接口电路 9 相连，经过第五数据控制线 22 与 CDMA 接口电路组成 13 相连；经过第一数据地址线 19 与随机存取电路 10 相连，经过第二数据地址线 20 与闪存电路 11 相连，经过第三数据地址线 21 与无线局域网接入模块接口电路 12 相连。

如图 2 所示，由电路模块 U2～U11 构成 CDMA 接口电路 13。CDMA 模块接口采用 4 路 CDMA2000 1X 数据链路连接到 CDMA 网，通过 CDMA 运营商现有的网络实现互联网访问，四路传输，增加数据传输速度。图中，U8～U11 是 R-UIM 智能卡它是专为 CDMA 蜂窝系统应用设计的。U4～U7 是韩国 GIGA 公司的 CM800A 模块用作 CDMA 通信，模块中的 Q2458 单边带模块提供一个 3.0V 的 R-UIM 接口。CM800A 是为数据通信而设计的 CDMA 调制解调器，支持 IS-95A,B,C 协议，拥有标准的 RS-232 接口，能够通过 AT 指令进行远程控制，数据传输最高达 153.6Kbps。U2 是 ST16C554D 芯片，通过外接晶振提供系统时钟，同时提供四路通用异步收发器（UART），将微处理器 Intel IXP425 的扩展总线扩展为四路 RS232 串口 TTL 电平电路。ST16C554D 主要为 UART 收、发单元的数据提供串行-并行、并行-串行转换。CM800A 模块通过 RS-232 接口与 ST16C554D 芯片相连。嵌入式微处理器 U1 通过扩展地址线控制 74138 译码器 U3 选择 ST16C554D 的一路 UART 通道；另一路扩展地址线控制 ST16C554D 的内部寄存器，这些状态寄存器为用户提供错误提示，操作状态，和调制解调器接口的控制， 并可以根据用户的需要定制系统中断；通用 I/O 接口连接 ST16C554D 的串口中断，微处理器根据中断信号执行相应的中断处理程序；扩展数据线和读写信号线协同工作完

成数据的读写过程。这一系列模块相互协作实现了 1～4 路 CDMA2000 1X 数据链路到 CDMA 网络的连接。作为整个系统的前端，它的实现直接影响到整个局域网在移动环境中通过无线方式接入 Internet 的实现。通过四路 CDMA 模块的连接，本系统的 CDMA 传输数上限可高达 600kbps，平均速率为 320kbps，可以达到一般的宽带标准。

图 3 中，U12、U13 是 10/100M 以太网接口，通过电平转换器 U16、U17，与以太网物理层 TX/FX 收发器 U18、U19 相连接。电平转换器事实上起了一个电平转换的的功能，实现 3.3V 到以太网电平的转换。U18 和 U19 是 DM9161 芯片，定位于 IEEE 802.3 物理层的应用，它为大多数 802.3 标准控制器到 100BASE-TX、100BASE-FX 和 10BASE-T 介质提供接口电路，实现了 802.3U 定义的 100BASE-TX 的全部的物理层功能，支持自动商议，对媒介速度和协议选择自动选择，另外，DM9161 内部具有整形滤波器，无需外部滤波器对信号进行转换。在该以太网接口的实现中使用 25MHz 外部时钟输入，芯片的信号线与微处理器 Intel IXP425 的 MII 接口相应的信号线相连接，MII 接口拥有独立的媒体接入控制器和网络处理引擎，符合 IEEE802.3 规范。以太网接口主要实现以有线方式接入 Internet 或作为监管数据的上传通路。U14 是一个 USB 接口，它与 USB 通用串行总线控制器 U20 相连接。USB 通用串行总线控制器 U20 采用 ISP1161A1 芯片，该芯片支持主机控制器（HC）和设备控制器（DC），遵循 USB2.0 规范，支持数据传送率在全速时达到 12Mbit/s，在低速时达到 1.5 Mbit/s。ISP1161A1 采用 6MHz 晶振输入，数据线和控制线分别与微处理器的扩展总线和通用 I/O 接口相连接，完成读写控制过程。U15 是串行通信接口，它与串行通信控制器 U21 相连。串行通信控制器采用 TTL 电平转换芯片 SP3232E。因为该硬件系统需要由宿主机调试，所以这里 UART 主要在开发阶段用来对系统进行配置与调试（作为控制口）。

图 4 中，由电路模块 U22、U23、U26、U27 构成了随机存取电路 10；由电路模块 U24 和 U28 构成了闪存电路 11；由电路模块 U25、U29、U30 构成了无线局域网接入模块接口电路 12；其次还包含了电源供电电路 1-2、时钟电路 3、复位电路 4 和 JTAG 调试电路 5。

电源供电电路 2 提供了系统所需要各种电压，本系统的供电部分共需要 4 种电平，分别是直流 5V、3.3V、1.3V 和 3.6V。其中，5V、3.3V、1.3V 的电源主要给

CPU 和大部分芯片供电，而 3.6V 电源是为 I/O 部分连接的 CDMA 模块提供所需要的电平。在电源模块电路中，采用外部整流提供的 5V 的直流电源，再通过 LT1084 电源调整芯片来完成第二步变压形成稳定低纹波的+3.3V 和+1.3V 的电压供应。+3.6V 的电压由于只在 CDMA 模块部分需要，所以单独使用 4 个 1117 系列电压调整芯片为四路 CDMA 模块提供稳定的+3.6V 电压。

时钟电路 3 主要是通过一个 33MHz 的晶振给出激励，产生的时钟信号先经过一个分频器，生成四路不变频率的信号，分别给 CPU 芯片，FLASH 芯片和 miniPCI 接口部分电路提供时钟信号。这些时钟信号帮助各部分在上电和复位的时候完成与 CPU 的同步。Intel IXP425 网络处理器工作 533MHz 的主频上，微处理器的输入时钟由处理器的内部乘法器倍频至 133MHz，用来驱动 PC133 SDRAM 接口。本平台采用 IDT2308-1H 芯片完成分频功能，它是一种高速相位锁存循环时钟乘法器，用于时钟信号分发，工作频率范围 10～133MHz。

复位电路 4 由开关器件和非门电路构成，完成整个系统的复位。非门由芯片 SN74AHC1G04 实现 。

JTAG 调试点路 5 是由调试接口和上拉电阻构成的，它与微处理器的 JTAG 接口相连接，主要用作程序的下载和调试。

随机存取电路 10 是系统的主存电路，微处理器 IXP425 支持 PC-133 的 16bit 宽度 SDRAM，最小是 32MB，最大是 256MB，在本系统中，SDRAM 由 4 片 16M*16 的 HY57V561620CT-H 芯片组成 128MB 的存储空间。随机存取电路和 Intel Xscale 网络处理器之间的数据通过数据线来连接，地址则通过地址线来连接。在这部分电路中，对 SDRAM 的读写操作是 32 位数据总线的数据传输，需要两片 SDRAM 组合从而提供 32Bits 的数据宽度。每组的两个 SDRAM 芯片要同时工作，要求两个 SDRAM 芯片使用相同的片选信号，相同的时钟输入，相同的地址线连接。而不同组的 SDRAM 之间是通过片选信号来区分的，另外控制线选择了外部命令到来的时候接受操作的芯片。闪存电路 5 由两片 16MByte 的 Intel TE28F128 芯片组成。

本系统中闪存电路 11 是通过 CPU 的扩展总线连接的，总线的数据总线为 16bit，地址总线为 24bit。通过外部总线自己的片选信号和总线上连接的其他设备区别开来。片选信号决定了选用的具体芯片，而片选信号是从 CPU 而来的读写控制

信号。另外还有来自 CPU 的 RESET_IN 信号，控制这部分电路的重启动。

无线局域网接入模块接口电路 12 主要提供 802.11 无线接入点功能。IXP425 支持 32bit 33/66MHz 的 PCI 控制器，这个 PCI 控制器内置 PCI arbiter，采用 host 模式，通过 PCI 总线连接无线局域网接入模块。无线基带处理芯片 U25 采用 Atheros 公司的 AR5212 芯片。它集成了 PCI\CARDBUS 主机接口。图中 IXP425 的 PCI 控制器的地址、PCI 数据线和 PCI 控制器与 AR5212 的对应信号线相连，完成嵌入式微处理器与无线接入设备电路 13 的交互。同时无线基带处理芯片 U25 集成了 MAC 层、基带处理器、数模\模数转换器，结合双边带多模式射频芯片 U29，组成一个低功耗高效率的无限局域网网卡和接入点的解决方案，双边带多模式射频芯片 U29 采用 AR5112 芯片。如图 4 所示，AR5212 芯片的模数转换接口，数模转换接口，数据输入接口和数据输出接口分别与 AR5112 芯片的对应信号线相连接完成了基带信号的处理和交互。AR5112 芯片提供双边带 2.4/5GHz 两种输出，其 2.4G 频率接口和 5G 频率接口与射频输出电路模块 U30 连接对应的信号线连接；同时 AR5212 的射频电路控制线与射频输出电路模块 U30 的对应信号线相连，完成输出模式的选择，可以支持所有的 IEEE 802.11a,802.11b,802.11g 的速率。作为整个系统的前端，无线接入设备电路担负着提供无线接入点功能和截获网络数据包的任务。

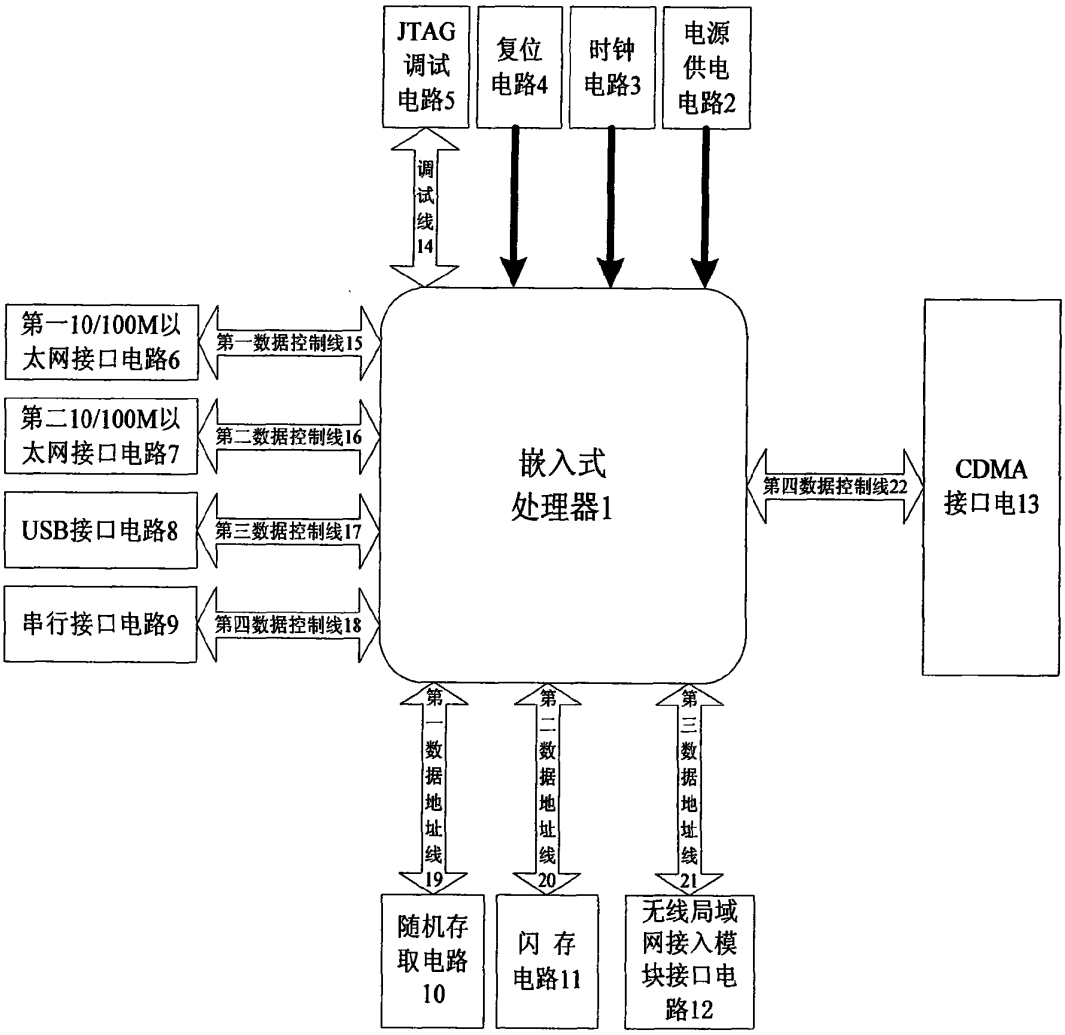

JTAG调试电路5
复位电路4
时钟电路3
电源供电电路2
调试线14
第一10/100M以太网接口电路6
第二10/100M以太网接口电路7
USB接口电路8
串行接口电路9
第一数据控制线15
第二数据控制线16
第三数据控制线17
第四数据控制线18
嵌入式处理器1
第四数据控制线22
CDMA接口电13
第一数据地址线19
第二数据地址线20
第三数据地址线21
随机存取电路10
闪 存电路11
无线局域网接入模块接口电路12

图 1

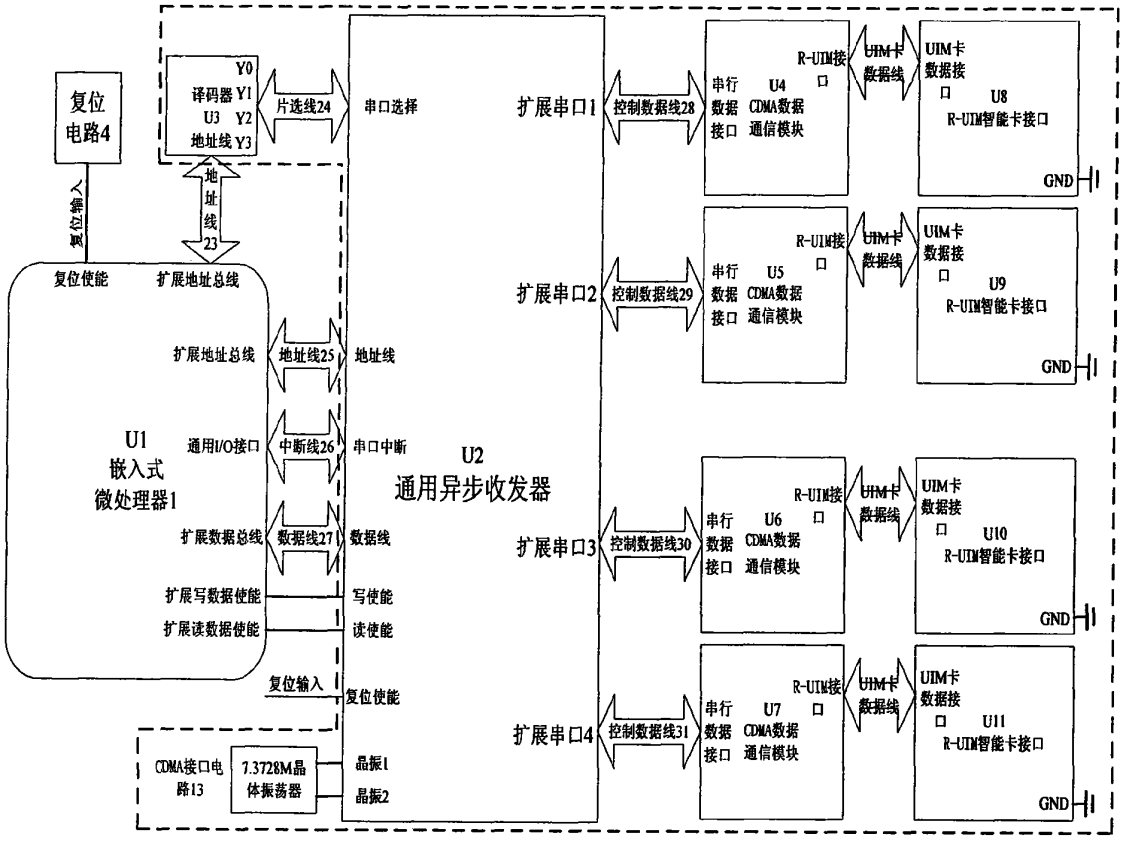

复位电路4
复位输入
复位使能
扩展地址总线
Y0
译码器 Y1
U3 Y2
地址线 Y3
片选线24
地址线23
串口选择
扩展串口1
扩展串口2
扩展串口3
扩展串口4
控制数据线28
控制数据线29
控制数据线30
控制数据线31
串行数据接口 U4 CDMA数据通信模块
串行数据接口 U5 CDMA数据通信模块
串行数据接口 U6 CDMA数据通信模块
串行数据接口 U7 CDMA数据通信模块
R-UIM接口
UIM卡数据线
UIM卡数据接口 U8 R-UIM智能卡接口
UIM卡数据接口 U9 R-UIM智能卡接口
UIM卡数据接口 U10 R-UIM智能卡接口
UIM卡数据接口 U11 R-UIM智能卡接口
GND
U1
嵌入式微处理器1
通用I/O接口
扩展地址总线
地址线25
地址线
中断线26
串口中断
U2
通用异步收发器
扩展数据总线
数据线27
数据线
扩展写数据使能
写使能
扩展读数据使能
读使能
复位输入
复位使能
CDMA接口电路13
7.3728M晶体振荡器
晶振1
晶振2

图 2

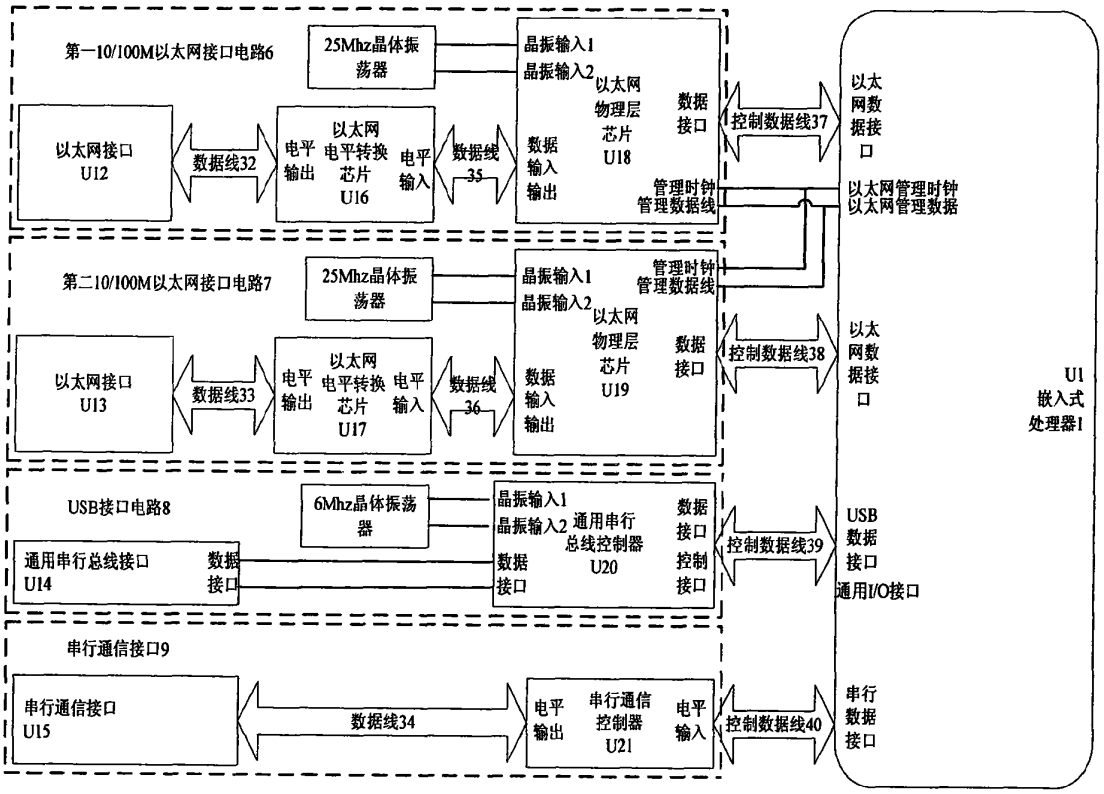

第一10/100M以太网接口电路6
25Mhz晶体振荡器
晶振输入1
晶振输入2
以太网物理层芯片U18
数据输入输出
数据接口
管理时钟
管理数据线
以太网接口U12
数据线32
以太网电平转换芯片U16
电平输出
电平输入
数据线35
控制数据线37
以太网数据接口
以太网管理时钟
以太网管理数据
第二10/100M以太网接口电路7
25Mhz晶体振荡器
晶振输入1
晶振输入2
以太网物理层芯片U19
数据输入输出
数据接口
管理时钟
管理数据线
以太网接口U13
数据线33
以太网电平转换芯片U17
电平输出
电平输入
数据线36
控制数据线38
以太网数据接口
U1
嵌入式处理器1
USB接口电路8
6Mhz晶体振荡器
晶振输入1
晶振输入2
通用串行总线控制器U20
数据接口
控制接口
通用串行总线接口U14
数据接口
控制数据线39
USB数据接口
通用I/O接口
串行通信接口9
串行通信接口U15
数据线34
电平输出
电平输入
串行通信控制器U21
控制数据线40
串行数据接口

图 3

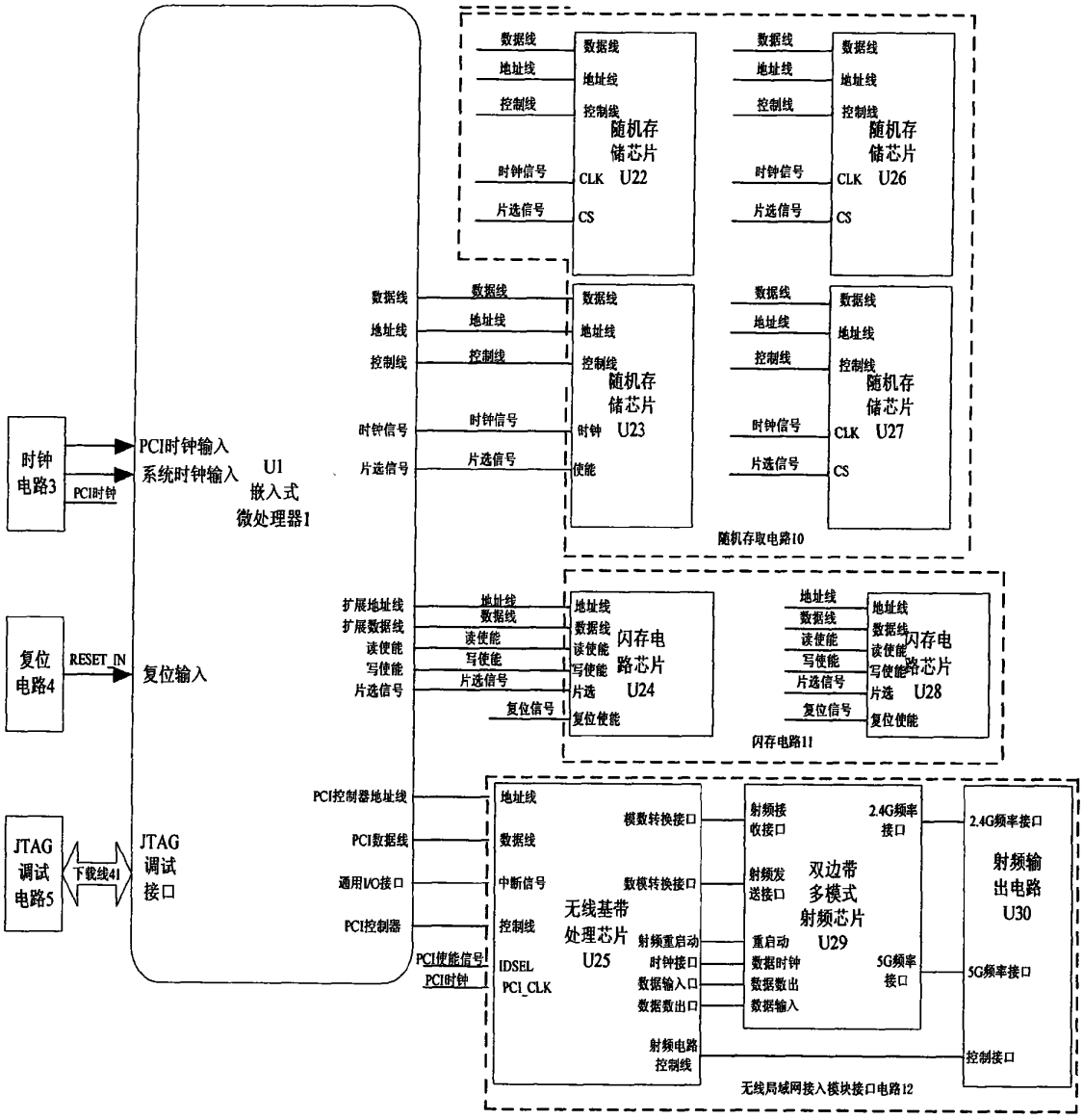

时钟电路3
PCI时钟
PCI时钟输入
系统时钟输入
U1
嵌入式微处理器1
复位电路4
RESET_IN
复位输入
JTAG调试电路5
下载线41
JTAG调试接口
数据线
地址线
控制线
时钟信号
片选信号
随机存储芯片
CLK U22
CS
CLK U26
时钟 U23
使能
CLK U27
随机存取电路10
扩展地址线
扩展数据线
读使能
写使能
闪存电路芯片
片选 U24
复位信号
复位使能
片选 U28
闪存电路11
PCI控制器地址线
PCI数据线
通用I/O接口
PCI控制器
PCI使能信号
PCI时钟
无线基带处理芯片 U25
IDSEL
PCI_CLK
模数转换接口
数模转换接口
射频重启动
时钟接口
数据输入口
数据数出口
射频电路控制线
双边带多模式射频芯片 U29
射频接收接口
射频发送接口
重启动
数据时钟
数据数出
数据输入
2.4G频率接口
5G频率接口
射频输出电路 U30
控制接口
无线局域网接入模块接口电路12

图 4

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 12/14 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200510086507.4

[43] 公开日 2007 年 3 月 28 日

[11] 公开号 CN 1937511A

[22] 申请日 2005.9.23
[21] 申请号 200510086507.4
[71] 申请人 中兴通讯股份有限公司
地址 210012 广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦 A 座 6 层
[72] 发明人 秦 霞

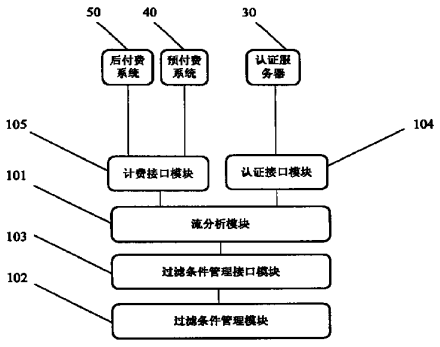
[74] 专利代理机构 北京律诚同业知识产权代理有限公司
代理人 梁 挥 徐金国
权利要求书 5 页 说明书 11 页 附图 5 页

[54] 发明名称

计费信息采集系统及采集方法和计费实现系统及实现方法

[57] 摘要

本发明公开了一种计费信息采集系统及采集方法和计费实现系统及实现方法，其中该计费信息采集系统包括一过滤条件管理模块，用于设置并存储有用于流分析和控制的过滤条件；流分析模块，用于根据过滤条件对移动终端访问数据业务的业务流进行分析，提取数据业务的业务内容特征码、业务标识及业务类别信息；过滤条件管理接口模块，连接过滤条件管理模块和流分析模块；认证接口模块，用于将业务内容特征码发送给认证服务器进行认证；及计费接口模块，用于将业务标识、业务类别发送给计费子系统进行计费处理。 应用本发明，可通过支持用户动态定制和修改过滤规则，扩展用户的业务特性，如 QOS 特性和安全特性。



1、一种计费信息采集系统，其特征在于，包括：

一过滤条件管理模块，用于设置并存储有用于流分析和控制的过滤条件；

一流分析模块，用于根据所述过滤条件对移动终端访问数据业务的业务流进行分析，提取数据业务的业务内容特征码、业务标识及业务类别信息；

一过滤条件管理接口模块，连接所述过滤条件管理模块和所述流分析模块；

一认证接口模块，用于将所述业务内容特征码发送给认证服务器进行认证；

一计费接口模块，用于将所述业务标识、业务类别发送给计费子系统进行计费处理。

2、根据权利要求 1 所述的计费信息采集系统，其特征在于，所述流分析模块还用于根据所述认证服务器、计费子系统的返回消息及过滤条件控制所述业务流。

3、根据权利要求 2 所述的计费信息采集系统，其特征在于，所述过滤条件管理模块用于设置过滤条件中的网络与传输层参数、应用层参数及策略和计费控制参数；所述流分析模块根据所述网络与传输层参数和应用层参数对业务流进行分析，并根据所述认证服务器、计费子系统的返回消息及所述策略和计费控制参数控制所述业务流。

4、一种计费实现系统，包括移动终端、计费子系统，其特征在于，还包括一业务流计费信息采集系统及一认证服务器，所述计费信息采集系统包括：

一过滤条件管理模块，用于设置并存储有用于流分析和控制的过滤条件；

一流分析模块，用于根据所述过滤条件对所述移动终端访问数据业务的业务流进行分析，提取数据业务的业务内容特征码、业务标识及业务类别信息；

一过滤条件管理接口模块，连接所述过滤条件管理模块和所述流分析模块；

一认证接口模块，用于将所述业务内容特征码发送给所述认证服务器进行认证；

一计费接口模块，用于将所述业务标识、业务类别发送给计费子系统进行

计费处理。

5、根据权利要求 4 所述的业务流计费实现系统，其特征在于，所述认证服务器 30 包括但不限于 AAA 服务器。

6、根据权利要求 4 所述的业务流计费实现系统，其特征在于，所述流分析模块还用于根据所述认证服务器、计费子系统的返回消息及过滤条件控制所述业务流。

7、根据权利要求 6 所述的计费信息采集系统，其特征在于，所述过滤条件管理模块具体用于设置过滤条件中的网络与传输层参数、应用层参数和策略和计费控制参数；

所述流分析模块根据所述网络与传输层参数和应用层参数对业务流进行分析，并根据所述认证服务器、计费子系统的返回消息及所述策略和计费控制参数控制所述业务流。

8、权利要求 1 所述的计费信息采集系统实现计费信息采集的方法，其特征在于，包括以下步骤：

步骤 1，过滤条件管理模块设置并存储用于流分析和控制的过滤条件；

步骤 2，流分析模块根据所述过滤条件对移动终端访问数据业务的业务流进行分析，提取数据业务的业务内容特征码、业务标识及业务类别信息；

步骤 3，所述流分析模块将所述业务内容特征码发送给认证服务器进行认证；

步骤 4，所述流分析模块将所述业务标识、业务类别发送给计费子系统进行计费处理。

9、根据权利要求 8 所述的计费信息采集方法，其特征在于，所述步骤 1 具体包括：

步骤 11，过滤条件管理模块设置过滤条件中的 IP 5 元组；

步骤 12，过滤条件管理模块设置过滤条件中的应用层参数；

步骤 13，过滤条件管理模块设置过滤条件中的策略和计费控制参数；

所述步骤 2 中，所述流分析模块根据所述网络与传输层参数和应用层参数对业务流进行分析。

10、根据权利要求 9 所述的计费信息采集方法，其特征在于，所述网络与传输层参数为 IP 5 元组，所述应用层参数包括应用协议类型和业务内容特征

码，所述步骤 2 具体包括以下步骤：

步骤 21，用户发出访问数据业务的 IP 报文，所述 IP 报文通过 Internet 网关送到所述流分析模块，所述流分析模块调用所述过滤条件管理模块对所述 IP 报文的 IP 5 元组信息与过滤条件的 IP 5 元组信息进行匹配；

步骤 22，匹配成功后，所述流分析模块调用所述过滤条件中的应用协议类型进行协议分析，获取所述 IP 报文的业务内容特征码；

步骤 23，所述流分析模块调用过滤条件管理模块将所述步骤 22 得到的业务内容特征码与所述过滤条件中的业务内容特征码进行匹配；

步骤 24，匹配成功，所述流分析模块调用所述过滤条件管理模块获取所述过滤条件对应的业务标识、业务类别；

步骤 25，所述流分析模块将业务特征码通过认证接口模块交给认证服务器进行内容认证；

步骤 26，用户访问数据业务的过程中，所述流分析模块周期性地采集所述 IP 5 元组、业务标识、业务类别及所述 IP 5 元组相关的计费信息通过计费接口模块送给计费系统进行计费处理；

步骤 27，转发所述 IP 报文。

11、根据权利要求 10 所述的计费信息采集方法，其特征在于，所述过滤条件为用户级过滤条件，且用户访问数据业务的过程中承载发生变化时，还包括更新过滤条件的步骤。

12、权利要求 4 所述的计费实现系统的计费实现方法，其特征在于，包括以下步骤：

步骤 S1，网关接收用户终端发出访问数据业务的 IP 报文并转发给流分析模块；

步骤 S2，过滤条件管理模块设置并存储用于流分析和控制的过滤条件；

步骤 S3，所述流分析模块根据所述过滤条件对移动终端访问数据业务的业务流进行分析，提取数据业务的业务内容特征码、业务标识及业务类别信息；

步骤 S4，所述流分析模块将所述业务内容特征码发送给认证服务器进行认证；

步骤 S5，所述流分析模块将所述业务标识、业务类别通过发送给计费子系统进行计费；

步骤 S6，所述计费子系统处理后返回计费响应消息给所述流分析模块。

13、根据权利要求 12 所述的计费实现方法，其特征在于，所述步骤 S2 具体包括：

步骤 S21，过滤条件管理模块设置过滤条件中的 IP 5 元组；

步骤 S22，过滤条件管理模块设置过滤条件中的应用层参数；

步骤 S23，过滤条件管理模块设置过滤条件中的策略和计费控制参数；

所述步骤 S3 中，所述流分析模块根据所述网络与传输层参数和应用层参数对业务流进行分析。

14、根据权利要求 13 所述的计费实现方法，其特征在于，所述网络与传输层参数为 IP 5 元组，所述应用层参数包括应用协议类型和业务内容特征码，所述步骤 S3 具体包括以下步骤：

步骤 S31，用户发出访问数据业务的 IP 报文，所述 IP 报文通过 Internet 网关送到所述流分析模块，所述流分析模块调用所述过滤条件管理模块对所述 IP 报文的 IP 5 元组信息与过滤条件的 IP 5 元组信息进行匹配；

步骤 S32，匹配成功后，所述流分析模块调用所述过滤条件管理模块根据应用协议类型进行协议分析，获取所述 IP 报文的业务内容特征码；

步骤 S33，所述流分析模块调用过滤条件管理模块将所述步骤 22 得到的业务内容特征码与所述过滤条件中的业务内容特征码进行匹配；

步骤 S34，匹配成功，所述流分析模块调用所述过滤条件管理模块获取所述过滤条件对应的业务标识、业务类别；

步骤 S35，所述流分析模块将业务特征码通过认证接口模块交给认证服务器进行内容认证；

步骤 S36，用户访问数据业务的过程中，所述流分析模块周期性地采集所述 IP 5 元组、业务标识、业务类别及所述 IP 5 元组相关的计费信息通过计费接口模块送给计费系统进行计费处理；

步骤 S37，转发所述 IP 报文。

15、根据权利要求 14 所述的计计费实现方法，其特征在于，所述过滤条件为用户级过滤条件，且用户访问数据业务的过程中承载发生变化时，还包括更新过滤条件的步骤。

16、根据权利要求 12、13、14 或 15 所述的计费信息采集方法，其特征在

于，所述计费系统为预付费系统和/或所述数据业务为预付费业务时，所述步骤 S5 具体以下步骤：

步骤 S51，向所述预付费系统上报计费请求和信用请求，请求消息中包括所述业务标识及业务类别；

步骤 S52，所述预付费系统收到所述计费请求后，取出所述业务标识和业务类别对应得到所述费率信息，再根据请求消息中包含的流量和时长计算用户消费的额度，从预付费账户中进行扣除，然后根据账户余额情况和该业务标识和业务类别所对应得业务逻辑生成计费响应消息发送；

步骤 S53，用户在访问数据过程中，周期性上报所述计费请求和信用请求，所述预付费系统周期性返回计费响应；

步骤 S54，所述流分析模块根据所述计费响应对业务流进行控制；

步骤 S55，用户去激活，所述流分析模块通知预付费系统计费停止。

17、根据权利要求 12、13、14 或 15 所述的计费实现方法，其特征在于，当所述计费系统为后付费系统和/或所述数据业务为后付费业务时，所述步骤 S5 具体以下步骤：

步骤 S51'，向所述后付费系统上报计费开始请求消息，所述计费开始请求消息中包含内容计费信息；

步骤 S52'，所述后付费系统对所述内容计费信息进行记录和存储；

步骤 S53'，用户访问数据过程中，周期性上报所述后付费系统更新所述内容计费信息；

步骤 S54'，用户去激活，通知所述后付费系统计费停止。

18、根据权利要求 12、13、14 或 15 所述的计费实现方法，其特征在于，所述认证服务器拒绝用户使用请求的数据业务，用户根据预先设定的重定向地址，将用户的访问重定向到 PORTAL 主页上，重新订阅业务，并由 PORTAL 服务器更新所述用户订阅的业务内容，并由所述认证服务器重新认证。

计费信息采集系统及采集方法和计费实现系统及实现方法

技术领域

本发明涉及移动分组域网络和业务网的计费系统及计费处理技术，特别是一种移动分组域网络和业务网共同实施内容计费时的计费系统及计费处理技术。

背景技术

目前针对数据业务的计费模式主要有包月制、流量计费和时长计费，而新兴的方式为按内容计费。

3G 是以分组交换网为网络核心，基于分组计费的流量计费，其计费要素是会话时间、数据流量、费率等，实现按总流量计费、上行流量计费、下行流量计费、按时段计费，按激活次数计费或包月制等，并可以对会话中的坏帧数减免费用，可以按时段、流量进行优惠处理。然而，这些传统的计费方式只能够简单得到用户在网络上传输的比特数量，无法挖掘数据业务因其内容所带来的深层次商业价值。

按内容计费方式下，数据业务本身通常是由第三方—内容提供商提供。数据多媒体业务根据业务内容大体有以下几类：浏览类业务、移动消息类业务、基于位置类业务、普通 Socket 业务、下载类业务、PUSH 类业务等。

数据业务的多类型势必要求计费的多样化和资费套餐的多样化。运营商已有的传统计费系统，在承载层只能够得到流量和时长的计费信息，而且不能够区分不同种类的业务；运营商网内只有多媒体消息服务器、WAP 网关和位置服务器等，只能提供有限的业务层计费信息；如何面向更广泛的数据业务，如何得到更丰富的计费信息，进而能够制定更丰富的资费策略、数据业务利润来源多样化，是今后各类移动运营商在数据业务方面所面临的重要问题。

基于流的内容计费技术（Content Based Charging）是指在网络侧，依据一定的规则把用户进行的业务区分出来，并分别统计时间、流量和事件信息，然后把这些信息用于预付费和后付费控制。

目前的基于流的内容计费技术解决方案只能静态进行内容计费，就是说在用户进行数据业务之前就需要配置好相关信息；这些配置好的信息在用户在线的时候，不能够随时的针对某个用户进行修改。这种方法的缺陷是不灵活，无法根据用户的个性化需求制订灵活的内容计费策略；而且规则的静态配置的扩展性不好，这种架构对其他业务特性（如 QOS、安全）支持不好。

发明内容

本发明的目的在于提供一种计费信息采集系统及采集方法和计费实现系统及实现方法，解决基于流的内容计费技术解决方案的不灵活、无法根据用户的个性化需求制订灵活的内容计费策略、扩展性不好、对其他业务特性（如 QOS、安全）支持不好的缺点。

为了实现上述目的，本发明提供了一种计费信息采集系统，其中，包括：

一过滤条件管理模块，用于设置并存储有用于流分析和控制的过滤条件；

一流分析模块，用于根据所述过滤条件对移动终端访问数据业务的业务流进行分析，提取数据业务的业务内容特征码、业务标识及业务类别信息；

一过滤条件管理接口模块，连接所述过滤条件管理模块和所述流分析模块；

一认证接口模块，用于将所述业务内容特征码发送给认证服务器进行认证；

一计费接口模块，用于将所述业务标识、业务类别发送给计费子系统进行计费处理；

上述的计费信息采集系统，其中，所述流分析模块还用于根据所述认证服务器、计费子系统的返回消息及过滤条件控制所述业务流。

上述的计费信息采集系统，其中，所述过滤条件管理模块用于设置过滤条件中的网络与传输层参数、应用层参数及策略和计费控制参数；所述流分析模块根据所述网络与传输层参数和应用层参数对业务流进行分析，并根据所述认证服务器、计费子系统的返回消息及所述策略和计费控制参数控制所述业务流。

为了更好的实现上述目的，本发明还提供了一种计费实现系统，包括移动终端、计费子系统，其中，还包括一业务流计费信息采集系统及一认证服务器，

所述计费信息采集系统包括：

一过滤条件管理模块，用于设置并存储有过滤条件；

一流分析模块，用于根据所述过滤条件对所述移动终端访问数据业务的业务流进行分析，提取数据业务的业务内容特征码、业务标识及业务类别信息；

一过滤条件管理接口模块，连接所述过滤条件管理模块和所述流分析模块；

一认证接口模块，用于将所述业务内容特征码发送给所述认证服务器进行认证；

一计费接口模块，用于将所述业务标识、业务类别发送给计费子系统进行计费处理。

为了更好的实现上述目的，本发明还提供了一种计费信息采集系统实现计费信息采集的方法，其中，包括以下步骤：

步骤 1，过滤条件管理模块设置并存储过滤条件；

步骤 2，流分析模块根据所述过滤条件对移动终端访问数据业务的业务流进行分析，提取数据业务的业务内容特征码、业务标识及业务类别信息；

步骤 3，所述流分析模块将所述业务内容特征码发送给认证服务器进行认证；

步骤 4，所述流分析模块将所述业务标识、业务类别发送给计费子系统进行计费处理。

为了更好的实现上述目的，本发明还提供了一种计费实现方法，其中，包括以下步骤：

步骤 S1，网关接收用户终端发出访问数据业务的 IP 报文并转发给流分析模块；

步骤 S2，过滤条件管理模块设置并存储过滤条件；

步骤 S3，所述流分析模块根据所述过滤条件对移动终端访问数据业务的业务流进行分析，提取数据业务的业务内容特征码、业务标识及业务类别信息；

步骤 S4，所述流分析模块将所述业务内容特征码发送给认证服务器进行认证；

步骤 S5，所述流分析模块将所述业务标识、业务类别通过发送给计费子系统进行计费；

步骤 S6，所述计费子系统处理后返回计费响应消息给所述流分析模块。

应用本发明的计费信息采集系统及采集方法和计费实现系统及实现方法，可通过支持用户动态定制和修改过滤规则，可以扩展用户的业务特性，如 QOS 特性和安全特性。

附图说明

图 1 为本发明的计费实现系统及计费信息采集系统结构图；

图 2 为本发明用于预付费系统的流程图；

图 3 为本发明用于后付费系统的流程图；

图 4 为本发明用户级过滤条件配置流程示意图；

图 5 为本发明过滤条件应用流程图。

具体实施方式

本发明提供了一种按内容计费的计费系统及其实现计费的方法，基于流分析实现，提供了一种动静结合的过滤条件管理方法。所谓动态过滤条件管理是指在用户在线的时候，也能够随时的针对某个用户所应用的规则进行修改。

按内容计费的计费系统实现计费的方法支持根据用户的个性化需求制订灵活的内容计费策略；另外，由于支持根据用户动态定制和修改过滤条件，过滤条件是采集内容计费信息的依据，可灵活地扩展用户的业务特性，如 QOS 特性和安全特性。

从作用范围来看，过滤条件还可以划分为两种：一种为全局性的过滤条件；另一种为专属于某个用户的过滤条件，即用户级过滤条件。

用户级过滤条件优先于全局性过滤条件，在两部分出现重叠的内容的时候，流分析的依据以用户级过滤条件为主，如果用户级过滤条件本身出现冲突，根据优先级大小决定采用哪一条过滤条件，本发明的按内容计费的计费系统可同时支持两种过滤条件。

如图 1 所示，本发明的按内容计费的计费系统包括：

计费信息采集系统，用于根据过滤条件采集计费信息，并控制业务流，包括流分析模块 101、过滤条件管理模块 102、过滤条件管理接口模块 103、认证接口模块 104 及计费接口模块 105；

认证服务器 30，通过认证接口模块 104 与流分析模块 101 相连，对计费信息采集系统 10 发送的请求认证消息进行认证；

计费系统，包括预付费系统 40 和后付费系统 50，根据流分析模块 101 采集的计费信息进行计费操作，并返回计费响应给流分析模块 101 对业务流进行控制。

本发明的按内容计费的计费系统包括如下模块：

流分析模块 101，根据过滤条件对流进行分析，提取业务内容特征码通过认证接口模块 104 送到认证服务器 30 进行内容的认证，同时提取过滤条件对应业务的标识和业务类别通过计费接口模块 105 送到预付费系统 40 或后付费系统 50 中进行批价、余额控制等处理；

过滤条件管理模块 102，用于管理和维护过滤条件，存储有过滤条件的集合，可配置在 PORTAL 服务器上，也可配置在认证服务器 30、预付费系统 40 或后付费系统 50 中，移动分组业务网中的 PORTAL 服务器是移动运营商向用户展示 ISP\ICP 服务提供商或内容提供商提供的诸多业务的平台，也是用户订阅业务、查询资费信息、查询帐户详情的自助服务平台；

该过滤条件管理模块 102 用于设置过滤条件，实现以下 3 部分功能：

设置过滤条件中的网络与传输层参数，包括源 IP 地址、目的 IP 地址、源端口号、目的端口号和协议类型，即 IP 5 元组；

设置过滤条件中的应用层参数，包括应用协议类型和业务内容特征码；

设置过滤条件中的策略和计费控制参数，包括对应业务的标识、业务类别、费率、优先级、触发动作列表、重定向地址、QOS 等级和参数、流量门限和时间门限等。

其中：

源 / 目的 IP 地址，为 IP 报文头中源地址/目的地址；

源 / 目的端口号，为 IP 报文头中源端口/目的端口；

协议类型，IP 报文头中的协议字段，表示传输层协议类型，UDP 或 TCP；

应用协议类型，指出流量分析的时候对符合上述源 / 目的 I P 地址、源 / 目的端口号源的流量使用何种应用协议特征进行分析；

业务内容特征码，该应用协议包含的可表示业务内容的信息，如对 http 来说，url 就是其业务内容特征码之一，但业务内容特征码不仅限于此；

过滤条件对应业务的标识，过滤条件所代表的业务的一个命名，可包含字符和数字的字符串，这个命名应当足够长，以避免重复；

业务类别，是对应过滤条件所代表的业务的分类，该分类的依据可以是费率，也可以是其他方便计费管理的依据；

费率，是指按照流量、时间或次数为服务制定的不同的价格策略；

优先级，表示过滤条件的优先程度，在多条过滤条件出现冲突的情况下，拥有较高优先级的规则胜出；

触发动作列表包含两项内容：承载事件和触发动作，用户的数据业务匹配到过滤条件之后，用户的承载发生了动作列表所列出的事件，就会触发列表中对应的动作；

重定向地址，指明将用户的数据重定向的目的地址，可以是 IP 地址，也可以是 URL；

QOS 等级和参数，指明过滤条件所匹配的业务的 QOS 等级和参数，在 diffserv（差分服务体系）中，要将流量映射到不同的服务等级，即 QOS 等级，QOS 参数就是用于流量策略和整形的具体参数，如平均速率、峰值速率等；

流量门限和时间门限是用户所能够使用的流量和时间的门限值。

网络传输层参数和应用层参数用于流量的分析，策略和计费控制参数用于实现对业务流的控制，可为上行和下行流量分别配置过滤条件，就是说可以对上下行流量应用不同的过滤条件；业务标识、流量门限和 QOS 等级和参数等都可以区分上下行设定，还可以在策略和计费控制部分扩展用户的其他属性，如安全特性；

过滤条件管理接口模块 103，与过滤条件管理模块 102 交互，负责配合管理和维护过滤条件，二者之间有多种接口形式可供使用，如 ftp、http、radius、cops 和 diameter-nasreq 协议等；

认证接口模块 104，负责和认证服务器 30 交互，认证服务器 30 包括但不限于 AAA 服务器，还可以是其他具备对用户和用户使用的业务内容进行认证能力的系统；

计费接口模块 105，负责与计费系统（包括预付费系统 40 和后付费系统 50）交互，将预付费的计费请求发给预付费系统 40，将后付费的话单信息交给后付费系统 50，并接受预付费系统 40 的计费响应，依据响应中的内容转化

为动作指示交给流分析模块 101，由流分析模块 101 进一步执行对流的控制和计费。

用户访问数据业务产生的流量在经过过滤条件的过滤后，才能判断出是否需要进行业务认证，再然后才有计费过程。这说明过滤条件是采集计费信息的依据，依据过滤条件确定哪些业务数据流需要计费后，仍然需要通过这些规则来确定数据业务所关联的流（IP 5 元组，包括）是哪些，这些流何时开始、何时结束，发生的流量有多少；进而上报这些计费信息，按内容计费的计费信息采集系统具体工作流程结合图 1 和如图 5，包括如下步骤：

步骤 S601，用户发出访问数据业务的 IP 报文，这些报文通过 Internet 的网关设备（如 GGSN）发送到流分析模块 101，流分析模块 101 调用过滤条件管理模块 102 对 IP 报文的 IP 5 元组信息与过滤条件的网络与传输层参数进行匹配；

步骤 S602，匹配成功后，流分析模块 101 调用过滤条件管理模块 102，并根据应用协议类型进行协议分析，获取协议的业务内容特征码，如过滤条件的应用协议类型指出为 HTTP 协议，协议分析就按照 HTTP 协议规范进行协议分析；

步骤 S603，流分析模块 101 将步骤 S602 得到的业务内容特征码与过滤条件中的业务内容特征码进行匹配；

步骤 S604，匹配成功，流分析模块 101 对应获取过滤条件对应的业务标识、业务类别，并由流分析模块 101 将业务特征码通过认证接口模块 104 交给认证服务器 30 进行内容认证；

步骤 S605，用户访问数据业务的过程中，流分析模块 101 周期性地采集该 IP 5 元组、业务标识、业务类别及该 IP 5 元组相关的计费信息（流量和时长）通过计费接口模块 105 送给计费系统（预付费系统 40 或后付费系统 50）；

步骤 S606，转发 IP 报文。

这样计费系统就依据过滤条件采集到了内容计费的计费信息。

结合图 1 所示，本发明的计费系统实现计费信息采集的方法中，流分析模块 101 根据全局性过滤条件，或根据全局性过滤条件和用户级过滤条件共同分析数据，并采集内容计费信息，向认证服务器 30 请求认证，并上报给计费系统 40 或 50。

对于匹配到全局过滤条件的业务流，处于移动分组域边缘的按内容计费的计费信息采集系统中的流分析模块101会通过认证接口模块104向认证服务器30发出认证请求（请求中可以包含IMSI、手机号码、IP地址、业务内容特征码等内容），请求认证该移动台是否有权限访问该业务；认证服务器30可以自行处理认证，也可以根据手机号码向用户所属的业务控制点（Service Control Point，SCP）进行认证；认证服务器30根据IMSI或手机号码检查用户的合法性；根据业务内容特征码和用户IMSI或手机号码的关联性验证用户是否具有使用该业务的合法性，然后返回认证请求响应消息给流分析模块101；

流分析模块101得到认证结果，如果认证失败，将用户的数据流重定向到运营商指定的 web 服务器给用户提示访问失败原因，这部分重定向的流量应该是免费的；如果认证成功，且是预付费类型的用户或预付费类型的业务，流分析模块101通过计费接口模块105向预付费系统40请求计费配额，根据响应中的配额决定转发多少数据流量或者时长；如果是后付费类型的用户或者后付费类型的业务，流分析模块101直接转发数据流，记录计费信息，并周期性的发送给后付费系统50。

移动台开始使用业务，流分析模块101定量或定时上报用户的使用量给付费系统；后付费系统50对计费信息进行记录；预付费系统40接受流分析模块101周期上报的计费请求，根据用户的帐户余额给出计费响应。用户下线，流分析模块101通知预付费系统40计费停止；通知后付费系统50计费停止；

运营商还可通过过滤条件管理模块 102 随时修改用户级过滤条件并实时生效，如果用户在线，用户级过滤条件会实时更新到流分析模块101。

下面结合图1和图2对本发明的按内容计费的计费系统实现预付费类型的内容计费及业务流控制的流程进行说明，其中过滤条件管理模块 102 设置在PORTAL服务器上或认证服务器30上，不包含用户级过滤条件，按内容计费的计费信息采集系统实现预付费类型的内容计费的方法包括如下具体步骤：

步骤S101a，在过滤条件管理模块102中定义全局过滤条件，并由PORTAL服务器下发，或

步骤S101b，在过滤条件管理模块102中定义全局过滤条件，并由认证服务器30下发，步骤S101a和步骤S101b不会同时存在，有一个发生另外一个就不需要重复进行，所以步骤S101b用虚线表示；

步骤 S102，移动终端激活上网，打开 Portal 门户主页，登录后，主页展示用户已经订阅的业务的超级链接和资费信息；

步骤 S103，用户点击某个服务提供商或内容提供商提供的超级链接，即某项业务，发出使用某业务的访问请求；

步骤 S104，流分析模块 101 根据全局过滤条件分析该访问请求，访问请求中可以包含 IMSI、手机号码、IP 地址、业务内容特征码等内容，请求认证该移动终端是否有权限访问该业务；认证服务器 30 可以自行处理认证，也可根据手机号码向用户所属的业务控制点（SCP）进行认证；认证服务器 30 根据 IMSI 或手机号码检查用户的合法性；根据业务内容特征码和用户 IMSI 或手机号码的关联性验证用户是否具有使用该业务的合法性，然后返回内容认证请求响应消息给流分析模块 101；也可只提取业务内容特征码交给内容认证服务器 30 进行认证，将认证结果返回给业务网关，如果认证服务器拒绝用户使用该内容的请求，进入步骤 S105，否则进入步骤 S106；

步骤 S105，流分析模块 101 根据过滤条件中定义的重定向地址，将用户的访问重定向到 PORTAL 主页上，由用户订阅业务，PORTAL 服务器更新用户新订阅的业务内容，以便认证服务器 30 可以正确的对用户进行认证，这两者的交互过程不在本案描述当中，用户在更新订阅业务内容后返回步骤 S103；

步骤 S106，流分析模块 101 根据过滤条件采集计费信息，并通过计费接口模块 105 向计费系统上报计费请求和信用请求，由于该用户属于预付费（在线计费）类型，因此再向预付费系统 40（在线计费系统）请求预付费控制，在请求中携带流分析模块 101 根据过滤条件分析业务流得到的过滤条件对应业务的标识及业务类别等信息；

步骤 S107，预付费系统 40 中保存有业务标识和业务类别对应的费率信息，收到流分析模块 101 的计费请求后，取出其中的业务标识和业务类别对应得到费率信息，再根据请求中包含的流量和时长计算用户消费的额度，从预付费账户中进行扣除，然后再根据账户余额情况和该业务标识和类别所对应得业务逻辑生成计费响应发给流分析模块 101，计费响应消息中可能携带计费信息；在此预付费系统 40 可由智能网实现，预付费根据计费请求中的用户信息、业务标识和业务类别决定业务的控制逻辑和计费，一个业务流的批价是在预付费系统中完成的；

步骤 S108，用户在访问数据过程中，流分析模块 101 周期性上报计费请求和信用请求，预付费系统 40 返回计费响应，可能携带有配额；

步骤 S109，流分析模块 101 根据预付费系统 40 给出的结果，对业务流进行控制；

步骤 S110，用户去激活，流分析模块 101 通知预付费系统计费停止。

如果用户属于后付费类型或业务属于后付费业务，按内容计费的计费信息采集系统直接转发业务数据，收集计费信息交给后付费系统，其中过滤条件管理模块 102 设置在 PORTAL 服务器上或认证服务器 30 上，同时不包含用户级过滤条件，结合图 1 和图 3 所示，包括以下步骤：

步骤 S201a，在过滤条件管理模块 102 中定义全局过滤条件，并由 PORTAL 服务器 60 下发，或

步骤 S201b，在过滤条件管理模块 102 中定义全局过滤条件，并由认证服务器 30 下发，步骤 S201a 和步骤 S201b 不会同时存在，有一个发生另外一个就不需要重复进行，所以步骤 S201b 用虚线表示；

步骤 S202，移动终端激活上网，打开 Portal 门户主页，登录后，主页展示用户已经订阅的业务的超级链接和资费信息；

步骤 S203，用户点击某个服务提供商或内容提供商提供的超级链接，即某项业务，发出使用某业务的访问请求；

步骤 S204，流分析模块 101 根据全局过滤条件分析服务请求，请求中可以包含 IMSI、手机号码、IP 地址和业务内容特征码等内容，请求认证该移动终端是否有权限访问该业务；认证服务器 30 可以自行处理认证，也可以根据手机号码向用户所属的业务控制点（SCP）进行认证；认证服务器 30 根据 IMSI 或手机号码检查用户的合法性；根据业务内容特征码和用户 IMSI 或手机号码的关联性验证用户是否具有使用该业务的合法性，然后返回内容认证请求响应消息给流分析模块 101；也可只提取业务内容特征码交给内容认证服务器 30 进行认证，将认证结果返回给业务网关，如果认证服务器 30 拒绝用户使用该内容的请求，进入步骤 S205，否则进入步骤 S206；

步骤 S205，流分析模块 101 根据过滤条件中定义的重定向地址，将用户的访问重定向到 PORTAL 主页上，由用户订阅业务，PORTAL 服务器更新用户新订阅的业务内容，以便认证服务器 30 可以正确的对用户进行认证，这两

者的交互过程不在本案描述当中，用户在更新订阅业务内容后返回步骤 S203；

步骤 S206，流分析模块 101 通过计费接口模块 105 向后付费系统 50 上报计费开始请求消息，该消息中包含报告内容计费信息；

步骤 S207，后付费系统 50 对这些信息进行记录和存储，用户访问数据过程中流分析模块 101 还会周期性上报后付费系统 50 更新这些信息；

步骤 S208，用户去激活，业务网关通知后付费系统计费停止。

图 2 和图 3 的流程不包括用户级过滤条件，在用户级过滤条件发生作用的情况下，用户级过滤条件配置流程结合图 1 和图 4 所示，对于步骤 S102 和步骤 S103（或步骤 S202 和步骤 S203）之间，还包含以下步骤：

步骤 S111，用户登录成功后，过滤条件管理模块 102 向流分析模块 101 发送触发授权请求消息，流分析模块 101 向过滤条件管理模块 102 返回触发授权请求响应消息；

步骤 S112，流分析模块 101 向过滤条件管理模块 102 发送授权请求消息，请求用户级过滤条件，过滤条件管理模块 102 在授权请求响应消息中携带用户级过滤条件发送给流分析模块 101；

步骤 S113，用户访问数据过程中，流分析模块 101 应用过滤条件，对流进行分析，其中过滤条件中的应用策略和计费控制部分对流进行控制，同时匹配到业务流之后，不再需要向认证服务器 30 进行认证；

步骤 S114，用户访问数据过程中，如果流的承载发生变化，且变化事件在过滤条件的触发动作列表之内，流分析模块 101 向过滤条件管理模块 102 发起更新用户级过滤条件的请求，在新规则到达之前，旧的规则继续生效；

步骤 S115，流分析模块 101 发送授权请求消息，过滤条件管理模块 102 在授权请求响应消息中携带新的用户级过滤条件发送给流分析模块 101。

如果不应用用户级过滤条件，上述流程就不需要发生。过滤条件中费率、优先级、触发动作列表、重定向地址、QOS 等级和参数、流量门限和时间门限等和用户属性关联起来，可出现在用户级过滤条件中。

当然，本发明还可有其它多种实施例，在不背离本发明精神及其实质的情况下，熟悉本领域的技术人员当可根据本发明作出各种相应的改变和变形，但这些相应的改变和变形都应属于本发明所附的权利要求的保护范围。

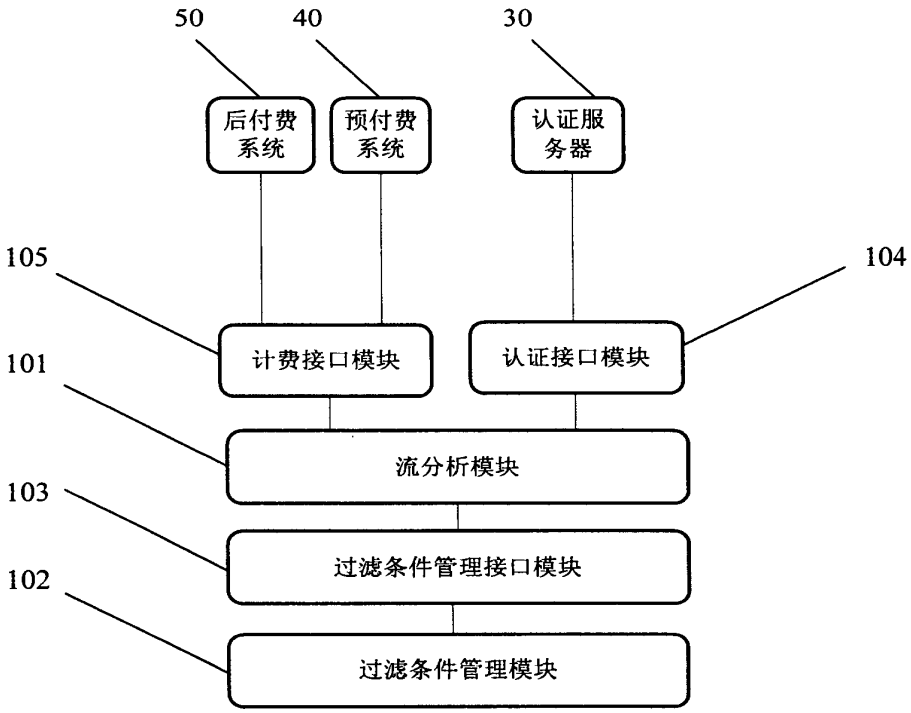

50
40
30
后付费系统
预付费系统
认证服务器
105
104
计费接口模块
认证接口模块
101
流分析模块
103
过滤条件管理接口模块
102
过滤条件管理模块

图 1

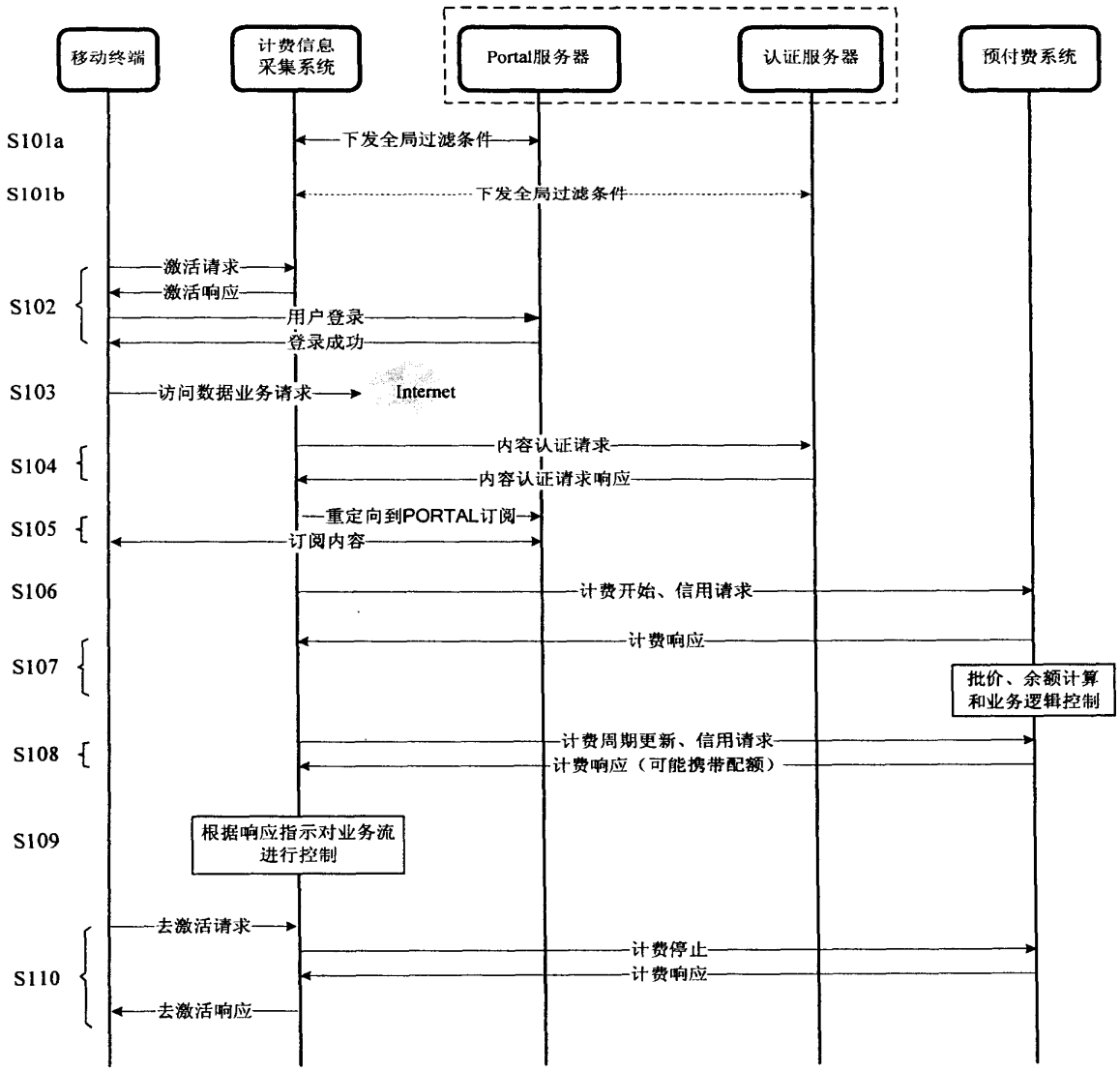

移动终端
计费信息采集系统
Portal服务器
认证服务器
预付费系统
S101a
下发全局过滤条件
S101b
下发全局过滤条件
S102
激活请求
激活响应
用户登录
登录成功
S103
访问数据业务请求
Internet
S104
内容认证请求
内容认证请求响应
S105
重定向到PORTAL订阅
订阅内容
S106
计费开始、信用请求
计费响应
S107
批价、余额计算和业务逻辑控制
S108
计费周期更新、信用请求
计费响应（可能携带配额）
S109
根据响应指示对业务流进行控制
S110
去激活请求
计费停止
计费响应
去激活响应

图 2

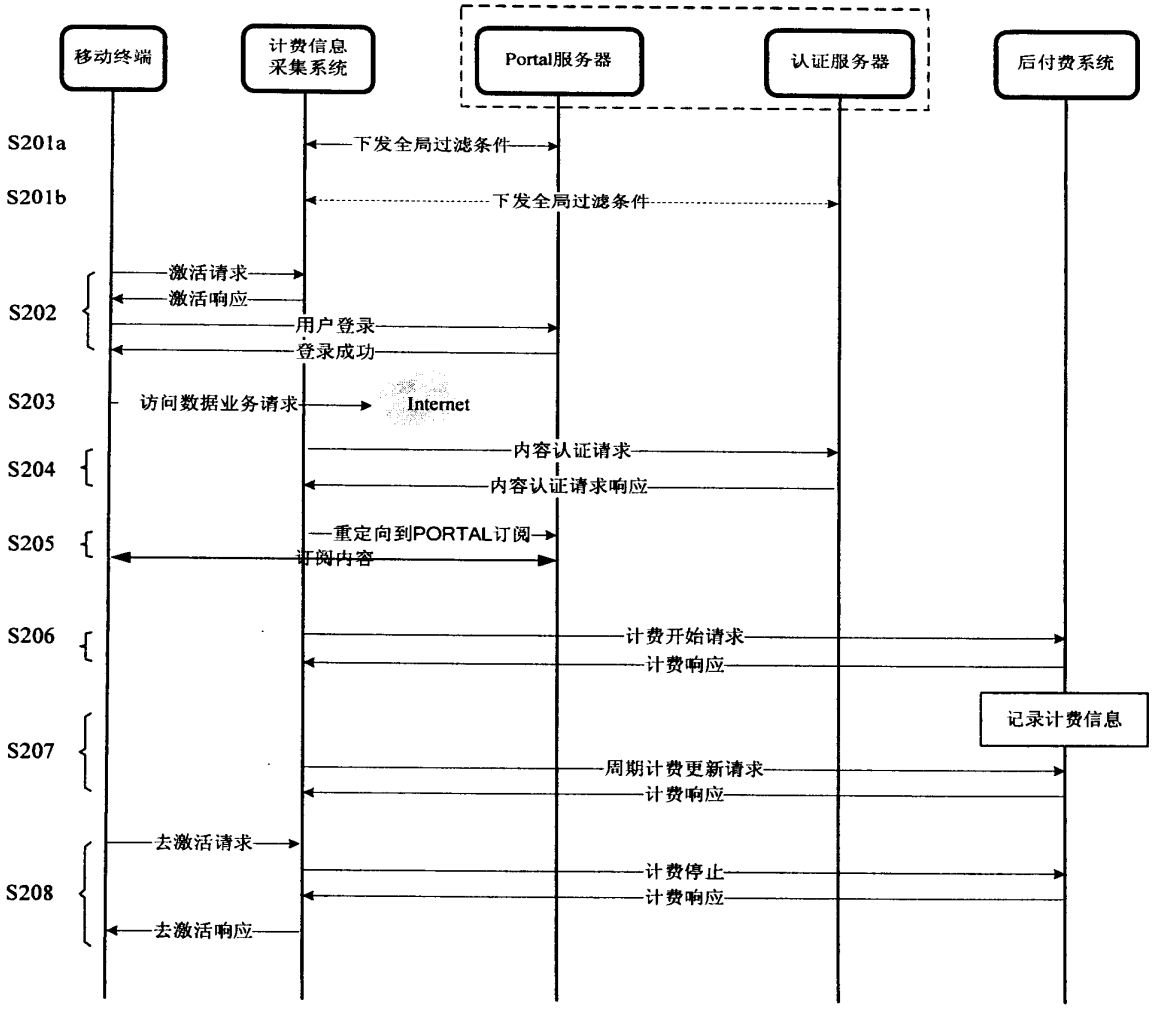

移动终端
计费信息采集系统
Portal服务器
认证服务器
后付费系统
S201a
下发全局过滤条件
S201b
下发全局过滤条件
S202
激活请求
激活响应
用户登录
登录成功
S203
访问数据业务请求
Internet
S204
内容认证请求
内容认证请求响应
S205
重定向到PORTAL订阅
订阅内容
S206
计费开始请求
计费响应
记录计费信息
S207
周期计费更新请求
计费响应
S208
去激活请求
计费停止
计费响应
去激活响应

图 3

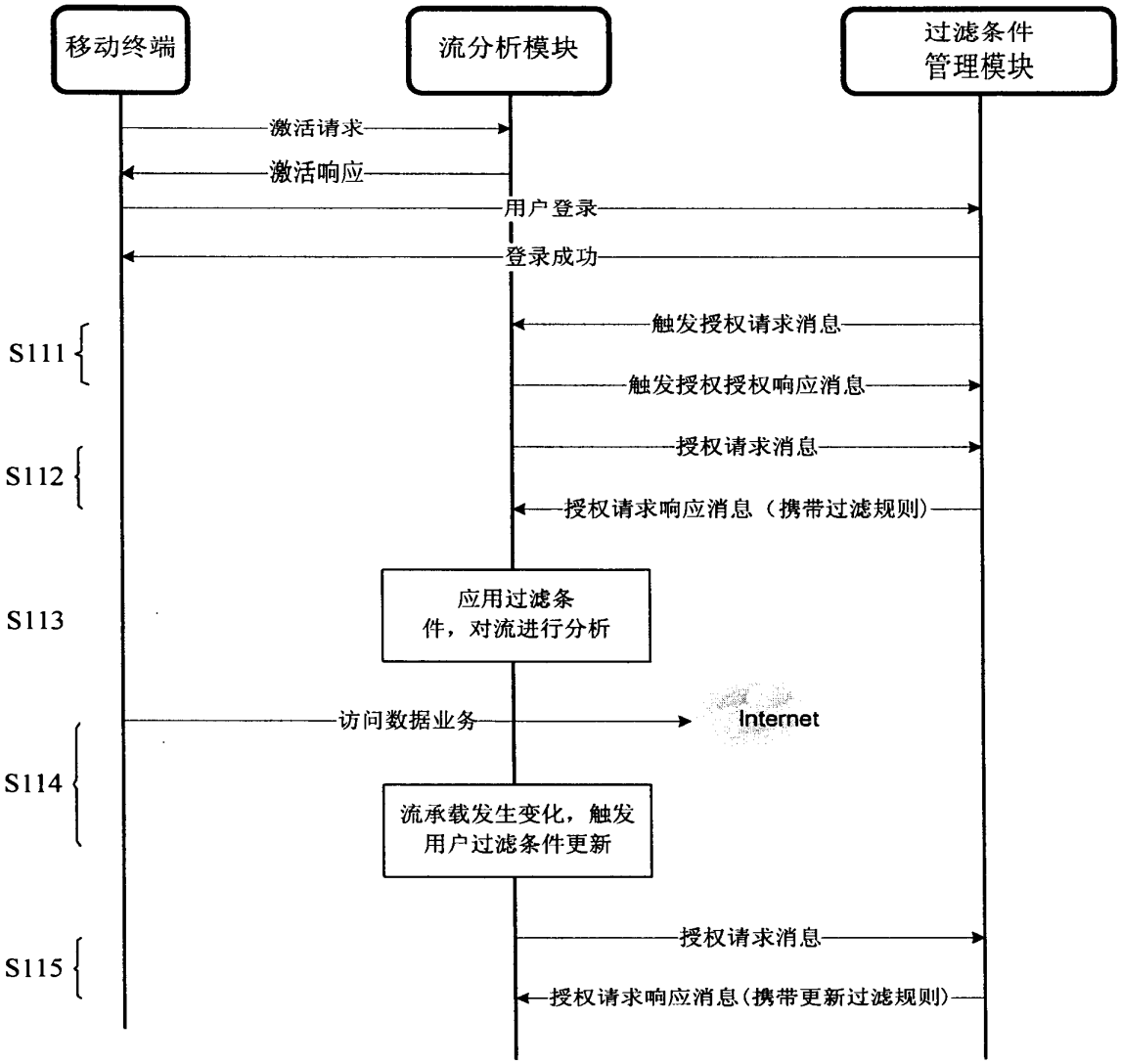

移动终端
流分析模块
过滤条件
管理模块
激活请求
激活响应
用户登录
登录成功
S111
触发授权请求消息
触发授权授权响应消息
S112
授权请求消息
授权请求响应消息（携带过滤规则）
S113
应用过滤条
件，对流进行分析
访问数据业务
Internet
S114
流承载发生变化，触发
用户过滤条件更新
S115
授权请求消息
授权请求响应消息(携带更新过滤规则)

图 4

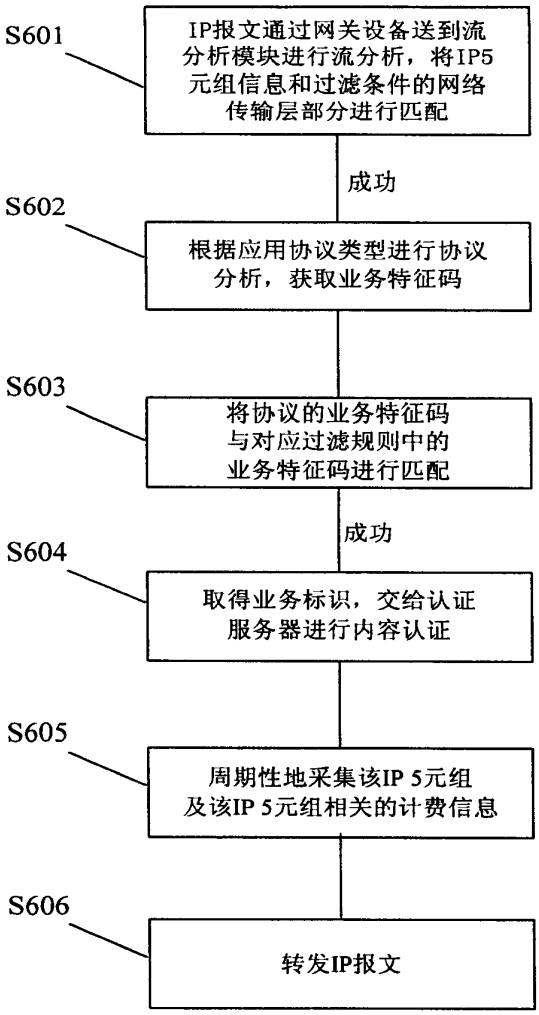

S601
IP报文通过网关设备送到流分析模块进行流分析，将IP5元组信息和过滤条件的网络传输层部分进行匹配
成功
S602
根据应用协议类型进行协议分析，获取业务特征码
S603
将协议的业务特征码与对应过滤规则中的业务特征码进行匹配
成功
S604
取得业务标识，交给认证服务器进行内容认证
S605
周期性地采集该IP 5元组及该IP 5元组相关的计费信息
S606
转发IP报文

图 5

Sign in

Patents Application Grant English Chinese

Find prior art Discuss this application View PDF Download PDF

Charged information acquisition system and method, and charge realizing system and method

CN 1937511 A

Publication number	CN1937511 A
Publication type	Application
Application number	CN 200510086507
Publication date	Mar 28, 2007
Filing date	Sep 23, 2005
Priority date	Sep 23, 2005
Also published as	CN100486167C
Inventors	[illegible]
Applicant	[illegible]
Export Citation	BiBTeX, EndNote, RefMan

Referenced by (2), Classifications (1), Legal Events (3)

External Links: SIPO, Espacenet

ABSTRACT

The fare charging info collect system includes a filter condition management module (FCM) for setting and storing the filter condition being useful for flow analyze and control, a flow analyze module (FA), according to the filter condition, analyzes the business flow that mobile terminals access the data business, draws the data business content character code, business beacon and the business type info, a filter condition management interface module (FCMI) connecting FCM and FA, a authentication interface module (AI) sending the business content character code to the authentication server to authenticate. A fare charge interface module (FCI) sends the business beacon and the business type to the fare charging sub-system to charge. Via supporting user to set and modify dynamically the filter rule, this scheme extends user business features, e.g. QOS and safety features.

DESCRIPTION [illegible] Chinese

Billing information collection systems and collection methods and billing systems and implementation methods to achieve

Technology

The present invention relates to a mobile packet domain network and service network billing system and billing processing technology, particularly a mobile packet domain network and service network jointly implement the billing system content billing and billing processing technology.

BACKGROUND

Currently billing model for data services are monthly system, traffic accounting and duration of billing, while new ways of billing by content.

3G is a packet-switched network for the network core, packet-based billing traffic accounting, billing elements of their session time, data traffic, rates, etc., to achieve the total traffic accounting, billing uplink traffic and downlink traffic accounting , according to time billing, according to the number of activations or monthly billing system, etc., and can be bad for the session frames fee waiver, you can press time, traffic preferential treatment. However, these traditional billing methods can only get the user to simply the number of bits transmitted over the network, you can not dig data services for its content brings deep business value.

By content billing, data business itself is usually caused by a third party - the content provider. Data multimedia content based on business generally have the following categories: View class of business, mobile messaging services, location-based class of business, general business Socket, download class of business, PUSH class business.

Multiple types of data services billing will require diversification and diversification of tariff packages. Operators of existing legacy billing system, the carrier layer can be obtained only when the length of the traffic and billing information, and can not distinguish between different types of services; operator

CLAIMS [illegible] [illegible] Chinese

1 A charging information collection system characterized in that, comprising: a filter management module is used for setting and storing a control flow analysis and filters; class analysis module according to the filter criteria for the mobile terminal access data services business flow analysis, extraction of data services business content signatures, business logo and business category information; a filter condition management interface module is connected to the filter condition management module and the flow analysis module; an authentication interface module for the signature of the service content sent to the authentication server for authentication; a billing interface module for the identification of the service, to a charging Category charge processing subsystem.

(2) as claimed in claim 1, wherein the charging information collecting system, characterized in that said flow analysis module is further configured according to the authentication server, and returns a message accounting subsystem for controlling the traffic flow filter.

3 according to claim 2, wherein the charging information collecting system, characterized in that said management module is used to set the filter conditions in the filter parameters of the network and transport layer, the application layer parameters, and policy and charging control parameters, the said flow analysis module according to the parameters of the network and transport layer and application layer traffic parameters are analyzed and based on the authentication server, and returns a message accounting subsystem of the policy and charging control parameter for controlling the traffic flow .

4 A charging implementation system includes a mobile terminal, billing subsystem, characterized in that it further comprises a service flow based charging information collecting system and an authentication server, the charging information collection system comprising: a filter condition management module is used for setting and storing a control flow analysis and filters; class analysis module according to said filter to said mobile terminal to access data services traffic analysis service business content data extraction pattern , the service

network only multimedia message server, WAP gateway and a location server, they just able to provide limited service layer charging information; how more extensive data-oriented business, how to get richer billing information, and then be able to develop a richer tariff policy, diversification of sources of data business profits, the future all kinds of mobile operators In the data services are facing important issues.

Stream-based content charging technology (Content Based Charging) refers to the network side, according to certain rules to distinguish the user's business, and were statistical time, flow and event information, and then using that information for pre-paid and post- payment control.

The contents of the current flow-based technology solutions can only be statically charging for content billing, that is in the user data traffic before it needs to configure relevant information; these configurations good information online when a user can not be readily against a user to modify. Drawback of this method is not flexible, not according to the user's individual needs and flexible content billing strategy formulation; and rules statically configured poor scalability, this architecture to other service features (such as QOS, Security) support does not good.

SUMMARY OF THE INVENTION

The object of the present invention is to provide an information collecting system and the charging and billing for system acquisition method and implement solutions to the contents of the stream-based charging technology solutions are not flexible to the individual needs of the user develop flexible content billing strategies, poor scalability to other service features (such as QOS, security) to support the bad shortcomings.

To achieve the above object, the present invention provides a charging information collection system, comprising: a filter management module is used for setting and storing a control flow analysis and filters; class analysis module, used according to the said filter data services for mobile terminals to access the service flow analysis, extraction of data services business content signatures, business logo and business category information; a filter condition management interface module is connected to the filter condition management module and the flow analysis module; an authentication interface module for the signature of the service content sent to the authentication server for authentication; a billing interface module for the identification of the service, to a charging Category charge processing subsystem; The charging information collection system, wherein said flow analysis module is further configured according to the authentication server, and returns a message accounting subsystem for controlling the traffic flow filter.

The charging information collection system, wherein said management module is used to set the filter conditions in the filter parameters of the network and transport layer, the application layer parameters, and policy and charging control parameters; the flow analysis module and the network according to Transport layer parameters and application layer traffic parameters are analyzed and based on the authentication server, and returns a message accounting subsystem of the policy and charging control parameter controls the traffic flow.

In order to achieve the above object, the present invention also provides a billing implementation system includes a mobile terminal, billing subsystem, further comprises a service flow based charging information collecting system and an authentication server, the billing information collection system comprising: a filter management module for setting and storing a filter; class analysis module according to the filtering conditions for the mobile terminal to access data services for traffic analysis, extraction of data services business Content signatures, business logo and business category information; a filter condition management interface module is connected to the filter condition management module and the flow analysis module; an authentication interface module for the signature of the business content transmitted to the the authentication server; a identifier and service type information; a filter condition management interface module coupled to said filter flow analysis module and the management module; an authentication interface module for the signature of the service content to the authentication server for certification; a billing interface module for the identification of the service, to a charging Category charge processing subsystem.

5 according to claim 4, wherein the billing service flow implementation system, characterized in that the authentication server 30, including but not limited to, the AAA server.

As claimed in claim 4, wherein the billing service flow implementation system, characterized in that said flow analysis module is further configured according to the authentication server, and returns a message accounting subsystem for controlling the traffic flow filter.

As claimed in claim 6, wherein the charging information collecting system, characterized in that said management module is specific filter criteria for setting the network and transport layer parameters, the application layer parameters, and policy and charging control parameters; The flow analysis module according to the parameters of the network and transport layer and application layer traffic parameters are analyzed and based on the authentication server, and returns a message accounting subsystem of the policy and charging control parameter controls the service stream.

The process of claim 1, wherein the charging information collecting system for accounting information collection method characterized by comprising the following steps: Step 1, the filter condition is set and storing the management module and the control flow analysis filters; step 2, flow analysis module based on the filter criteria to access data services for mobile terminals business flow analysis, extraction of data services business content signatures, business logo and business category information; Step 3, wherein said traffic flow analysis module Content signature sent to the authentication server for authentication; step 4, the flow analysis module to said service identifier, type of business accounting subsystem to perform the charging process.

(10) according to claim 8, wherein the charging information collection method, wherein said step 1 specifically comprises: step 11, the filter condition management module is set in the filter IP5 tuples; step 12, the filter condition management module settings The application layer of filter parameters; step 13, the filter condition management module is set in the filter policy and charging control parameter, the step 2, the flow analysis module according to the parameters of the network and transport layer and application layer parameters for traffic analysis.

A process according to claim 9, wherein the charging information collection method characterized in that said network and transport layer parameter tuple to IP5, the application layer parameters include the application protocol service content type and pattern, the step 2 includes the following steps: Step 21, the user access to the data issued by the business IP packets, the IP packets flow through the Internet gateway to said analysis module, a flow analysis module calls the filter condition management module for the IP IP5 tuple packet of information and filter conditions IP5 matching tuple information; step 22, the matching is successful, the flow analysis module calls the filter criteria in the application protocol type protocol analysis, obtaining the IP packet business content signature; step 23, the flow analysis module called filter management module will be described in step 22 business content with the signature of the business content filter pattern matching; step 24, the match is successful, The flow analysis module calls the filter condition management module for the filter condition

billing interface module for the identification of the service, to a charging Category charge processing subsystem.

In order to achieve the above object, the present invention also provides a system to achieve charging information collecting method of collecting charging information, comprising the following steps: Step 1, the management module to set filter condition and stores the filter criteria; step 2, Flow analysis module based on the filter criteria to access data services for mobile terminals business flow analysis, extraction of data services business content signatures, business logo and business category information; Step 3, wherein said traffic flow analysis module content feature code is sent to the authentication server for authentication; step 4, the flow analysis module to said service identifier, type of business accounting subsystem to perform the charging process.

in order to achieve the above object, the present invention also provides a charging method, comprising the steps of: step S1, the gateway receives the user terminal to access data services send IP packets and forwards to the flow analysis module; step S2 , filter and store management module set filter conditions; step S3, the flow analysis module based on the filter criteria to access data services for mobile terminals business flow analysis, extraction of data services business content signatures, business logo and business class information; step S4, the analysis module of the flow pattern of said service content sent to the authentication server for authentication; step S5, the analysis module of the flow of said service identifier, type of business by charging to a charging subsystem ;

Step S6, the charging subsystem processes the accounting response message returned to the flow analysis module.

Application of the present invention billing information collection systems and collection methods and billing systems and implementation methods to achieve, through support for users to dynamically customize and modify filtering rules, you can extend the user's business features, such as QOS characteristics and security features.

BRIEF DESCRIPTION

Figure 1 of the present invention for system charging and billing information collecting system; Fig invention, Figure 2 is a flowchart for the pre-payment system; Figure 3 of the present invention system for postpaid flow; Figure 4 The present invention configured user-level flow diagram of filter conditions; Figure 5 is a flowchart invention applied filter criteria.

Specific embodiments

The present invention provides a method according to content billing billing billing system and its implementation method based on flow analysis implementation, provides a combination of static and dynamic filter condition management. Management called dynamic filter means when the user is online, it is possible for a user in time of the application of the rules to be modified.

By content billing billing billing system implementation method supports the user's individual needs and flexible content billing strategy formulation; addition, the support according to the user dynamically customize and modify filters, filter content billing information is collected basis, the flexibility to expand the user's business features, such as QOS characteristics and security features.

From the scope point of view, filter conditions can also be divided into two: one for global filter conditions; another is specific to a user's filter criteria, namely the user-level filters.

User-level filtering criteria take precedence over global filter conditions, in two parts overlapping the content, flow analysis based on user-level filtering criteria based, user-level filtering condition itself if there is a conflict, according to the priority decide which one size filter of the present invention by content billing corresponds business logos, business class; step 25, the signature of the business flow analysis module interface module certified to the authentication server for content authentication; step 26, user access to data services of the process, the flow analysis module periodically collect the IP5 tuples, business logos, business class, and said IP5 tuples related charging information to a billing through the billing interface module system for billing processing; Step 27, forwarding the IP packet

Claimed in claim 10, wherein the charging information collection method, wherein said filter criteria is the user level, and the user access to data services changes during the load, further comprising the step of updating the filter criteria.

Of claim 4, wherein the charging charging method implementation system, characterized by comprising the steps of: step S1, the gateway receives the user terminal to access data services send IP packets and forwards to the flow analysis module; step S2 , set the filter criteria and store management module for flow analysis and control filters; step S3, the flow analysis module based on the filter criteria to access data services for mobile terminals business flow analysis, extraction of data services business content characteristics code, the service identifier and service type information; step S4, the analysis module of the flow pattern of said service content sent to the authentication server for authentication; step S5, the flow analysis module of the identifier of the service, by sending to Category Billing Billing subsystem; step S6, the charging subsystem processes the accounting response message returned to the flow analysis module.

13 according to claim 12, wherein the charging method, characterized in that said step S2 specifically comprises: step S21, the filter management module is set in the filter IP5 tuples; step S22, the filter management module set filters Conditions in layer parameters; step S23, the filter management module is set in the filter policy and charging control parameter; said step S3, the flow analysis module according to the parameters of the network and transport layer and application layer parameters traffic analysis.

14 according to claim 13, wherein the charging method, characterized in that said network and transport layer parameter tuple to IP5, the application includes an application layer protocol parameters and service content signatures, said step S3 specific includes the following steps: Step S31, the business users to access data sent IP packets, the IP packets flow through the Internet gateway to said analysis module, a flow analysis module calls the filter condition management module for the IP packet IP5 text tuples of information and filter conditions IP5 matching tuple information; step S32, the match is successful, the flow analysis module calls the filter condition management module according to the application protocol type protocol analysis, obtaining the IP packet business content signature; step S33, the flow analysis module called filter management module will be described in step 22 business content with the signature of the business content filter pattern matching; step S34, the match is successful, The flow analysis module calls the filter condition management module for the filter condition corresponds business logos, business class; step S35, the flow pattern of the business analysis module interface module certified to the authentication server for content authentication; step S36, user access to data services of the process, the flow analysis module periodically collect the IP5 tuples, business logos, business class, and said IP5 tuples related charging information to a billing through the billing interface module system for billing processing; step S37, forwarding the IP packet.

billing system can simultaneously support two filters.

Shown in Figure 1, according to the present invention, content billing billing system comprising: a charging information collection system for collecting the accounting information based on the filter criteria, and to control traffic flow, including the flow analysis module 101, a filter management module 102, a filter condition management interface module 103, authentication and billing interface module 104 interface module 105;

Authentication server 30 through the authentication interface module 104 and flow analysis module 101 is connected to the billing information collection system 10 sends a request authentication message authentication; billing system, including pre-paid and post-paid system 40 system 50, according to the flow analysis module 101 charging information collected for billing operations, and returns the response to the flow of billing module 101 to control the flow of the business.

According to the present invention includes content billing billing system following modules: flow analysis module 101, according to the filter criteria convection analysis, extraction business content signatures certified interface module 104 to the authentication server 30 for content authentication, the simultaneous extraction filter condition corresponds to the identity and business class service through billing interface module 105 to the pre-paid or post-paid system 40 system 50 for grant price, balance control processing; filter management module 102, for the management and maintenance of filters, storage There are a collection of filters that can be configured in the PORTAL server can also be configured in the authentication server 30, pre-paid or post-paid system 40 system 50, the mobile packet service network in the PORTAL server is a mobile operator to show users ISP \ ICP ISP or content provider platform for many businesses, but also the user subscription service, query tariff information, check their account details of self-service platform; This filter condition management module 102 is used to set the filter criteria to achieve the following 3 functions: setting filter conditions in the network and transport layer parameters, including source IP address, destination IP address, source port number, destination port number, and protocol type, ie IP5 tuples; setting filter conditions in the application layer parameters, including the type and business application protocol Content signature; setting filter conditions in the policy and charging control parameters, including corresponding business logos, business class, rates, priority, trigger action list, redirection address, QOS levels and parameters, flow threshold and time threshold, etc. .

Where: source / destination IP address, the IP packet header source address / destination address; source / destination port number for the IP packet header source port / destination port; protocol type, IP packet header protocol field, represents the transport layer protocol type, UDP, or TCP; application protocol type, the time that the traffic analysis for compliance with the above source / destination IP address, source / destination port number source of traffic using the kind of application protocol characteristics were analyzed; business content signatures, The application can be expressed agreement contains business information, such as http it, url is one of their business content signature, but the signature is not limited to business content;

Filters corresponding business logo, filter conditions represent a business name can contain a string of characters and numbers, the name should be long enough to avoid duplication; business category is represented by the corresponding filter business classification, The classification may be based rates may also be the basis for other convenient billing management; rates is in accordance with flow, time or times to serve different pricing strategies developed; priority, which means that the level of priority criteria, In a number of filter conditions in the case of conflict, the rules have higher priority wins; trigger action list contains two elements: hosting events and trigger actions, the user's data services matching to the filter, the user action occurred bearer List of the events listed, the list will trigger the corresponding action; redirect address, specify the user's data redirection destination address can be an IP address, it can be URL; QOS levels and parameters, specify filter conditions QOS level matching operations and parameters, in diffserv (differentiated services architecture), to route traffic is mapped to different service levels, namely QOS level, QOS parameter is used for traffic policing and shaping of specific parameters, such as average speed, peak rate, etc.; flow threshold and time threshold can be used by the user and the flow rate and the time threshold.

Network transport layer and application layer parameters parameters for traffic analysis, policy and charging control

15 according to claim 14, wherein the total charging method, characterized in that the filter criteria for the user level, and the user access to data services changes during the load, further comprising the step of updating the filter criteria.

Method according to claim 12, 13 or 15, wherein the charging information collection method, characterized in that the charging system for the pre-payment system and / or the data service is a prepaid service, the said step S5 concrete following steps: Step S51, reported to the prepaid billing system requests and credit request, the request message includes the service identifier and type of business; step S52, the pre-paid billing system receives the request , remove the service identifier and type of business to get the corresponding tariff information, according to the request contained in the message flow and duration of the amount of user consumption calculated from the pre-paid account for deduction, then the account balances of the business situation and the identification and business class, corresponding to the business logic generates accounting response message, step S53, the user access to the data during the billing request periodic reporting and credit requests, the pre-paid billing system periodically return response, step S54, the flow analysis module based on the billing respond to traffic control; step S55, the user to activate the flow analysis module notifies prepaid billing system to stop.

17 according to claim 12, 13 or 15, wherein the charging method, characterized in that when the billing system for the post-payment system and / or the data service to the postpaid service, said step S5 concrete following steps: Step S51 ', submitted to the post-paid system start-accounting request message, and the start-accounting request message contains content billing information, step S52', the post-paid meter system to the content Fee information is recorded and stored; step S53 ', users access data process, periodically reporting the post-paid billing system update said content information; step S54', the user to activate notification to stop the post-paid billing system .

18 according to claim 12, 13 or 15, wherein the charging method, characterized in that the authentication server denies the user with the requested data service, the user according to the preset redirection address, the user's access PORTAL redirected to the home page, re-subscribe services by PORTAL server updates the user subscribes to business content, recertification by the authentication server.

parameters used to implement traffic control, for the upstream and downstream flow filter are configured, that is, upstream and downstream traffic can apply different filtering criteria; service identification, flow threshold and QOS parameters and so can distinguish between grades and setting down the line, but also in policy and charging control section extended user's other attributes, such as security features; filter condition management interface module 103, and filtering condition management module 102 interacts with the responsibility to manage and maintain the filter criteria, there are a variety of interfaces between the two forms is available, such as ftp, http, radius, cops and diameter-nasreq agreements; authentication interface module 104 is responsible and certification interactive server 30, the authentication server 30, including but not limited to, the AAA server, but may be other users and users with the service capabilities of the system to authenticate the content; billing interface module 105, responsible for the billing system (including the prepaid system 40 and postpaid system 50) interact to prepaid billing request to the prepaid system 40, the post-paid to post-paid, then a single information system 50 and accept prepaid billing system 40 in response, according to the response of the content into action instructions given flow analysis module 101, the flow analysis module 101 further implementation of the convection control and billing.

Users access the data traffic generated from operations after filtration through filter conditions to determine the need for service authentication, and then and then only the billing process. This shows that the filter is to collect charging information is based, according to the filtering criteria to determine which business data stream requires billing and still need these rules to determine the data stream associated businesses (IP5 tuple including) Which of these streams when to start and when to end, the number of flow occurs; then report the charging information, billing accounting information by content acquisition system with the specific workflow in Figure 1 and Figure 5, comprises the following steps: Step S601, the user accessing data services issue IP packets, these packets through Internet gateway device (eg GGSN) is sent to the flow analysis module 101, flow analysis module 101 call management module 102 filters the IP packets IP5 tuple information and filter conditions network and transport layer parameters to match; step S602, the match is successful, the flow analysis module 101 call filter management module 102, and according to the application protocol type protocol analysis, business content access agreement signature, such as the application protocol filtering conditions Type indicates the HTTP protocol, protocol analysis conducted in accordance with the HTTP protocol specification protocol analysis; step S603, flow analysis module 101 in step S602 signature obtained business content and filtering criteria for matching business content signature; step S604, the match succeeds , flow analysis module 101 corresponding filter condition to obtain the corresponding business identity, type of business, by the business flow analysis module 101 signatures certified interface module 104 to the authentication server 30 for content certification; step S605, the process of user access to data services , the stream analyzing module 101 periodically collect the IP5 tuple, service identifier, type of business and the associated tuple IP5 charging information (flow and length) by charging the interface module 105 to a billing system (prepaid system 40 or postpaid system 50); step S606, forward IP packets.

Such billing system based on content filtering criteria to collect billing billing information.

Combined in Figure 1, the present invention is implemented billing system billing information collection methods, flow analysis module 101 according to global filters, or filtering criteria based on global and user-level filtering criteria jointly analyze data, and collect content meter Fee information request authentication to the authentication server 30, and reported to the billing system 40 or 50.

For matching to the global filter traffic conditions, at the edge of the mobile packet domain by content billing billing information collection system flow analysis module 101 through authentication interface module 104 to the authentication server 30 authentication request (the request may contain IMSI, phone number, IP address, signature and other content business content), request authentication of the mobile station has permission to access the service; authentication server 30 can handle their own certification, also according to the user's phone number belongs to a service control point (Service ControlPoint, SCP) for certification; authentication server 30 based on IMSI check the user's phone number or legality; signatures based on business content and user IMSI or mobile number relevance verify the user has to use the legitimacy of the business, and then returns the authentication request response message to the flow analysis module 101; flow analysis module 101 to get certified results if authentication fails, the user's data stream redirected to the operator-specific web server to the user prompt access failure reason, this part of the redirected traffic should be free The; If the authentication is successful and the user types are prepaid or pre-paid type of service, billing flow analysis module 101 via the interface module 105 requests the prepaid billing system 40, the quota, the quota according to the response determines how to forward data traffic or duration; if it is the type of post-paid or post-paid users type of business, traffic analysis module 101 forwards the data stream, record billing information, and periodically sent postpaid system 50.

Mobile station starts using business, quantitative flow analysis module 101 or the use of regularly reported to the user pay system; postpaid billing system 50 pairs of recording information; prepaid system 40 accepts flow analysis module 101 cycles reported accounting request, according to the given user's account balance billing response. User offline notification flow analysis module 101 prepaid billing system 40 stops; notice postpaid billing system 50 stops; operators can also filter management module 102 are subject to change user-level filtering conditions with immediate effect, if the user is online, User-level real-time updates to the filter conditions will flow analysis module 101.

Referring to Figures 1 and 2 according to the present invention is to achieve content billing prepaid billing system for billing type of content and business process flow control will be described, wherein the filter module 102 is provided on the PORTAL management server 30 or the authentication server , do not contain user-level filtering criteria, by content billing billing information collection system to achieve pre-paid type of content billing methods include the following specific steps: Step S101a, the filter condition management module 102 define global filters and issued by the PORTAL server, or step S101b, the filter condition management module 102 define global filters, issued by the authentication server 30, step S101a and S101b step will exist, there is an occurrence of another one do not need to be repeated Therefore, step S101b shown in phantom;

Step S102, the mobile terminal activates the Internet, open Portal Portal home page, log in, home show business user has subscribed to the hyperlink and tariff information; step S103, the user clicks on a service provider or content provider hyperlinks, ie a business, a business issue with an access request; step S104, the flow analysis module 101 according to the global filtering criteria to analyze the access request, access request may contain IMSI, phone number, IP address, signature and other business content content request authentication whether the mobile terminal has access to the service; authentication server 30 can handle their own certification, but also according to the user's phone number belongs to a service control point (SCP) for certification; authentication server 30 based on IMSI checks the user's phone number or legality; signatures based on business content and user IMSI or mobile number correlation verify the user has to use the business legitimacy, and then returns a response message content authentication request to the flow analysis module 101; business content can be extracted only certified signatures to content authentication server 30, the authentication result is returned to the service gateway, if the authentication server rejects the user to use the content of the request, the process proceeds to step S105, otherwise it proceeds to step S106; step S105, the flow analysis module 101 according to defined filtering criteria redirection address, will be redirected to the PORTAL user's access on the home page, the user subscription service, PORTAL server updates the user a new subscription service content so that you can correct authentication server 30 authenticates the user, both of which describe the interaction process is not the case, user After updating the content subscription service returns to step S103; step S106, the flow analysis module 101 based on the filter criteria collect billing information, and the interface module 105 via billing report accounting request to the billing system and credit requests, because the user is prepaid (online billing) type, so again prepaid system 40 (Online Charging System) requests prepaid control flow analysis carried in the request module 101 based on analysis of traffic flow filter conditions resulting filter condition corresponds business logo and business class and other information; step S107, the prepaid system 40 preservation and business class service identifier corresponding tariff information, traffic analysis module 101 receives the billing request, remove one of the business logo and business categories correspond to obtain rate information, according to the request contained in the flow rate and duration of the amount of user consumption calculated from the pre-paid account for deduction, then according to circumstances and the account balance service identification and classification of the corresponding business logic generates accounting response was circulated flow analysis module 101 , accounting response message may carry billing information; Here prepaid intelligent network system 40 may be implemented, prepaid billing request according to the user information, business logo and business class determines the control logic and billing services, a business stream batch price is pre-paid system completed;

Step S108, the user access to data in the process, the stream analyzing module 101 periodically reported to the billing request and credit requests prepaid billing system 40 returns the response, may carry a quota; step S109, the flow analysis module 101 according to the prepaid system 40 The results given the traffic control; step S110, the user to activate the flow analysis module 101 Notification prepaid billing system to stop.

If the user belongs postpaid postpaid type or business is business, accounting information by content billing service data acquisition system forwarded directly to gather information to postpaid billing system, which filters the management module 102 is set on the server or on the PORTAL authentication server 30, but does not contain user-level filter conditions, combined with Figure 1 and Figure 3, comprising the following steps: Step S201a, the filter condition management module 102 define global filters, issued by the PORTAL server 60, or step S201b, the filter condition management module 102 define global filters, issued by the authentication server 30, step S201a and S201b step will exist, there is an occurrence of another one do not need to be repeated, so step S201b dotted line ; step S202, the mobile terminal activates the Internet, open Portal Portal home page, log in, home show business user has subscribed to the hyperlink and tariff information; step S203, the user clicks on an ISP or content provider hyperlinks, that is a business, a business issue access requests to use; step S204, the flow analysis module 101 according to the global filter criteria analysis service request, the request may contain IMSI, phone number, IP address, and business content signatures, etc., requesting certification of the whether the mobile terminal has access to the service; authentication server 30 can handle their own certification, also according to the user's phone number belongs to a service control point (SCP) for certification; authentication server 30 based on IMSI check the user's phone number or legality; under business content signatures and user IMSI or mobile number relevance verify the user has to use the legality of the service, and then returns a response message content authentication request to the flow analysis module 101; business content can also extract only the contents of the signature to the authentication server 30 for authentication, the authentication result is returned to the service gateway, if the authentication server 30 denies the user's request to use the content, proceeds to step S205, otherwise proceeds to step S206; step S205, flow analysis module 101 is defined based on the filter criteria redirection address, will be redirected to the PORTAL user's access on the home page,

the user subscription service, PORTAL server updates the user a new subscription service content so that you can correct authentication server 30 authenticates the user, both of which describe the interaction process is not the case, user After updating the content subscription service returns to step S203; step S206, the flow analysis module 101 via the interface module 105 post-paid billing system 50 is reported to the accounting start request message that contains the contents of the report accounting information; step S207, postpaid System 50 information on these records and store the user to access the data during the mid-stream analysis module 101 also reported postpaid system 50 periodically update this information; step S208, the user to activate the notification service gateway billing system billing stops.

Figure 2 and Figure 3 is a flowchart does not include the user-level filtering condition, the user level criteria play a role, the user-level filtering condition configuration process with reference to Figs 1 and 4, as for the step S102 and step S103 (step S202 or and step S203) between, but also includes the following steps: step S111, the user login is successful, filter management module 102 to trigger flow analysis module 101 sends an authorization request message flow analysis module 101 to the filter condition triggered management module 102 returns authorization request response message; step S112, the flow analysis module 101 to the filter condition management module 102 sends an authorization request message requesting the user-level filters, filter management module 102 in the authorization request response message carries user-level filter to flow analysis module 101; step S113, the user access to the data process flow analysis application filter module 101, convection analysis, in which the application filter policy and charging control section to control the flow, while matching to the business stream, no longer need to the authentication server 30 for authentication; step S114, the user access to data process, if the carrier stream changes, and the change event triggering the filter criteria in the action list, the flow analysis module 101 to the filter condition management module 102 initiates a user-level filtering condition profile request, before the arrival of the new rules, the old rules remain in force; step S115, flow analysis module 101 sends an authorization request message filter management module 102 in the authorization request response message carries the new user-level filter to flow analysis module 101 .

If you do not apply user-level filtering criteria, the processes do not need to happen. Rates of the filter conditions, the priority, the trigger action list, the redirection address, QOS levels and parameters, flow threshold and the time threshold, etc., and user attributes associated, may appear in the user-level filtering condition.

Of course, the present invention may have other various embodiments, without departing from the spirit and essence of the present invention, the person skilled in the technical field of the present invention, when made according to various corresponding changes and modifications, but these respective changes and modifications shall belong to the appended claims, the present invention is the scope of protection.

REFERENCED BY

Citing Patent	Filing date	Publication date	Applicant	Title
WO2009018759A1 *	Jul 31, 2008	Feb 12, 2009	Shibi Huang	Control device, execution device, method and system of generating filter rule
WO2011009337A1 *	May 26, 2010	Jan 27, 2011	Zte Corporation	Method and monitoring system for monitoring data service system

* Cited by examiner

CLASSIFICATIONS

International Classification	H04L12/14

LEGAL EVENTS

Date	Code	Event	Description
May 6, 2009	C14	Granted	
May 23, 2007	C10	Request of examination as to substance	
Mar 28, 2007	C06	Publication	

Google Home - Sitemap - USPTO Bulk Downloads - Privacy Policy - Terms of Service - About Google Patents - Send Feedback
©2012 Google

Electronic Acknowledgement Receipt

EFS ID:	18528097
Application Number:	14082040
International Application Number:	
Confirmation Number:	1015
Title of Invention:	Device-Assisted Services for Protecting Network Capacity
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	Krista Susan Jacobsen
Filer Authorized By:	
Attorney Docket Number:	RALEP032C1
Receipt Date:	19-MAR-2014
Filing Date:	15-NOV-2013
Time Stamp:	17:53:31
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	P032C1IDS.pdf	613023 de46a668b7699a7bcce0e4144e0f05f18973edc0	no	7

Warnings:	
Information:	

2	Foreign Reference	2041_CN101123553A.pdf	1975496 77fe4b0fe9cee8cb2bf4c46f64443dee1117f80e	no	16
Warnings:					
Information:					
3	Foreign Reference	2042_CN1937511A.pdf	3222683 57d4f0e05771df6cf8790dcaecf3a418734fec42	no	29
Warnings:					
Information:					
			Total Files Size (in bytes):	5811202	

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

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

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

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Raleigh et al.	Examiner:	not yet assigned
Serial No.:	14/082,040	Art Unit:	2447
Filed:	November 15, 2013	Conf. No.:	1015
Title:	Device-Assisted Services for Protecting Network Capacity		

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

SECOND REQUEST FOR A CORRECTED FILING RECEIPT

Madam:

Applicant respectfully requests a corrected filing receipt for the above-captioned application. Submitted with this request are:

(1) The application data sheet (ADS) filed on November 15, 2013 with Applicant's filing of a new application, that ADS reflecting the correct benefit claim.

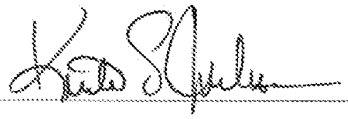
(2) A copy of the Filing Receipt mailed February 25, 2014 with the requested changes noted thereon.

Applicant respectfully notes that this request is not a request to add or correct a benefit claim. Applicant is simply seeking a filing receipt that reflects the correct benefit claim as provided in the ADS originally submitted on November 15, 2013.

CONCLUSION

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

Respectfully submitted,

Date: February 27, 2014 By: 

Krista S. Jacobsen
Reg. No. 59,374
(408) 455-5539

CERTIFICATE OF ELECTRONIC TRANSMISSION

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

Date: Feb. 27, 2014 By: 
Krista S. Jacobsen

Application Data Sheet	Attorney Docket No.	RALEP032C1
	Application Number	
Title of Invention	DEVICE-ASSISTED SERVICES FOR PROTECTING NETWORK CAPACITY	

Inventor Information:

Inventor 1 -

Legal Name:

First Name:	Gregory
Middle Name:	G.
Family Name:	Raleigh

Residence Information:

City:	Woodside
State:	CA
Country of Residence:	USA

Mailing Address of Inventor: 350 Marine Parkway, Suite 300
Redwood Shores, CA 94065
USA

Inventor 2 -

Legal Name:

First Name:	Alireza
Middle Name:	
Family Name:	Raissinia

Residence Information:

City:	Monte Sereno
State:	CA
Country of Residence:	USA

Mailing Address of Inventor: 350 Marine Parkway, Suite 300
Redwood Shores, CA 94065
USA

Application Data Sheet	Attorney Docket No.	RALEP032C1
	Application Number	
Title of Invention	DEVICE-ASSISTED SERVICES FOR PROTECTING NETWORK CAPACITY	

Inventor 3 -

Legal Name:

First Name:	James
Middle Name:	
Family Name:	Lavine

Residence Information:

City:	Corte Madera
State:	CA
Country of Residence:	USA

Mailing Address of Inventor: 350 Marine Parkway, Suite 300
Redwood Shores, CA 94065
USA

Correspondence Information:

Correspondence Address:	Customer Number 106963
E-mail address:	patent@headwaterllc.com

Application Information:

Title of Invention:	DEVICE-ASSISTED SERVICES FOR PROTECTING NETWORK CAPACITY
Attorney Docket Number:	RALEP032C1
Small Entity Status Claimed:	Yes
Application Type:	Nonprovisional
Subject Matter:	Utility
Total Number of Drawing Sheets:	29

Application Data Sheet		Attorney Docket No.	RALEP032C1
		Application Number	
Title of Invention	DEVICE-ASSISTED SERVICES FOR PROTECTING NETWORK CAPACITY		

Suggested Drawing Figure for Publication: ___

Representative Information:

Customer Number: 106963

Domestic Benefit/National Stage Information:

This application is a DIV of Application No. 13/134,028, filed 05/25/2011

and said Application No. 13/134,028, filed 05/25/2011
is a CIP of Application No. 12/380,759, filed 03/02/2009 (PAT 8270310)
and is a CIP of Application No. 12/380,779, filed 03/02/2009
and is a CIP of Application No. 12/380,758, filed 03/02/2009
and is a CIP of Application No. 12/380,778, filed 03/02/2009 (PAT 8321526)
and is a CIP of Application No. 12/380,768, filed 03/02/2009
and is a CIP of Application No. 12/380,767, filed 03/02/2009 (PAT 8355337)
and is a CIP of Application No. 12/380,780, filed 03/02/2009
and is a CIP of Application No. 12/380,755, filed 03/02/2009 (PAT 8331901)
and is a CIP of Application No. 12/380,756, filed 03/02/2009 (PAT 8250207)
and is a CIP of Application No. 12/380,770, filed 03/02/2009 (ABN)
and is a CIP of Application No. 12/380,772, filed 03/02/2009
and is a CIP of Application No. 12/380,782, filed 03/02/2009 (PAT 8270952)
and is a CIP of Application No. 12/380,783, filed 03/02/2009
and is a CIP of Application No. 12/380,757, filed 03/02/2009 (PAT 8326958)
and is a CIP of Application No. 12/380,781, filed 03/02/2009 (PAT 8229812)
and is a CIP of Application No. 12/380,774, filed 03/02/2009
and is a CIP of Application No. 12/380,771, filed 03/02/2009 (PAT 8023425)
and is a CIP of Application No. 12/380,773, filed 03/02/2009
and is a CIP of Application No. 12/380,769, filed 03/02/2009
and is a CIP of Application No. 12/380,777, filed 03/02/2009 (PAT 8583781)
and is a CIP of Application No. 12/695,019, filed 01/27/2010 (PAT 8275830)
and is a CIP of Application No. 12/695,020, filed 01/27/2010 (PAT 8406748)
and is a CIP of Application No. 12/694,445, filed 01/27/2010 (PAT 8391834)
and is a CIP of Application No. 12/694,451, filed 01/27/2010 (PAT 8548428)

and is a CIP of Application No. 12/694,455, filed 01/27/2010 (PAT 8402111)
and is a CIP of Application No. 12/695,021, filed 01/27/2010 (PAT 8346225)
and is a CIP of Application No. 12/695,980, filed 01/28/2010 (PAT 8340634)
and is a CIP of Application No. 13/134,005, filed 05/25/2011
and claims benefit of Application No. 61/348,022, filed 05/25/2010
and claims benefit of Application No. 61/381,159, filed 09/09/2010
and claims benefit of Application No. 61/381,162, filed 09/09/2010
and claims benefit of Application No. 61/384,456, filed 09/20/2010
and claims benefit of Application No. 61/385,020, filed 09/21/2010
and claims benefit of Application No. 61/387,243, filed 09/28/2010
and claims benefit of Application No. 61/387,247, filed 09/28/2010
and claims benefit of Application No. 61/389,547, filed 10/04/2010
and claims benefit of Application No. 61/407,358, filed 10/27/2010
and claims benefit of Application No. 61/418,507, filed 12/01/2010
and claims benefit of Application No. 61/418,509, filed 12/01/2010
and claims benefit of Application No. 61/420,727, filed 12/07/2010
and claims benefit of Application No. 61/422,565, filed 12/13/2010
and claims benefit of Application No. 61/422,572, filed 12/13/2010
and claims benefit of Application No. 61/422,574, filed 12/13/2010
and claims benefit of Application No. 61/435,564, filed 01/24/2011
and claims benefit of Application No. 61/472,606, filed 04/06/2011

and said Application No. 12/380,759, filed 03/02/2009 (PAT 8270310)
claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,779, filed 03/02/2009
claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,758, filed 03/02/2009
claims benefit of Application No. 61/206,354, filed 01/28/2009

and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,778, filed 03/02/2009 (PAT 8321526)
claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,768, filed 03/02/2009
claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,767, filed 03/02/2009 (PAT 8355337)
claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,780, filed 03/02/2009
claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,755, filed 03/02/2009 (PAT 8331901)
claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,756, filed 03/02/2009 (PAT 8250207)
claims benefit of Application No. 61/206,354, filed 01/28/2009

and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,770, filed 03/02/2009 (ABN)
claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,772, filed 03/02/2009
claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,782, filed 03/02/2009 (PAT 8270952)
claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,783, filed 03/02/2009
claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,757, filed 03/02/2009 (PAT 8326958)
claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,781, filed 03/02/2009 (PAT 8229812)
claims benefit of Application No. 61/206,354, filed 01/28/2009

and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,774, filed 03/02/2009
claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,771, filed 03/02/2009 (PAT 8023425)
claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,773, filed 03/02/2009
claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,769, filed 03/02/2009
claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,777, filed 03/02/2009 (PAT 8583781)
claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/695,019, filed 01/27/2010 (PAT 8275830)
is a CIP of Application No. 12/380,778, filed 03/02/2009 (PAT 8321526)

and is a CIP of Application No. 12/380,771, filed 03/02/2009 (PAT 8023425)
and claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009
and claims benefit of Application No. 61/270,353, filed 07/06/2009
and claims benefit of Application No. 61/264,126, filed 11/24/2009

and said Application No. 12/695,020, filed 01/27/2010 (PAT 8406748)
is a CIP of Application No. 12/380,780, filed 03/02/2009
and claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009
and claims benefit of Application No. 61/275,208, filed 08/25/2009
and claims benefit of Application No. 61/237,753, filed 08/28/2009

and said Application No. 12/694,445, filed 01/27/2010 (PAT 8391834)
is a CIP of Application No. 12/380,780, filed 03/02/2009
and claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009
and claims benefit of Application No. 61/252,151, filed 10/15/2009

and said Application No. 12/694,451, filed 01/27/2010 (PAT 8548428)
is a CIP of Application No. 12/380,780, filed 03/02/2009
and claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009
and claims benefit of Application No. 61/270,353, filed 07/06/2009
and claims benefit of Application No. 61/252,153, filed 10/15/2009

and said Application No. 12/694,455, filed 01/27/2010 (PAT 8402111)
is a CIP of Application No. 12/380,780, filed 03/02/2009

and claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009
and claims benefit of Application No. 61/264,120, filed 11/24/2009

and said Application No. 12/695,021, filed 01/27/2010 (PAT 8346225)
is a CIP of Application No. 12/380,780, filed 03/02/2009
and claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009
and claims benefit of Application No. 61/252,151, filed 10/15/2009
and claims benefit of Application No. 61/252,153, filed 10/15/2009

and said Application No. 12/695,980, filed 01/28/2010 (PAT 8340634)
is a CIP of Application No. 12/380,780, filed 03/02/2009
and is a CIP of Application No. 12/695,019, filed 01/27/2010 (PAT 8275830)
and is a CIP of Application No. 12/695,021, filed 01/27/2010 (PAT 8346225)
and claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009
and claims benefit of Application No. 61/270,353, filed 07/06/2009

and said Application No. 13/134,005, filed 05/25/2011
is a CIP of Application No. 12/380,759, filed 03/02/2009 (PAT 8270310)
and is a CIP of Application No. 12/380,779, filed 03/02/2009
and is a CIP of Application No. 12/380,758, filed 03/02/2009
and is a CIP of Application No. 12/380,778, filed 03/02/2009 (PAT 8321526)
and is a CIP of Application No. 12/380,768, filed 03/02/2009
and is a CIP of Application No. 12/380,767, filed 03/02/2009 (PAT 8355337)
and is a CIP of Application No. 12/380,780, filed 03/02/2009
and is a CIP of Application No. 12/380,755, filed 03/02/2009 (PAT 8331901)
and is a CIP of Application No. 12/380,756, filed 03/02/2009 (PAT 8250207)
and is a CIP of Application No. 12/380,770, filed 03/02/2009 (ABN)

and is a CIP of Application No. 12/380,772, filed 03/02/2009
and is a CIP of Application No. 12/380,782, filed 03/02/2009 (PAT 8270952)
and is a CIP of Application No. 12/380,783, filed 03/02/2009
and is a CIP of Application No. 12/380,757, filed 03/02/2009 (PAT 8326958)
and is a CIP of Application No. 12/380,781, filed 03/02/2009 (PAT 8229812)
and is a CIP of Application No. 12/380,774, filed 03/02/2009
and is a CIP of Application No. 12/380,771, filed 03/02/2009 (PAT 8023425)
and is a CIP of Application No. 12/380,773, filed 03/02/2009
and is a CIP of Application No. 12/380,769, filed 03/02/2009
and is a CIP of Application No. 12/380,777, filed 03/02/2009 (PAT 8583781)
and is a CIP of Application No. 12/695,019, filed 01/27/2010 (PAT 8275830)
and is a CIP of Application No. 12/695,020, filed 01/27/2010 (PAT 8406748)
and is a CIP of Application No. 12/694,445, filed 01/27/2010 (PAT 8391834)
and is a CIP of Application No. 12/694,451, filed 01/27/2010 (PAT 8548428)
and is a CIP of Application No. 12/694,455, filed 01/27/2010 (PAT 8402111)
and is a CIP of Application No. 12/695,021, filed 01/27/2010 (PAT 8346225)
and is a CIP of Application No. 12/695,980, filed 01/28/2010 (PAT 8340634)
and claims benefit of Application No. 61/348,022, filed 05/25/2010
and claims benefit of Application No. 61/381,159, filed 09/09/2010
and claims benefit of Application No. 61/381,162, filed 09/09/2010
and claims benefit of Application No. 61/384,456, filed 09/20/2010
and claims benefit of Application No. 61/385,020, filed 09/21/2010
and claims benefit of Application No. 61/387,243, filed 09/28/2010
and claims benefit of Application No. 61/387,247, filed 09/28/2010
and claims benefit of Application No. 61/389,547, filed 10/04/2010
and claims benefit of Application No. 61/407,358, filed 10/27/2010
and claims benefit of Application No. 61/418,507, filed 12/01/2010
and claims benefit of Application No. 61/418,509, filed 12/01/2010
and claims benefit of Application No. 61/420,727, filed 12/07/2010
and claims benefit of Application No. 61/422,565, filed 12/13/2010
and claims benefit of Application No. 61/422,572, filed 12/13/2010
and claims benefit of Application No. 61/422,574, filed 12/13/2010
and claims benefit of Application No. 61/435,564, filed 01/24/2011
and claims benefit of Application No. 61/472,606, filed 04/06/2011

Application Data Sheet		Attorney Docket No.	RALEP032C1
		Application Number	
Title of Invention	DEVICE-ASSISTED SERVICES FOR PROTECTING NETWORK CAPACITY		

Foreign Priority Information:

None.

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications:

☐	This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013. NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Authorization to Permit Access:

Applicant's completed Authorization to Permit Access to Application by Participating Offices, Form PTO/SB/39, accompanies this filing.

Applicant Information:

Assignee is:	The Assignee, which is an Organization
Organization Name:	Headwater Partners I LLC
Mailing Address Information for Applicant:	Headwater Partners I LLC 350 Marine Parkway, Suite 300 Redwood Shores, CA 94065 U.S.A. (650) 517-2786
E-mail Address:	patent@headwaterllc.com

Application Data Sheet		Attorney Docket No.	RALEP032C1
		Application Number	
Title of Invention	DEVICE-ASSISTED SERVICES FOR PROTECTING NETWORK CAPACITY		

Signature:

Signature: /Krista S. Jacobsen/

Date: November 15, 2013

Printed/Typed Name: Krista S. Jacobsen

Registration Number: 59,374

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
14/082,040	11/15/2013	2447	1050	RALEP032C1	23	3

CONFIRMATION NO. 1015

CORRECTED FILING RECEIPT

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



Date Mailed: 02/25/2014

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

Inventor(s)

Gregory G. Raleigh, Woodside, CA;
Alireza Raissinia, Monte Sereno, CA;
James Lavine, Corte Madera, CA;

Applicant(s)

Headwater Partners I LLC, Redwood Shores, CA

Assignment For Published Patent Application

Headwater Partners I LLC, Redwood Shores, CA

Power of Attorney: The patent practitioners associated with Customer Number 106938

Domestic Priority data as claimed by applicant ~~CIP~~ DIV ← change from CIP to DIV

This application is a ~~CIP of~~ 13/134,028 05/25/2011 PAT 8589541
which is a CIP of 12/380,759 03/02/2009 PAT 8270310
and is a CIP of 12/380,779 03/02/2009
and is a CIP of 12/380,758 03/02/2009
and is a CIP of 12/380,778 03/02/2009 PAT 8321526
and is a CIP of 12/380,768 03/02/2009
and is a CIP of 12/380,767 03/02/2009 PAT 8355337
and is a CIP of 12/380,780 03/02/2009
and is a CIP of 12/380,755 03/02/2009 PAT 8331901
and is a CIP of 12/380,756 03/02/2009 PAT 8250207
and is a CIP of 12/380,770 03/02/2009 ABN
and is a CIP of 12/380,772 03/02/2009
and is a CIP of 12/380,782 03/02/2009 PAT 8270952
and is a CIP of 12/380,783 03/02/2009
and is a CIP of 12/380,757 03/02/2009 PAT 8326958

and is a CIP of 12/380,781 03/02/2009 PAT 8229812
and is a CIP of 12/380,774 03/02/2009 PAT 8630192
and is a CIP of 12/380,771 03/02/2009 PAT 8023425
and is a CIP of 12/380,773 03/02/2009
and is a CIP of 12/380,769 03/02/2009
and is a CIP of 12/380,777 03/02/2009 PAT 8583781
and is a CIP of 12/695,019 01/27/2010 PAT 8275830
and is a CIP of 12/695,020 01/27/2010 PAT 8406748
and is a CIP of 12/694,445 01/27/2010 PAT 8391834
and is a CIP of 12/694,451 01/27/2010 PAT 8548428
and is a CIP of 12/694,455 01/27/2010 PAT 8402111
and is a CIP of 12/695,021 01/27/2010 PAT 8346225
and is a CIP of 12/695,980 01/28/2010 PAT 8340634
and is a CIP of 13/134,005 05/25/2011 PAT 8635335
and claims benefit of 61/348,022 05/25/2010
and claims benefit of 61/381,159 09/09/2010
and claims benefit of 61/381,162 09/09/2010
and claims benefit of 61/384,456 09/20/2010
and claims benefit of 61/385,020 09/21/2010
and claims benefit of 61/387,243 09/28/2010
and claims benefit of 61/387,247 09/28/2010
and claims benefit of 61/389,547 10/04/2010
and claims benefit of 61/407,358 10/27/2010
and claims benefit of 61/418,507 12/01/2010
and claims benefit of 61/418,509 12/01/2010
and claims benefit of 61/420,727 12/07/2010
and claims benefit of 61/422,565 12/13/2010
and claims benefit of 61/422,572 12/13/2010
and claims benefit of 61/422,574 12/13/2010
and claims benefit of 61/435,564 01/24/2011
and claims benefit of 61/472,606 04/06/2011
and said 12/380,759 03/02/2009
claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 12/380,779
claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 12/380,758
claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 12/380,778
claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009

and said 12/380,768
claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 12/380,767
claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 12/380,780
claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 12/380,755
claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 12/380,756
claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 12/380,770
claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 12/380,772
claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 12/380,782
claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 12/380,783
claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 12/380,757
claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and said 12/380,757
claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009

and said 12/380,781
claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 12/380,774
claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 12/380,771 03/02/2009
claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 12/380,773 03/02/2009
claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 12/380,769 03/02/2009
claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 12/380,777 03/02/2009
claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 12/695,019 ~~03/02/2009~~ [01/27/2010]
is a CIP of 12/380,778 03/02/2009 PAT 8321526
and is a CIP of 12/380,771 03/02/2009 PAT 8023425
and claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and claims benefit of 61/270,353 07/06/2009
and claims benefit of 61/264,126 11/24/2009
and said 12/695,020 ~~03/02/2009~~ [01/27/2010]
is a CIP of 12/380,780 03/02/2009
and claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and claims benefit of 61/275,208 08/25/2009
and claims benefit of 61/237,753 08/28/2009
and said 12/694,445 ~~03/02/2009~~ [01/27/2010]
is a CIP of 12/380,780 03/02/2009
and claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009

and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and claims benefit of 61/252,151 10/15/2009
and said 12/694,451 ~~03/02/2009~~ [01/27/2010]
is a CIP of 12/380,780 03/02/2009
and claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and said 12/694,451 01/27/2010
claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and claims benefit of 61/270,353 07/06/2009
and claims benefit of 61/252,153 10/15/2009
and said 12/694,455 01/27/2010
is a CIP of 12/380,780 03/02/2009
and claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and claims benefit of 61/264,120 11/24/2009
and said 12/695,021 01/27/2010
is a CIP of 12/380,780 03/02/2009
and claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and claims benefit of 61/252,151 10/15/2009
and claims benefit of 61/252,153 10/15/2009
and said 12/695,980 ~~01/27/2010~~ [01/28/2010]
is a CIP of 12/380,780 03/02/2009
and is a CIP of 12/695,019 01/27/2010 PAT 8275830
and is a CIP of 12/695,021 01/27/2010 PAT 8346225
and claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and claims benefit of 61/270,353 07/06/2009
and said 13/134,005 ~~01/27/2010~~ [05/25/2011]
is a CIP of 12/380,759 03/02/2009 PAT 8270310
and is a CIP of 12/380,779 03/02/2009
and is a CIP of 12/380,758 03/02/2009
and is a CIP of 12/380,778 03/02/2009 PAT 8321526
and is a CIP of 12/380,768 03/02/2009
and is a CIP of 12/380,767 03/02/2009 PAT 8355337
and is a CIP of 12/380,780 03/02/2009
and is a CIP of 12/380,755 03/02/2009 PAT 8331901
and is a CIP of 12/380,756 03/02/2009 PAT 8250207
and is a CIP of 12/380,770 03/02/2009 ABN
and is a CIP of 12/380,772 03/02/2009
and is a CIP of 12/380,782 03/02/2009 PAT 8270952
and is a CIP of 12/380,783 03/02/2009
and is a CIP of 12/380,757 03/02/2009 PAT 8326958

and is a CIP of 12/380,781 03/02/2009 PAT 8229812
and is a CIP of 12/380,774 03/02/2009 PAT 8630192
and is a CIP of 12/380,771 03/02/2009 PAT 8023425
and is a CIP of 12/380,773 03/02/2009
and is a CIP of 12/380,769 03/02/2009
and is a CIP of 12/380,777 03/02/2009 PAT 8583781
and is a CIP of 12/695,019 01/27/2010 PAT 8275830
and is a CIP of 12/695,020 01/27/2010 PAT 8406748
and is a CIP of 12/694,445 01/27/2010 PAT 8391834
and is a CIP of 12/694,451 01/27/2010 PAT 8548428
and is a CIP of 12/694,455 01/27/2010 PAT 8402111
and said 13/134,005
is a CIP of 12/695,021 01/27/2010 PAT 8346225
and is a CIP of 12/695,980 01/28/2010 PAT 8340634
and claims benefit of 61/348,022 05/25/2010
and claims benefit of 61/381,159 09/09/2010
and claims benefit of 61/381,162 09/09/2010
and claims benefit of 61/384,456 09/20/2010
and claims benefit of 61/385,020 09/21/2010
and claims benefit of 61/387,243 09/28/2010
and claims benefit of 61/387,247 09/28/2010
and claims benefit of 61/389,547 10/04/2010
and claims benefit of 61/407,358 10/27/2010
and claims benefit of 61/418,507 12/01/2010
and claims benefit of 61/418,509 12/01/2010
and claims benefit of 61/420,727 12/07/2010
and claims benefit of 61/422,565 12/13/2010
and claims benefit of 61/422,572 12/13/2010
and claims benefit of 61/422,574 12/13/2010
and claims benefit of 61/435,564 01/24/2011
and claims benefit of 61/472,606 04/06/2011

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

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

If Required, Foreign Filing License Granted: 12/17/2013

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 14/082,040**

Projected Publication Date: 04/03/2014

Non-Publication Request: No

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

Title

Device-Assisted Services for Protecting Network Capacity

Preliminary Class

709

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

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

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

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

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

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

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

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

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

NOT GRANTED

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

SelectUSA

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

Electronic Acknowledgement Receipt

EFS ID:	18319289
Application Number:	14082040
International Application Number:	
Confirmation Number:	1015
Title of Invention:	Device-Assisted Services for Protecting Network Capacity
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	Krista Susan Jacobsen
Filer Authorized By:	
Attorney Docket Number:	RALEP032C1
Receipt Date:	27-FEB-2014
Filing Date:	15-NOV-2013
Time Stamp:	12:38:19
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Request for Corrected Filing Receipt	P32C1_2FRcorr.pdf	2992960 4ba53da798c43269cfa2944cc38ef1aa9126c966	no	22

Warnings:	
Information:	

Total Files Size (in bytes):	2992960

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

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

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

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
14/082,040	11/15/2013	2447	1050	RALEP032C1	23	3

CONFIRMATION NO. 1015

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

CORRECTED FILING RECEIPT

OC000000066736472

Date Mailed: 02/25/2014

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

Inventor(s)

Gregory G. Raleigh, Woodside, CA;
Alireza Raissinia, Monte Sereno, CA;
James Lavine, Corte Madera, CA;

Applicant(s)

Headwater Partners I LLC, Redwood Shores, CA

Assignment For Published Patent Application

Headwater Partners I LLC, Redwood Shores, CA

Power of Attorney: The patent practitioners associated with Customer Number 106938

Domestic Priority data as claimed by applicant

This application is a CIP of 13/134,028 05/25/2011 PAT 8589541
which is a CIP of 12/380,759 03/02/2009 PAT 8270310
and is a CIP of 12/380,779 03/02/2009
and is a CIP of 12/380,758 03/02/2009
and is a CIP of 12/380,778 03/02/2009 PAT 8321526
and is a CIP of 12/380,768 03/02/2009
and is a CIP of 12/380,767 03/02/2009 PAT 8355337
and is a CIP of 12/380,780 03/02/2009
and is a CIP of 12/380,755 03/02/2009 PAT 8331901
and is a CIP of 12/380,756 03/02/2009 PAT 8250207
and is a CIP of 12/380,770 03/02/2009 ABN
and is a CIP of 12/380,772 03/02/2009
and is a CIP of 12/380,782 03/02/2009 PAT 8270952
and is a CIP of 12/380,783 03/02/2009
and is a CIP of 12/380,757 03/02/2009 PAT 8326958

and is a CIP of 12/380,781 03/02/2009 PAT 8229812
and is a CIP of 12/380,774 03/02/2009 PAT 8630192
and is a CIP of 12/380,771 03/02/2009 PAT 8023425
and is a CIP of 12/380,773 03/02/2009
and is a CIP of 12/380,769 03/02/2009
and is a CIP of 12/380,777 03/02/2009 PAT 8583781
and is a CIP of 12/695,019 01/27/2010 PAT 8275830
and is a CIP of 12/695,020 01/27/2010 PAT 8406748
and is a CIP of 12/694,445 01/27/2010 PAT 8391834
and is a CIP of 12/694,451 01/27/2010 PAT 8548428
and is a CIP of 12/694,455 01/27/2010 PAT 8402111
and is a CIP of 12/695,021 01/27/2010 PAT 8346225
and is a CIP of 12/695,980 01/28/2010 PAT 8340634
and is a CIP of 13/134,005 05/25/2011 PAT 8635335
and claims benefit of 61/348,022 05/25/2010
and claims benefit of 61/381,159 09/09/2010
and claims benefit of 61/381,162 09/09/2010
and claims benefit of 61/384,456 09/20/2010
and claims benefit of 61/385,020 09/21/2010
and claims benefit of 61/387,243 09/28/2010
and claims benefit of 61/387,247 09/28/2010
and claims benefit of 61/389,547 10/04/2010
and claims benefit of 61/407,358 10/27/2010
and claims benefit of 61/418,507 12/01/2010
and claims benefit of 61/418,509 12/01/2010
and claims benefit of 61/420,727 12/07/2010
and claims benefit of 61/422,565 12/13/2010
and claims benefit of 61/422,572 12/13/2010
and claims benefit of 61/422,574 12/13/2010
and claims benefit of 61/435,564 01/24/2011
and claims benefit of 61/472,606 04/06/2011
and said 12/380,759 03/02/2009
claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 12/380,779
claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 12/380,758
claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 12/380,778
claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009

and said 12/380,768
claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 12/380,767
claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 12/380,780
claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 12/380,755
claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 12/380,756
claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 12/380,770
claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 12/380,772
claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 12/380,782
claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 12/380,783
claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 12/380,757
claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and said 12/380,757
claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009

and said 12/380,781
claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 12/380,774
claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 12/380,771 03/02/2009
claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 12/380,773 03/02/2009
claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 12/380,769 03/02/2009
claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 12/380,777 03/02/2009
claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 12/695,019 03/02/2009
is a CIP of 12/380,778 03/02/2009 PAT 8321526
and is a CIP of 12/380,771 03/02/2009 PAT 8023425
and claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and claims benefit of 61/270,353 07/06/2009
and claims benefit of 61/264,126 11/24/2009
and said 12/695,020 03/02/2009
is a CIP of 12/380,780 03/02/2009
and claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and claims benefit of 61/275,208 08/25/2009
and claims benefit of 61/237,753 08/28/2009
and said 12/694,445 03/02/2009
is a CIP of 12/380,780 03/02/2009
and claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009

and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and claims benefit of 61/252,151 10/15/2009
and said 12/694,451 03/02/2009
is a CIP of 12/380,780 03/02/2009
and claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and said 12/694,451 01/27/2010
claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and claims benefit of 61/270,353 07/06/2009
and claims benefit of 61/252,153 10/15/2009
and said 12/694,455 01/27/2010
is a CIP of 12/380,780 03/02/2009
and claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and claims benefit of 61/264,120 11/24/2009
and said 12/695,021 01/27/2010
is a CIP of 12/380,780 03/02/2009
and claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and claims benefit of 61/252,151 10/15/2009
and claims benefit of 61/252,153 10/15/2009
and said 12/695,980 01/27/2010
is a CIP of 12/380,780 03/02/2009
and is a CIP of 12/695,019 01/27/2010 PAT 8275830
and is a CIP of 12/695,021 01/27/2010 PAT 8346225
and claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and claims benefit of 61/270,353 07/06/2009
and said 13/134,005 01/27/2010
is a CIP of 12/380,759 03/02/2009 PAT 8270310
and is a CIP of 12/380,779 03/02/2009
and is a CIP of 12/380,758 03/02/2009
and is a CIP of 12/380,778 03/02/2009 PAT 8321526
and is a CIP of 12/380,768 03/02/2009
and is a CIP of 12/380,767 03/02/2009 PAT 8355337
and is a CIP of 12/380,780 03/02/2009
and is a CIP of 12/380,755 03/02/2009 PAT 8331901
and is a CIP of 12/380,756 03/02/2009 PAT 8250207
and is a CIP of 12/380,770 03/02/2009 ABN
and is a CIP of 12/380,772 03/02/2009
and is a CIP of 12/380,782 03/02/2009 PAT 8270952
and is a CIP of 12/380,783 03/02/2009
and is a CIP of 12/380,757 03/02/2009 PAT 8326958

and is a CIP of 12/380,781 03/02/2009 PAT 8229812
and is a CIP of 12/380,774 03/02/2009 PAT 8630192
and is a CIP of 12/380,771 03/02/2009 PAT 8023425
and is a CIP of 12/380,773 03/02/2009
and is a CIP of 12/380,769 03/02/2009
and is a CIP of 12/380,777 03/02/2009 PAT 8583781
and is a CIP of 12/695,019 01/27/2010 PAT 8275830
and is a CIP of 12/695,020 01/27/2010 PAT 8406748
and is a CIP of 12/694,445 01/27/2010 PAT 8391834
and is a CIP of 12/694,451 01/27/2010 PAT 8548428
and is a CIP of 12/694,455 01/27/2010 PAT 8402111
and said 13/134,005
is a CIP of 12/695,021 01/27/2010 PAT 8346225
and is a CIP of 12/695,980 01/28/2010 PAT 8340634
and claims benefit of 61/348,022 05/25/2010
and claims benefit of 61/381,159 09/09/2010
and claims benefit of 61/381,162 09/09/2010
and claims benefit of 61/384,456 09/20/2010
and claims benefit of 61/385,020 09/21/2010
and claims benefit of 61/387,243 09/28/2010
and claims benefit of 61/387,247 09/28/2010
and claims benefit of 61/389,547 10/04/2010
and claims benefit of 61/407,358 10/27/2010
and claims benefit of 61/418,507 12/01/2010
and claims benefit of 61/418,509 12/01/2010
and claims benefit of 61/420,727 12/07/2010
and claims benefit of 61/422,565 12/13/2010
and claims benefit of 61/422,572 12/13/2010
and claims benefit of 61/422,574 12/13/2010
and claims benefit of 61/435,564 01/24/2011
and claims benefit of 61/472,606 04/06/2011

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

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

If Required, Foreign Filing License Granted: 12/17/2013

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 14/082,040**

Projected Publication Date: 04/03/2014

Non-Publication Request: No

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

Title

Device-Assisted Services for Protecting Network Capacity

Preliminary Class

709

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

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

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

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

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

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

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

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

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

NOT GRANTED

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

SelectUSA

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

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	2447
	Examiner Name	Raleigh, Gregory G.
	Attorney Docket Number	RALEP032C1

U.S.PATENTS						
Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5774532	A	1998-06-30	Gottlieb et al.	
If you wish to add additional U.S. Patent citation information please click the Add button.						
U.S.PATENT APPLICATION PUBLICATIONS						
Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20040225898	A	2004-11-11	Frost, D. et al.	
	2	20050079863	A	2005-04-14	Macaluso, Anthony G.	
	3	20060114832	A	2006-06-01	Hamilton et al.	
	4	20060156398	A	2006-07-13	Ross et al.	
	5	20060173959	A	2006-08-03	Mckelvie et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	2447
	Examiner Name	Raleigh, Gregory G.
	Attorney Docket Number	RALEP032C1

	6	20070033194	A	2007-02-08	Srinivas et al.	
	7	20080070550	A	2008-03-20	Hose, David Alan	
	8	20080201266	A	2008-08-21	Chua et al.	
	9	20100284327	A	2010-11-11	Miklos, Gyorgy	

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

FOREIGN PATENT DOCUMENTS

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

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

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	"Communication Concepts for Mobile Agent Systems," by Joachim Baumann et al.; Inst. Of Parallel and Distributed High-Performance Systems, Univ. of Stuttgart, Germany, pp. 123-135, 1997	☐

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

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

EFS Web 2.1.17

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	2447
	Examiner Name	Raleigh, Gregory G.
	Attorney Docket Number	RALEP032C1

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	2447
	Examiner Name	Raleigh, Gregory G.
	Attorney Docket Number	RALEP032C1

CERTIFICATION STATEMENT

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

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

OR

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

☐ See attached certification statement.

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

☒ None

SIGNATURE

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

Signature		Date (YYYY-MM-DD)	2014-01-29
Name/Print	Krista S. Jacbosen	Registration Number	59374

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Electronic Acknowledgement Receipt

EFS ID:	18088694
Application Number:	14082040
International Application Number:	
Confirmation Number:	1015
Title of Invention:	Device-Assisted Services for Protecting Network Capacity
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	Krista Susan Jacobsen/Ann Taylor
Filer Authorized By:	Krista Susan Jacobsen
Attorney Docket Number:	RALEP032C1
Receipt Date:	31-JAN-2014
Filing Date:	15-NOV-2013
Time Stamp:	19:52:27
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Non Patent Literature	3034_Baumann.pdf	2145168 7dcd8af1ff9cab4f61cecb7522d5e0d9c220729a	no	13
Warnings:					
Information:					

2	Information Disclosure Statement (IDS) Form (SB08)	P032C1IDS.pdf	824579 74569fbd86109507bb1553e511bd265b41a69070	no	4

Warnings:	
Information:	
This is not an USPTO supplied IDS fillable form	
Total Files Size (in bytes):	2969747

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

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

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

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Raleigh et al.	Examiner:	not yet assigned
Serial No.:	14/082,040	Art Unit:	2447
Filed:	November 15, 2013	Conf. No.:	1015
Title:	Device-Assisted Services for Protecting Network Capacity		

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

REQUEST FOR A CORRECTED FILING RECEIPT

Madam:

Applicant respectfully requests a corrected filing receipt for the above-captioned application. Submitted with this request are:

(1) The application data sheet (ADS) filed on November 15, 2013 with Applicant's filing of a new application, that ADS reflecting the correct benefit claim.

(2) A copy of the Filing Receipt mailed December 26, 2013 with the requested changes noted thereon.

Applicant respectfully notes that this request is not a request to add or correct a benefit claim. Applicant is simply seeking a filing receipt that reflects the correct benefit claim as provided in the ADS originally submitted on November 15, 2013.

CONCLUSION

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

Respectfully submitted,

Date: January 15, 2014 By: _____

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

CERTIFICATE OF ELECTRONIC TRANSMISSION

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

Date: Jan. 15, 2014 By: _____
Ann Taylor

Application Data Sheet	Attorney Docket No.	RALEP032C1
	Application Number	
Title of Invention	DEVICE-ASSISTED SERVICES FOR PROTECTING NETWORK CAPACITY	

Inventor Information:

Inventor 1 -

Legal Name:

First Name:	Gregory
Middle Name:	G.
Family Name:	Raleigh

Residence Information:

City:	Woodside
State:	CA
Country of Residence:	USA

Mailing Address of Inventor: 350 Marine Parkway, Suite 300
Redwood Shores, CA 94065
USA

Inventor 2 -

Legal Name:

First Name:	Alireza
Middle Name:	
Family Name:	Raissinia

Residence Information:

City:	Monte Sereno
State:	CA
Country of Residence:	USA

Mailing Address of Inventor: 350 Marine Parkway, Suite 300
Redwood Shores, CA 94065
USA

Application Data Sheet	Attorney Docket No.	RALEP032C1
	Application Number	
Title of Invention	DEVICE-ASSISTED SERVICES FOR PROTECTING NETWORK CAPACITY	

Inventor 3 -

Legal Name:

First Name:	James
Middle Name:	
Family Name:	Lavine

Residence Information:

City:	Corte Madera
State:	CA
Country of Residence:	USA

Mailing Address of Inventor: 350 Marine Parkway, Suite 300
Redwood Shores, CA 94065
USA

Correspondence Information:

Correspondence Address:	Customer Number 106963
E-mail address:	patent@headwaterllc.com

Application Information:

Title of Invention:	DEVICE-ASSISTED SERVICES FOR PROTECTING NETWORK CAPACITY
Attorney Docket Number:	RALEP032C1
Small Entity Status Claimed:	Yes
Application Type:	Nonprovisional
Subject Matter:	Utility
Total Number of Drawing Sheets:	29

Application Data Sheet		Attorney Docket No.	RALEP032C1
		Application Number	
Title of Invention	DEVICE-ASSISTED SERVICES FOR PROTECTING NETWORK CAPACITY		

Suggested Drawing Figure for Publication: —

Representative Information:

Customer Number: 106963

Domestic Benefit/National Stage Information:

This application is a DIV of Application No. 13/134,028, filed 05/25/2011

and said Application No. 13/134,028, filed 05/25/2011
is a CIP of Application No. 12/380,759, filed 03/02/2009 (PAT 8270310)
and is a CIP of Application No. 12/380,779, filed 03/02/2009
and is a CIP of Application No. 12/380,758, filed 03/02/2009
and is a CIP of Application No. 12/380,778, filed 03/02/2009 (PAT 8321526)
and is a CIP of Application No. 12/380,768, filed 03/02/2009
and is a CIP of Application No. 12/380,767, filed 03/02/2009 (PAT 8355337)
and is a CIP of Application No. 12/380,780, filed 03/02/2009
and is a CIP of Application No. 12/380,755, filed 03/02/2009 (PAT 8331901)
and is a CIP of Application No. 12/380,756, filed 03/02/2009 (PAT 8250207)
and is a CIP of Application No. 12/380,770, filed 03/02/2009 (ABN)
and is a CIP of Application No. 12/380,772, filed 03/02/2009
and is a CIP of Application No. 12/380,782, filed 03/02/2009 (PAT 8270952)
and is a CIP of Application No. 12/380,783, filed 03/02/2009
and is a CIP of Application No. 12/380,757, filed 03/02/2009 (PAT 8326958)
and is a CIP of Application No. 12/380,781, filed 03/02/2009 (PAT 8229812)
and is a CIP of Application No. 12/380,774, filed 03/02/2009
and is a CIP of Application No. 12/380,771, filed 03/02/2009 (PAT 8023425)
and is a CIP of Application No. 12/380,773, filed 03/02/2009
and is a CIP of Application No. 12/380,769, filed 03/02/2009
and is a CIP of Application No. 12/380,777, filed 03/02/2009 (PAT 8583781)
and is a CIP of Application No. 12/695,019, filed 01/27/2010 (PAT 8275830)
and is a CIP of Application No. 12/695,020, filed 01/27/2010 (PAT 8406748)
and is a CIP of Application No. 12/694,445, filed 01/27/2010 (PAT 8391834)
and is a CIP of Application No. 12/694,451, filed 01/27/2010 (PAT 8548428)

and is a CIP of Application No. 12/694,455, filed 01/27/2010 (PAT 8402111)
and is a CIP of Application No. 12/695,021, filed 01/27/2010 (PAT 8346225)
and is a CIP of Application No. 12/695,980, filed 01/28/2010 (PAT 8340634)
and is a CIP of Application No. 13/134,005, filed 05/25/2011
and claims benefit of Application No. 61/348,022, filed 05/25/2010
and claims benefit of Application No. 61/381,159, filed 09/09/2010
and claims benefit of Application No. 61/381,162, filed 09/09/2010
and claims benefit of Application No. 61/384,456, filed 09/20/2010
and claims benefit of Application No. 61/385,020, filed 09/21/2010
and claims benefit of Application No. 61/387,243, filed 09/28/2010
and claims benefit of Application No. 61/387,247, filed 09/28/2010
and claims benefit of Application No. 61/389,547, filed 10/04/2010
and claims benefit of Application No. 61/407,358, filed 10/27/2010
and claims benefit of Application No. 61/418,507, filed 12/01/2010
and claims benefit of Application No. 61/418,509, filed 12/01/2010
and claims benefit of Application No. 61/420,727, filed 12/07/2010
and claims benefit of Application No. 61/422,565, filed 12/13/2010
and claims benefit of Application No. 61/422,572, filed 12/13/2010
and claims benefit of Application No. 61/422,574, filed 12/13/2010
and claims benefit of Application No. 61/435,564, filed 01/24/2011
and claims benefit of Application No. 61/472,606, filed 04/06/2011

and said Application No. 12/380,759, filed 03/02/2009 (PAT 8270310)
claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,779, filed 03/02/2009
claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,758, filed 03/02/2009
claims benefit of Application No. 61/206,354, filed 01/28/2009

and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,778, filed 03/02/2009 (PAT 8321526)
claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,768, filed 03/02/2009
claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,767, filed 03/02/2009 (PAT 8355337)
claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,780, filed 03/02/2009
claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,755, filed 03/02/2009 (PAT 8331901)
claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,756, filed 03/02/2009 (PAT 8250207)
claims benefit of Application No. 61/206,354, filed 01/28/2009

and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,770, filed 03/02/2009 (ABN)
claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,772, filed 03/02/2009
claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,782, filed 03/02/2009 (PAT 8270952)
claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,783, filed 03/02/2009
claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,757, filed 03/02/2009 (PAT 8326958)
claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,781, filed 03/02/2009 (PAT 8229812)
claims benefit of Application No. 61/206,354, filed 01/28/2009

and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,774, filed 03/02/2009
claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,771, filed 03/02/2009 (PAT 8023425)
claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,773, filed 03/02/2009
claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,769, filed 03/02/2009
claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,777, filed 03/02/2009 (PAT 8583781)
claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/695,019, filed 01/27/2010 (PAT 8275830)
is a CIP of Application No. 12/380,778, filed 03/02/2009 (PAT 8321526)

and is a CIP of Application No. 12/380,771, filed 03/02/2009 (PAT 8023425)
and claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009
and claims benefit of Application No. 61/270,353, filed 07/06/2009
and claims benefit of Application No. 61/264,126, filed 11/24/2009

and said Application No. 12/695,020, filed 01/27/2010 (PAT 8406748)
is a CIP of Application No. 12/380,780, filed 03/02/2009
and claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009
and claims benefit of Application No. 61/275,208, filed 08/25/2009
and claims benefit of Application No. 61/237,753, filed 08/28/2009

and said Application No. 12/694,445, filed 01/27/2010 (PAT 8391834)
is a CIP of Application No. 12/380,780, filed 03/02/2009
and claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009
and claims benefit of Application No. 61/252,151, filed 10/15/2009

and said Application No. 12/694,451, filed 01/27/2010 (PAT 8548428)
is a CIP of Application No. 12/380,780, filed 03/02/2009
and claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009
and claims benefit of Application No. 61/270,353, filed 07/06/2009
and claims benefit of Application No. 61/252,153, filed 10/15/2009

and said Application No. 12/694,455, filed 01/27/2010 (PAT 8402111)
is a CIP of Application No. 12/380,780, filed 03/02/2009

and claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009
and claims benefit of Application No. 61/264,120, filed 11/24/2009

and said Application No. 12/695,021, filed 01/27/2010 (PAT 8346225)
is a CIP of Application No. 12/380,780, filed 03/02/2009
and claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009
and claims benefit of Application No. 61/252,151, filed 10/15/2009
and claims benefit of Application No. 61/252,153, filed 10/15/2009

and said Application No. 12/695,980, filed 01/28/2010 (PAT 8340634)
is a CIP of Application No. 12/380,780, filed 03/02/2009
and is a CIP of Application No. 12/695,019, filed 01/27/2010 (PAT 8275830)
and is a CIP of Application No. 12/695,021, filed 01/27/2010 (PAT 8346225)
and claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009
and claims benefit of Application No. 61/270,353, filed 07/06/2009

and said Application No. 13/134,005, filed 05/25/2011
is a CIP of Application No. 12/380,759, filed 03/02/2009 (PAT 8270310)
and is a CIP of Application No. 12/380,779, filed 03/02/2009
and is a CIP of Application No. 12/380,758, filed 03/02/2009
and is a CIP of Application No. 12/380,778, filed 03/02/2009 (PAT 8321526)
and is a CIP of Application No. 12/380,768, filed 03/02/2009
and is a CIP of Application No. 12/380,767, filed 03/02/2009 (PAT 8355337)
and is a CIP of Application No. 12/380,780, filed 03/02/2009
and is a CIP of Application No. 12/380,755, filed 03/02/2009 (PAT 8331901)
and is a CIP of Application No. 12/380,756, filed 03/02/2009 (PAT 8250207)
and is a CIP of Application No. 12/380,770, filed 03/02/2009 (ABN)

and is a CIP of Application No. 12/380,772, filed 03/02/2009
and is a CIP of Application No. 12/380,782, filed 03/02/2009 (PAT 8270952)
and is a CIP of Application No. 12/380,783, filed 03/02/2009
and is a CIP of Application No. 12/380,757, filed 03/02/2009 (PAT 8326958)
and is a CIP of Application No. 12/380,781, filed 03/02/2009 (PAT 8229812)
and is a CIP of Application No. 12/380,774, filed 03/02/2009
and is a CIP of Application No. 12/380,771, filed 03/02/2009 (PAT 8023425)
and is a CIP of Application No. 12/380,773, filed 03/02/2009
and is a CIP of Application No. 12/380,769, filed 03/02/2009
and is a CIP of Application No. 12/380,777, filed 03/02/2009 (PAT 8583781)
and is a CIP of Application No. 12/695,019, filed 01/27/2010 (PAT 8275830)
and is a CIP of Application No. 12/695,020, filed 01/27/2010 (PAT 8406748)
and is a CIP of Application No. 12/694,445, filed 01/27/2010 (PAT 8391834)
and is a CIP of Application No. 12/694,451, filed 01/27/2010 (PAT 8548428)
and is a CIP of Application No. 12/694,455, filed 01/27/2010 (PAT 8402111)
and is a CIP of Application No. 12/695,021, filed 01/27/2010 (PAT 8346225)
and is a CIP of Application No. 12/695,980, filed 01/28/2010 (PAT 8340634)
and claims benefit of Application No. 61/348,022, filed 05/25/2010
and claims benefit of Application No. 61/381,159, filed 09/09/2010
and claims benefit of Application No. 61/381,162, filed 09/09/2010
and claims benefit of Application No. 61/384,456, filed 09/20/2010
and claims benefit of Application No. 61/385,020, filed 09/21/2010
and claims benefit of Application No. 61/387,243, filed 09/28/2010
and claims benefit of Application No. 61/387,247, filed 09/28/2010
and claims benefit of Application No. 61/389,547, filed 10/04/2010
and claims benefit of Application No. 61/407,358, filed 10/27/2010
and claims benefit of Application No. 61/418,507, filed 12/01/2010
and claims benefit of Application No. 61/418,509, filed 12/01/2010
and claims benefit of Application No. 61/420,727, filed 12/07/2010
and claims benefit of Application No. 61/422,565, filed 12/13/2010
and claims benefit of Application No. 61/422,572, filed 12/13/2010
and claims benefit of Application No. 61/422,574, filed 12/13/2010
and claims benefit of Application No. 61/435,564, filed 01/24/2011
and claims benefit of Application No. 61/472,606, filed 04/06/2011

Application Data Sheet		Attorney Docket No.	RALEP032C1
		Application Number	
Title of Invention	DEVICE-ASSISTED SERVICES FOR PROTECTING NETWORK CAPACITY		

Foreign Priority Information:

None.

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications:

☐	This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013. NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Authorization to Permit Access:

Applicant's completed Authorization to Permit Access to Application by Participating Offices, Form PTO/SB/39, accompanies this filing.

Applicant Information:

Assignee is:	The Assignee, which is an Organization
Organization Name:	Headwater Partners I LLC
Mailing Address Information for Applicant:	Headwater Partners I LLC 350 Marine Parkway, Suite 300 Redwood Shores, CA 94065 U.S.A. (650) 517-2786
E-mail Address:	patent@headwaterllc.com

Application Data Sheet		Attorney Docket No.	RALEP032C1
		Application Number	
Title of Invention	DEVICE-ASSISTED SERVICES FOR PROTECTING NETWORK CAPACITY		

Signature:

Signature: /Krista S. Jacobsen/

Date: November 15, 2013

Printed/Typed Name: Krista S. Jacobsen

Registration Number: 59,374

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
14/082,040	11/15/2013	2447	1050	RALEP032C1	23	3

CONFIRMATION NO. 1015

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

FILING RECEIPT

OC000000065599185

Date Mailed: 12/26/2013

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

Inventor(s)

Gregory G. Raleigh, Woodside, CA;
Alireza Raissinia, Monte Sereno, CA;
James Lavine, Corte Madera, CA;

Applicant(s)

Headwater Partners I LLC, Redwood Shores, CA

Assignment For Published Patent Application

Headwater Partners I LLC, Redwood Shores, CA

Power of Attorney: The patent practitioners associated with Customer Number 106938

Domestic Priority data as claimed by applicant

This application is a DIV of 13/134,028 05/25/2011 PAT 8589541
which is a CIP of 12/380,759 03/02/2009 PAT 8270310
and claims benefit of 61/472,606 04/06/2011
and claims benefit of 61/435,564 01/24/2011
and claims benefit of 61/422,574 12/13/2010
and claims benefit of 61/422,572 12/13/2010
and claims benefit of 61/422,565 12/13/2010
and claims benefit of 61/420,727 12/07/2010
and claims benefit of 61/418,509 12/01/2010
and claims benefit of 61/418,507 12/01/2010
and claims benefit of 61/407,358 10/27/2010
and claims benefit of 61/389,547 10/04/2010
and claims benefit of 61/387,247 09/28/2010
and claims benefit of 61/387,243 09/28/2010
and claims benefit of 61/385,020 09/21/2010

and claims benefit of 61/384,456 09/20/2010
and claims benefit of 61/381,162 09/09/2010
and claims benefit of 61/381,159 09/09/2010
and claims benefit of 61/348,022 05/25/2010
and is a CIP of 13/134,005 05/25/2011
which is a CIP of 12/380,759 03/02/2009 PAT 8270310
and is a CIP of 12/380,779 03/02/2009
and is a CIP of 12/380,758 03/02/2009
and is a CIP of 12/380,778 03/02/2009 PAT 8321526
and is a CIP of 12/380,768 03/02/2009
and is a CIP of 12/380,767 03/02/2009 PAT 8355337
and is a CIP of 12/380,780 03/02/2009
and is a CIP of 12/380,755 03/02/2009 PAT 8331901
and is a CIP of 12/380,756 03/02/2009 PAT 8250207
and is a CIP of 12/380,782 03/02/2009 PAT 8270952
and is a CIP of 12/380,770 03/02/2009 ABN
and is a CIP of 12/380,772 03/02/2009
and is a CIP of 12/380,783 03/02/2009
and is a CIP of 12/380,757 03/02/2009 PAT 8326958
and is a CIP of 12/380,781 03/02/2009 PAT 8229812
and is a CIP of 12/380,774 03/02/2009 PAT 8630192
and is a CIP of 12/380,771 03/02/2009 PAT 8023425
and is a CIP of 12/380,773 03/02/2009
and is a CIP of 12/380,769 03/02/2009
and is a CIP of 12/380,777 03/02/2009 PAT 8583781
which claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 13/134,005 05/25/2011
is a CIP of 12/695,019 01/27/2010 PAT 8275830
which is a CIP of 12/380,778 03/02/2009 PAT 8321526
and is a CIP of 12/380,771 03/02/2009 PAT 8023425
and claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and said 12/695,019 01/27/2010
claims benefit of 61/207,739 02/13/2009
and claims benefit of 61/270,353 07/06/2009
and claims benefit of 61/264,126 11/24/2009
and said 13/134,005 ~~01/27/2010~~ [05/25/2011]
is a CIP of 12/695,020 01/27/2010 PAT 8406748
which is a CIP of 12/380,780 03/02/2009
and claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and claims benefit of 61/275,208 08/25/2009
and claims benefit of 61/237,753 08/28/2009
and said 13/134,005 ~~01/27/2010~~ [05/25/2011]
is a CIP of 12/694,445 01/27/2010 PAT 8391834

which is a CIP of 12/380,780 03/02/2009
and claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and claims benefit of 61/252,151 10/15/2009
and said 13/134,005 ~~01/27/2010~~ [05/25/2011]
is a CIP of 12/694,451 01/27/2010 PAT 8548428
which is a CIP of 12/380,780 03/02/2009
and claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and claims benefit of 61/270,353 07/06/2009
and claims benefit of 61/252,153 10/15/2009
and said 13/134,005 ~~01/27/2010~~ [05/25/2011]
is a CIP of 12/694,455 01/27/2010 PAT 8402111
which is a CIP of 12/380,780 03/02/2009
and claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and claims benefit of 61/264,120 11/24/2009
and said 13/134,005 ~~01/27/2010~~ [05/25/2011]
is a CIP of 12/695,021 01/27/2010 PAT 8346225
which is a CIP of 12/380,780 03/02/2009
and claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and claims benefit of 61/252,151 10/15/2009
and claims benefit of 61/252,153 10/15/2009
and said 13/134,005 ~~01/27/2010~~ [05/25/2011]
is a CIP of 12/695,980 01/28/2010 PAT 8340634
which is a CIP of 12/380,780 03/02/2009
and is a CIP of 12/695,019 01/27/2010 PAT 8275830
and is a CIP of 12/695,021 01/27/2010 PAT 8346225
and claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and claims benefit of 61/270,353 07/06/2009
and said 13/134,028
is a CIP of 12/695,980 01/28/2010 PAT 8340634
which is a CIP of 12/380,780 03/02/2009
and is a CIP of 12/695,019 01/27/2010 PAT 8275830
and is a CIP of 12/695,021 01/27/2010 PAT 8346225
and claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009

and claims benefit of 61/270,353 07/06/2009
and said 13/134,028
is a CIP of 12/695,021 01/27/2010 PAT 8346225
which is a CIP of 12/380,780 03/02/2009
and claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and claims benefit of 61/252,151 10/15/2009
and claims benefit of 61/252,153 10/15/2009
and said 13/134,028
is a CIP of 12/694,455 01/27/2010 PAT 8402111
which is a CIP of 12/380,780 03/02/2009
and claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and claims benefit of 61/264,120 11/24/2009
and said 13/134,028
is a CIP of 12/694,451 01/27/2010 PAT 8548428
which is a CIP of 12/380,780 03/02/2009
and claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and claims benefit of 61/270,353 07/06/2009
and claims benefit of 61/252,153 10/15/2009
and said 13/134,028
is a CIP of 12/694,445 01/27/2010 PAT 8391834
which is a CIP of 12/380,780 03/02/2009
and claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and claims benefit of 61/252,151 10/15/2009
and said 13/134,028
is a CIP of 12/695,020 01/27/2010 PAT 8406748
which is a CIP of 12/380,780 03/02/2009
and claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and claims benefit of 61/275,208 08/25/2009
and claims benefit of 61/237,753 08/28/2009
and said 13/134,028
is a CIP of 12/695,019 01/27/2010 PAT 8275830
which is a CIP of 12/380,778 03/02/2009 PAT 8321526
and is a CIP of 12/380,771 03/02/2009 PAT 8023425
and said 12/695,019
claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009

and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and claims benefit of 61/270,353 07/06/2009
and claims benefit of 61/264,126 11/24/2009
and said 13/134,028
is a CIP of 12/380,777 03/02/2009 PAT 8583781
which claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 13/134,028
is a CIP of 12/380,769 03/02/2009
which claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 13/134,028
is a CIP of 12/380,773 03/02/2009
which claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 13/134,028
is a CIP of 12/380,774 03/02/2009 PAT 8630192
which claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 13/134,028
is a CIP of 12/380,781 03/02/2009 PAT 8229812
which claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 13/134,028
is a CIP of 12/380,757 03/02/2009 PAT 8326958
which claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 13/134,028
is a CIP of 12/380,783 03/02/2009
which claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 13/134,028
is a CIP of 12/380,782 03/02/2009 PAT 8270952
which claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009

and claims benefit of 61/207,739 02/13/2009
and said 13/134,028
is a CIP of 12/380,772 03/02/2009
which claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and said 12/380,772
claims benefit of 61/207,739 02/13/2009
and said 13/134,028
is a CIP of 12/380,771 03/02/2009 PAT 8023425
which claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 13/134,028
is a CIP of 12/380,770 03/02/2009 ABN
which claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 13/134,028
is a CIP of 12/380,756 03/02/2009 PAT 8250207
which claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 13/134,028
is a CIP of 12/380,755 03/02/2009 PAT 8331901
which claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 13/134,028
is a CIP of 12/380,780 03/02/2009
which claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 13/134,028
is a CIP of 12/380,767 03/02/2009 PAT 8355337
which claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,739 02/13/2009
and claims benefit of 61/207,393 02/10/2009
and said 13/134,028
is a CIP of 12/380,768 03/02/2009
which claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 13/134,028

ADD:

is a CIP of 12/380,778 03/02/2009 PAT 8321526
which claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 13/134,028
is a CIP of 12/380,758 03/02/2009
which claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 13/134,028
is a CIP of 12/380,779 03/02/2009
which claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and said 12/380,779
claims benefit of 61/207,739 02/13/2009
and said 12/380,759
claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009

and said 13/134,005 05/25/2011
claims benefit of 61/348,022 05/25/2010
and claims benefit of 61/381,159 09/09/2010
and claims benefit of 61/381,162 09/09/2010
and claims benefit of 61/384,456 09/20/2010
and claims benefit of 61/385,020 09/21/2010
and claims benefit of 61/387,243 09/28/2010
and claims benefit of 61/387,247 09/28/2010
and claims benefit of 61/389,547 10/04/2010
and claims benefit of 61/407,358 10/27/2010
and claims benefit of 61/418,507 12/01/2010
and claims benefit of 61/418,509 12/01/2010
and claims benefit of 61/420,727 12/07/2010
and claims benefit of 61/422,565 12/13/2010
and claims benefit of 61/422,572 12/13/2010
and claims benefit of 61/422,574 12/13/2010
and claims benefit of 61/435,564 01/24/2011
and claims benefit of 61/472,606 04/06/2011

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

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

If Required, Foreign Filing License Granted: 12/17/2013

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 14/082,040**

Projected Publication Date: 04/03/2014

Non-Publication Request: No

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

Device-Assisted Services for Protecting Network Capacity

Preliminary Class

709

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

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

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

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

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

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

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

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

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

NOT GRANTED

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

SelectUSA

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

Electronic Acknowledgement Receipt

EFS ID:	17926644
Application Number:	14082040
International Application Number:	
Confirmation Number:	1015
Title of Invention:	Device-Assisted Services for Protecting Network Capacity
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	Krista Susan Jacobsen/Ann Taylor
Filer Authorized By:	Krista Susan Jacobsen
Attorney Docket Number:	RALEP032C1
Receipt Date:	15-JAN-2014
Filing Date:	15-NOV-2013
Time Stamp:	21:56:39
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Request for Corrected Filing Receipt	P032C1Request.pdf	3414111 082a7a6399b74c36a71b9c7d50d4dcf0cd9ce132	no	23

Warnings:	
Information:	

Total Files Size (in bytes):	3414111

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

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

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

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/082,040	11/15/2013	Gregory G. Raleigh	RALEP032C1

CONFIRMATION NO. 1015

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

POA ACCEPTANCE LETTER

OC000000065590561

Date Mailed: 12/26/2013

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 11/27/2013.

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

/cma/

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

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 14/082,040

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	70		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	300		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	360		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	23 minus 20 =	* 3	x 40 =	120	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*	x 210 =	0.00			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			200			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	1050		TOTAL	

APPLICATION AS AMENDED - PART II

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

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

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

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

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

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
14/082,040	11/15/2013	2447	1050	RALEP032C1	23	3

CONFIRMATION NO. 1015

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

FILING RECEIPT



Date Mailed: 12/26/2013

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

Inventor(s)

Gregory G. Raleigh, Woodside, CA;
Alireza Raissinia, Monte Sereno, CA;
James Lavine, Corte Madera, CA;

Applicant(s)

Headwater Partners I LLC, Redwood Shores, CA

Assignment For Published Patent Application

Headwater Partners I LLC, Redwood Shores, CA

Power of Attorney: The patent practitioners associated with Customer Number 106938

Domestic Priority data as claimed by applicant

This application is a DIV of 13/134,028 05/25/2011 PAT 8589541
which is a CIP of 12/380,759 03/02/2009 PAT 8270310
and claims benefit of 61/472,606 04/06/2011
and claims benefit of 61/435,564 01/24/2011
and claims benefit of 61/422,574 12/13/2010
and claims benefit of 61/422,572 12/13/2010
and claims benefit of 61/422,565 12/13/2010
and claims benefit of 61/420,727 12/07/2010
and claims benefit of 61/418,509 12/01/2010
and claims benefit of 61/418,507 12/01/2010
and claims benefit of 61/407,358 10/27/2010
and claims benefit of 61/389,547 10/04/2010
and claims benefit of 61/387,247 09/28/2010
and claims benefit of 61/387,243 09/28/2010
and claims benefit of 61/385,020 09/21/2010

and claims benefit of 61/384,456 09/20/2010
and claims benefit of 61/381,162 09/09/2010
and claims benefit of 61/381,159 09/09/2010
and claims benefit of 61/348,022 05/25/2010
and is a CIP of 13/134,005 05/25/2011
which is a CIP of 12/380,759 03/02/2009 PAT 8270310
and is a CIP of 12/380,779 03/02/2009
and is a CIP of 12/380,758 03/02/2009
and is a CIP of 12/380,778 03/02/2009 PAT 8321526
and is a CIP of 12/380,768 03/02/2009
and is a CIP of 12/380,767 03/02/2009 PAT 8355337
and is a CIP of 12/380,780 03/02/2009
and is a CIP of 12/380,755 03/02/2009 PAT 8331901
and is a CIP of 12/380,756 03/02/2009 PAT 8250207
and is a CIP of 12/380,782 03/02/2009 PAT 8270952
and is a CIP of 12/380,770 03/02/2009 ABN
and is a CIP of 12/380,772 03/02/2009
and is a CIP of 12/380,783 03/02/2009
and is a CIP of 12/380,757 03/02/2009 PAT 8326958
and is a CIP of 12/380,781 03/02/2009 PAT 8229812
and is a CIP of 12/380,774 03/02/2009 PAT 8630192
and is a CIP of 12/380,771 03/02/2009 PAT 8023425
and is a CIP of 12/380,773 03/02/2009
and is a CIP of 12/380,769 03/02/2009
and is a CIP of 12/380,777 03/02/2009 PAT 8583781
which claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 13/134,005 05/25/2011
is a CIP of 12/695,019 01/27/2010 PAT 8275830
which is a CIP of 12/380,778 03/02/2009 PAT 8321526
and is a CIP of 12/380,771 03/02/2009 PAT 8023425
and claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and said 12/695,019 01/27/2010
claims benefit of 61/207,739 02/13/2009
and claims benefit of 61/270,353 07/06/2009
and claims benefit of 61/264,126 11/24/2009
and said 13/134,005 01/27/2010
is a CIP of 12/695,020 01/27/2010 PAT 8406748
which is a CIP of 12/380,780 03/02/2009
and claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and claims benefit of 61/275,208 08/25/2009
and claims benefit of 61/237,753 08/28/2009
and said 13/134,005 01/27/2010
is a CIP of 12/694,445 01/27/2010 PAT 8391834

which is a CIP of 12/380,780 03/02/2009
and claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and claims benefit of 61/252,151 10/15/2009
and said 13/134,005 01/27/2010
is a CIP of 12/694,451 01/27/2010 PAT 8548428
which is a CIP of 12/380,780 03/02/2009
and claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and claims benefit of 61/270,353 07/06/2009
and claims benefit of 61/252,153 10/15/2009
and said 13/134,005 01/27/2010
is a CIP of 12/694,455 01/27/2010 PAT 8402111
which is a CIP of 12/380,780 03/02/2009
and claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and claims benefit of 61/264,120 11/24/2009
and said 13/134,005 01/27/2010
is a CIP of 12/695,021 01/27/2010 PAT 8346225
which is a CIP of 12/380,780 03/02/2009
and claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and claims benefit of 61/252,151 10/15/2009
and claims benefit of 61/252,153 10/15/2009
and said 13/134,005 01/27/2010
is a CIP of 12/695,980 01/28/2010 PAT 8340634
which is a CIP of 12/380,780 03/02/2009
and is a CIP of 12/695,019 01/27/2010 PAT 8275830
and is a CIP of 12/695,021 01/27/2010 PAT 8346225
and claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and claims benefit of 61/270,353 07/06/2009
and said 13/134,028
is a CIP of 12/695,980 01/28/2010 PAT 8340634
which is a CIP of 12/380,780 03/02/2009
and is a CIP of 12/695,019 01/27/2010 PAT 8275830
and is a CIP of 12/695,021 01/27/2010 PAT 8346225
and claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009

and claims benefit of 61/270,353 07/06/2009
and said 13/134,028
is a CIP of 12/695,021 01/27/2010 PAT 8346225
which is a CIP of 12/380,780 03/02/2009
and claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and claims benefit of 61/252,151 10/15/2009
and claims benefit of 61/252,153 10/15/2009
and said 13/134,028
is a CIP of 12/694,455 01/27/2010 PAT 8402111
which is a CIP of 12/380,780 03/02/2009
and claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and claims benefit of 61/264,120 11/24/2009
and said 13/134,028
is a CIP of 12/694,451 01/27/2010 PAT 8548428
which is a CIP of 12/380,780 03/02/2009
and claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and claims benefit of 61/270,353 07/06/2009
and claims benefit of 61/252,153 10/15/2009
and said 13/134,028
is a CIP of 12/694,445 01/27/2010 PAT 8391834
which is a CIP of 12/380,780 03/02/2009
and claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and claims benefit of 61/252,151 10/15/2009
and said 13/134,028
is a CIP of 12/695,020 01/27/2010 PAT 8406748
which is a CIP of 12/380,780 03/02/2009
and claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and claims benefit of 61/275,208 08/25/2009
and claims benefit of 61/237,753 08/28/2009
and said 13/134,028
is a CIP of 12/695,019 01/27/2010 PAT 8275830
which is a CIP of 12/380,778 03/02/2009 PAT 8321526
and is a CIP of 12/380,771 03/02/2009 PAT 8023425
and said 12/695,019
claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009

and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and claims benefit of 61/270,353 07/06/2009
and claims benefit of 61/264,126 11/24/2009
and said 13/134,028
is a CIP of 12/380,777 03/02/2009 PAT 8583781
which claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 13/134,028
is a CIP of 12/380,769 03/02/2009
which claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 13/134,028
is a CIP of 12/380,773 03/02/2009
which claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 13/134,028
is a CIP of 12/380,774 03/02/2009 PAT 8630192
which claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 13/134,028
is a CIP of 12/380,781 03/02/2009 PAT 8229812
which claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 13/134,028
is a CIP of 12/380,757 03/02/2009 PAT 8326958
which claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 13/134,028
is a CIP of 12/380,783 03/02/2009
which claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 13/134,028
is a CIP of 12/380,782 03/02/2009 PAT 8270952
which claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009

and claims benefit of 61/207,739 02/13/2009
and said 13/134,028
is a CIP of 12/380,772 03/02/2009
which claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and said 12/380,772
claims benefit of 61/207,739 02/13/2009
and said 13/134,028
is a CIP of 12/380,771 03/02/2009 PAT 8023425
which claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 13/134,028
is a CIP of 12/380,770 03/02/2009 ABN
which claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 13/134,028
is a CIP of 12/380,756 03/02/2009 PAT 8250207
which claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 13/134,028
is a CIP of 12/380,755 03/02/2009 PAT 8331901
which claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 13/134,028
is a CIP of 12/380,780 03/02/2009
which claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 13/134,028
is a CIP of 12/380,767 03/02/2009 PAT 8355337
which claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,739 02/13/2009
and claims benefit of 61/207,393 02/10/2009
and said 13/134,028
is a CIP of 12/380,768 03/02/2009
which claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 13/134,028

is a CIP of 12/380,778 03/02/2009 PAT 8321526
which claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 13/134,028
is a CIP of 12/380,758 03/02/2009
which claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and said 13/134,028
is a CIP of 12/380,779 03/02/2009
which claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and said 12/380,779
claims benefit of 61/207,739 02/13/2009
and said 12/380,759
claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009

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

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

If Required, Foreign Filing License Granted: 12/17/2013

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 14/082,040**

Projected Publication Date: 04/03/2014

Non-Publication Request: No

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

Device-Assisted Services for Protecting Network Capacity

Preliminary Class

709

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

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

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

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

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

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

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

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

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

NOT GRANTED

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

SelectUSA

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

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

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO

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

I hereby appoint:

☒ Practitioners associated with Customer Number: 106963

OR

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

Name	Registration Number

Name	Registration Number

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

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

☒ The address associated with Customer Number: 106963

OR

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

Assignee Name and Address: Headwater Partners I, LLC
350 Marine Parkway, Suite 300
Redwood Shores, CA 94065 U.S.A.

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

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

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

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

Electronic Acknowledgement Receipt

EFS ID:	17528730
Application Number:	14082040
International Application Number:	
Confirmation Number:	1015
Title of Invention:	Device-Assisted Services for Protecting Network Capacity
First Named Inventor/Applicant Name:	
Customer Number:	106963
Filer:	Krista Susan Jacobsen/Ann Taylor
Filer Authorized By:	Krista Susan Jacobsen
Attorney Docket Number:	RALEP032C1
Receipt Date:	27-NOV-2013
Filing Date:	
Time Stamp:	19:52:33
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Assignee showing of ownership per 37 CFR 3.73.	P032C1Statement.pdf	511394 308b7c61b37e21f70edfea6a340baea6a0fc4e2d	no	2

Warnings:	
Information:	

2	Power of Attorney	POA.pdf	353925 5554f20ce32139c25d995e55caf22e05a09baa90	no	1

Warnings:	
Information:	
Total Files Size (in bytes):	865319

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

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

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

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

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

STATEMENT UNDER 37 CFR 3.73(c)

Applicant/Patent Owner: Headwater Partners I LLC

Application No./Patent No.: 14/082,040 Filed/Issue Date: Nov. 15, 2013

Titled: Device-Assisted Services for Protecting Network Capacity

Headwater Partners I LLC, a limited liability company

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

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

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

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

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

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

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

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

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

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

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

A. ☑ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel 031671, Frame 0512, or for which a copy thereof is attached.

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

   1. From: _____ To: _____

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

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

   2. From: _____ To: _____

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

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

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

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

STATEMENT UNDER 37 CFR 3.73(c)

3. From: _____ To: _____

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

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

4. From: _____ To: _____

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

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

5. From: _____ To: _____

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

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

6. From: _____ To: _____

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

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

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

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

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

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

Signature — Date: Nov. 27, 2013

Krista S. Jacobsen — Printed or Typed Name

59374 — Title or Registration Number

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

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

Application Number	14082040
Filing Date	2013-11-15
First Named Inventor	Raleigh
Art Unit	2447
Examiner Name	not yet assigned
Attorney Docket Number	RALEP032C1

U.S.PATENTS Remove

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	174	8064896		2011-11-22	BELL, Kris M. et al.	
	175	8160015		2012-04-17	RASHID, Mohammed H. et al.	
	176	8275830		2012-09-25	Raleigh, Gregory G.	
	177	7609700		2009-10-27	Ying, Wen-Ping et al.	
	178	8255515		2012-08-28	MELMAN, David et al.	
	179	7945240		2011-05-17	KLOCK, Jacqueline et al.	
	180	7912056		2011-03-22	BRASSEM, Wayne	
	181	7920529		2011-04-05	MAHLER, Roger et al.	
	182	8184530		2012-05-22	SWAN, Tim L. et al.	
	183	8214536		2012-07-03	ZHAO, Wen	
	184	8213363		2012-07-03	Ying, Wen-Ping et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	185	8255689		2012-08-28	KIM, Eun Ah et al.	
	186	7746854		2010-06-29	AMBE, Shekhar et al.	
	187	7068600		2006-06-27	CAIN, Joseph Bibb	
	188	6876653		2005-04-05	AMBE, Shekhar et al.	
	189	6631122		2003-10-07	ARUNACHALAM, Vaidhyanathan et al.	
	190	7599288		2009-10-06	COLE, Raymond E. et al.	
	191	7546629		2009-06-09	ALBERT, Anthony et al.	
	192	7747730		2010-06-29	HARLOW, James D.	
	193	7609650		2009-10-27	ROSKOWSKI, Steve et al.	
	194	6581092		2003-06-17	MOTOYAMA, Tetsuro	
	195	7283963		2007-10-16	FITZPATRICK, John E. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	196	8271049		2012-09-18	SILVER, Andrew et al.	
	197	7644151		2010-01-05	JERRIM, John et al.	
	198	8291238		2012-10-16	GINTER, Karl L. et al.	
	199	8068824		2011-11-29	SHAN, Xueshan et al.	
	200	7228354		2007-06-05	CHAMBLISS, David Darden et al.	
	201	5283904		1994-02-01	CARSON, David G. et al.	
	202	8208919		2012-06-26	KOTECHA, Lalit Ratilal	
	203	8185152		2012-05-22	GOLDNER, Alla	
	204	7844728		2010-11-30	ANDERSON, Thomas W. et al.	
	205	7873344		2011-01-18	BOWSER, Robert et al.	
	206	7856226		2010-12-21	WONG, Ellis L. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	207	7948952		2011-05-24	HURTTA, Tuija et al.	
	208	7957020		2011-06-07	MINE, Ryuta et al.	
	209	7346410		2008-03-18	UCHIYAMA, Kenji	
	210	7167078		2007-01-23	POURCHOT, Shawn C.	
	211	8102814		2012-01-24	RAHMAN, Shahriar I. et al.	
	212	7970350		2011-06-28	SHEYNMAN, Arnold	
	213	8094551		2012-01-10	HUBER, Kurt Donald et al.	
	214	8335161		2012-12-18	Foottit, Tom et al.	
	215	8315594		2012-11-20	Mauser, Edward Ronald et al.	
	216	8135388		2012-03-13	Gailloux, Michael A. et al.	
	217	6947723		2005-09-20	Gurnani, Roger et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	218	8353001		2013-01-08	Herrod, Allan	
	219	8195093		2013-06-05	Garrett, Darrin et al.	
	220	8036600		2011-10-11	Garrett, Darrin et al.	
	221	8301513		2012-10-30	Peng, Shih-Ta et al.	
	222	8230061		2012-07-24	Hassan, Amer A. et al.	
	223	8204794		2012-06-19	Peng, Shih-Ta et al.	
	224	8350700		2013-01-08	Fast, Raymond D. et al.	
	225	8204190		2012-06-19	Bang, Jung-Hee et al.	
	226	7865182		2011-01-04	Macaluso, Anthony G.	
	227	7962622		2011-06-14	Friend, John et al.	
	228	7583964		2009-09-01	Wong, Gregory A.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	229	7565141		2009-06-21	Macaluso, Anthony G.	
	230	7373179		2008-05-13	Stine, Ted et al.	
	231	7236780		2007-06-26	Benco, David S.	
	232	7039403		2006-05-02	Wong, Gregory A.	
	233	8370477		2013-02-05	Short, Joel E. et al.	
	234	8364806		2013-01-29	Short, Joel E. et al.	
	235	8279067		2012-10-02	BERGER, Thomas R. et al.	
	236	8213296		2012-07-03	SHANNON, Frank M. et al.	
	237	8019868		2011-09-13	RAO, Goutham et al.	
	238	8005988		2011-08-23	MAES, Stephane H.	
	239	7978627		2011-07-12	TAYLOR, William Scott et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	240	7711848		2010-05-04	MAES, Stephane H.	
	241	6782412		2004-08-24	BROPHY, Kevin et al.	
	242	6081591		2000-06-27	SKOOG, Frederick H.	
	243	6064878		2000-05-16	DENKER, John Stewart et al.	
	244	7730123		2010-06-01	ERICKSON, Richard R. et al.	
	245	8024397		2011-09-20	ERICKSON, Richard R. et al.	
	246	8156206		2012-04-10	KILEY, Kevin J. et al.	
	247	8126722		2010-02-28	ROBB, Terence Alan et al.	
	248	8364089		2013-01-29	PHILLIPS, Derek	
	249	6754470		2004-06-22	Hendrickson, Keith et al.	
	250	8122128		2012-02-21	Burke, II, Robert M. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	251	8149823		2012-04-03	Turcan, Diane Brown et al.	
	252	8326359		2012-12-04	Kauffman, Donald C.	
	253	8131256		2012-03-06	MARTTI, Jyrki et al.	
	254	6381316		2002-04-30	JOYCE, Simon James et al.	
	255	7965983		2011-06-21	SWAN, Tim et al.	
	256	8284740		2012-10-09	O'CONNOR, Dennis M.	
	257	8116223		2012-02-14	TIAN, Dan et al.	
	258	6154738		2000-11-28	CALL, Charles Gainor	
	259	8423016		2013-04-16	BUCKLEY, Adrian et al.	
	260	8306518		2012-11-06	GAILLOUX, Michael A.	
	261	8422988		2013-04-16	KESHAV, Srinivasan	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	262	6035281		2000-03-07	Crosskey, James P. et al.	
	263	6996393		2006-02-07	Pyhalammi, Seppo et al.	
	264	7760711		2010-07-20	Kung, Fen-Chung et al.	
	265	8000318		2011-08-16	Wiley, William L. et al.	
	266	8098579		2012-01-17	Ray, Amar N. et al.	
	267	8155670		2012-04-10	Fullam, Scott et al.	
	268	8374090		2013-02-12	Morrill, Robert J. et al.	
	269	7457265		2008-11-25	Julka, Vibhor et al.	
	270	7729326		2010-06-01	Sekhar, Ramesh	
	271	7929973		2011-04-19	Zavalkovsky, Arthur et al.	
	272	7945945		2011-05-17	Graham, Richard et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	273	8059530		2011-11-15	Cole, Terry L.	
	274	8266681		2012-09-11	Deshpande, Sumit B. et al.	
	275	8280354		2012-10-02	Smith, Christopher et al.	
	276	8331293		2012-12-11	Sood, Kapil	
	277	8019820		2011-09-13	Son, Giyeong et al.	
	278	8191116		2012-05-29	Gazzard, Daryl	
	279	6292828		2001-09-18	Williams, David L.	
	280	7043226		2006-05-09	Yamauchi, Toshiaki	
	281	7472189		2008-12-30	Mallya, Arvind R. et al.	
	282	7944948		2011-05-17	Chow, Albert T. et al.	
	283	7802724		2010-09-28	Nohr, Steven Paul	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	284	8155155		2012-04-10	Chow, Albert T. et al.	
	285	8447324		2013-05-21	Shuman, Mohammed Ataur et al.	
	286	8005009		2011-08-23	McKee, Neil et al.	
	287	7760861		2010-07-20	Croak, Marian et al.	
	288	8060463		2011-11-15	Spiegel, Joel R.	
	289	8224773		2012-07-17	Spiegel, Joel R.	
	290	8352980		2013-01-08	Howcroft, Jerald Robert	
	291	8386386		2013-02-26	Zhu, Kevin	
	292	8347362		2013-01-01	Cai, Yigang et al.	
	293	8340718		2012-12-25	Colonna, Massimo et al.	
	294	8385896		2013-02-26	Proctor Jr., James A. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	295	8320949		2012-11-27	Matta, Sudheer Poorna Chandra	
	296	8279864		2012-10-02	Wood, Daniel M.	
	297	8271045		2012-09-18	Parolkar, Satish et al.	
	298	8233883		2012-07-31	De Froment, Eric	
	299	8224382		2012-07-17	Bultman, Michael J.	
	300	8184590		2012-05-22	Rosenblatt, Ariel	

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

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

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

FOREIGN PATENT DOCUMENTS Remove

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

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

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

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	3rd Generation Partnership Project, "Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) Enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) Access," Release 8, Document No. 3GPP TS 23.401, V8.4.0, December 2008	☐
	2	3rd Generation Partnership Project, "Technical Specification Group Services and System Aspects; Policy and Charging Control Architecture," Release 8, Document No. 3GPP TS 23.203, V8.4.0, December 2008	☐
	3	ALONISTIOTI et al., "Intelligent Architectures Enabling Flexible Service Provision and Adaptability," 2002	☐
	4	Amazon Technologies, Inc., "Kindle™ User's Guide," 3rd Edition, Copyright 2004-2009	☐
	5	CHANDRASEKHAR et al., "Femtocell Networks: A Survey," June 28, 2008	☐
	6	CHAOUCHI et al., "Policy Based Networking in the Integration Effort of 4G Networks and Services," 2004 IEEE	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	18	LI, Yu, "Dedicated E-Reading Device: The State of the Art and The Challenges," Scroll, Vol. 1, No. 1, 2008	☐
	19	NILSSON et al., "A Novel MAC Scheme for Solving the QoS Parameter Adjustment Problem in IEEE802.11e EDCA," February 2006	☐
	20	OPPLIGER, Rolf, "Internet Security: Firewalls and Bey," Communications of the ACM, May 1997, Vol. 40. No. 5	☐
	21	RAO et al., "Evolution of Mobile Location-Based Services," Communication of the ACM, December 2003	☐
	22	STEGLICH, Stephan, "I-Centric User Interaction," November 21, 2003	☐
	23	VAN EIJK, et al., "GigaMobile, Agent Technology for Designing Personalized Mobile Service Brokerage," July 1, 2002	☐
	24	ZHU et al., "A Survey of Quality of Service in IEEE 802.11 Networks," IEEE Wireless Communications, August 2004	☐
	25	ANTON, B. et al., "Best Current Practices for Wireless Internet Service Provider (WISP) Roaming"; Release Date February 2003, Version 1.0; Wi-Fi Alliance – Wireless ISP Roaming (WISPr)	☐
	26	Ruckus Wireless – White Paper; "Smarter Wi-Fi for Mobile Operator Infrastructures" 2010	☐
	27	Accuris Networks, "The Business Value of Mobile Data Offload – a White Paper", 2010	☐
	28	Wireless Broadband Alliance, "WISPr 2.0, 08 April, 2010"; Doc. Ref. No.: WBA/RM/WISPr, Version 01.00	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	29	THURSTON, Richard, "WISPr 2.0 Boosts Roaming Between 3G and Wi-Fi"; June 23, 2010; Web page from zdnet.com; Zdnet.com/wispr-2-0-boosts-roaming-between-3g-and-wi-fi-3040089325/	☐
	30	Wi-Fi Alliance Technical Committee Hotspot 2.0 Technical Task Group, "Hotspot 2.0 (Release 1) Technical Specification – Version 1.0.0"; 2012	☐
	31	Wi-Fi Alliance Hotspot 2.0 Technical Task Group, "Wi-Fi Certified Passpoint™ (Release 1) Deployment Guidelines – Version 1.0 – October 2012"	☐

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

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

CERTIFICATION STATEMENT

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

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

OR

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

☐ See attached certification statement.

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

☐ A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/Krista S. Jacobsen/	Date (YYYY-MM-DD)	2013-11-25
Name/Print	Krista S. Jacobsen	Registration Number	59374

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

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

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

Application Number	14082040
Filing Date	2013-11-15
First Named Inventor	Raleigh
Art Unit	2447
Examiner Name	not yet assigned
Attorney Docket Number	RALEP032C1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	8174970		2012-05-08	Adamczyk, Maria et al.	
	2	8165576		2012-04-24	Raju, Vishwanath et al.	
	3	8073721		2011-12-06	Lewis, Lundy	
	4	8032899		2011-10-04	Archer, Charles J. et al.	
	5	7974624		2011-07-05	Gallagher, Michael D. et al.	
	6	7907970		2011-03-15	Park, Vincent D. et al.	
	7	7778176		2010-08-17	Morford, Michael Robert	
	8	7725570		2010-05-25	Lewis, Lundy	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	9	7634388		2009-12-15	Archer, Charles J. et al.	
	10	7633438		2009-12-15	Tysowski, Piotr Konrad	
	11	7593417		2009-09-22	Wang, James et al.	
	12	7551922		2009-06-23	Roskowski, Steve et al.	
	13	7545782		2009-06-09	Rayment, Stephen G. et al.	
	14	7039037		2006-05-02	Wang, Jiwei R. et al.	
	15	6928280		2005-08-09	Xanthos, James et al.	
	16	6765925		2004-07-20	Sawyer, Wilson et al.	
	17	5889477		1999-03-30	Fastenrath, Ulrich	
	18	8332517		2012-12-11	Russell, Jesse E.	
	19	8315718		2012-11-20	Caffrey, Paul Oliver et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	20	8447980		2013-05-21	Godfrey, James A. et al.	
	21	8429403		2013-04-23	Moret, Eric et al.	
	22	8411587		2013-04-02	Curtis, William et al.	
	23	8396929		2013-03-12	Helfman, Nadav et al.	
	24	8363658		2013-01-29	Delker, Jason R. et al.	
	25	8265004		2012-09-11	Toutonghi, Michael J.	
	26	8233895		2012-07-31	Tysowski, Piotr Konrad	
	27	7685254		2010-03-23	Pandya, Ashish A.	
	28	7181017		2007-02-20	Nagel, Robert H. et al.	
	29	6965872		2005-11-15	Grdina, Jerome M.	
	30	8406427		2013-03-26	Chand, Naresh et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	31	8429409		2013-04-23	Wall, Jonathan et al.	
	32	8402540		2013-03-19	Kapoor, Harsh et al.	
	33	8135657		2013-03-13	Kapoor, Harsh et al.	
	34	8271992		2012-09-18	Chatley, Scott P. et al.	
	35	8315999		2012-11-20	Chatley, Scott P. et al.	
	36	8332375		2012-12-11	Chatley, Scott P. et al.	
	37	8468337		2013-06-18	Gaur, Santosh P. et al.	
	38	8477778		2013-07-02	Lehmann Jr., L. Curtis et al.	
	39	8352630		2013-01-08	Hart, Justin Scott	
	40	6640097		2003-10-28	Corrigan, Louis et al.	
	41	7039713		2006-05-02	Van Gunter, David et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	42	5915008		1999-06-22	Dulman, Scott	
	43	8126476		2012-02-28	Vardi, Yosef et al.	
	44	8000276		2011-08-16	Scherzer, Shimon et al.	
	45	8358638		2013-01-22	Scherzer, Tamir et al.	
	46	8356336		2013-01-15	Johnston, Keith et al.	
	47	8307067		2012-11-06	Ryan, Nicholas M.	
	48	7286848		2007-10-23	Vireday, Richard P. et al.	
	49	7313237		2007-12-25	Bahl, Paramvir et al.	
	50	7444669		2008-10-28	Bahl, Paramvir et al.	
	51	7548976		2009-06-16	Bahl, Paramvir et al.	
	52	8027339		2011-09-27	Short, Joel E. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	53	8095112		2012-01-10	Chow, Richard et al.	
	54	8369274		2013-02-05	Sawai, Ryo	
	55	7881697		2011-02-01	Baker, Matthew Donald et al.	
	56	7899438		2011-03-01	Baker, Matthew Donald et al.	
	57	7945238		2011-05-17	Baker, Matthew Donald et al.	
	58	8078140		2011-12-13	Baker, Matthew Donald et al.	
	59	8285249		2012-10-09	Baker, Matthew Donald et al.	
	60	7493659		2009-02-17	Wu, Handong et al.	
	61	7801985		2010-09-21	Pitkow, Jim et al.	
	62	8242959		2012-08-14	Mia, Rashidus S. et al.	
	63	8326319		2012-12-04	Davis, Richard W.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	64	8019886		2011-09-13	Harrang, Jeffrey Paul et al.	
	65	7102620		2006-09-05	Harries, Andrew Stanely Guy et al.	
	66	7139569		2006-11-21	Kato, Akira	
	67	7529204		2009-05-05	Bourlas, Yair et al.	
	68	7720960		2010-05-18	Pruss, Richard Manfred et al.	
	69	7969950		2011-06-28	Iyer, Pradeep J. et al.	
	70	8032409		2011-10-04	Mikurak, Michael G.	
	71	8045973		2011-10-25	Chambers, Michael D.	
	72	8116781		2012-02-14	Chen, Xixian et al.	
	73	8126396		2012-02-28	Bennett, James D.	
	74	8351898		2013-01-08	Raleigh, Gregory G.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	75	5630159		1997-05-13	Zancho, William F.	
	76	5633484		1997-05-27	Zancho, William F. et al.	
	77	5814798		1998-09-29	Zancho, William F.	
	78	7039403		2006-05-02	Wong, Gregory A.	
	79	7583964		2009-09-01	Wong, Gregory A.	
	80	7593730		2009-09-22	Khandelwal, Deepak et al.	
	81	7948953		2011-05-24	Melkote, Keerti G. et al.	
	82	8200509		2012-06-12	Kenedy, Andrew Alexander et al.	
	83	8270972		2012-09-18	Otting, Marcia J. et al.	
	84	7929959		2011-04-19	DeAtley, Dallas et al.	
	85	7478420		2009-01-13	Wright, Michael et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	86	7502672		2009-03-10	Kolls, H. Brock	
	87	7756757		2010-07-13	Oakes III, Charles Lee	
	88	7930446		2011-04-19	Kesselman, Alex et al.	
	89	8078163		2011-12-13	Lemond, Eric et al.	
	90	8068829		2011-11-29	Lemond, Eric et al.	
	91	8086497		2011-12-27	Oakes III, Charles Lee	
	92	8166040		2012-04-24	Brindisi, Richard G. et al.	
	93	6934249		2005-08-23	Bertin, Olivier et al.	
	94	7774456		2010-08-10	Lownsbrough, Derek Leigh et al.	
	95	8447607		2013-05-21	Weider, Chris et al.	
	96	8504729		2013-08-06	Pezzutti, David A.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	97	8495227		2013-07-23	Kaminsky, David L. et al.	
	98	8472371		2013-06-25	Bari, Farooq et al.	
	99	8134954		2012-03-13	Godfrey, James A. et al.	
	100	7535880		2009-05-19	Hinman, Brian L. et al.	
	101	7499438		2009-03-03	Hinman, Brian L. et al.	
	102	7496652		2009-02-24	Pezzutti, David	
	103	6957067		2005-10-18	Iyer, Pradeep J. et al.	
	104	6654814		2003-11-25	Britton, Kathryn H. et al.	
	105	8374592		2013-02-12	Proctor, Jr. James A. et al.	
	106	8325638		2012-12-04	Jin, Haipeng et al.	
	107	8116749		2012-02-14	Proctor Jr., James Arthur et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	108	8090616		2012-01-03	Proctor Jr., James Arthur et al.	
	109	8090359		2012-01-03	Proctor Jr., James Arthur et al.	
	110	8150431		2012-04-03	Wolovitz, Lionel et al.	
	111	8483135		2013-07-09	Cai, Yigang et al.	
	112	6104700		2000-08-15	Haddock, Stephen R. et al.	
	113	8185127		2012-05-22	Cai, Zheng et al.	
	114	8521110		2013-08-27	Rofougaran, Ahmadreza	
	115	7310424		2007-12-18	Gehring, Stephan Walter et al.	
	116	7356011		2008-04-08	Waters, Christopher J.F. et al.	
	117	7546460		2009-06-09	Maes, Stephane H.	
	118	7921463		2011-04-05	Sood, Kapil et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	119	7940751		2011-05-10	Hansen, Christopher J.	
	120	8122249		2012-02-21	Falk, Rainer et al.	
	121	8495360		2013-07-23	Falk, Rainer et al.	
	122	8520589		2013-08-27	Bhatt, Yogesh et al.	
	123	6542992		2003-04-01	Peirce, Kenneth L. et al.	
	124	8379847		2013-02-19	Bell, Robert H. et al.	
	125	8185093		2012-05-22	Jheng, Yu-Syuan et al.	
	126	8296404		2012-10-23	McDysan, Dave et al.	
	127	8195163		2012-06-05	Gisby, Doug et al.	
	128	8437734		2013-05-07	Ray, Amar N. et al.	
	129	8280351		2012-10-02	Ahmed, Shahid et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	130	7460837		2008-12-02	Diener, Neil R.	
	131	7653394		2010-01-26	McMillin, Brian K.	
	132	8130793		2012-03-06	Edwards, Stephen K. et al.	
	133	8509082		2013-08-13	Heinz, John M. et al.	
	134	8526329		2013-09-03	Mahany, Ronald L. et al.	
	135	5983270		1999-11-09	Abraham, Dalen M. et al.	
	136	6598034		2003-07-22	Kloth, Axel K.	
	137	7032072		2006-04-18	Quinn, Michael J. et al.	
	138	7580356		2009-08-25	Mishra, Sanjeev K. et al.	
	139	7742406		2010-06-22	Muppala, Suresh	
	140	7953877		2011-05-31	Vemula, Narendra et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	141	7957381		2011-06-07	Clermidy, Fabien et al.	
	142	8031601		2011-10-04	Feroz, Azeem et al.	
	143	8255534		2012-08-28	Assadzadeh, Alireza	
	144	8489720		2013-06-16	Morford, Michael Robert et al.	
	145	7774323		2010-08-10	Helfman, Nadav	
	146	7043268		2006-05-09	Yukie, Satoru et al.	
	147	8391262		2013-03-05	Maki, Lasse et al.	
	148	7113780		2006-09-26	McKenna, Daniel Bernard et al.	
	149	8166554		2012-04-24	John, Pramod	
	150	7697540		2010-04-13	Haddad, Reda et al.	
	151	6748195		2004-06-08	Phillips, W. Garland	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	152	8583499		2013-11-12	De Judicibus, Dario et al.	
	153	8352360		2013-01-08	De Judicibus, Dario et al.	
	154	8463232		2013-06-11	Tuli, Amol et al.	
	155	7958029		2011-06-07	Bobich, Thomas et al.	
	156	7540408		2009-06-02	Levine, Judah Joseph et al.	
	157	7826427		2010-11-02	Sood, Kapil et al.	
	158	8185088		2012-05-22	Klein, Robert S. et al.	
	159	8548428		2013-10-01	Raleigh, Gregory G.	
	160	8483694		2013-07-09	Lewis, Allan D. et al.	
	161	8351592		2013-01-08	Freeny, Jr., Charles C. et al.	
	162	8452858		2013-05-28	Wu, John et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	163	7610396		2009-10-27	Taglienti, Claudio et al.	
	164	7984511		2011-07-19	Kocher, Paul Carl et al.	
	165	7987510		2011-07-26	Kocher, Paul C. et al.	
	166	8571993		2013-10-29	Kocher, Paul C. et al.	
	167	8543265		2013-09-24	Ekhaguere, David E. et al.	
	168	8385975		2013-02-26	Forutanpour, Babak	
	169	6873988		2005-03-29	Hermann, Conrad K. et al.	
	170	7013469		2006-03-14	Smith, Adam W. et al.	
	171	7203169		2007-04-10	Okholm, Jon Eric et al.	
	172	7286834		2007-10-23	Walter, Edward	
	173	7555757		2009-06-30	Smith, Adam W. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	174	7574509		2009-08-11	Nixon, Mark J. et al.	
	175	7826607		2010-11-02	de Carvalho Resende, Mauricio Guilherme et al.	
	176	7940685		2011-05-10	Breslau, Lee Michel et al.	
	177	8196199		2012-06-05	Hrastar, Scott E. et al.	
	178	8204505		2012-06-19	Jin, Haipeng et al.	
	179	8228818		2012-07-24	Chase, Christopher J. et al.	
	180	8320244		2012-11-27	Muqattash, Alaa et al.	
	181	8411691		2013-04-02	Aggarwal, Rahul	
	182	8461958		2013-06-11	Saenz, Jorge E. et al.	
	183	8484327		2013-07-09	Werner, Eran et al.	
	184	8522039		2013-08-27	Hyndman, Arn et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	185	8544105		2013-09-24	Mclean, Ivan H. et al.	
	186	8571474		2013-10-29	Chavez, Timothy R. et al.	
	187	8194572		2012-06-05	Horvath, Robert et al.	
	188	8516552		2013-08-20	Raleigh, Gregory G.	
	189	8441955		2013-05-14	Wilkinson, Robert Todd et al.	

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

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

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	1538730A	CN		2004-10-20	Zhongxing Communication Co., Ltd.		☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

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

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

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5
	1	VerizonWireless.com news, "Verizon Wireless Adds to Portfolio of Cosumer-Friendly Tools With Introduction of Usage Controls, Usage Controls and Chaperone 2.0 Offer Parents Full Family Security Solution," August 18, 2008	☐
	2	"The Construction of Intelligent Residential District in Use of Cable Television Network," Shandong Science, Vol. 13, No. 2, June 2000	☐

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

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

CERTIFICATION STATEMENT

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

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

OR

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

☐ See attached certification statement.

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

☐ A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/Krista S. Jacobsen/	Date (YYYY-MM-DD)	2013-11-25
Name/Print	Krista S. Jacobsen	Registration Number	59374

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

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

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

Application Number	14082040
Filing Date	2013-11-15
First Named Inventor	Raleigh
Art Unit	2447
Examiner Name	not yet assigned
Attorney Docket Number	RALEP032C1

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

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	204	20080005285		2008-01-03	ROBINSON, James David et al.	
	205	20090315735		2009-12-24	BHAVANI, Neeraj S. et al.	
	206	20090219170		2009-09-03	CLARK, Ryan C. et al.	
	207	20090067372		2009-03-12	SHAH, Keyur C. et al.	
	208	20080262798		2008-10-23	KIM, Eun Ah et al.	
	209	20100103820		2010-04-29	FULLER, Randy et al.	
	210	20100153781		2010-06-17	HANNA, Stephen R.	
	211	20120029718		2012-02-02	DAVIS, Edward L.	
	212	20110241624		2011-10-06	PARK, Jun-seok et al.	
	213	20090307746		2009-12-10	DI, Jinwen et al.	
	214	20050009499		2005-01-13	KOSTER, Karl	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	215	20010053694		2001-12-20	IGARASHI, Yoichiro et al.	
	216	20100041364		2010-02-18	LOTT, Robert Wayne et al.	
	217	20100027469		2010-02-04	GURAJALA, Ravindra Babu et al.	
	218	20090299857		2009-12-03	BRUBAKER, Curtis M.	
	219	20080051076		2008-02-28	O'Shaughnessy, John et al.	
	220	20080313730		2008-12-18	Iftimie, Sorin et al.	
	221	20110173678		2011-07-14	KAIPPALLIMALIL, John et al.	
	222	20080235511		2008-09-25	O'BRIEN, William G. et al.	
	223	20080240373		2008-10-02	WILHELM, Robert D.	
	224	20100027559		2010-02-04	LIN, Hung-Ming et al.	
	225	20020116338		2002-08-22	GONTHIER, Jean-Charles et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	226	20070061878		2007-03-15	HAGIU, Costin et al. et al.	
	227	20100020822		2010-01-28	ZERILLO, Anthony J. et al.	
	228	20040203755		2004-10-14	BRUNET, Jeffrey et al.	
	229	20090172077		2009-07-02	ROXBURGH, David et al.	
	230	20080120668		2008-05-22	Yau, Frank Chuen-Foo	
	231	20030171112		2003-09-11	Lupper, Alfred et al.	
	232	20070300252		2007-12-27	Acharya, Swarup et al.	
	233	20050007993		2005-01-13	Chambers, Mahdi et al.	
	234	20020164983		2002-11-07	Raviv, Li-On et al.	
	235	20070280453		2007-12-06	Kelley, Sean S.	
	236	20100241544		2010-09-23	Benson, Dan et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	237	20090157792		2009-06-18	Fiatal, Trevor	
	238	20070109983		2007-05-17	Shankar, Rohit et al.	
	239	20020049074		2002-04-25	Eisinger, Bernd et al.	
	240	20020161601		2002-10-31	Nauer, Bernhard et al.	
	241	20040132427		2004-07-08	Lee, Wan-Yeon et al.	
	242	20060068796		2006-03-30	Millen, Stephanie L. et al.	
	243	20010048738		2001-12-06	Baniak, Paul G. et al.	
	244	20070033197		2007-02-08	Scherzer, Shimon et al.	
	245	20110013569		2011-01-20	Scherzer, Shimon et al.	
	246	20110159818		2011-06-30	Scherzer, Shimon et al.	
	247	20120020296		2012-01-26	Scherzer, Shimon et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	248	20120196644		2012-08-02	Scherzer, Shimon et al.	
	249	20120238287		2012-09-20	Scherzer, Shimon	
	250	20130058274		2013-03-07	Scherzer, Shimon et al.	
	251	20130084835		2013-04-04	Scherzer, Shimon et al.	
	252	20090005000		2009-01-01	Baker, Matthew et al.	
	253	20090006116		2009-01-01	Baker, Matthew et al.	
	254	20090006200		2009-01-01	Baker, Matthew et al.	
	255	20110081881		2011-04-07	Baker, Matthew Donald et al.	
	256	20110082790		2011-04-07	Baker, Matthew Donald et al.	
	257	20130029653		2013-01-31	Baker, Matthew Donald et al.	
	258	20130065555		2013-03-14	Baker, Matthew Donald et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	259	20120155296		2012-06-21	Kashanian, Nematolah	
	260	20120330792		2012-12-27	Kashanian, Nematolah	
	261	20130030960		2013-01-31	Kashanian, Nematolah	
	262	20130095787		2013-04-18	Kashanian, Nematolah	
	263	20130117140		2013-05-09	Kashanian, Nematolah	
	264	20130183937		2013-07-18	Neal, Daniel John et al.	
	265	20060135144		2006-06-22	Jothipragasam, Premkumar	
	266	20080089295		2008-04-17	Keeler, James D. et al.	
	267	20080022354		2008-01-24	Grewal, Karanvir et al.	
	268	20040102182		2004-05-27	Reith, Lothar et al.	
	269	20030233332		2003-12-18	Keeler, James D. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	270	20080250053		2008-10-09	Aaltonen, Janne et al.	
	271	20110195700		2011-08-11	Kukuchka, Robert et al.	
	272	20070155365		2007-07-05	Kim, Sung-Jun et al.	
	273	20130144789		2013-06-06	Aaltonen, Janne et al.	
	274	20100131584		2010-05-27	Johnson, William J.	
	275	20100080202		2010-04-01	Hanson, Mark	
	276	20070147324		2007-06-28	McGary, Faith	
	277	20130024914		2013-01-24	Ahmed, Shahid et al.	
	278	20130103376		2013-04-25	Gaddam, Venkat et al.	
	279	20130111572		2013-05-02	Gaddam, Venkat et al.	
	280	20130117382		2013-05-09	Gaddam, Venkat et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	281	20130149994		2013-06-13	Gaddam, Venkat et al.	
	282	20070168499		2007-07-19	Chu, Jing-Long	
	283	20070025301		2007-02-01	Petersson, Justus et al.	
	284	20070140145		2007-06-21	Kumar, Surender et al.	
	285	20080120129		2008-05-22	Seubert, Michael et al.	
	286	20060174035		2006-08-03	Tufail, Mudassir	
	287	20110264923		2011-10-27	Kocher, Paul C. et al.	

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

FOREIGN PATENT DOCUMENTS Remove

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

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

NON-PATENT LITERATURE DOCUMENTS Remove

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		☐

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

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

CERTIFICATION STATEMENT

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

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

OR

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

☐ See attached certification statement.

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

☐ A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/Krista S. Jacobsen/	Date (YYYY-MM-DD)	2013-11-25
Name/Print	Krista S. Jacobsen	Registration Number	59374

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Examiner:
Gregory G. Raleigh et al.	Not yet assigned
Serial No. 14/082,040	Art Unit: 2447
Filed: Nov. 15, 2013	Conf. No.: 1015

Title: Device-Assisted Services for Protecting Network Capacity

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

INFORMATION DISCLOSURE STATEMENT

Madam:

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

In accordance with 37 CFR §1.98(d), copies of the references can be found in related U.S. Patent Application No. 13/134,028 filed May 25, 2011.

It is respectfully requested that the cited references be expressly considered during the prosecution of this application, and the references be made of record therein and appear among the "references cited" on any patent to issue therefrom.

As provided for by 37 CFR § 1.97(g) and (h), no inference should be made that the information and references cited are prior art merely because they are in this statement and no representation is being made that a search has been conducted or that this statement encompasses all the possible relevant information.

Applicant believes that no fee is required for submission of this statement, but if for any reason an insufficient fee has been paid, please charge the insufficiency to Deposit Account No. **50-5876**.

Respectfully submitted,

Date: November 25, 2013

By: _____

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

CERTIFICATE OF ELECTRONIC TRANSMISSION

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

Date: Nov. 25, 2013 By: _____
Ann Taylor

[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04M 11/06
H04M 15/00 H04M 17/00
H04L 9/32 H04L 12/14

[12] 发明专利申请公开说明书

[21] 申请号 03113227.8

[43] 公开日 2004 年 10 月 20 日

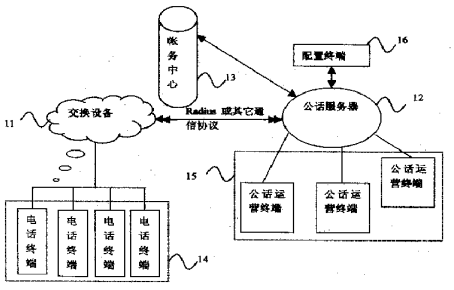
[11] 公开号 CN 1538730A

[22] 申请日 2003.4.15 [21] 申请号 03113227.8
[71] 申请人 中兴通讯股份有限公司
地址 518057 深圳市南山区高新技术产业园科技南路中兴通讯大厦法律部
[72] 发明人 贾廷尧 潘红兵 朱 越
权利要求书 2 页 说明书 5 页 附图 3 页

[54] 发明名称 一种宽带公话系统及其实现方法

[57] 摘要

本发明提供一种宽带公话系统及其实现方法，该系统包括交换设备、公话服务器、帐务中心、公话运营终端和电话终端，其中所述电话终端挂接在所述交换设备上，在所述公话运营终端的数据控制下，与所述公话服务器之间进行通讯；该实现方法包含以下步骤：对用户发起的呼叫进行认证；以及对用户资费结帐。采用本发明提供的宽带公话系统，能够提供具有良好的开放性、易于扩充规模的公话系统，可跨地域运行，很好地适应了现代通信网的高度智能化的要求，降低了投资，易于维护，具有良好的性价比；其实现方法可对多个公话运营点进行集中控制和管理，防止了人为违规资费发生，具有较高的可靠性、安全性，不易被攻击，同时还可达到计费准确度高的效果。



ISSN1008-4274

知识产权出版社出版

1．一种宽带公话系统，该系统包括交换设备、公话服务器、帐务中心、公话运营终端和电话终端，其中电话终端挂接在交换设备上，在公话运营终端的数据控制下，与公话服务器之间进行通讯。

2．如权利要求1所述的宽带公话系统，其中所述交换设备和所述公话服务器之间采用标准的RADIUS协议，或其他等效通信协议。

3．如权利要求 1 所述的宽带公话系统，其中所述公话服务器和所述公话运营终端 15 之间采用标准的 RADIUS 协议，或其他等效通信协议。。

4．如权利要求 1 所述的宽带公话系统，其特征在于所述系统还可采用一个交换设备带多个公话服务器的连接方式。

5．如权利要求 1 所述的宽带公话系统，其特征在于所述系统还采用多个交换设备共用一个公话服务器的连接方式。

6．如权利要求 1 所述的宽带公话系统，对于在网上不具有支持 RADIUS 协议功能的交换设备，可将这些设备接入软交换系统，从而获得支持这些通信协议的能力。

7．一种宽带公话系统实现方法，其特征在于该方法包含以下步骤：

对用户发起的呼叫进行认证；及

对用户资费结帐。

8．如权利要求 7 所述的宽带公话系统实现方法，其特征在于所述对用户发起的呼叫进行认证的步骤，还包括以下步骤：

用户到运营终端申请使用公话业务；

管理员在运营终端指定的所述电话终端，并输入该终端的信用额度；

公话服务器接受运营终端的输入，指定电话终端处于开启状态；

用户使用终端发起呼叫；

交换设备向公话服务器进行该终端信用认证；

若认证不能通过，则终端话机被置于闭锁状态，用户不能使用业务；

若认证通过，则公话服务器向交换设备传递信用额度；

用户开始使用该终端，进行呼叫业务；

如果用户结束业务使用，或信用额度不足，则业务结束。

9．如权利要求 7 所述的宽带公话系统实现方法，其特征在于所述对用户发起的呼叫进行认证的步骤，还包括以下步骤：

授权认证业务结束后，交换设备向公话服务器发出业务结束指示；

公话服务器向帐务中心(或独立的计费服务器)传递详细通话记录；

公话服务器从帐务中心(或独立的计费服务器)获得该此通话的费用帐单；

公话服务器将此帐单传递给指定的公话运营终端；

公话运营终端向用户输出通话帐单，整个公话系统业务结束。

一种宽带公话系统及其实现方法

技术领域

本发明涉及电信网络运营系统，特别是涉及该系统中的有人值守宽带公话系统及其实现方法。

背景技术

在现代电信固话运营业务中，公用电话（以下简称公话）系统是运营商获得利润的一个重要手段。特别是随着目前 IP 电话的广泛使用，宽带公话运营已是运营商重要的利润增长点，通过提供这种立即付费的公话业务，可以为广大用户提供方便。

现有技术的公话系统大致可分为无人值守和有人值守两种模式：其中对于无人值守公话系统，常见的为磁卡、IC 卡电话；而有人值守公话系统，常见的为电信营业厅或者写字楼的商务中心中使用的公用电话系统，对于有人值守公话系统，其主要的功能为：

1. 由控制终端设备发起呼叫，防止未授权用户使用业务；

2. 用户使用终端通话结束后输出通话费用.运营商获得收入.

本发明正是针对有人值守公话系统，而提出的一种新的公话系统及其实现方法。

目前的宽带公话系统的实现一般独立于交换系统，只是在交换终端对终端设备予以计量控制，一般采用以下几种模式：

1. 使用公话计费器来提供服务

只需配置计费器，将话机和计费器连接即可，由计费器对话机进行控制，并在通话结束后显示通话费用。 这种模式的实现较为简单，但存在着计费精度低，易引发用户话费纠纷等缺点，特别是如遇资费调整则存在着巨大的数据配置工作量，平时也具有较大的维护工作量；

2. 使用公话计费服务器

增加硬件设备，将若干用户线进行转接集成，（或在环路中继上进行控制，）由服务器对终端设备进行控制，采用内置计费服务器的办法，因此可能于帐务中心的帐单输出有差异，并且同样存在着计费精度低的缺点；

3. 使用小交换系统完成

在需要配置为公话的终端话机上接入小交换设备，从而使其接入交换网，在

小交换设备上对话机终端控制，利用小交换设备的计费系统完成资费计算。这和第二种实现方式本质相同，存在计费精度底、投资成本高的缺点。

并且，当运营商需要设置多个营业点时，利用现有的以上这些系统，需要相应的投资多套软硬件设备，因此其成本较高，维护工作量较大。

并且这些实现方式，普遍存在以下缺点：

1. 智能化较低，不能高效进行集中管理；
2. 在资费政策变化时，数据修改工作量巨大；
3. 内部接口不具有很好的开放性；
4. 由于计算电话费用的设备一般配置较低，无法获得精确计费；
5. 在运营规模扩大时需要投入多套设备，投资成本高，维护工作量大；
6. 系统运营受地域限制，一套系统一般集中在一个城市的一个地域，不能跨地域城市运营。

经检索，“ 深圳市冠日高科技发展有限公司”申请获得了“公用电话网的构成及其实现方法”专利，其核心内容是建立独立的公话交换系统，并对其予以公话网管，接入到运营电信网上，其思想内容类似于上述第三种实现方式，该发明需要建立独立的公话交换网，不能充分利用网上的现有设备，同时， 需要建立独立的计费模块，不能从已有的帐务中心获取计费信息，存在着投资大、实际建设困难的弱点。

上述现有的公话系统的实现都是基于运营的交换系统，其具有相对的封闭性，和第三方设备不具有开放的通信能力，因此第三方设备无法控制交换设备的动作，不便于直接从交换设备采集话单. 因此其实现基于对交换终端附以另外的设备，或加以计价设备，或建立另外的交换设备从而达到控制终端话机，采集话单的目的.

随着电信网的演变，宽带交换系统（例如软交换系统）已经推向市场，这种系统以 IP 协议为基石，其系统具有良好的开放性和扩充性，也为新的公话系统的实现提供了基础。

本发明正是在现代交换网络（特别使软交换网络）的智能化程度越来越高的情况下，充分运用电信网上的已有资源，使得交换设备和第三方设备更易于进行信息交流，保护运营商的已有投资；采用灵活的框架结构,实现公话系统。

发明内容

本发明的目的是针对上述背景技术中存在的缺陷，提供一种宽带公话系统及其实现方法，即在公话服务器的控制下，利用交换设备完成对电话终端的控制，实现通话，并由公话服务器提供费用帐单，由公话运营终端来完成和用户的界面交互。

为了达到上述目的，本发明提供一种宽带公话系统，该系统包括交换设备、公话服务器、帐务中心、信令处理模块，公话运营终端和电话终端，其中所述电话终端挂接在所述交换设备上，在所述公话运营终端的数据控制下，与所述公话服务器之间进行通讯。

本发明还提供一种宽带公话系统实现方法，其特征在于该方法包含以下步骤：

对用户发起的呼叫进行认证，；

对用户资费结帐。

采用本发明提供的宽带公话系统，能够提供具有良好的开放性、易于扩充规模的公话系统，可跨地域运行，很好地适应了现代通信网的高度智能化的要求，降低运营商投资，且该系统易于操作维护，具有良好的性价比；其实现方法可对多个公话运营点进行集中控制和管理，防止了人为违规资费发生，具有较高的可靠性、安全性，不易被攻击，同时还可达到计费准确度高的效果。

下面将结合实施例并参照附图对该发明的技术方案进行详细说明。

附图说明

图 1 为本发明的系统结构图。

图 2 为本发明的实现方法流程图。

图 3 为本发明系统结构扩充形态图一。

图 4 为本发明系统结构扩充形态图二。

具体实施方式

如图 1 所示，为本发明系统结构图，也是本发明系统结构的基本形态，它由一个公话服务器接入一个交换设备，带有多个运营终端，系统规模可以为某一城市地域，，可为跨地域模式，即系统不受地域限制，该系统由以下几部分组成：交换设备 11，它是电话业务的提供者，主要用于实现电话业务，在实际应用中一般是指运营商网上运营的交换设备，具有支持鉴权认证通信协议的能力；公话服务器 12，用于控制并完成话机终端的认证、授权操作，通过帐务中心（或计费服务器）13 完成通话资费，并将帐单传递给公话运营终端；在公话服务器 12 上，可通过配置终端 16 配置不同的策略服务，以便对由不同运营终端控制的话机终端提供不同的控制方式，实现个性化的服务（例如指定有的用户可先打电话后付费；有的需要交付押金后才可打电话；有的可以进行通话累计优惠活动）；公话运营终端 15，它是运营商的业务使用界面，用于指定话机的开放/闭锁状态、

录入指定终端的信用额度、配合公话服务器完成终端话机的认证，实现授权操作，以及在通话输出后,从公话服务器获得通话帐单，完成电信运营收入；电话终端14，它是用户使用终端，用于完成用户通话，可以是普通的电话机或其他智能终端，它在本发明的系统可以有任意多个；

以上各单元的连接关系是：电话终端14挂接在交换设备11上，在公话运营终端的数据控制下，与公话服务器12之间进行通讯，其中交换设备11和公话服务器之间可采用标准的RADIUS协议（或其他通信协议）；公话服务器12和公话运营终端15之间也采用标准的RADIUS协议（或其他通信协议）。

图2所示为为本发明公话系统的实现方法流程图，该流程的具体步骤包括：首先，对用户发起的呼叫进行认证，以防止未授权的用户使用业务，步骤201；对用户资费结帐，步骤202。

本发明所采用的系统结构除了如图 1 所示的基本形态外，还可以有如图 3和图4所示的两种扩充形态，其中图3所示的扩充形态一，系统可由一个交换设备11带多个公话服务器32组成,这些公话服务器分布在不同地域,以不同的策略提供个性化的服务；图 4 所示的扩充形态二，采用多个交换设备 41 共用一个公话服务器 12 的连接方式，并且此时的交换设备可以为异种交换设备(如交换机、软交换设备等)。

下面试举一具体实例，更进一步说明本发明的技术方案：

在实际应用中，本发明所提到的宽带公话系统，其硬件部分包括帐务中心、交换设备、公话服务器、公话运营终端、电话终端设备，其中帐务中心和交换设备为运营商已有的系统，公话服务器可根据运营规模选用市场上的商用服务器，公话运营终端可为普通的PC机；该系统的实现方法可通过执行以下步骤来完成：

1．在交换设备上指定若干话机为公话话机终端，并指定受控公话服务器地址；

2．在公话服务器的配置终端上，对公话服务器进行配置,将所控制的公话终端，分配到相应的公话运营终端作用域；

3．用户使用公话终端进行通话，需到该终端的公话运营终端进行业务使用申请；

4．公话运营终端受理用户申请，并向服务器报告该终端当前的信用情况；

5．用户摘机发起呼叫，交换设备判断为公话服务，则向指定的公话服务器发起认证请求；

6．公话服务器依据该用户的信用情况，控制认证结果，如果信用不足以发起呼叫,则通知交换设备，闭锁话机；

7．如果该用户有足够的信用，则判断用户可使用业务的时间长度（或字节流量）；

8．当用户主动结束业务，或用户业务使用耗尽其信用额度，则交换设备主动中止业务.此时业务结束；

9.业务结束后,公话服务器向计费中心,或指定的计费服务器索取通话帐单,并安全传递给公话运营终端；

10．运营终端接受帐单和用户结算；

11．运营商可在公话服务器侧对各运营终端进行业务统计，决定各运营点设备的增加或减少。

该系统的软件部分分为：用户认证和资费结账两部分。

其中用户认证步骤具体还包括以下处理内容：（在本过程中可使用 RADIUS 协议，或其他通信协议）

用户到运营终端申请使用公话业务；

管理员在运营终端指定的电话终端，并输入该终端的信用额度；

公话服务器接受运营终端的输入，指定电话终端处于开启状态；

用户使用终端发起呼叫；

交换设备向公话服务器进行该终端信用认证；

认证不能通过则终端话机被置于闭锁状态，用户不能使用业务；

认证通过则公话服务器向交换设备传递信用额度；

用户开始使用该终端，进行呼叫业务；

如果用户结束业务使用，或信用额度不足，则业务结束，至此，认证授权步骤结束。

资费结帐部分：

授权认证业务结束后，交换设备指示公话服务器业务结束；

公话服务器向帐务中心(或独立的计费服务器)传递详细通话记录；

公话服务器从帐务中心(或独立的计费服务器)获得该此通话的费用帐单；

公话服务器将此帐单传递给指定的公话运营终端；

公话运营终端向用户输出通话帐单，整个公话系统业务结束。

很明显本系统要求交换系统能够支持一定的通信协议,比如 RADIUS 协议,以实现和公话服务器的通讯,对于网上不具有此功能的交换设备,运营商可将这些设备接入软交换系统,从而获得支持这些通信协议的能力。

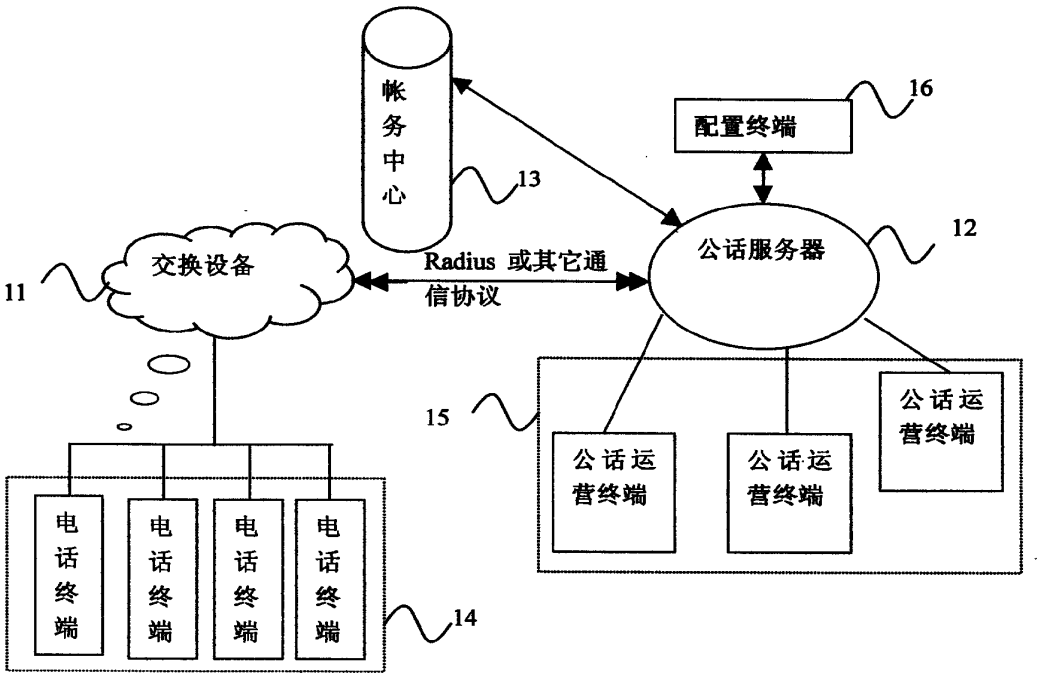

帐务中心
13
配置终端
16
公话服务器
12
交换设备
11
Radius 或其它通信协议
15
公话运营终端
公话运营终端
公话运营终端
电话终端
电话终端
电话终端
电话终端
14

图 1

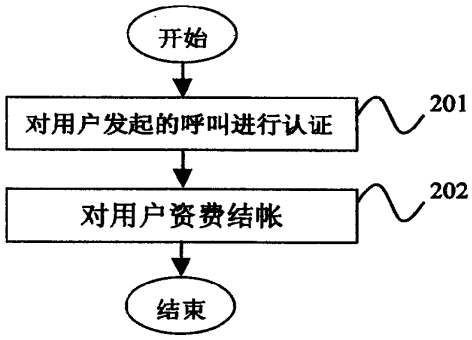

开始
对用户发起的呼叫进行认证
201
对用户资费结帐
202
结束

图 2

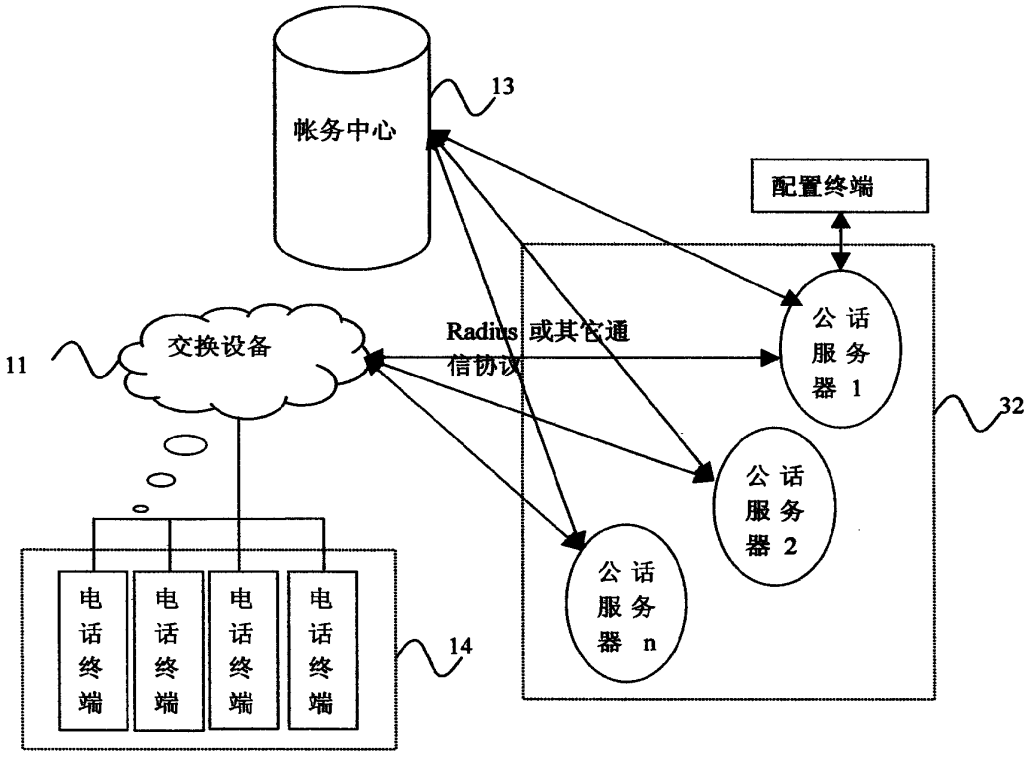

帐务中心
13
配置终端
交换设备
11
Radius 或其它通信协议
公话服务器 1
32
公话服务器 2
公话服务器 n
电话终端
电话终端
电话终端
电话终端
14

图 3

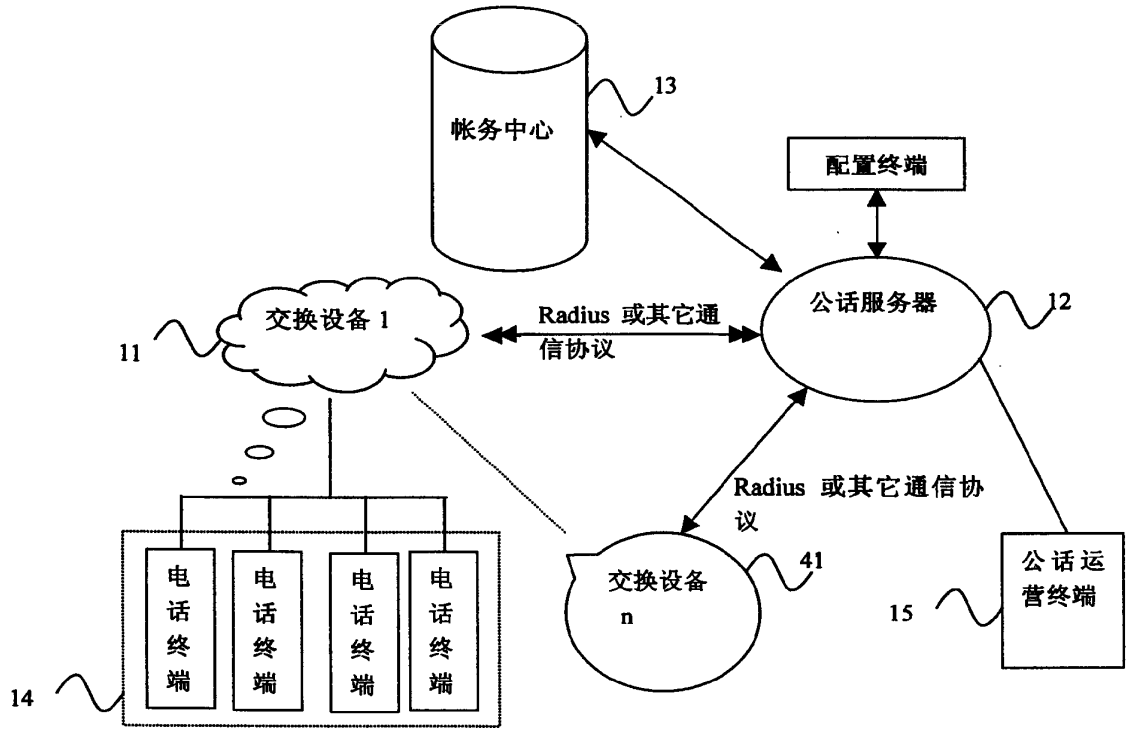

帐务中心
13
配置终端
交换设备 1
11
Radius 或其它通信协议
公话服务器
12
Radius 或其它通信协议
电话终端
电话终端
电话终端
电话终端
14
交换设备 n
41
公话运营终端
15

图 4

(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101115248 B
(45)授权公告日 2010.05.12

(21)申请号 200610107772.0

(22)申请日 2006.07.25

(73)专利权人 联想（北京）有限公司
地址 100085 北京市海淀区上地信息产业基地创业路 6 号

(72)发明人 周阳霖

(74)专利代理机构 北京银龙知识产权代理有限公司 11243
代理人 许静

(51)Int.Cl.
H04W 28/14(2009.01)
H04W 84/12(2009.01)
H04W 88/06(2009.01)

(56)对比文件
CN 1625868 A,2005.06.08, 全文.
WO 2006023108 A2,2006.03.02, 全文.
EP 1662726 A1,2006.05.31, 全文.
CN 1496171 A,2004.05.12, 全文.
CN 1653499 A,2005.08.10, 全文.

审查员 刘宁

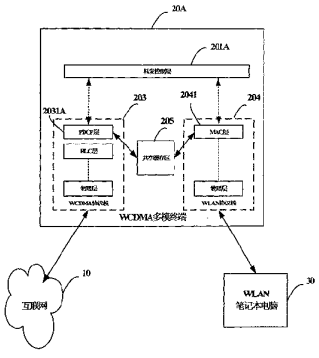
权利要求书 2 页 说明书 7 页 附图 5 页

(54)发明名称

多模终端及其数据转发方法

(57)摘要

本发明公开了一种多模终端及其数据转发方法。本发明的多模终端，具有至少一个移动通信协议栈，至少一个无线局域网协议栈，共享缓存区以及转发控制器。其中，移动通信协议栈用于将从互联网接收到的 IP 数据包存放到共享缓存区后通知转发控制层；转发控制层用于将 IP 数据包在共享缓存区中的存放地址通知无线局域网协议栈；无线局域网协议栈用于从共享缓存区取出 IP 数据包并将其发送到无线设备，移动通信协议栈、转发控制层、无线局域网协议栈中的任何一个将 IP 数据包的目的 IP 地址修改为无线设备在无线局域网连接中的 IP 地址。本发明的多模终端及其数据转发方法可以有效的提高数据传输效率。



CN 101115248 B

1. 一种多模终端，具有至少一个移动通信协议栈，至少一个无线局域网协议栈，以及转发控制层，其特征在于，多模终端进一步包括共享缓存区，其中，

移动通信协议栈用于将从互联网接收到的 IP 数据包存放到共享缓存区后通知转发控制层；

转发控制层用于将 IP 数据包在共享缓存区中的存放地址通知无线局域网协议栈；

无线局域网协议栈用于从共享缓存区取出 IP 数据包并将其发送到无线设备，

移动通信协议栈、转发控制层、无线局域网协议栈中的任何一个将 IP 数据包的目的 IP 地址修改为无线设备在无线局域网连接中的 IP 地址。

2. 根据权利要求 1 所述的多模终端，其特征在于，

无线局域网协议栈，进一步用于将从无线设备接收到的 IP 数据包转送到共享缓存区，并通知所述转发控制层；

转发控制层，进一步用于将从无线设备接收到的 IP 数据包在共享缓存区中的存放地址通知移动通信协议栈；

移动通信协议栈，进一步用于从共享缓存区取出从无线设备接收到的 IP 数据包，将该 IP 数据包发送到互联网，

移动通信协议栈、转发控制层、无线局域网协议栈中的任何一个将 IP 数据包的源地址修改为多模终端在互联网中对应的 IP 地址。

3. 根据权利要求 1 或 2 所述的多模终端，其特征在于，无线局域网协议栈为 WiFi、WiMax、BlueTooth、UWB、Zigbee、RFID 中的一个。

4. 根据权利要求 1 或 2 所述的多模终端，其特征在于，移动通信协议栈为 TD-SCDMA、WCDMA、GSM、CDMA 1x、CDMA2000、GPRS 中的一个。

5. 一种多模式终端的数据转发方法，其特征在于，包括以下步骤：

移动通信协议栈将从互联网接收到的 IP 数据包存放到共享缓存区后通知转发控制层；

转发控制层将 IP 数据包在共享缓存区中的存放地址通知无线局域网协议栈；

无线局域网协议栈从共享缓存区取出 IP 数据包并将其发送到无线设备，

移动通信协议栈、转发控制层、无线局域网协议栈中的任何一个将 IP 数据包的目的 IP 地址修改为无线设备在无线局域网连接中的 IP 地址。

6. 根据权利要求 5 所述的方法，其特征在于，所述方法进一步包括以下步骤：

无线局域网协议栈将从无线设备接收到的 IP 数据包转送到共享缓存区，并通知所述转发控制层；

转发控制层将从无线设备接收到的 IP 数据包在共享缓存区中的存放地址通知移动通信协议栈；

移动通信协议栈从共享缓存区取出从无线设备接收到的 IP 数据包，将该 IP 数据包发送到互联网，

移动通信协议栈、转发控制层、无线局域网协议栈中的任何一个将 IP 数据包的源地址修改为多模终端在互联网中对应的 IP 地址。

7. 根据权利要求 5 或 6 所述的方法，其特征在于，无线局域网协议栈为 WiFi、WiMax、BlueTooth、UWB、Zigbee、RFID 中的一个。

8. 根据权利要求 5 或 6 所述的方法，其特征在于，移动通信协议栈为 TD-SCDMA、WCDMA、GSM、CDMA 1x、CDMA2000、GPRS 中的一个。

9. 一种多模终端，具有至少一个移动通信协议栈，至少一个无线局域网协议栈，以及转发控制层，其特征在于，多模终端进一步包括共享缓存区，其中，

无线局域网协议栈用于将从无线设备接收到的 IP 数据包转送到共享缓存区，并通知转发控制层；

转发控制层用于将从无线设备接收到的 IP 数据包在共享缓存区中的存放地址通知移动通信协议栈；

移动通信协议栈用于从共享缓存区取出从无线设备接收到的 IP 数据包，将该 IP 数据包发送到互联网，

移动通信协议栈、转发控制层、无线局域网协议栈中的任何一个将 IP 数据包的源地址修改为多模终端在互联网中对应的 IP 地址。

10. 根据权利要求 9 所述的多模终端，其特征在于，无线局域网协议栈为 WiFi、WiMax、BlueTooth、UWB、Zigbee、RFID 中的一个。

11. 根据权利要求 9 所述的多模终端，其特征在于，移动通信协议栈为 TD-SCDMA、WCDMA、GSM、CDMA 1x、CDMA2000、GPRS 中的一个。

12. 一种多模终端的数据转发方法，其特征在于，包括以下步骤：

无线局域网协议栈将从无线设备接收到的 IP 数据包转送到共享缓存区，并通知转发控制层；

转发控制层将从无线设备接收到的 IP 数据包在共享缓存区中的存放地址通知移动通信协议栈；

移动通信协议栈从共享缓存区取出从无线设备接收到的 IP 数据包，将该 IP 数据包发送到互联网，

移动通信协议栈、转发控制层、无线局域网协议栈中的任何一个将 IP 数据包的源地址修改为多模终端在互联网中对应的 IP 地址。

13. 根据权利要求 12 所述的方法，其特征在于，无线局域网协议栈为 WiFi、WiMax、BlueTooth、UWB、Zigbee、RFID 中的一个。

14. 根据权利要求 12 所述的方法，其特征在于，移动通信协议栈为 TD-SCDMA、WCDMA、GSM、CDMA 1x、CDMA2000、GPRS 中的一个。

多模终端及其数据转发方法

技术领域

[0001] 本发明涉及一种移动通信技术，特别是一种多模终端及其数据转发方法。

背景技术

[0002] 当今科技的发展带来了多种无线接入技术和蜂窝通信技术，下一代网络将出现由多种不同无线技术支撑的混合网络环境。能在多种不同的蜂窝移动通信网络或无线接入网络中使用或支持多种无线网络的移动通信终端称为“多模移动通信终端”，以下简称“多模终端”。目前，移动终端多模融合已经成为移动通信终端发展的趋势。

[0003] 现有多模终端一般包括蜂窝移动通信网络 (PLMN) 模块，例如 TD-SCDMA、WCDMA、GSM、CDMA1x、CDMA2000，GPRS 等，以及无线接入网络 (RAN) 模块，例如 WiFi、WiMax、BlueTooth、UWB、Zigbee、RFID 等。多模终端可以通过不同的模块执行不同的业务，例如，用户可以通过蜂窝移动通信网络模块连接到移动通信网络来进行语音或者数据业务，也可以通过无线接入网络模块连接无线接入网络，构成无线局域网 (WLAN) 来连接其它设备进行无线业务。

[0004] 目前，多模终端的各个模块之间主要采用多模分离协议栈。例如移动通信协议栈和无线接入协议栈（为了说明的目的，本发明中将多模终端的蜂窝移动通信协议栈简称为移动通信协议栈，将多模终端的无线接入协议栈称为 WLAN 协议栈），分别处理移动通信业务和无线接入业务。

[0005] 当用户通过蜂窝移动通信网络模块连接到移动通信网络来进行数据业务时，移动通信协议栈中的分组数据集中协议 (Packet Data ConvergenceProtocol，PDCP) 层将下层解压的数据进行 PDCP 数据包的解包操作，将恢复出来的 IP 数据包提交给移动通信协议栈的上层用户，例如 TCP/IP 协议层，进行 TCP/IP 数据包的解包等操作，再由互联网浏览器之类的用户应用程序使用；或者，移动通信协议栈中的 PDCP 层将上层用户要发送的 TCP/IP 数据包进行 PDCP 数据包的打包，转发到移动通信协议栈下层的协议层，最终通过移动通信网络发送出去。

[0006] 当用户通过 WLAN 与其它设备建立连接时，数据以 MAC 帧格式进行传递。WLAN 协议栈中的 MAC 层从下层收到的 MAC 帧数据中恢复出 IP 数据包，并提交给 WLAN 协议栈的上层用户，例如 TCP/IP 协议层，进行 TCP/IP 数据包的解包等操作，再由其它用户应用程序使用；或者，WLAN 协议栈中的 MAC 层将上层用户要发送的 TCP/IP 数据包进行 MAC 数据帧的打包，转发到 WLAN 协议栈下层的协议层，最终通过 WLAN 网络发送出去。

[0007] 然而，不同目前多模终端的各种无线协议栈之间的用户面之间没有交互，因此对于移动通信协议栈和 WLAN 协议栈之间的业务数据的传递，需要在两套协议栈的上层增加一个转发控制层来协调处理两套协议栈的数据转发。

[0008] 例如，在火车上使用 WLAN 笔记本电脑通过身边的 3G/WLAN 双模手机上网时，手机通过 3G 网络从互联网下载的数据，经过手机的移动通信网络协议栈处理之后，解压出互联网 IP 数据包，发送到手机的互联网通信协议栈，由手机的互联网通信协议栈从互联网 IP 数

据包中解压出原始数据，转发到手机用户面控制层，再由手机用户面控制层调用 IP 层再次进行数据打包之后，交给手机的 WLAN 协议栈，通过 WLAN 微网络发送到笔记本电脑的 WLAN 协议栈。

[0009] 或者，手机的 WLAN 协议栈在收到笔记本电脑通过 WLAN 微网络发送的数据之后，解压出 IP 数据包，交给用户面控制层，由用户面控制层调用 IP 层再次进行数据打包之后，交给手机的互联网通信协议栈，通过手机的移动通信网络协议栈发送出去。

[0010] 以上是一种协议栈之间松耦合的方式，这种方式的问题是分组交换域（PS 域）的用户数据需要经过两套协议栈的数据处理，进行了两次 IP 数据的打包，并需要单独开发一个用户面控制层进行数据转发，效率比较低。

发明内容

[0011] 本发明的目的在于提供一种多模终端。

[0012] 本发明的另一目的在于提供上述多模终端的数据转发方法。

[0013] 本发明的一种多模终端，具有至少一个移动通信协议栈，至少一个无线局域网协议栈，共享缓存区以及转发控制器。其中，移动通信协议栈用于将从互联网接收到的 IP 数据包存放到共享缓存区后通知转发控制层；转发控制层用于将修改后的 IP 数据包在共享缓存区中的存放地址通知无线局域网协议栈；无线局域网协议栈用于从共享缓存区取出修改后的 IP 数据包并将其发送到无线设备，移动通信协议栈、转发控制层、无线局域网协议栈中的任何一个将 IP 数据包的目的 IP 地址修改为无线设备在无线局域网连接中的 IP 地址。

[0014] 在上述多模终端中，无线局域网协议栈进一步用于将从无线设备接收到的 IP 数据包转送到共享缓存区，并通知所述转发控制层；转发控制层进一步用于将从无线设备接收到的 IP 数据包在共享缓存区中的存放地址通知移动通信协议栈；移动通信协议栈进一步用于从共享缓存区取出从无线设备接收到的 IP 数据包，将该 IP 数据包发送到互联网，移动通信协议栈、转发控制层、无线局域网协议栈中的任何一个将 IP 数据包的的源地址修改为互联网中对应的 IP 地址。

[0015] 本发明的一种多模式终端的数据转发方法，包括以下步骤：

[0016] 移动通信协议栈将从互联网接收到的 IP 数据包存放到共享缓存区后通知转发控制层；

[0017] 转发控制层将 IP 数据包在共享缓存区中的存放地址通知无线局域网协议栈；

[0018] 无线局域网协议栈从共享缓存区取出 IP 数据包并将其发送到无线设备，

[0019] 移动通信协议栈、转发控制层、无线局域网协议栈中的任何一个将 IP 数据包的目的 IP 地址修改为无线设备在无线局域网连接中的 IP 地址。

[0020] 在上述方法中，可以进一步包括以下步骤：

[0021] 无线局域网协议栈将从无线设备接收到的 IP 数据包转送到共享缓存区，并通知所述转发控制层；

[0022] 转发控制层将从无线设备接收到的 IP 数据包在共享缓存区中的存放地址通知移动通信协议栈；

[0023] 移动通信协议栈从共享缓存区取出从无线设备接收到的 IP 数据包，将该 IP 数据

包发送到互联网，

[0024] 移动通信协议栈、转发控制层、无线局域网协议栈中的任何一个将 IP 数据包的的源地址修改为互联网中对应的 IP 地址。本发明的另一种多模终端，具有至少一个移动通信协议栈，至少一个无线局域网协议栈，共享缓存区以及转发控制器。其中，无线局域网协议栈用于将从无线设备接收到的 IP 数据包转送到共享缓存区，并通知转发控制层；转发控制层用于将从无线设备接收到的 IP 数据包在共享缓存区中的存放地址通知移动通信协议栈；移动通信协议栈用于从共享缓存区取出从无线设备接收到的 IP 数据包，将该 IP 数据包发送到互联网，移动通信协议栈、转发控制层、无线局域网协议栈中的任何一个将 IP 数据包的的源地址修改为互联网中对应的 IP 地址。

[0025] 本发明的另一种多模终端的数据转发方法，包括以下步骤：

[0026] 无线局域网协议栈将从无线设备接收到的 IP 数据包转送到共享缓存区，并通知转发控制层；转发控制层将从无线设备接收到的 IP 数据包在共享缓存区中的存放地址通知移动通信协议栈；移动通信协议栈从共享缓存区取出从无线设备接收到的 IP 数据包，将该 IP 数据包发送到互联网，移动通信协议栈、转发控制层、无线局域网协议栈中的任何一个将 IP 数据包的的源地址修改为互联网中对应的 IP 地址。

[0027] 在上述多模终端及其数据转发方法中，无线局域网协议栈为 WiFi、WiMax、BlueTooth、UWB、Zigbee、RFID 中的一个，移动通信协议栈为 TD-SCDMA、WCDMA、GSM、CDMA1x、CDMA2000，GPRS 中的一个。

[0028] 应用本发明提供的技术，通过将 IP 数据包的目的 IP 地址修改为无线设备在无线局域网连接中的 IP 地址，实现了在将数据从互联网转发到无线局域网的过程中，仅对数据进行一次打包；通过将 IP 数据包的源地址修改为多模终端在互联网中对应的 IP 地址，实现了在将数据从无线局域网转发到互联网的过程中，仅对数据进行一次打包；本发明通过修改 IP 地址的方式避免了现有技术中数据转发需要两次打包，从而可以有效的提高数据传输效率。

附图说明

[0029] 图 1 所示为根据现有技术，笔记本电脑通过连接互联网的多模终端从互联网获取数据或者发送数据到互联网时数据移动路径的示意图；

[0030] 图 2 所示为描述根据现有技术笔记本电脑通过连接互联网的多模终端从互联网获取数据的过程的流程图；

[0031] 图 3 所示为描述根据现有技术笔记本电脑通过连接互联网的多模终端发送数据到互联网的过程的流程图；

[0032] 图 4 所示为根据本发明的一种实施方式，笔记本电脑通过连接互联网的多模终端从互联网获取数据或者发送数据到互联网时数据移动路径的示意图；

[0033] 图 5 所示为描述根据本发明一种实施方式，笔记本电脑通过连接互联网的多模终端从互联网获取数据的过程的流程图；

[0034] 图 6 所示为描述根据本发明的一种实施方式，笔记本电脑通过连接互联网的多模终端发送数据到互联网的过程的流程图。

具体实施方式

[0035] 实际上，当多模手机通过移动通信协议栈与互联网建立 IP 连接，并同时通过 WLAN 协议栈与诸如笔记本的其它终端建立 IP 连接时，两个连接之间传递的底层数据格式都是 IP 数据包，因此，有可能通过 IP 地址映射，找到一种数据包之间简单的转换方法。

[0036] 根据本发明的方法，当笔记本通过 WLAN 微网络连接多模手机，通过多模手机进行互联网业务时，在多模手机的移动通信协议栈的 PDCP 层解压出互联网 IP 数据包之后，进行 IP 地址转换，将 IP 数据包的目的 IP 地址转换为笔记本在 WLAN 微网络中的 IP 地址，并直接调用 WLAN 协议栈的接口发送给笔记本；或者，手机的 WLAN 协议栈在收到笔记本发送的微网络 IP 数据包之后，将微网络 IP 数据包转发给移动通信协议栈的 PDCP 层，由 PDCP 层将该数据包的源 IP 地址转换为手机在互联网中的 IP 地址，并通过移动通信协议栈发送出去。本发明的方法可以实现 3G 移动通信协议栈和 WLAN 无线接入协议栈用户面数据直接交互，提高数据传输效率。

[0037] 移动通信协议栈中的 PDCP 层的主要功能是 IP 数据流的头部压缩与解压缩，用于从移动通信协议栈下层的无线链路层 (RLC) 接收无线数据之后，使用 RFC25.07 算法进行解压缩之后传递给移动通信协议栈的上层用户，例如 TCP/IP 等高层网络协议；或者将从移动通信协议栈的上层用户接收的数据按照 RFC25.07 算法进行压缩，再发送到移动通信协议栈下层转发出去。

[0038] 另外，WLAN 协议栈中的 MAC 层的主要功能是 IP 数据流的 MAC 帧打包或者解包，用于从 WLAN 协议栈下层的基带层接收 MAC 帧格式的无线数据之后，进行 MAC 帧解包之后传递给 WLAN 栈的上层用户，例如 TCP/IP 等高层网络协议；或者将从 WLAN 协议栈的上层用户接收的数据打包为 MAC 帧数据，再发送到 WLAN 协议栈的下层转发出去。

[0039] 当例如在上面所述的场景中，即多模终端通过移动通信协议栈连接互联网，笔记本电脑通过 WLAN 微网络与多模终端连接从而连接到互联网的场景下，此时多模终端在互联网中具有 IP 地址，而在 WLAN 微网络中，多模终端与笔记本电脑也分别具有该 WLAN 微网络中的 IP 地址。

[0040] 图 1 所示为根据现有技术，笔记本电脑通过连接互联网的多模终端从互联网获取数据或者发送数据到互联网的数据移动路径的示意图。

[0041] 现在首先参考图 2 的流程图并结合图 1 来描述根据现有技术笔记本电脑通过连接互联网的多模终端从互联网获取数据的过程。

[0042] 从图 1 可见具有 WCDMA 协议栈 203 的 WCDMA 多模终端 20 同时具有 WLAN（可以是 WiFi、WiMax、BlueTooth、UWB、Zigbee、RFID 中任何一种）协议栈 204。

[0043] 当多模终端 20 在 WLAN 连接中利用 ad hoc 模式建立了与附近的 WLAN 笔记本电脑 30 的联系，完成了 WLAN 节点之间的链路建立工作，并且同时已经使用 WCDMA 移动链路建立流程，完成了与互联网 10 之间的空中链路的建立。

[0044] 此时，当笔记本电脑 30 通过多模终端 20 从互联网下载数据时，数据移动过程如下：

[0045] 在步骤 S1，多模终端 20 中的 WCDMA 协议栈 203 中的 PDCP 层 2031 将从 WCDMA 协议栈 203 下层的无线链路层 (RLC 层) 接收来自互联网的无线数据之后，使用 RFC25.07 算法进行解压缩，得到以多模终端 20 在互联网中的 IP 地址为目标地址的 IP 数据包，并传递给

WCDMA 协议栈的上层用户，即 TCP/IP 协议层 202。

[0046] 在步骤 S2，TCP/IP 协议层 202 对 IP 数据包进行解包操作，恢复出 IP 数据包的内容并转交给转发控制层 201。

[0047] 在步骤 S3，转发控制层 201 调用 TCP/IP 协议层，按照 WLAN 笔记本电脑 30 在 WLAN 微网络中的 IP 地址（作为目的地址）再次将原 IP 数据包的内容打包为新的 IP 数据包并发送到 WLAN 协议栈 204。

[0048] 之后，在步骤 S4 中，由 WLAN 协议栈 204 中的 MAC 层 2041 将新打包的 IP 数据包再次打包为 MAC 帧的格式之后通过 WLAN 协议栈 204 的下层发送出去由 WLAN 笔记本电脑 30 接收。

[0049] 可以看到，由于多模终端的移动通信协议栈与 WLAN 协议栈之间不能进行数据交互，数据在多模终端 20 中进行了多次转发，并且有一次 IP 数据包的解包操作以及一次 IP 数据包的打包操作。这很大的占用了多模终端的系统资源并且效率很低。

[0050] 下面参考图 3 描述根据现有技术笔记本电脑通过连接互联网的多模终端发送数据到互联网的过程。

[0051] 在步骤 R1，笔记本电脑 30 通过 WLAN 将要发送的数据发送到多模终端 20 的 WLAN 协议栈 204。

[0052] 在步骤 R2，WLAN 协议栈 204 的 MAC 层从 MAC 帧数据中恢复出 IP 数据包，并交给 TCP/IP 层 202，该 IP 数据包的源地址为 WLAN 笔记本电脑 30。

[0053] 在步骤 R3，TCP/IP 协议层 202 对 IP 数据包进行解包操作，恢复出 IP 数据包中的数据并转交给转发控制层 201。

[0054] 在步骤 R4，转发控制层 201 调用 TCP/IP 层，按照多模终端 20 在互联网中的 IP 地址（作为源地址）再次将原 IP 数据包中的内容打包为新 IP 数据包并发送到 WCDMA 协议栈 203。

[0055] 在步骤 R5，WCDMA 协议栈 203 中的 PDCP 层 2031 将新 IP 数据包按照 RFC25.07 算法进行压缩之后，再通过 WCDMA 协议栈下层转发出去。

[0056] 可以看到，与前面一样，由于多模终端的移动通信协议栈与 WLAN 协议栈之间不能进行数据交互，数据在多模终端 20 中进行了多次转发，并且有一次 IP 数据包的解包操作以及一次 IP 数据包的打包操作。

[0057] 而根据本发明的方法，在多模终端移动通信协议栈的 PDCP 层和 WLAN 协议层的 MAC 协议层之间直接进行数据传递，在数据转发过程中对 IP 数据包进行 IP 地址变化，从而避免多余的 IP 数据包解压和压缩操作，以及多次的数据转发，从而避免资源的浪费。

[0058] 图 4 所示为根据本发明，笔记本电脑通过连接互联网的多模终端从互联网获取数据或者发送数据到互联网的数据移动路径的示意图。

[0059] 可以看到，本发明的多模终端 20A 中，使多模终端 20A 的 WCDMA 协议栈 203 的 PDCP 层 2031A 具备了 IP 地址变化的功能，PDCP 层 2031A 和 WLAN 协议栈 204 的 MAC 协议层 2041 之间通过共享缓存区 205 进行数据传递。可以使多模终端 20A 在执行数据转发的状态下，在多模终端 20A 中设定一个网络协同工作模式，使其按照本发明的方法进行数据的转发。

[0060] 下面参考图 5 的流程图并结合图 4 来描述根据本发明的一种实施方式，笔记本电脑通过连接互联网的多模终端从互联网获取数据的过程。

[0061] 当多模终端 20A 在 WLAN 连接中利用 ad hoc 模式建立了与附近的 WLAN 笔记本电脑 30 的联系，完成了 WLAN 节点之间的链路建立工作，并且同时已经使用 WCDMA 移动链路建立流程，完成了与互联网 10 之间的空中链路的建立。

[0062] 并且，假定此时多模终端 20A 设定了网络协同工作模式。

[0063] 此时，当笔记本电脑 30 通过多模终端 20A 从互联网下载数据时，数据移动过程如下：

[0064] 在步骤 M1，多模终端 20A 中的 WCDMA 协议栈 203 中的 PDCP 层 2031A 从 WCDMA 协议栈 203 下层的无线链路层（RLC 层）接收来自互联网的无线数据后，使用 RFC25.07 算法进行解压缩，得到以多模终端 20 在互联网中的 IP 地址为目标地址的 IP 数据包之后，由于设定了网络协同工作模式，因此 PDCP 层 2031A 将 IP 数据包的目标 IP 地址变化为笔记本在 WLAN 微网络中的 IP 地址，存放在共享缓存区 205，并通知转发控制层 201A。

[0065] 在步骤 M2，转发控制层 201 将 IP 数据包在缓存区的地址通知 WLAN 协议栈 204 的 MAC 层 2041。

[0066] 在步骤 M3，MAC 层 2041 从共享缓存区取出经过地址改变的 IP 数据包再次打包为 MAC 帧的格式之后通过 WLAN 协议栈 204 的下层发送出去由 WLAN 笔记本电脑 30 接收。

[0067] 可以看到，数据直接由 PDCP 层发送到 MAC 层，并且没有 IP 数据包的解包操作和打包操作。

[0068] 上面的实施方式中由 PDCP 层改变接收到的 IP 数据包的目标 IP 地址，然而，PDCP 层也可以不改变接收到的 IP 数据包的 IP 地址而直接将它存放到共享缓存区中，由转发控制层来将 IP 数据包的目标 IP 地址变化为笔记本在 WLAN 微网络中的 IP 地址，再通知 MAC 层将数据包从共享缓存区取出发送出去；或者 PDCP 层和转发控制层都不改变 IP 数据包的目标 IP 地址，由 MAC 层在将 IP 数据包发送出去之前将 IP 数据包的目标 IP 地址变化为笔记本在 WLAN 微网络中的 IP 地址。

[0069] 下面参考图 6 描述根据本发明的一种实施方式，笔记本电脑通过连接互联网的多模终端发送数据到互联网的过程。

[0070] 在步骤 N1，笔记本电脑 30 通过 WLAN 将要发送的数据发送到多模终端 20 的 WLAN 协议栈 204。

[0071] 在步骤 N2，WLAN 协议栈 204 的 MAC 层 2041 从 MAC 帧数据中恢复出 IP 数据包，该 IP 数据包的源 IP 地址为 WLAN 笔记本电脑 30 在 WLAN 微网络中的 IP 地址，由于设置了网络协同工作模式，因此 MAC 层 2041 将数据存放在共享缓存区之后，通知转发控制层 201A。

[0072] 在步骤 N3，转发控制层 201 将 IP 数据包在缓存区的地址通知 WCDMA 协议栈 203 中的 PDCP 层 2031A。

[0073] 在步骤 N4，WCDMA 协议栈 203 中的 PDCP 层 2031 将 IP 数据包从共享缓存区中取出，将数据包的源 IP 地址修改为多模终端 20 在互联网中的 IP 地址，之后按照 RFC25.07 算法进行压缩，再通过 WCDMA 协议栈下层转发出去。

[0074] 可以看到，数据直接由 MAC 层发送到 PDCP 层，而不需要进行多次的转发，并且没有 IP 数据包的解包操作和打包操作。

[0075] 上面的实施方式中由 PDCP 层改变要发送的 IP 数据包的源 IP 地址，然而，也可以由转发控制层在 MAC 层将 IP 数据包存放在共享缓存区之后改变 IP 数据包的源 IP 地址，或

者由MAC层将通过无线局域网协议栈接收的IP数据包改变源IP地址之后放到共享缓存区中，再由转发控制层通知PDCP层取出源IP地址改变的IP数据包发送出去。

[0076] 另外，以上以多模终端的移动通信协议栈为WCDMA协议栈为例进行了说明，然而，本领域技术人员应该可以理解，多模终端的移动通信协议栈还可以是具有PDCP层的任何一种移动通信协议栈，例如TD-SCDMA、GSM、CDMA 1x、CDMA2000，GPRS等。

[0077] 根据本发明的数据转发方式可以让多模手机在后台完成网络数据传递功能，同时手机可以进行提供其它如打电话、收发短信等通信服务，不占用前台人机操作界面。

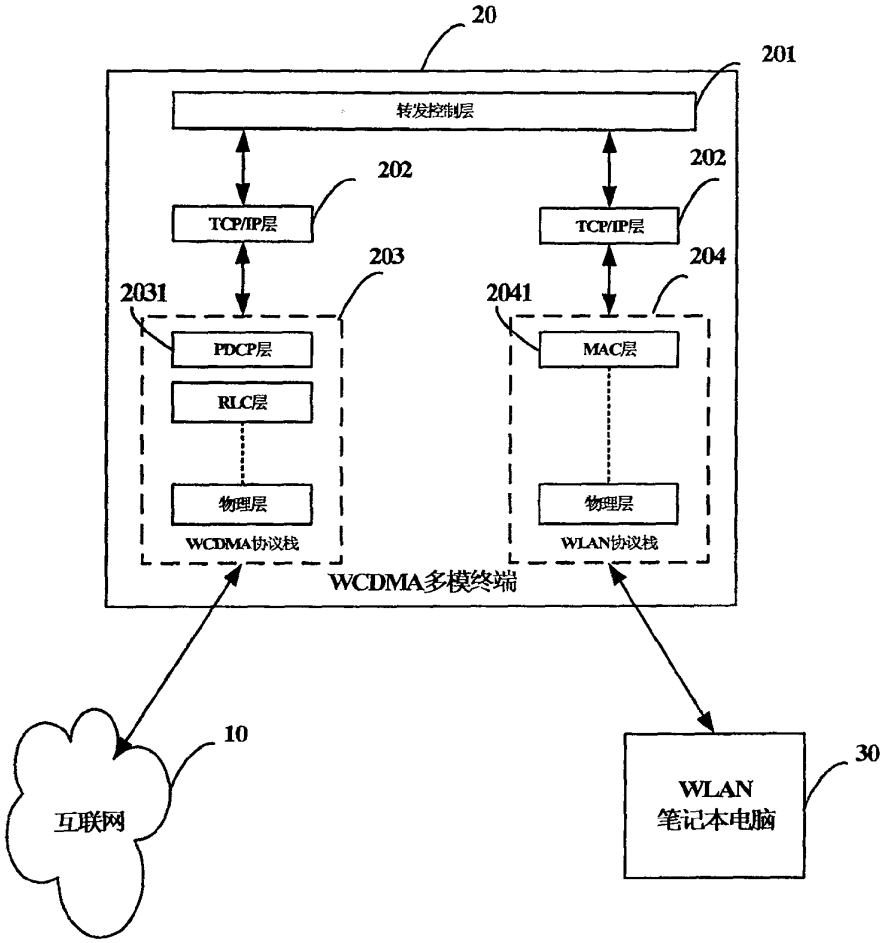

20
201
转发控制层
202
TCP/IP层
202
TCP/IP层
203
2031
PDCP层
RLC层
物理层
WCDMA协议栈
204
2041
MAC层
物理层
WLAN协议栈
WCDMA多模终端
10
互联网
30
WLAN
笔记本电脑

图 1

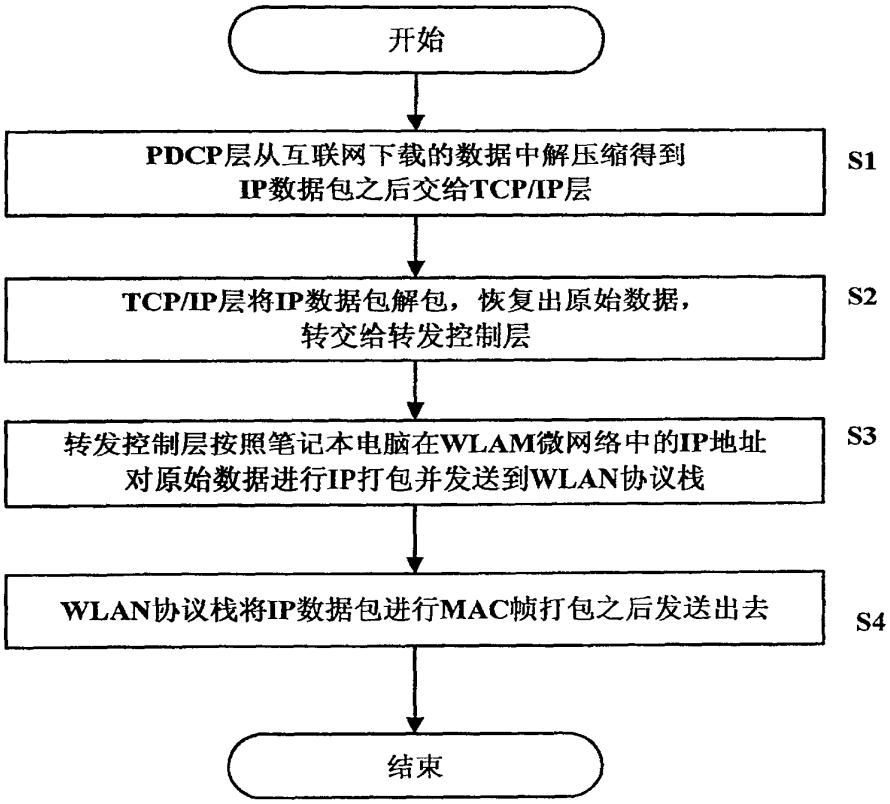

开始
PDCP层从互联网下载的数据中解压缩得到IP数据包之后交给TCP/IP层
S1
TCP/IP层将IP数据包解包，恢复出原始数据，转交给转发控制层
S2
转发控制层按照笔记本电脑在WLAM微网络中的IP地址对原始数据进行IP打包并发送到WLAN协议栈
S3
WLAN协议栈将IP数据包进行MAC帧打包之后发送出去
S4
结束

图 2

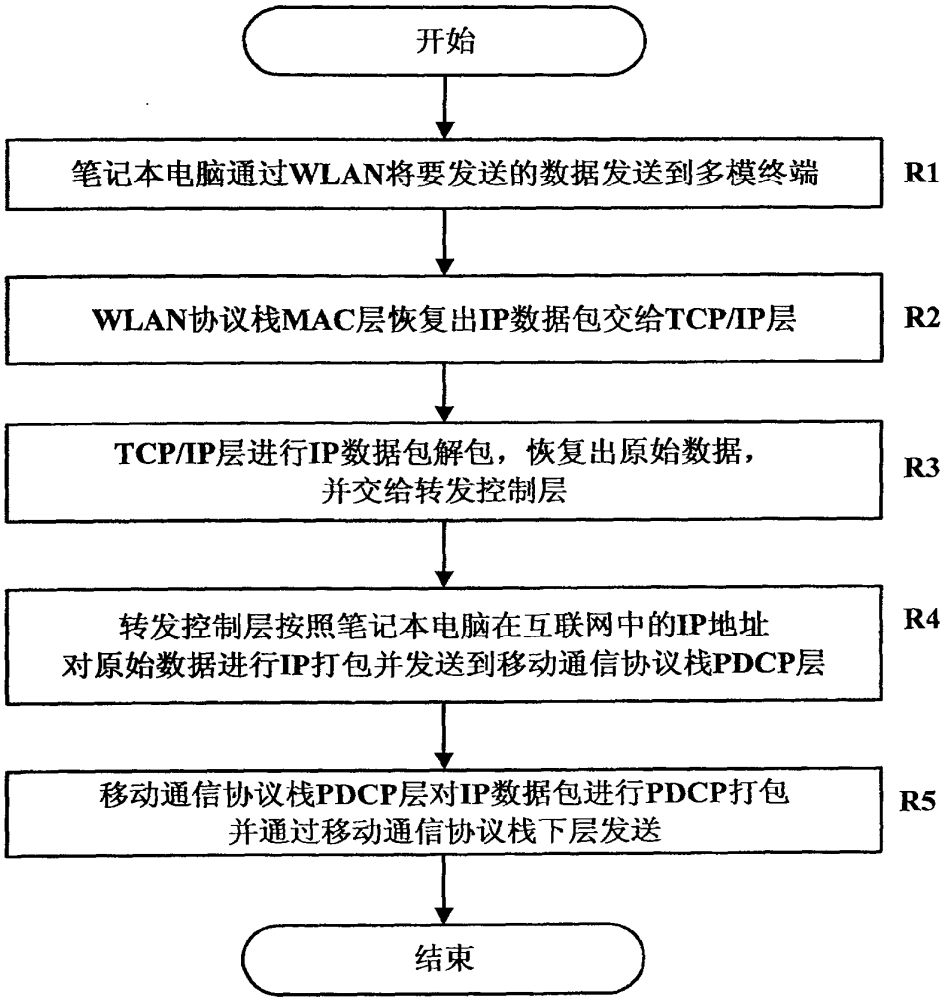

开始
笔记本电脑通过WLAN将要发送的数据发送到多模终端
R1
WLAN协议栈MAC层恢复出IP数据包交给TCP/IP层
R2
TCP/IP层进行IP数据包解包，恢复出原始数据，
并交给转发控制层
R3
转发控制层按照笔记本电脑在互联网中的IP地址
对原始数据进行IP打包并发送到移动通信协议栈PDCP层
R4
移动通信协议栈PDCP层对IP数据包进行PDCP打包
并通过移动通信协议栈下层发送
R5
结束

图 3

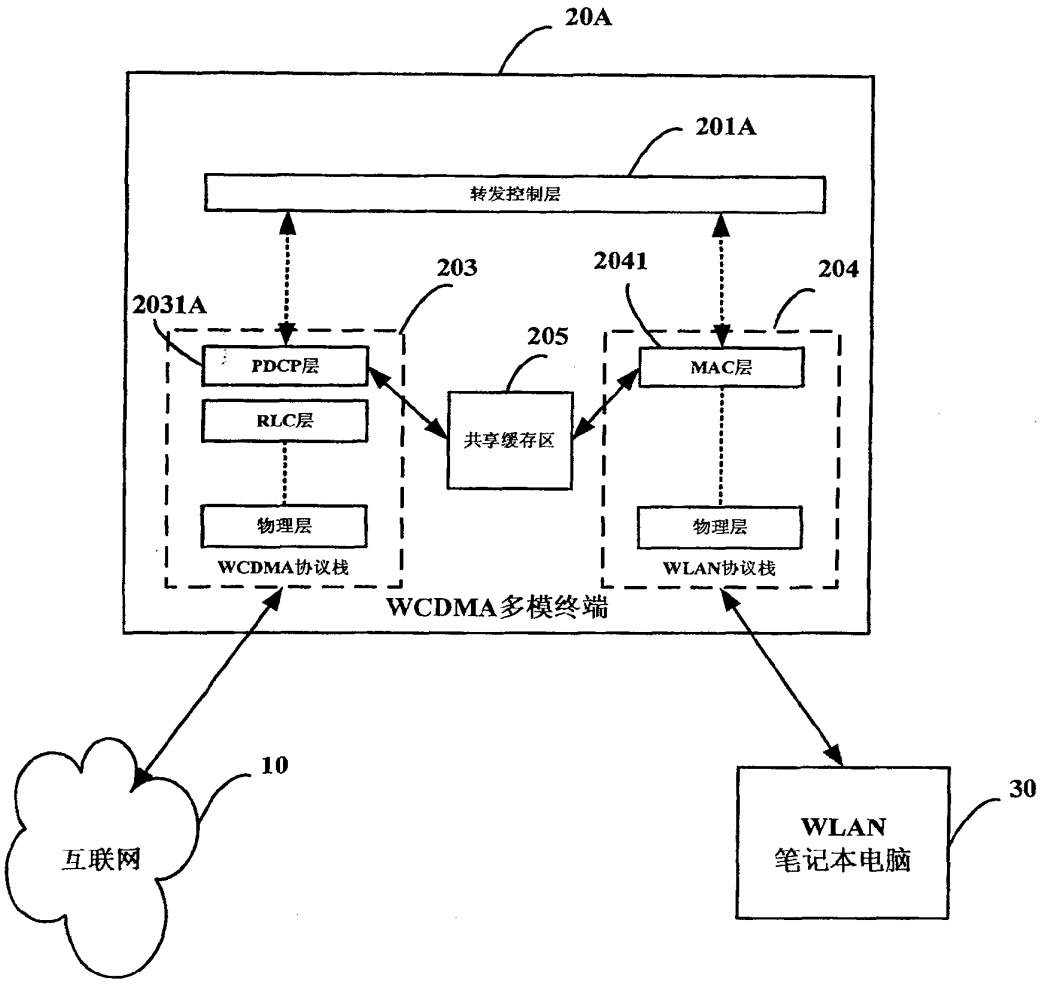

20A
201A
转发控制层
203
2041
204
2031A
205
PDCP层
RLC层
物理层
WCDMA协议栈
共享缓存区
MAC层
物理层
WLAN协议栈
WCDMA多模终端
10
互联网
30
WLAN
笔记本电脑

图 4

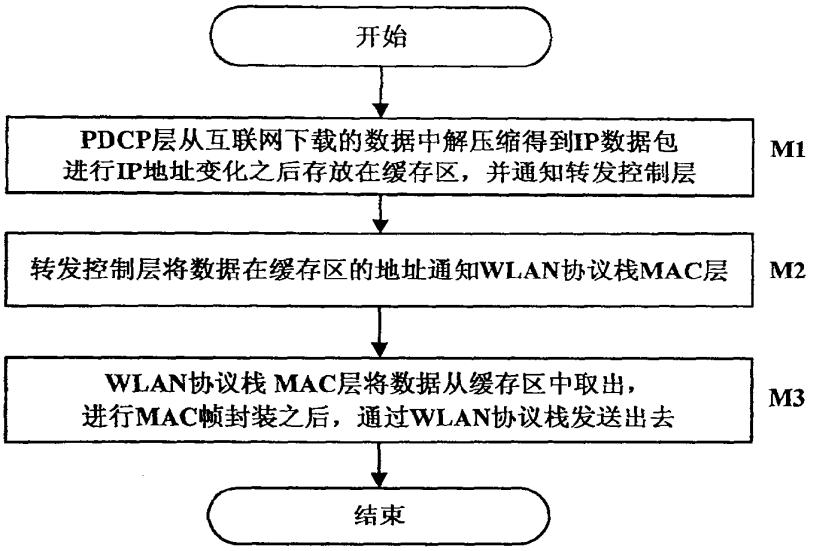

开始
PDCP层从互联网下载的数据中解压缩得到IP数据包
进行IP地址变化之后存放在缓存区，并通知转发控制层
M1
转发控制层将数据在缓存区的地址通知WLAN协议栈MAC层
M2
WLAN协议栈 MAC层将数据从缓存区中取出，
进行MAC帧封装之后，通过WLAN协议栈发送出去
M3
结束

图 5

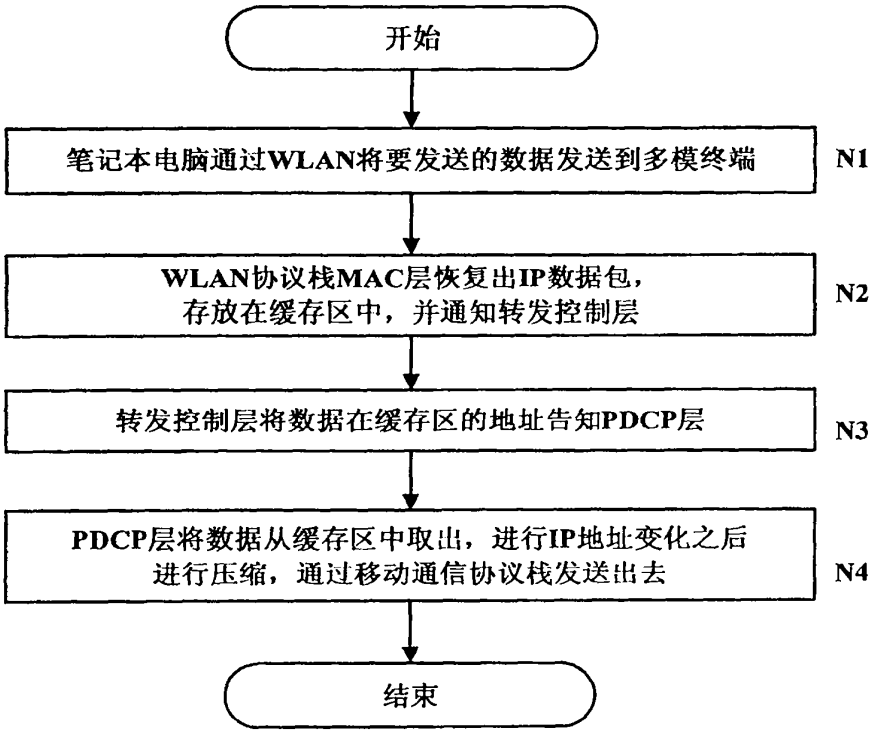

开始
笔记本电脑通过WLAN将要发送的数据发送到多模终端
N1
WLAN协议栈MAC层恢复出IP数据包，
存放在缓存区中，并通知转发控制层
N2
转发控制层将数据在缓存区的地址告知PDCP层
N3
PDCP层将数据从缓存区中取出，进行IP地址变化之后
进行压缩，通过移动通信协议栈发送出去
N4
结束

图 6

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04Q 3/00 (2006.01)
H04Q 7/24 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200580052316.4

[43] 公开日 2009 年 1 月 7 日

[11] 公开号 CN 101341764A

[22] 申请日 2005.12.16
[21] 申请号 200580052316.4
[86] 国际申请 PCT/EP2005/056843 2005.12.16
[87] 国际公布 WO2007/068288 英 2007.6.21
[85] 进入国家阶段日期 2008.6.16
[71] 申请人 艾利森电话股份有限公司
地址 瑞典斯德哥尔摩
[72] 发明人 R·诺尔杜斯 A·沙马

[74] 专利代理机构 中国专利代理(香港)有限公司
代理人 王 岳 张志醒

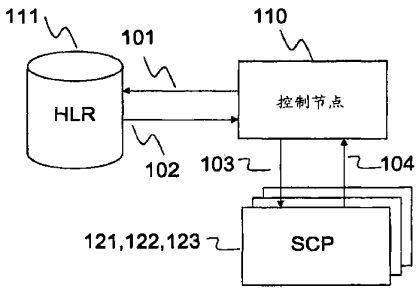
权利要求书 3 页 说明书 15 页 附图 6 页

[54] 发明名称

智能网服务

[57] 摘要

公开了用于处理与对移动电信网络的订户的呼叫相关联的智能网服务的方法、控制节点(110)和计算机程序，该网络包括所述控制节点(110)、HLR 5(111)和一个或多个 SCP(121、122、123)。所述控制节点(110)a)向所述 HLR(111)发送(101)与所述呼叫相关的路由信息的一个或多个请求；b)从所述 HLR(111)接收(102)与所述服务相关联的服务触发元素；c)使用所述触发元素在所述一个或多个(SCP)(121、122、123)中调用(103)所述服务；和 d)从所述一个或多个 SCP(121、122、123)接收与所述触发元素所关联的服务相关的信息。



1. 一种用于处理与对移动电信网络的订户的呼叫相关联的智能网服务的方法，该网络包括控制节点（110）、归属位置寄存器（111）和一个或多个服务控制点（121、122、123），该方法包括以下步骤：

a. 所述控制节点（110）向所述归属位置寄存器（111）发送（101）与所述呼叫相关的路由信息的一个或多个请求；

b. 所述控制节点（110）从所述归属位置寄存器（111）接收（102）与所述服务相关联的服务触发元素；

c. 所述控制节点（110）使用所述触发元素在所述一个或多个服务控制点（121、122、123）中调用（103）所述服务；

d. 所述控制节点（110）从所述一个或多个服务控制点（121、122、123）接收（104）与所述触发元素所关联的所述服务相关的信息。

2. 根据权利要求 1 所述的方法，其中所述归属位置寄存器（111）响应于路由信息的第一请求发送所述多个服务触发元素中的第一服务触发元素，并且响应于路由信息的第二请求发送所述多个服务触发元素中的第二服务触发元素。

3. 根据权利要求 1 所述的方法，其中所述归属位置寄存器（111）响应于路由信息的第一请求发送所述多个服务触发元素。

4. 根据权利要求 2 或 3 所述的方法，其中所述归属位置寄存器（111）响应于路由信息的第二请求发送所请求的路由信息。

5. 根据权利要求 2-4 中任何一个权利要求所述的方法，其中所述路由信息的第二请求与所述控制节点（110）和被访问移动服务交换中心（112）之间信令连接的建立相关联。

6. 根据前面任何一个权利要求所述的方法，其中所述请求的路由信息包括用于对所述订户的呼叫的移动站漫游号码。

7. 根据前面任何一个权利要求所述的方法，其中多个所述服务触发元素包括在一个移动应用部分消息中。

8. 根据权利要求 7 所述的方法，其中由于移动应用部分的分段，所述一个移动应用部分消息在多个信令连接控制部分消息中从所述归属位置寄存器（111）发送到所述控制节点。

9. 根据权利要求 1-6 中任何一个权利要求所述的方法，其中所述一个或多个所述服务触发元素作为前缀或后缀包括在移动站漫游号码

中。

10. 根据权利要求 1-6 中任何一个权利要求所述的方法，其中所述服务触发元素包括分离的参数。

11. 根据前面任何一个权利要求所述的方法，其中所述服务的第一服务在所述一个或多个服务控制点（121、122、123）中的第一服务控制点（121）中执行，并且所述服务的第二服务在所述一个或多个服务控制点（121、122、123）中的第二服务控制点（122）中执行。

12. 根据权利要求 11 所述的方法，其中所述服务的第一服务是预付费计费服务。

13. 根据权利要求 11 或 12 所述的方法，其中所述服务的第二服务是诸如个人问候服务的移动被叫服务。

14. 根据前面任何一个权利要求所述的方法，其中所述控制节点（110）是网关移动交换中心（110）。

15. 根据权利要求 2-14 中任何一个权利要求所述的方法，其中所述第一请求包含所述订户的移动站 ISDN 号码。

16. 根据权利要求 2-15 中任何一个权利要求所述的方法，其中所述第二请求包含所述订户的移动站 ISDN 号码和“抑制 T-CSI”参数。

17. 根据前面任何一个权利要求所述的方法，其中所述路由信息的一个或多个请求中的第一或第二请求包括移动应用部分发送路由信息消息。

18. 一种用于处理与对移动电信网络的订户的呼叫相关联的智能网服务的控制节点（110），该网络包括控制节点（110）、归属位置寄存器（111）和一个或多个服务控制点（121、122、123）；控制节点（110）配置用于向所述归属位置寄存器（111）发送对与所述呼叫相关联的路由信息的一个或多个请求；控制节点（110）还配置用于从所述归属位置寄存器(111)接收与所述服务相关联的多个服务触发元素，并且用于通过使用所述触发元素在所述一个或多个服务控制点（121、122、123）中调用所述服务；控制节点还配置用于从所述一个或多个服务控制点（121、122、123）接收与所述触发元素所关联的所述服务相关的信息。

19. 一种计算机程序，其包括致使计算机执行依照权利要求 1-17 中任何一个所述的方法的程序指令。

20. 一种载体上的计算机程序，其包括致使计算机执行依照权利要求 1-17 的方法的计算机可执行指令。

21. 根据权利要求 19 所述的计算机程序，其中所述载体是记录介质、计算机存储器、只读存储器或电载体信号。

智能网服务

技术领域

本发明涉及用于处理与对移动电信网络的订户的呼叫相关的智能网服务的方法和控制节点。

背景技术

在当前的电信网络技术诸如GSM（全球移动通信系统）中，智能网服务是众所周知的。

GSM网络的核心网络子系统的中央部件是移动服务交换中心（MSC）。它起类似于PSTN或ISDN的交换节点的作用，并且另外提供用于处理移动订户所需的所有功能，诸如注册、鉴权、位置更新、移交和到漫游订户的呼叫路由。这些服务连同几个功能实体一起被提供，它们一起构成了核心网络子系统。网关MSC（GMSC）提供到固定网络（诸如PSTN或ISDN）的连接。核心网络子系统中的功能实体之间的信令使用7号信令系统，7号信令系统在ISDN中用于中继信令并且在当前的公共网络中广泛使用。

归属位置寄存器（HLR）和访问位置寄存器（VLR）与MSC一起提供GSM的呼叫路由和漫游能力。HLR包含在相应的GSM网络中注册的每个订户的所有管理信息，以及该移动站的当前位置。移动站的位置通常是与该移动站相关联的VLR的信令地址的形式。在逻辑上说，每个GSM网络一个HLR，尽管它可以实现为分布式数据库。

VLR为当前位于由该VLR控制的地理区域内并且当前由该VLR服务的每个移动站包含对于呼叫控制和提供预订的服务所必须的来自HLR的选定管理信息。尽管每个功能实体可以实现为独立的单元，当前所有的交换设备制造商将VLR与MSC一起实现，这样由MSC控制的地理区域与VLR所控制的地理区域相对应，从而简化了所需的信令。MSC不包含关于特定移动站的信息；这个信息在位置寄存器中存储。

接下来，将描述GSM网络中典型的入局呼叫建立（移动被叫（mobile terminating call））。

当订户对移动电话发起呼叫，它拨打与该电话用户相关联的电话号

码，即所谓的移动站 ISDN（MSISDN）号码，并且该呼叫被路由到该移动电话运营商的网关 MSC。网关是用于互连两个网络的节点。网关通常在 MSC 中实现，在这种情况下 MSC 称为 GMSC。GMSC 作为从公共交换电话网络的外面部分到供应商网络的入口。

如上所述，电话可以自由地漫游到运营商网络之中或漫游合作商的网络上的任何地方，包括其它国家。因此，网关 MSC 的第一个任务是确定移动电话的当前位置以便连接该呼叫。它通过咨询 HLR 来做到这一点，如上所述 HLR 知道在该时刻该电话与哪个访问位置寄存器（VLR）相关联（如果有的话）。

当 HLR 接收到这个查询消息，它确定是否应该将该呼叫路由到另一个号码（称为转移）或者应该将该呼叫直接路由到被呼叫订户的移动站。

如果电话的所有者先前已经请求将所有的入局呼叫转接到另一个号码，该补充服务也称为到被转接号码（FTN）的无条件呼叫转接（CFU），那么这个 FTN 被存储在 HLR 中。如果是这种情况，那么将 FTN 返回该网关 MSC 以便立即路由到那个目的地。

如果移动站当前不与 VLR 相关联（例如因为电话已经关机），那么 HLR 返回称为呼叫不可转接（CFNR）号的号码给 GMSC，并且该呼叫被转接到那里。许多运营商可以将这个值自动设置为该电话的语音邮箱号码，这样呼叫者可以留下消息。

最后，如果 HLR 知道该电话在特定 VLR 的管辖范围之内，那么它将从该 VLR 请求一个临时号码，即所谓的移动站漫游号（MSRN）。这个号码被中继到 GMSC，GMSC 使用它将该呼叫路由到称为被访问 MSC（VMSC）的另一个 MSC。

当 VMSC 接收到该呼叫时，使用 MSRN 在 VLR 中寻找该电话的记录。这个记录标识该电话的位置区域。对该区域中的所有移动电话杆（mobile phone mast）发生寻呼。当订户的移动电话响应时，该电话的确定位置被返回给 VMSC。VMSC 随后将呼叫转接到合适的电话杆，并且该电话响铃。如果订户应答，通过该 VMSC 和 GMSC 创建回到人进行呼叫的网络的语音通路，并且随后是一般的电话呼叫。

也可能呼叫没有被应答。如果订户在忙于另一个呼叫（并且没有使用呼叫等待），那么 VMSC 将呼叫路由到预定的遇忙呼叫转接（CFB）

号码。类似的 ，如果订户在一段时间（通常是 30 秒）之后没有应答呼叫，那么 VMSC 将该呼叫路由到预定的无应答呼叫转接（CFNRy）号码。再次的，运营商可以决定默认将这个值设置为该电话的语音邮箱，以便呼叫者能够留下消息。

智能网（IN）是与电信网络耦合的使得运营商能够采用运营商特有的增值服务（VAS）的网络。通过来自智能网的智能增加了交换机中驻留的智能，智能网中的智能安置在分布在网络中各处的计算机节点中。这给网络运营商提供了更有效地开发、采用和控制服务的方式。新的服务可以快速引入到电信网络中。一旦引入，服务可以容易地定制以满足个体客户的需求。

IN 服务通常由服务控制点（SCP）提供。SCP 是与电信网络中的其它节点和实体通信的控制计算机。SCP 包括一个或多个 IN 服务的服务逻辑，并且可选包括 IN 服务预订数据，该预订数据允许 SCP 依照订户的特定设置执行 IN 服务，即特制对该订户的服务执行。当建立了呼叫时，电信网络可以询问 SCP 并且请求处理这个呼叫的指令。例如，SCP 被咨询提供 800 号码到实际电话号码的翻译，并且为该呼叫对该 800 号码的所有者计费。SCP 在物理上可以与智能网的其它组件分离，或者可以与这些其它组件组合到单个节点中。

在 GSM 网络中，IN 服务预订信息在 HLR 中存储。HLR 中驻留两个类型的信息：（1）静态订户信息和（2）动态订户信息。后者例如需要允许将入局呼叫路由到该移动订户。HLR 存储以下信息及其它：

- 国际移动订户身份（IMSI）；只由该网络使用的内部订户身份；
- MSISDN 号码；
- VLR 地址；
- 关于补充服务的订户数据。

IN 服务可以分为两个种类。一个种类包括为发起呼叫（终端发起呼叫-MOC）的订户调用的服务。这些服务称为终端发起（MO）服务。MO 服务的一个例子是出局呼叫屏蔽。

每个 IN 服务订户在他的 HLR 中用发起 CAMEL 预订信息（O-CSI）元素标记，该元素用于在 SCP 标识特定服务。一旦订户启动 MO 呼叫，O-SCI 启动 MOC 服务的触发。在上述例子中采用了 CAMEL，其代表“用于移动网络增强逻辑的定制应用”。CAMEL 发展为用于扩展陆地线路 IN 电话

服务的标准，诸如呼叫等待和到 GSM 移动电话的呼叫转接。

另一种类包括为接收呼叫（移动被叫-MTC）的订户调用的服务。这些服务称为移动被叫（mobile terminating,MT）服务。移动被叫服务的例子是呼叫转移服务和个人问候服务（PGS）。PGS 是与漫游支线相关的服务。PGS 使得当在 GMSC 和 VMSC 之间（所谓的漫游支线）建立了信令连接，向呼叫方显示个人化的问候。个人化问候替换了传统的警报音调（“响铃音调”）。这样，个人化问候主要与漫游支线的建立相关；只有当漫游支线建立并且警报了被呼叫方的时候响铃音调才变得有效。每个 IN 服务订户在他的 HLR 中利用终止 CAMEL 预订信息（T-SCI）标志来标记，该标记用于在 SCP 标识特定服务。这在试图对订户呼叫期间启动 MTC 服务的触发。

依照当前技术，控制节点在 MTC 处理期间可以询问 HLR 以便获得来自 HLR 的指令。控制节点可以是 GMSC。响应于控制节点的询问，HLR 可以发送用于被叫的 IN 触发信息。在 HLR 和控制节点之间交换的 IN 触发信息已经被标准化。例如，如在 3GPP TS 29.002 中由 3GPP（第三代合作伙伴计划）指定的，T-CSI 是 GSM 标准化的用于被叫的 IN 触发信息。IN 触发信息包括 IN 服务所驻留的 SCP 的地址和标识该 SCP 内的特定 IN 服务的服务关键字。

按照在 IN 触发信息中为订户指定的，控制节点使用该 IN 触发信息来调用 SCP 中的 IN 服务。响应于服务调用，SCP 依赖于该服务执行的结果向控制节点发送指令，例如继续建立呼叫或被叫。当前网络通常设置为为一个 MTC 处理 IN 服务的单个调用。但是近来的发展显示，在被叫处理期间需要调用两个或更多 IN 服务。

专利申请 WO00/25528 公开了在 SCP 中包含的服务交互管理器。服务交互管理器的任务是确定应该为订户执行 SCP 中的哪些可用服务并且以特定顺序调用这些服务。

发明内容

本发明的目的是提供通过允许订户对于一个呼叫拥有多于一种 IN 服务来克服当前技术的缺点的方法和设备。

在本发明的第一方面，提出了一种处理与对移动电信网络的订户的呼叫相关的智能网服务的方法，该网络包括控制节点、归属位置寄存

器和一个或多个服务控制点，该方法包括以下步骤：

a. 所述控制节点向所述归属位置寄存器发送与所述呼叫相关的路由信息的一个或多个请求；

b. 所述控制节点从所述归属位置寄存器接收与所述服务相关的服务触发元素；

c. 所述控制节点使用所述服务触发元素在所述一个或多个服务控制点中调用所述服务；

d. 所述控制节点从所述一个或多个服务控制点接收与所述触发元素所关联的所述服务相关的信息。

以此方式，可以为预订了属于订户的一个呼叫的一个或多个 IN 服务的该订户处理多个服务触发元素。IN 服务不需知道在用于该呼叫的控制节点中一个或多个其它 IN 服务的存在。换句话说，第一服务不需知道是否将调用第二服务，反之亦然。因为服务不要求关于为这个呼叫可能调用其它 IN 服务的知识，服务可以运行在不同平台上并且可以由不同的卖主供应。

存在本发明的若干实施例。

例如，本发明可以规定归属位置寄存器响应于路由信息的第一请求而发送所述多个服务触发元素中的第一服务触发元素，并且响应于路由信息的第二请求而发送所述多个服务触发元素中的第二服务触发元素。

所述路由信息的第一请求可以包括：

- 订户的 MSISDN 号码。

对路由信息的第一请求的响应可以包括：

- 第一服务触发元素。

路由信息的第二请求可以包括：

- 订户的 MSISDN 号码；
- HLR 应该在所述响应中抑制第一服务触发元素的指示。这个指示可以是例如“抑制 T-SCI”参数。

对路由信息的第二请求的响应可以包括：

- 用于呼叫被服务订户的 MSRN；
- 第二服务触发元素；
- 订户的 MSRN 的前缀或后缀。

由于 MAP 分段，MAP 消息可以在多个信令连接控制部分消息中被从 HLR 发送给 GMSC。第一服务，例如预付费计费服务，在第一服务控制点中执行，第二服务，例如 PGS，在第二 SCP 中执行。

以此方式，可以将预付费服务和 PGS 提供给相同订户；预付费服务和 PGS 可以在不同平台上运行并且彼此不相关。

当本发明用于 PGS 时，呼叫订户可以收听任何呼叫进程消息，即使当利用最优路由的早期呼叫转接或晚期呼叫转接发生的时候。

本发明的另一个优点是可以将 PGS 提供给虚拟私人网（VPN）订户。

在本发明的第二方面，提出了一种处理与对移动电信网络的订户的呼叫相关的智能网服务的控制节点，该网络包括所述控制节点、HLR 和一个或多个 SCP；控制节点配置用于向所述 HLR 发送与所述呼叫相关的路由信息的一个或多个请求；控制节点还配置用于从所述 HLR 接收与所述服务相关联的多个服务触发元素，并且用于通过使用所述触发元素在所述一个或多个 SCP 中调用所述服务；控制节点进一步配置用于从所述一个或多个 SCP 接收与所述触发元素所关联的服务相关的信息。

在优选实施例中，控制节点包括 GMSC。无论如何，控制节点也可以包括诸如 MSC 或 SCP 的设备。

本发明的第三方面提出了一种计算机程序，该计算机程序包括致使计算机执行依照本发明的方法的程序指令。

计算机程序可以存储在载体上，并且可以包括致使计算机执行依照本发明的方法的计算机可执行指令。

计算机程序的载体可以是记录介质、计算机存储器、只读存储器或电载体信号。

本发明提出可以为对订户的特定呼叫类型提供多种 IN 服务。至此，HLR 可以已经注册了特定 IN 呼叫类型预订的多个指示（此后称为 IN 触发元素）。

附图说明

图 1 是移动电信网络中设备的当前技术配置的框图。

图 2 是依照本发明的方法和设备的信令图。

图 3 是依照本发明的设备的框图。

图 4 是本发明的方法实施例的信令图。

图 5 是本发明的方法实施例的信令图。

图 6 是本发明的方法实施例的信令图。

具体实施方式

为了本发明的目的，GMSC 中的 MT 呼叫处理可以分为两个逻辑部分：

（1） 被叫处理；

（2） 漫游支线处理。

被叫处理包括从 HLR 获取 T-CSI 并且调用第一 CAMEL 服务。第一 CAMEL 服务可以强加呼叫限制或者可以施加呼叫转接。通常，对于被呼叫订户漫游的情况，第一 CAMEL 服务也可以用于终止计费。HLR 也可以与 T-CSI 一起返回其它 IN 触发元素。

漫游支线处理包括从 HLR 获取 MSRN 并且将呼叫从 GMSC 路由到终止 MSC，在终止 MSC 被呼叫方在该时刻注册。注意“漫游支线”同等适用于订户在被访问公共陆地移动网络（VPLMN）和订户在归属公共陆地移动网络（HPLMN）中的情况。也就是说，在这个例子中“漫游”不与“在另一个网络或另一个国家中”相关联。

本发明提出了沿着上述区别的线路，为 MT 呼叫进行两个 IN 服务的调用。依照本发明，可以定义用于 MT 呼叫的两种类型的 IN 服务：

（1）需要对 MT 呼叫的控制并且可能需要影响该呼叫的路由的能力的 IN 服务。这些类型的 IN 服务还需要知道目的地订户的位置，从而可以施加计费。

（2）只要求到目的地订户的漫游支线的 IN 服务。这类 IN 服务只有在建立了漫游支线，即 GMSC 已经从 HLR 接收到 MSRN 的时候，才被调用。

如果 HLR 返回转接号码（FTN）而不是 MSRN，那么将不存在漫游支线，并且随后将不会调用与漫游支线相关的 IN 服务。

图 1 是移动电信网络中的设备的当前技术配置的框图。所示的实体至少在概念上属于不同于移动通信网络的智能网。智能网包括 HLR 111、SCP1 121、SCP2 122 和 GMSC 110。GMSC 110 与 SCP1 和 SCP2 以及 HLR 111 对接，以执行众所周知的 IN 触发功能。SCP1 和 SCP2 包括在处理移动被叫期间可以被顺序调用的智能网服务。

图 2 是依照本发明的方法和设备的信令图，其具有各种元件之间的

关系的概览。该方法包括以下步骤:

步骤 101 控制节点 110 向 HLR 111 发送与所述呼叫相关的路由信息的一个或多个请求;

步骤 102 HLR 111 向所述控制节点 110 发送与所述服务相关联的多个服务触发元素;

步骤 103 控制节点 110 使用所述触发元素在一个或多个服务控制点 121、122、123 中调用一个或多个服务;

步骤 104 所述一个或多个服务控制点 121、122、123 向所述控制节点 110 发送与所述触发元素所关联的一个或多个服务相关的信息。

图 3 是依照本发明的设备和它们的相互关系的框图。

所述块(设备)之间的线表示通信路径。HLR 111 可以与 GMSC 110 和 VMSC 112 通信。GMSC 可以与 SCP1 121 和其它随后被调用的 SCP(SCPn) 122 通信。GMSC 110 可以与 VMSC 112 通信。

图 4 是本发明的方法实施例的信令图,该实施例包括图 3 所示的设备之间的通信序列,所述设备包括 GMSC 110、HLR 111、多个 SCP121、122 和 VMSC 112。在这个例子中,订户预订了 CAMEL 服务并且另外预订了可能是 IN 服务的至少一个服务。对于这个例子,只示出了与两个 SCP 121、122 的通信。但是,可以为第三个 SCP 重复步骤 6-11,并且以此类推。以下步骤发生:

步骤 401 ISUP 初始地址消息(IAM)到达 GMAC 110; GMSC 110 分析 ISUP IAM 中的被呼叫方号码并且推导出该被呼叫方号码是属于它自己的网络的 MSISDN。

步骤 402 GMSC 110 向 HLR 111 发送 MAP 发送路由信息(SRI)。GMSC 110 在 MAP SRI 中指示它支持 CAMEL。

步骤 403 被呼叫方具有对用于 MT 呼叫处理的 CAMEL 服务的预订。结果是,HLR 111 向 GMSC 110 发送 MAP SRI-Res,其包括用于 MT 呼叫的 IN 触发信息,T-CSI。

步骤 404 GMSC 110 使用 T-CSI 来调用 CAMEL 服务。GMSC 110 例示内部 GSM 服务交换功能(gsmSSF)实体; gsmSSF 向 SCP 发送 CAP 初始检测点(IDP)。SCP1 121 的地址和与这个 IN 对话相关的其它数据从 T-CSI 获得。GsmSSF 功能与 GMSC 交互工作。基于在用户的预订中定义的并且从 HLR 发送给 GMSC 的信息,设置 GMSC 和 gsmSSF 内的服务触发。

这些触发用于指示 gsmSSF 何时应该与 gsmSCF 通信。这接下来将确定如何处理基于 IN 的服务。

步骤 405 SCP1 121 以 CAP 继续（CUE）响应，以便通知 GMSC 110 MT 呼叫处理可以继续，即可以将呼叫传递给被呼叫订户。SCP1 121 和 GMSC 110 之间的控制会话可以保持。SCP1 121 中的 CAMEL 服务不需要具有关于除了该 CAMEL 服务外当前执行的其它 IN 服务的知识。

步骤 406 GMSC110 向 HLR 111 发送第二询问，即向 HLR 111 发送第二 MAP SRI。第二 MAP SRI 包括“抑制 T-CSI”标志。

步骤 407 HLR 111 通过“抑制 T-CSI”的存在识别出该 MAP SRI 是第二 SRI，并且通过向被呼叫方当前所注册的 VMSC 112 发送 MAP 提供漫游号码（PRN）来响应。

步骤 408 VMSC 112 分配用于这个呼叫的 MSRN，并且通过向 HLR 111 发送 MAP PRN-Res 而向 HLR 111 返回该 MSRN。

步骤 409 HLR 111 通过向 GMSC 110 发送 MAP SRI 响应（SRI-Res）而将该 MSRN 转发给 GMSC 110。被呼叫订户预订了用于 MT 呼叫处理的第二 IN 服务。第二 IN 服务是如前面本发明的公开部分所述的漫游支线处理类型。HLR 111 在所述 MAP SRI-Res 中包括与这个第二 IN 服务相关联的 IN 触发信息。为了本发明的目的，这个第二 IN 触发信息命名为“RICK”（漫游支线 IN 种类关键字）。RICK 可以具有如 T-CSI 或 TICK（终止 IN 种类关键字）的结构。为了能够接收 RICK，GMSC 110 在第二 MAP SRI（步骤 6）中指示它支持这个信息元素，即它支持 RICK。“支持 RICK”的指示类似于“支持 TICK”的指示。从 GMSC 向 HLR 发送的“支持 TICK”向 HLR 表明它支持 TICK。TICK 具有与 T-CSI 可比的功能性；但是，TICK 不是标准化的。

步骤 410 GMSC 110 认识到 MSRN 伴随有 RICK。RICK 对于 GMSC 110 作为表明漫游支线应该服从 IN 服务的指示。因此，GMSC 110 通过向 SCPn 122 发送 CAP IDP，使用 RICK 调用 IN 服务。SCPn 122 的地址和与这个 IN 对话相关的其它数据从 RICK 获得。

步骤 411 SCPn 122 以 CAP CUE 响应，通知 GMSC 110 该 MT 呼叫处理可以继续，即可以建立到被呼叫订户的漫游支线。

步骤 412 GMSC 110 通过向目的地交换机发送 ISUP IAM，建立到被叫订户的漫游支线。该 ISUP IAM 包含从 HLR 111 接收到的 MSRN。

步骤 401-408 表示一般 GSM 呼叫处理。

步骤 409 表示对现有 MT 呼叫处理的改进。HLR 111 一般将只返回 MSRN 给 GMSC 110。步骤 409 对 MAP SRI-Res 添加了 RICK。

步骤 410 和 411 在现有漫游支线处理中不存在。这些步骤表示在 GMSC 110 中对用于 MT 呼叫处理的第二 IN 服务的调用。

当该呼叫被传递到被呼叫订户时，两个 IN 服务可以维持有效。作为向 GMSC 110 发送 T-CSI 的结果而触发的第一 IN 服务可以对整个呼叫维持有效，并且按照用于那个服务的 IN 协议所允许的具有完全可用的能力。

作为向 GMSC 110 发送 RICK 的结果而触发的第二 IN 服务也可以对整个呼叫维持有效。但是，这个 IN 服务应该使用具有某些限制的 IN 能力。作为一个例子，这个服务不应该应用呼叫转接，因为那将影响该呼叫的预付费服务。

本发明可以应用在不同类型的 GSM 呼叫转接上。通过取类似于个人问候服务（PGS）的服务作为例子，可以充分显示出这一点。在呼叫转接的情况下，呼叫的目的地发生变化。一些运营商要求当到语音邮箱的呼叫转接发生时，PGS 服务终止。

关于在呼叫转接的情况下终止 PGS 服务，基本存在两种类型的呼叫转接：早期呼叫转接（ECF）和晚期呼叫转接（LCF），当在 GMSC 110 中发生早期呼叫转接的时候，GMSC 110 没有从 HLR 111 接收用于这个呼叫的 MSRN 并且没有建立漫游支线。GMSC 110 将不建立到被呼叫方的漫游支线，并且作为结果，将不调用漫游支线 IN 服务。

在早期呼叫转接的情况中，HLR 111 不在第二 SRI 结果中返回 MSRN 并且依照本发明不返回 RICK。GMSC 110 现在将该呼叫转接到转接目的地，其可以是例如语音邮箱或者是呼叫结束服务。因为 HLR 111 没有返回 RICK，将不存在 PGS 调用。呼叫订户现在可以收听语音邮箱播放的任何通告，即使语音邮箱将 ISUP 应答消息（ISUP ANM）的生成推迟了限定的持续时间。

当在 VMSC 112 中发生晚期转接的时候，随后可以应用晚期呼叫转接的最佳路由（ORLCF）以便将呼叫处理返回给 GMSC 110。GMSC 110 终止该漫游支线，并且因而漫游支线 IN 服务同样将被终止。在晚期呼叫转接的情况下，所述呼叫已经被路由到被呼叫订户的目的地 MSC。当晚

期呼叫转接的情况发生，VMSC 112 可以向 GMSC 110 发送 MAP 恢复呼叫处理（RCH）；MAP RCH 的发送是 ORLCF 的一部分。

当 GMSC 110 接收到 MAP RCH 并且批准对 ORLCF 的请求，它释放漫游支线并且创建转接支线。呼叫方可以收听由转接目的地生成的任何通告。

一些运营商采用语音邮箱系统，由此初始通告是免费的。这可以通过令语音邮箱推迟 ISUP ANM 的生成来实现。如果 PGS 在这样的情况下保持有效，那么呼叫方将不会收听到在 ISUP 地址完成消息（ACM）和 ISUP ANM 之间播放的任何通告。原因是个人问候服务保持有效，直到检测到 ISUP ANM。在那种情况下将不会收听到语音邮箱的初始通告。

本发明解决了那个问题，因为在晚期呼叫转接联合 ORLCF 的情况下 PGS 将被终止。

如果晚期呼叫转接没有经受 ORLCF，那么漫游支线服务可以监视诸如呼叫进程（CPG）和 ACM 的 ISUP 消息。这些 ISUP 消息可以指示转接正在发生。

一些运营商应用 PGS 的服务节点解决方案。这意味着对于 PGS 订户，漫游支线需要通过特殊的服务节点（位于内嵌在用于漫游支线的 ISUP 通信链路内）路由。服务节点将把该呼叫广播给目的地 MSC。依照本发明可以实现通过服务节点的漫游支线的路由。利用 RICK 调用的 IN 服务可以为 MSRN 提供前缀，导致呼叫被通过所述服务节点路由。

可替换地，包括在 SRI-Res 中的 RICK 可以具有数字前缀的形式；诸如 GMSC 的交换节点在将该呼叫转接到下一个交换节点之前，将该 RICK 放置在 MSRN 的前面。

可以配置在这个转换节点中的 B-号码分析，使得 RICK 导致选择到所述服务节点的路由。

漫游支线的预订的或一般的 IN 服务的概念可以用于以下类型的服务：

- 个人问候：只有当漫游支线成功建立的时候需要播放个人问候；如果由于无论什么原因，漫游支线没有能够建立或者在应答之前终止，那么不需要个人问候。运营商可以希望在为呼叫分配 MSRN 之前调用 PGS。那样的效果可能是，当到第二被呼叫方的转接发生时，呼叫方将仍然听到第一方的个人问候。另外，这样的配置将具有可能没有收听

到呼叫转接通告的效果。

- 服务节点路由：对于特定订户，漫游支线可能需要通过服务节点被路由。

- 载体选择：订户可以预订只适用于漫游支线的载体选择服务。

当 HLR 111 向 GMSC 110 发送包括 MSRN 的 SRI-Res 时，它可以包括 RICK。作为可选的实施方式，HLR 111 可以应用在 SRI-Res 中包括 RICK 的标准，类似于借此 HLR 111 应用在第一 SRI-Res 中包括 T-CSI 的标准的情况。这些标准可以是例如：

- 只有当订户在 HPLMN 中的时候在 SRI-Res 中包括 RICK;
- 只有当入局呼叫是语音呼叫的时候在 SRI-Res 中包括 RICK。

不是所有的 MT 呼叫需要终止 IN 服务。类似的，不是所有的 MT 呼叫需要 RICK 服务。作为一个例子，当预付费订户在 HPLMN 中的时候，HLR 111 可以在 SRI 中抑制 T-CSI。结果是，将没有 MT 呼叫服务被触发。如果在这种情况下仍然需要调用漫游支线服务，那么 HLR 111 可以在第一 SRI-Res 中包括 RICK。GMSC 110 中对 RICK 的进一步处理如前所述。

图 5 是本发明的方法实施例的信令图，其中通过在 GMSC 110 建立漫游支线之前由 GMSC 110 向 HLR 111 询问多个（IN）服务来执行对多个服务的调用。在这个实施例中，HLR 111 在第一询问发送所述 IN 服务的所有信息。步骤 501-502 依照当前技术执行。在这里例子中涉及 3 个 SCP，尽管本发明可以应用于多个 SCP。

步骤 501 ISUP IAM 到达 GMSC 110。

步骤 502 GMSC 110 分析 ISUP IAM 中的被呼叫方号码并且推导出该被呼叫方号码是属于它自己的网络的 MSISDN。GMSC 110 向 HLR 111 发送 MAP SRI。GMSC 110 在 MAP SRI 中指示它支持 CAMEL。GMSC 可以支持多个 CAMEL 阶段。

步骤 503 被呼叫方具有对用于 MT 呼叫处理的 CAMEL 服务的预订。结果是，HLR 111 向 GMSC 110 发送 MAP SRI-Res，其包括用于 MT 呼叫的 IN 触发信息，T-CSI。

步骤 504 GMSC 110 使用 T-CSI 来调用 CAMEL 服务。GMSC 110 例示内部 gsmSSF 实体；gsmSSF 向 SCP 121 发送 CAP IDP。SCP1 121 的地址和与这个 IN 对话相关的其它数据从 T-CSI 获得。

步骤 505 SCP1 121 以 CAP 继续（CUE）或 CAP 连接（CON）响应，以便通知 GMSC 110 MT 呼叫处理可以继续，即可以将呼叫传递给被呼叫订户。依赖于 IN 服务的要求，SCP1 121 和 GMSC 110 之间的控制会话可以保持或者终止。SCP1 121 中的 CAMEL 服务不具有关于除了该 CAMEL 服务外当前执行的其它 IN 服务的知识。

步骤 506 GSMC 110 基于 T-CSI 通过调用第二 IN 服务响应，第二 IN 服务可以仍是 CAMEL 服务。SCPn 122 的地址从第二 T-CSI 获得。

步骤 507 SCP 以 CAP CUE 或 CAP CON 响应，以便通知 GMSC 110 该呼叫处理可以继续，即可以将呼叫传递给被呼叫订户。这里，同样的，SCP2 122 中的 CAMEL 服务不具有关于这个呼叫的第一服务和第三服务的知识。

步骤 508 GMSC 110 检查是否为该订户提供了其它 IN 服务；如果提供的有，那么它基于 T-CSI 通过调用第三 IN 服务进行响应，该第三 IN 服务还可以是 CAMEL 服务。SCP3 123 的地址从第三 T-CSI 获得。

步骤 509 SCP 123 以 CAP CUE 或 CAP CON 响应，以便通知 GMSC 110 该呼叫处理可以继续，即可以将呼叫传递给被呼叫订户。SCP3 123 中的 CAMEL 服务不具有关于这个呼叫的第一服务和第二服务的知识。

步骤 510 GMSC 110 检查是否为该订户提供了其它 IN 服务；如果没有用于该订户的更多 IN 服务，那么 GMSC 110 通过向 HLR 111 发送第二询问进行响应，即向 HLR 111 发送第二 MAP SRI。

步骤 511 HLR 111 识别出该 MAP SRI 是第二 SRI 并且通过向被呼叫方当前被注册的 VMSC 112 发送 MAP 提供漫游号码（PRN）进行响应。

步骤 512 VMSC 112 分配 MSRN，并且通过向 HLR 111 发送 MAP PRN-Res 而向 HLR 111 返回该 MSRN。

步骤 513 HLR 111 通过向 GMSC 110 发送 MAP RSI-Res 将 MSRN 转发给 GMSC 110。

步骤 514 GMSC 110 通过向目的地交换机发送 ISUP IAM 建立到被呼叫订户的漫游支线。ISUP IAM 包含从 HLR 111 接收到的 MSRN。

图 6 是本发明的方法实施例的信令图，由此为 MO 呼叫调用多个 IN 服务。在这个实施例中发生以下步骤：

步骤 601 订户 621 利用 MSC 623 在被访问 GSM 网络中注册。

步骤 602 MSC 623 联系订户 621 的归属 PLMN 中的 HLR 111。

步骤 603 HLR 111 向 MSC 623 发送用于 IN 服务的多个触发元素。这些触发元素与用于终端发起呼叫和移动转接呼叫的 IN 服务相关联。

步骤 604 订户 621 建立 MO 呼叫。

步骤 605 MSC 623 使用第一触发元素以调用在与所述第一触发元素相关联的 SCP1 121 中的第一 IN 服务。

步骤 606 SCP1 121 中的第一 IN 服务通过发送 CAP 继续消息或 CAP 连接消息将呼叫的控制交回 MSC 623。

步骤 607 MSC 623 使用来自触发元素列表的第二触发元素在 SCP2 122 中调用第二 IN 服务。

对 SCP2 122（步骤 607 和 608）和 SCP3 123（609、610）重复步骤 605 和 606，并且直到调用了所有指示的 IN 服务。MSC 623 中的呼叫处理一般继续步骤 611:

步骤 611 MSC 623 将该呼叫路由到目的地 627。任何调用的 IN 服务可以在该呼叫的整个持续时间保持有效，或者可以在较早的阶段终止。

本发明覆盖以下情景:

1） GMSC 中用于 MT 呼叫处理的 IN 服务调用后跟随 GMSC 中用于漫游支线的 IN 服务调用。

2） GMSC 中用于漫游支线的 IN 服务调用。

3） 如同（1），由此 HLR 在第一询问响应中发送多个 IN 服务触发元素，目的是这些多个触发元素用于与所述 MT 呼叫相关联的多个 IN 服务的调用。

4） 如同（1），由此 HLR 在第二询问响应中发送多个 IN 服务触发元素，目的是这些多个触发元素用于与所述漫游支线相关联的多个 IN 服务的调用。

5） 如同（2），由此 HLR 在第二询问响应中发送多个 IN 服务触发元素，目的是这些多个触发元素用于与所述漫游支线相关联的多个 IN 服务的调用。

6） 如同（1），由此（3）和（4）组合。

7） 如同（1），由此 HLR 在第一询问响应中发送多个 IN 服务触发元素，目的是这些多个触发元素中的一些用于与所述 MT 呼叫相关联的多个 IN 服务的调用，并且这些多个触发元素中的一些用于与所述漫游支线相关联的多个 IN 服务

的调用。

8） 只有当漫游支线建立的时候需要用于 MT 呼叫的某些 IN 服务。本发明提供实现这一点的工具。

9） 本发明可以用于在预订的基础上或者对于所有服务的订户通过 ISUP 服务节点路由漫游支线。

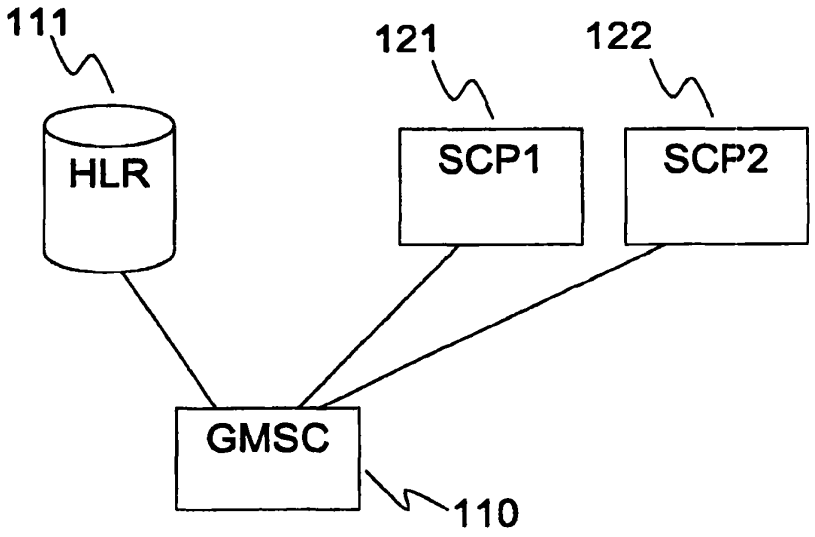


图 1

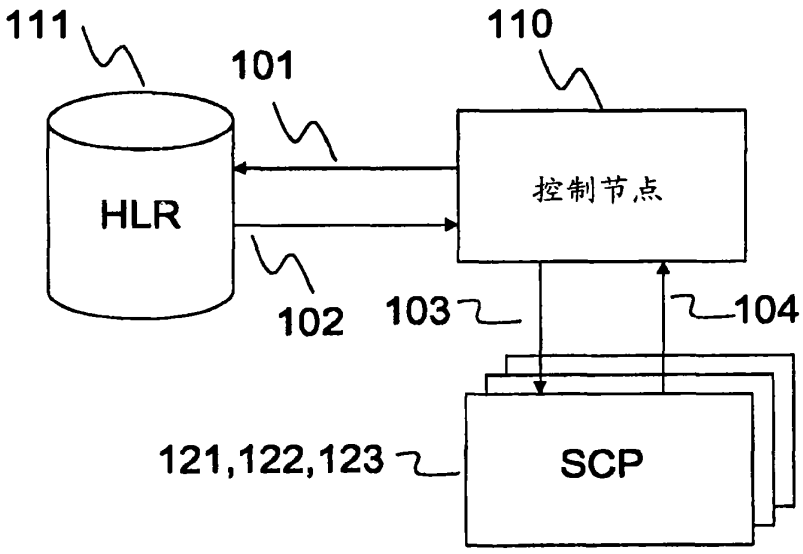


图 2

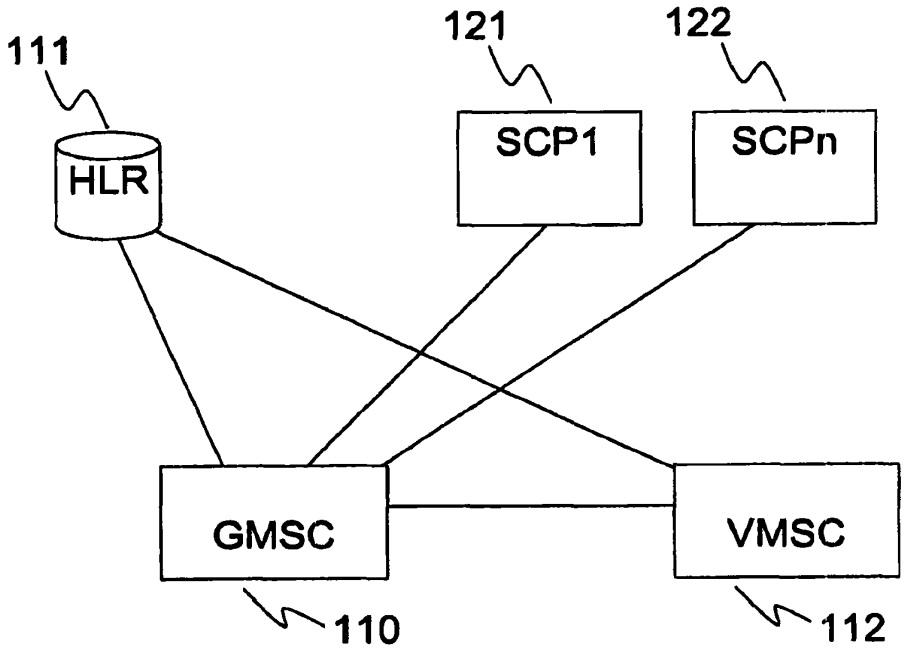


图 3

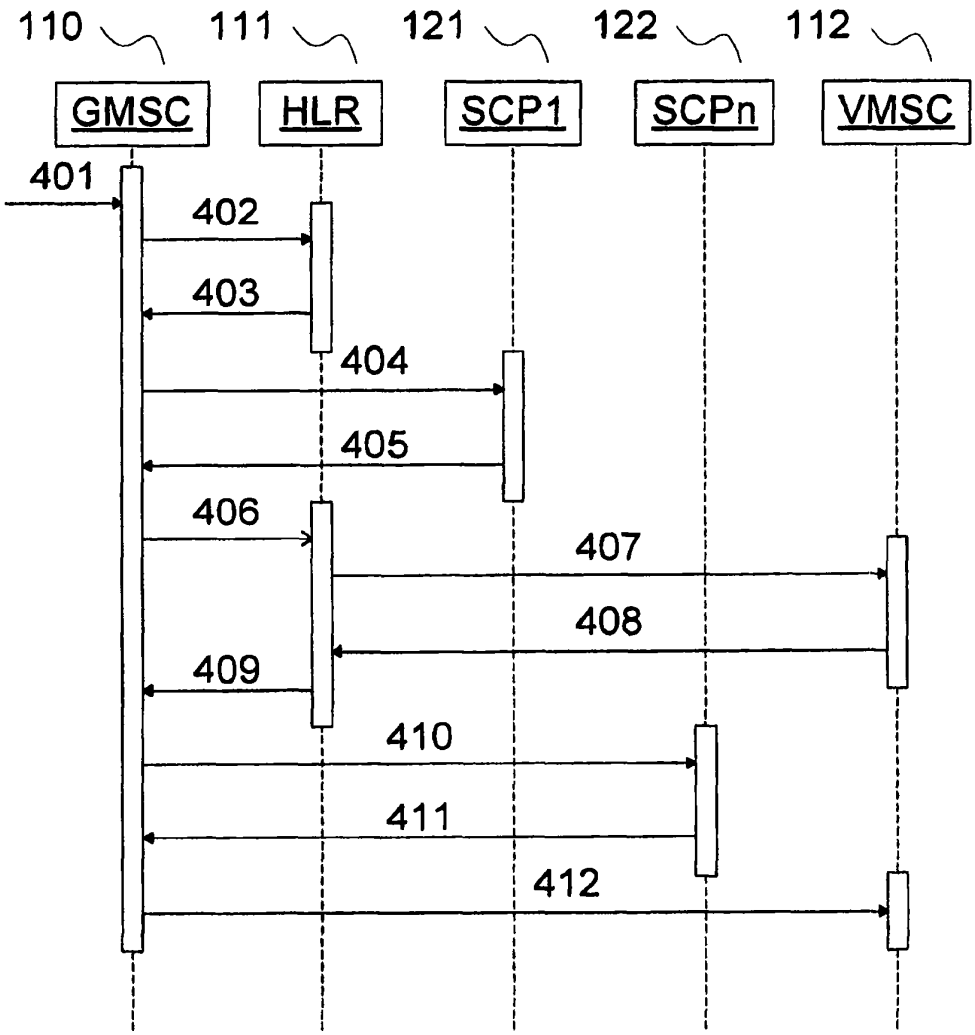

110
111
121
122
112
GMSC
HLR
SCP1
SCPn
VMSC
401
402
403
404
405
406
407
408
409
410
411
412

图 4

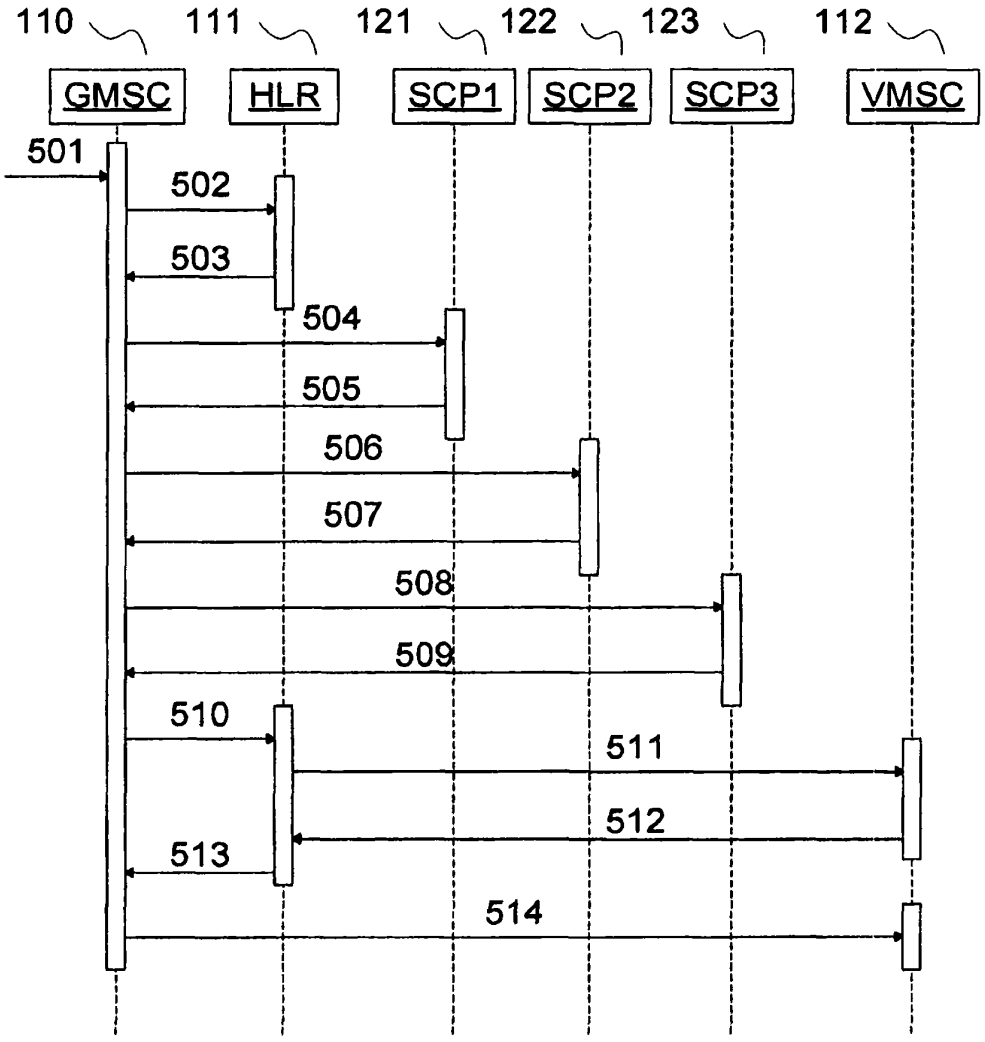

110
111
121
122
123
112
GMSC
HLR
SCP1
SCP2
SCP3
VMSC
501
502
503
504
505
506
507
508
509
510
511
512
513
514

图 5

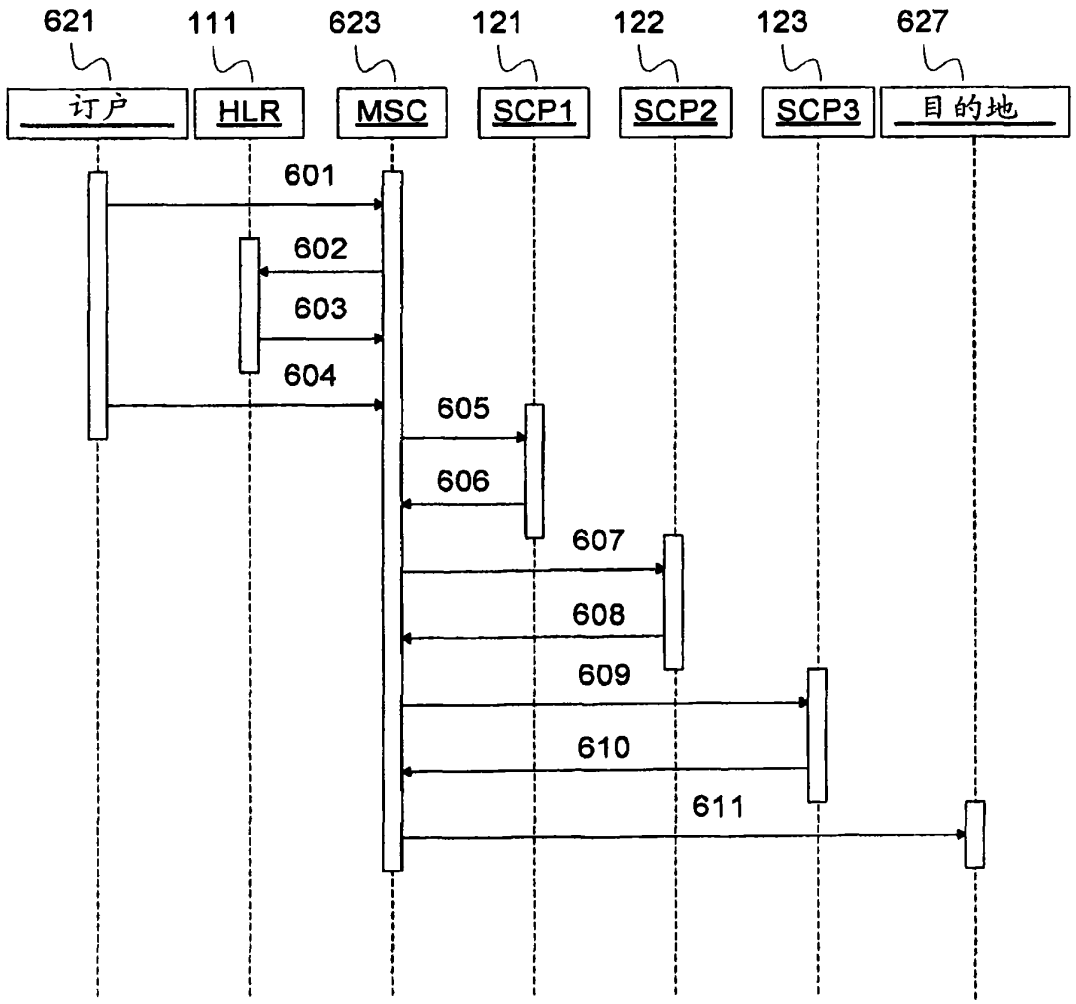

621
111
623
121
122
123
627
订户
HLR
MSC
SCP1
SCP2
SCP3
目的地
601
602
603
604
605
606
607
608
609
610
611

图 6

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 June 2007 (21.06.2007)

PCT

(10) International Publication Number
WO 2007/068288 A1

(51) International Patent Classification:
H04Q 3/00 (2006.01) *H04Q 7/24* (2006.01)

(21) International Application Number:
PCT/EP2005/056843

(22) International Filing Date:
16 December 2005 (16.12.2005)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **TELEFONAKTIEBOLAGET LM ERICSSON (publ)** [SE/SE]; S-16483 Stockholm (SE).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **NOLDUS, Rogier** [NL/NL]; Naardenstraat 46, NL-5045 ML Tilburg (NL). **SHARMA, Arvind** [NL/NL]; Esperenkamp 21, NL-5632 PX Eindhoven (NL).

(74) Agent: **NORIN, Klas**; Ericsson AB, Patent Unit Core Networks Kista, S-16480 Stockholm (SE).

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

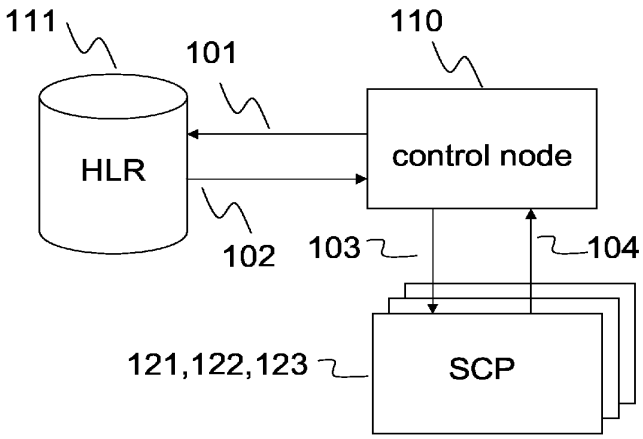
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT,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

Declaration under Rule 4.17:
— *of inventorship (Rule 4.17(iv))*

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: INTELLIGENT NETWORK SERVICES



(57) Abstract: A method and control node (110) and computer program are disclosed for handling Intelligent Network services associated with a call to a subscriber of a mobile telecommunications network, the network comprising said c ontrol node (110), a HLR 5 (111) and one or more SCPs (121, 122, 123). Said control node (110) a) sends (101) to said HLR (111) one or more requests for routing information associated with said call; b) receives (102) from said HLR (111) service trigger elements associated with said services; c) uses said trigger elements for invoking (103) said services in said one ore more SCPs (121, 122, 123); and d) receives (104) from said one or more 10 SCPs (121, 122, 123) information related to said services associated with said trigger elements.

WO 2007/068288 A1

INTELLIGENT NETWORK SERVICES

FIELD OF INVENTION

The invention relates to a method and control node for handling Intelligent Network services associated with a call to a subscriber of a mobile telecommunications network.

BACKGROUND

Intelligent Network services are well known in the state of the art telecommunications networks such as GSM (Global System for Mobile communications).

The central component of the Core Network subsystem of a GSM network is the Mobile services Switching Center (MSC). It acts like a switching node of the PSTN or ISDN, and additionally provides all the functionality needed to handle a mobile subscriber, such as registration, authentication, location updating, handovers, and call routing to a roaming subscriber. These services are provided in conjunction with several functional entities, which together form the Core Network subsystem. A Gateway MSC (GMSC) provides the connection to the fixed networks (such as the PSTN or ISDN). Signaling between functional entities in the Core Network subsystem uses Signaling System Number 7 (SS7), used for trunk signaling in ISDN and widely used in current public networks.

The Home Location Register (HLR) and Visitor Location Register (VLR), together with the MSC, provide the call-routing and roaming capabilities of GSM. The HLR contains all the administrative information of each subscriber registered in the corresponding GSM network, along with the current location of the mobile station. The location of the mobile station is typically in the form of the signaling address of the VLR associated with the mobile station. There is logically one HLR per GSM network, although it may be implemented as a distributed database.

The VLR contains selected administrative information from the HLR, necessary for call control and provision of the subscribed services, for each mobile station currently located in the geographical area controlled by the VLR and currently served by that VLR. Although each functional entity can be implemented as an independent unit, currently all manufacturers of switching equipment implement the VLR together with the MSC, so that the geographical area controlled by the MSC corresponds to that controlled by the VLR, thus simplifying the signaling required. The MSC contains no information about particular mobile stations; this information is stored in the location registers.

Next, a typical incoming call setup (mobile terminating call) in a GSM network is described.

When a subscriber places a call to a mobile phone, he dials the telephone number associated with the phone user, the so-called Mobile Station ISDN (MSISDN) number, and the call is routed to the mobile phone operator's Gateway MSC. A gateway is a node used to interconnect two networks. The gateway is often implemented in an MSC, in which case the MSC is referred to as the GMSC. The GMSC acts as the "entrance" from exterior portions of the Public Switched Telephone Network onto the provider's network.

As noted above, the phone is free to roam anywhere in the operator's network or on the networks of roaming partners, including in other countries. So the first job of the Gateway MSC is to determine the current location of the mobile phone in order to connect the call. It does this by consulting the HLR, which, as described above, knows which Visited Location Register (VLR) the phone is associated with at the moment, if any.

When the HLR receives this query message, it determines whether the call should be routed to another number (called a divert), or the call should be routed directly to the mobile station of the called subscriber.

If the owner of the phone has previously requested that all incoming calls be diverted to another number, which supplementary service is also known as Call Forwarding Unconditional (CFU) to a Forwarded-to-Number (FTN), then this FTN is stored in the HLR. If that is the case, then the FTN is returned to the Gateway MSC for immediate routing to that destination.

If the mobile station is not currently associated with a VLR (e.g. because the phone has been turned off), then the HLR returns a number known as the Call Forwarding Not Reachable (CFNRc) number to the GMSC, and the call is forwarded there. Many operators may set this value automatically to the phone's voice mail number, so that callers may leave a message.

Finally, if the HLR knows that the phone is in the jurisdiction of a particular VLR, then it will request a temporary number, a so called Mobile Station Roaming Number (MSRN) from that VLR. This number is relayed to the GMSC, which uses it to route the call to another MSC, called the Visited MSC (VMSC).

When the call is received by the VMSC, the MSRN is used to find the phone's record in the VLR. This record identifies the phone's location area. Paging occurs to all mobile phone masts in that area. When the subscriber's mobile responds, the exact location of the mobile is returned to the VMSC. The VMSC then forwards the call to the appropriate phone mast, and the phone rings. If the subscriber answers, a speech path is created through the VMSC and GMSC back to the network of the person making the call, and a normal telephone call follows.

It is also possible that the phone call is not answered. If the subscriber is busy on another call (and call waiting is not being used), then the VMSC routes the call to a pre-determined Call Forwarding Busy (CFB) number. Similarly, if the subscriber does not answer the call after a period of time (typically 30 seconds), then the VMSC routes the call to a pre-determined Call Forwarding No Reply (CFNRy) number. Once again, the operator may decide to set this value by default to the voice mail of the mobile so that callers can leave a message.

An Intelligent Network (IN) is a network that is coupled to a telecommunications network that enables operators to deploy operator-specific Value Added Services (VAS). The intelligence that resides in the switch is augmented by intelligence from the Intelligent Network, which is placed in computer nodes that are distributed throughout the network. This provides the network operator with the means to develop, deploy and control services more efficiently. New services can be rapidly introduced into the telecommunications network. Once introduced, services are easily customized to meet individual customers' needs.

IN services are typically provided by a Service Control Point (SCP). An SCP is a control computer that communicates with other nodes and entities in the telecommunications network. The SCP comprises the service logic of one or more IN services and optionally IN service subscription data that allows the SCP to execute an IN service in accordance with the specific settings of a subscriber, i.e. tailor the service execution to the subscriber. When a call is established, the telecommunications network may query the SCP and ask for instructions for handling this call. For instance, an SCP is consulted to provide the translation of an 800 number to an actual phone number and to bill the owner of the 800 number for the call. SCPs may be physically separated from other components of the Intelligent Network or may be combined with these other components into a single node.

In a GSM network the IN service subscription information is stored in the HLR. Two types of information reside in the HLR: (1) static subscriber information and (2) dynamic subscriber information. The latter is e.g. needed to allow incoming calls to be routed to the mobile subscriber. The HLR stores, amongst others:

- the International Mobile Subscriber Identity (IMSI); an internal subscriber identity used only by the network;
- MSISDN number;
- VLR address;
- subscriber data on supplementary services.

IN services may be divided into two categories. One category comprises services to be invoked for subscribers who initiate a call (Mobile Originated Call – MOC). These services are called Mobile Originating (MO) services. An example of an MO service is outgoing call screening.

Each IN service subscriber is marked in his HLR with an Originating CAMEL Subscription Information (O-CSI) element, which is used to identify a specific service at the SCP. The O-CSI initiates the triggering of the MOC service as soon as the subscriber initiates a MO call. In the above example CAMEL is deployed, which stands for “Customised Applications for Mobile network Enhanced Logic”. CAMEL was developed as a standard for extending landline IN telephony services such as call waiting and call forwarding to GSM mobile phones.

The other category comprises services to be invoked for subscribers who receive a call (Mobile Terminated Call – MTC). These services are called mobile terminating (MT) services. Examples of mobile terminating services are call diversion services and Personal Greeting Service (PGS). PGS is a service that is associated with a roaming leg. PGS entails that when a signalling connection is established between a GMSC and VMSC (a so called "roaming leg"), then a personalised greeting is played to the calling party. The personalised greeting replaces the conventional alerting tone ("ring tone"). As such, the personalised greeting is primarily related to the establishment of the roaming leg; the ring tone becomes active only when the roaming leg is established and the called party is alerted. Each IN service subscriber is marked in his HLR with a Terminating CAMEL Subscription Information (T-CSI) flag, which is used to identify a specific service at the SCP. This initiates the triggering of the MTC service during a call attempt to the subscriber.

According to the state of the art, a control node may query a HLR during MTC handling to obtain instructions from the HLR. The control node may be a GMSC. In response to the query by the control node, the HLR may send IN trigger information for the terminating call. The IN trigger information exchanged between the HLR and the control node has been standardized. For example T-CSI is the GSM standardized IN trigger information for terminating calls, as specified by 3GPP (3rd Generation Partnership Project) in 3GPP TS 29.002. IN trigger information comprises among others the address of the SCP where the IN service resides and the service key, which identifies a particular IN service within the SCP.

The control node uses the IN trigger information to invoke the IN service in the SCP as specified for the subscriber in the IN trigger information. In response to the service invocation, the SCP sends an instruction to the control node to e.g. continue call set up or to terminate the call depending on the outcome of the service execution.
Current networks are typically arranged to handle a single invocation of an IN service for an MTC. Recent developments show however, that there is a need to invoke two or more IN services during terminating call handling.

Patent application WO00/25528 discloses a Service Interaction Manager, which is included in an SCP. The task of the Service Interaction Manager is to determine which

of the available services in the SCP should be executed for a subscriber and to invoke those services in a particular sequence.

SUMMARY

It is an object of the invention to provide a method and devices that overcome the drawbacks of the state of the art by permitting subscribers to have more than one IN Service for one call.

In a first aspect of the invention a method is proposed for handling Intelligent Network services associated with a call to a subscriber of a mobile telecommunications network, the network comprising a control node, a Home Location Register and one or more Service Control Points, the method comprising the steps of:

a. said control node sending to said Home Location Register, one or more requests for routing information associated with said call;
b. said control node receiving from said Home Location Register service trigger elements associated with said services;
c. said control node using said trigger elements for invoking said services in said one ore more Service Control Points;
d. said control node receiving from said one or more Service Control Points information related to said services associated with said trigger elements.

In this way multiple service trigger elements may be handled for a subscriber who is subscribed to one or more IN services pertaining to one call of the subscriber. IN Services need not be aware of the existence of one or more other IN services in that control node for that call. In other words, a first service does not need to know whether a second service will be invoked and vice versa. Since the services do not require knowledge about the possible invocation of other IN services for this call, the services may run on different platforms and may be supplied by different vendors.

There are several embodiments of the invention.

For example, the invention may provide for a Home Location Register to send a first service trigger element of said multiple service trigger elements, in response to a first request for routing information and a second service trigger element of said multiple service trigger elements in response to a second request for routing information.

The first request for routing information may comprise:

- MSISDN number of the subscriber.

The response to the first request for routing information may comprise:

- the first service trigger element.

The second request for routing information may comprise:

- MSISDN number of the subscriber;
- an indication that the HLR shall suppress the first service trigger element in the response. This indication may e.g. be the "suppress T-CSI" parameter.

The response to the second request for routing information may comprise:

- an MSRN to be used for the call to the served subscriber;
- the second service trigger element;
- a prefix or a suffix to the MSRN of the subscriber.

The MAP message may be sent from the HLR to a GMSC in multiple Signalling Connection Control Part messages, due to MAP segmentation. A first service, for example a pre-paid charging service, is executed in a first service control point and a second service, for example PGS, is executed in a second SCP.

In this way the pre-paid service and PGS may be offered to the same subscriber; the pre-paid service and PGS may run on different platforms and are not related to one another.

When the present invention is used for PGS, the calling subscriber may hear any call progress message even when early call forwarding or late call forwarding with optimal routing takes place.

Another advantage of the invention is, that PGS may be offered to Virtual Private Network (VPN) subscribers.

In a second aspect of the invention a control node is proposed for handling Intelligent Network services associated with a call to a subscriber of a mobile telecommunications network, the network comprising said control node, an HLR and one or more SCPs; the control node configured to send to said HLR one or more requests for routing information associated with said call; the control node further configured to receive from said HLR multiple service trigger elements associated with said services, and for invoking said services in said one ore more SCPs by using said trigger elements;

the control node further configured to receive from said one or more SCPs information related to said services associated with said trigger elements.

In a preferred embodiment the control node comprises a GMSC. The control node may however also comprise a device such as an MSC or an SCP.

A third aspect of the invention proposes a computer program, comprising program instructions for causing a computer to perform the method according to the invention.
The computer program may be stored on a carrier and may comprise computer executable instructions for causing a computer to perform the method according to invention.
The carrier of the computer program may be a record medium, computer memory, read-only memory or an electrical carrier signal.

The present invention proposes that multiple IN services may be provided for a particular call type to a subscriber. Hereto, an HLR may have registered multiple indications of particular IN call type subscriptions (hereinafter referred to as IN trigger elements).

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a block diagram of a prior art configuration of devices in a mobile telecommunications network.
Figure 2 is a signalling diagram of the method and devices according to the present invention.
Figure 3 is a block diagram of devices according to the present invention.
Figure 4 is a signalling diagram of an embodiment of the method of the present invention.
Figure 5 is a signalling diagram of an embodiment of the method of the present invention.
Figure 6 is a signalling diagram of an embodiment of the method of the present invention.

DETAILED DESCRIPTION

For the purpose of the present invention, MT call handling in the GMSC may be divided in two logical parts:

(1) Terminating call handling;

(2) Roaming leg handling.

The terminating call handling includes the retrieving of T-CSI from the HLR and the invocation of the first CAMEL service. The first CAMEL service may enforce call restriction or may apply call forwarding. Typically, this first CAMEL service is also used for terminating charging, for the case that the called subscriber is roaming. The HLR may also return other IN trigger elements in combination with T-CSI.

The roaming leg handling includes the retrieving of the MSRN from HLR and the routing of the call from the GMSC to the terminating MSC, where the called party is registered at that moment. It is noticed that "roaming leg" is equally applicable for the case that the subscriber is in the Visited Public Land Mobile Network (VPLMN) and for the case that the subscriber is in the Home Public Land Mobile Network (HPLMN). I.e. "roaming" shall in this case not be associated with "being in another network or in another country".

The present invention proposes that the invocation of two IN services for an MT call is done along the line of above-described distinction. According to the present invention, two types of IN services for MT call may be defined:

(1) IN services that need control over the MT call and that may need the capability to influence the routing of the call. These kind of IN services also need to know the location of the destination subscriber, so charging may be applied.

(2) IN services that are required only for the roaming leg to the destination subscriber. This type of IN service is invoked only when a roaming leg is established, i.e. the GMSC has received an MSRN from the HLR.

If the HLR returns a Forwarded-to-Number (FTN) instead of an MSRN, then there will not be a roaming leg and consequently, no roaming leg-associated IN service will be invoked.

Figure 1 is a block diagram of a prior art configuration of devices in a mobile telecommunications network. The shown entities belong, at least conceptually, to an intelligent network that is distinct from the mobile communications network. The intelligent network includes HLR 111, SCP1 121, SCP2 122 and GMSC110. GMSC 110 interfaces to SCP1 and SCP2 as well as to HLR 111 for performing well known IN triggering functions. SCP1 and SCP2 contain intelligent network services that may be invoked sequentially during the handling of a mobile terminating call.

Figure 2 is a signalling diagram of the method and devices according to the present invention with a general overview of relations between various elements. The method comprises next steps:

Step 101 A control node 110 sends to a HLR 111, one or more requests for routing information associated with said call;

Step 102 The HLR 111 sends to said control 110 node multiple service trigger elements associated with said services;

Step 103 The control node 110 uses said trigger elements to invoke one or more services in one ore more Service Control Points 121, 122, 123;

Step 104 The one or more Service Control Points 121, 122, 123 sends to said control node 110 information related to on one or more services associated with said trigger elements.

Figure 3 is a block diagram of devices and their interrelations according to the present invention.

The lines between the blocks (devices) represent communication paths. HLR 111 may communicate with GMSC 110 and to VMSC 112. GMSC may communicate with SCP1 121 and other subsequently invoked SCPs (SCPn) 122. GMSC 110 may communicate with VMSC 112.

Figure 4 is a signalling diagram of an embodiment of the method of the present invention comprising a communication sequence between the devices as shown in figure 3, comprising GMSC 110, HLR 111, multiple SCPs 121, 122 and a VMSC 112. In this example a subscriber is subscribed to a CAMEL service and additionally to at least one service, which may be an IN, service. For this example only the communication with two

SCPs 121, 122 is shown. However, steps 6-11 may be repeated for a third SCP and so on. The following steps occur:

Step 401 ISUP Initial Address Message (IAM) arrives at the GMSC 110; the GMSC 110 analyses the Called Party Number in ISUP IAM and deduces that the Called Party Number is an MSISDN belonging to its own network.

Step 402 The GMSC 110 sends MAP Send Routing Information (SRI) to the HLR 111. The GMSC 110 indicates in MAP SRI that it supports CAMEL.

Step 403 The called subscriber has a subscription to a CAMEL service for MT call handling. As a result, the HLR 111 sends MAP SRI-Res to the GMSC 110, including the IN trigger information for MT calls, T-CSI.

Step 404 The GMSC 110 uses T-CSI to invoke a CAMEL service. The GMSC 110 instantiates an internal GSM Service Switching Function (gsmSSF) entity; the gsmSSF sends CAP Initial Detection Point (IDP) to the SCP. The address of the SCP1 121, and other data related to this IN dialogue, is obtained from T-CSI. The gsmSSF function interworks with the GMSC. Based on information defined in the user's subscription, and sent from the HLR to the GMSC, service triggers within the GMSC and gsmSSF are set. These triggers are used to dictate when the gsmSSF shall communicate with the gsmSCF. This in turn will determine how IN based services are handled.

Step 405 The SCP1 121 responds with CAP Continue (CUE), to inform the GMSC 110 that MT call handling may continue, i.e. the call may be delivered to the called subscriber. The control dialogue between SCP1 121 and GMSC 110 may be retained. The CAMEL service in SCP1 121 does not need to have knowledge about other IN services than the CAMEL service it's currently executing.

Step 406 The GMSC 110 sends a second interrogation to the HLR 111, i.e. sends a second MAP SRI to the HLR 111. The second MAP SRI includes the flag "suppress T-CSI".

Step 407 The HLR 111 recognizes the MAP SRI as a second SRI, by virtue of the presence of "suppress T-CSI", and responds by sending MAP Provide

Roaming Number (PRN) to the VMSC 112 where the called party is currently registered.

Step 408 The VMSC 112 allocates an MSRN for this call and returns the MSRN to the HLR 111, by sending MAP PRN-Res to the HLR 111.

Step 409 The HLR 111 forwards the MSRN to the GMSC 110, by sending MAP SRI Response (SRI-Res) to the GMSC 110. The called subscriber subscribes to a second IN service for MT call handling. The second IN service is of the type Roaming Leg handling, as described in an earlier part of the present invention disclosure. The HLR 111 includes the IN trigger information associated with this second IN service, in the MAP SRI-Res. For the purpose of the present invention, this second IN trigger information is named "RICK" (Roaming leg IN Category Key). RICK may have the structure as T-CSI or TICK (Terminating IN Category Key). In order to be able to receive RICK, the GMSC 110 would have indicated in the 2nd MAP SRI (step 6) that it supports this information element, i.e. it supports RICK. This indication of "RICK support" is similar to the indication of "TICK support". The "TICK support", which is sent from GMSC to HLR, indicates to HLR that it supports the TICK. The TICK has functionality that may be compared with T-CSI; TICK is, however, not standardised.

Step 410 The GMSC 110 recognizes that the MSRN is accompanied by a RICK. The RICK serves as an indication for the GMSC 110 that the roaming leg shall be subject to an IN service. The GMSC 110 therefore uses RICK to invoke an IN service, by sending CAP IDP to the SCPn 122. The address of the SCPn 122, and other data related to this IN dialogue, is obtained from RICK.

Step 411 The SCPn 122 responds with CAP CUE, to inform the GMSC 110 that MT call handling may continue, i.e. the roaming leg towards the called subscriber may be established.

Step 412 The GMSC 110 establishes the roaming leg towards the called subscriber, by sending ISUP IAM towards the destination exchange. The ISUP IAM contains the MSRN that was received from the HLR 111.

Steps 401 – 408 represent normal GSM call handling.

Step 409 represents an enhancement to the existing MT call handling. The HLR 111 will normally return only the MSRN to the GMSC 110. Step 409 adds the RICK to the MAP SRI-Res.

Step 410 and step 411 do not exist in existing Roaming Leg handling. These steps represent the invocation of the second IN service for the MT call handling in the GMSC 110.

When the call is delivered to the called subscriber, the two IN services may remain active. The first IN service, triggered as a result of the sending of T-CSI to the GMSC 110, may remain active for the entire call and has the full capability available as allowed by the IN protocol used for that service.

The second IN service, triggered as a result of the sending of RICK to the GMSC 110, may also remain active for the entire call. This IN service shall, however, use the IN capability with certain restrictions. As an example, this service shall not apply call forwarding, as that would affect a pre-paid service for the call.

The present invention may be applied on various types of GSM call forwarding. This may be shown most adequately by taking a service like Personal Greeting Service (PGS) as an example. In the case of call forwarding, the destination of the call changes. Some operators require that the PGS service be terminated when call forwarding to a voice mailbox takes place.

With regard to terminating a PGS service in a call forwarding situation there are basically two types of call forwarding: Early call forwarding (ECF) and Late Call Forwarding (LCF)

When early call forwarding takes place in the GMSC 110, the GMSC 110 does not receive an MSRN form the HLR 111 for this call and no roaming leg is established. The GMSC 110 will not establish a roaming leg to the called party and as a result, no roaming-leg IN service will be invoked.

In the case of early call forwarding, the HLR 111 does not return an MSRN in the second SRI Result and, according to the present invention, does not return the RICK. The GMSC 110 now forwards the call to the forwarded-to destination, which may e.g. be a voice mailbox or call completion service. Since the HLR 111 has not returned RICK,

there will not be a PGS invocation. The calling subscriber may now hear any announcement that is played by the voice mailbox, even when the voice mailbox defers the generation of the ISUP Answer Message (ISUP ANM) for a defined duration.

When late call forwarding takes place in the VMSC 112, then Optimal Routing of Late Call Forwarding (ORLCF) may be applied to return the call handling to the GMSC 110. The GMSC 110 terminates the roaming leg and hence, the roaming-leg IN service will be terminated as well. In the case of late call forwarding, the call is already routed to the destination MSC of the called subscriber. When the late call forwarding condition occurs, the VMSC 112 may send MAP Resume Call Handling (RCH) to the GMSC 110; the sending of MAP RCH is part of ORLCF.

When the GMSC 110 receives MAP RCH and approves the request for ORLCF, it releases the roaming leg and creates a forwarded leg. The calling party may hear any announcement generated by the forwarded-to destination.

Some operators deploy a voice mailbox system whereby the initial announcement is free of charge. This may be accomplished by having the voice mailbox defer the generation of the ISUP ANM. If PGS remains active in such situation, then the calling party will not hear any announcement that is played between ISUP Address Complete Message (ACM) and ISUP ANM. Reason is that the personal greeting remains active until the ISUP ANM is detected. The initial announcement of the voice mail would in that case not be heard.

The present invention resolves that problem, since PGS will be terminated in the case of late call forwarding in combination with ORLCF.

If late call forwarding is not subject to ORLCF, then the Roaming Leg service may monitor for ISUP messages such as Call Progress (CPG) and ACM. These ISUP messages may indicate that forwarding is taking place.

Some operators apply a service node solution for PGS. This means that for PGS subscribers, the roaming leg needs to be routed through a special service node (located in-line with the ISUP traffic link for the roaming leg). The service node will propagate the call to the destination MSC. The routing of the roaming leg through a service node may be accomplished in accordance with the present invention. The IN service that is

invoked with RICK may provide a prefix for the MSRN, resulting in that the call is routed through the service node.

Alternatively, the RICK that is included in the SRI-Res may have the form of a number prefix; a switching node such as a GMSC places the RICK in front of the MSRN, prior to forwarding the call to a next switching node.

The B-number analysis in this transition node may be configured such that the RICK results in the selection of a route to the service node.

The concept of a subscribed or generic IN service for a roaming leg may be used for the following type of services:

- Personal greeting: the playing of the personal greeting is required only when the roaming leg is successfully established; if the roaming leg can, for whatever reason, not be established or is terminated before answer, then the personal greeting is not required. An operator may wish to invoke PGS prior to the allocation of a MSRN for the call. The effect of that may be that when forwarding to a second called party takes place, the calling party will still hear a first party's personalised greeting. In addition, such configuration would have the effect that call forwarding announcements may not be heard.
- Service-node routing: for a particular subscriber, the roaming leg may need to be routed through a service node.
- Carrier selection: a subscriber may subscribe to a carrier selection service that is applicable for roaming leg only.

When the HLR 111 sends SRI-Res to GMSC 110 including MSRN, it may include RICK. As an implementation option, the HLR 111 may apply criteria for the inclusion of RICK in SRI-Res, similar to the case whereby the HLR 111 applies criteria for the inclusion of T-CSI in the first SRI-Res. These criteria may e.g. be:

- include RICK in SRI-Res only when subscriber is in HPLMN;
- include RICK in SRI-Res only when the incoming call is a speech call

Not all MT calls need a terminating IN service. Likewise, not all MT calls need a RICK service. As an example, when a pre-paid subscriber is in the HPLMN, the HLR

111 may suppress T-CSI in SRI. As a result, there will not be a MT call service triggered. If the invocation of the Roaming leg service is still required in this case, then the HLR 111 may include RICK in the first SRI-Res. The further handling of RICK in the GMSC 110 is as described earlier.

Figure 5 is a signalling diagram of an embodiment of the method of the present invention, wherein the invocation of multiple services is performed by a GMSC 110 interrogating an HLR 111 for multiple (IN) services before the GMSC 110 sets up the roaming leg. In this embodiment the HLR 111 sends all the information of the IN services at the first interrogation. Steps 501-502 are performed according to the current state of the art. In this example 3 SCPs are involved, although the invention is applicable to multiple SCPs.

Step 501 ISUP IAM arrives at the GMSC 110.

Step 502 The GMSC 110 analyses the Called Party Number in ISUP IAM and deduces that the Called Party Number is an MSISDN belonging to its own network. The GMSC 110 sends MAP SRI to the HLR 111. The GMSC 110 indicates in MAP SRI that it supports CAMEL. The GMSC may support multiple CAMEL phases.

Step 503 The called subscriber has a subscription to a CAMEL service for MT call handling. As a result, the HLR 111 sends MAP SRI-Res to the GMSC 110 including IN trigger information for MT calls, T-CSI.

Step 504 The GMSC 110 uses T-CSI to invoke a CAMEL service. The GMSC 110 instantiates an internal gsmSSF entity; the gsmSSF sends CAP IDP to the SCP 121. The address of the SCP1 121, and other data related to this IN dialogue, is obtained from T-CSI.

Step 505 The SCP1 121 responds with CAP Continue (CUE) or CAP Connect (CON), to inform the GMSC 110 that MT call handling may continue, i.e. the call may be delivered to the called subscriber. The control dialogue between SCP1 121 and GMSC 110 may be retained or terminated, depending on IN service requirements. The CAMEL service in SCP1 121 has no knowledge about other IN services than the CAMEL service that it is currently executing.

Step 506 The GMSC 110 responds by invoking a second IN service, which could again be a CAMEL service, based on T-CSI. The address of SCPn 122 is obtained from the second T-CSI.

Step 507 The SCP responds with CAP CUE or CAP CON, to inform the GMSC 110 that call handling may continue, i.e. the call may be delivered to the called subscriber. Here as well, the CAMEL service in SCP2 122 has no knowledge about the first service and the third service for this call.

Step 508 The GMSC 110 checks whether further IN services are provisioned for the subscriber; if they are, then it responds by invoking the third IN service, which could again be a CAMEL service, based on T-CSI. The address of SCP3 123 is obtained from the third T-CSI.

Step 509 The SCP 123 responds with CAP CUE or CAP CON, to inform the GMSC 110 that call handling may continue, i.e. the call may be delivered to the called subscriber. The CAMEL service in SCP3 123 has no knowledge about the first service and the second service for this call.

Step 510 The GMSC 110 checks whether further IN services are provisioned for the subscriber; if there are no more IN services for the subscriber, then the GMSC 110 responds by sending a second interrogation to the HLR 111, i.e. sends a second MAP SRI to the HLR 111.

Step 511 The HLR 111 recognises the MAP SRI as a second SRI and responds by sending MAP Provide Roaming Number (PRN) to the VMSC 112 where the called party is currently registered.

Step 512 The VMSC 112 allocates an MSRN and returns the MSRN to the HLR 111, by sending MAP PRN-Res to the HLR 111.

Step 513 The HLR 111 forwards the MSRN to the GMSC 110, by sending MAP SRI-Res to the GMSC 110.

Step 514 The GMSC 110 establishes the roaming leg towards the called subscriber, by sending ISUP IAM towards the destination exchange. The ISUP IAM contains the MSRN that was received from the HLR 111.

Figure 6 is a signalling diagram of an embodiment of the method of the present invention, whereby multiple IN services are invoked for an MO call. The following steps occur in this embodiment.

Step 601 A subscriber 621 registers with an MSC 623 in a visited GSM network.

Step 602 The MSC 623 contacts the HLR 111 in the Home PLMN of the subscriber 621.

Step 603 HLR 111 sends multiple trigger elements for IN services to the MSC 623. These trigger elements are associated to IN services for mobile originating calls and mobile forwarding calls.

Step 604 The subscriber 621 establishes an MO call.

Step 605 The MSC 623 uses a first trigger element to invoke a first IN service in SCP1 121 associated with the first trigger element.

Step 606 The first IN service in SCP1 121 gives control of the call back to the MSC 623, by sending a CAP Continue message or a CAP Connect message

Step 607 The MSC 623 uses the second trigger element from the list of trigger elements to invoke a second IN service in SCP2 122.

The steps 605 and 606 are repeated with SCP 2 122 (steps 607, 608) and SCP3 123 (609, 610) and further, until all indicated IN services are invoked. Call processing in MSC 623 continues with step 611 as normal:

Step 611 The MSC 623 routes the call to the destination 627. Any of the invoked IN services may remain active for the entire duration of the call, or may terminate at an earlier stage.

The following scenarios are covered by the invention:

1) IN service invocation in GMSC for MT call handling, followed by IN service invocation in GMSC for roaming leg.
2) IN service invocation in GMSC for roaming leg.

3) As (1), whereby the HLR sends multiple IN service trigger elements in the first interrogation response, with the purpose that these multiple trigger elements are used for the invocation of multiple IN services associated with the MT call.

4) As (1), whereby the HLR sends multiple IN service trigger elements in the second interrogation response, with the purpose that these multiple trigger elements are used for the invocation of multiple IN services associated with the roaming leg.

5) As (2), whereby the HLR sends multiple IN service trigger elements in the second interrogation response, with the purpose that these multiple trigger elements are used for the invocation of multiple IN services associated with the roaming leg.

6) As (1), whereby (3) and (4) are combined.

7) As (1), whereby the HLR sends multiple IN service trigger elements in the first interrogation response, with the purpose that some of these multiple trigger elements are used for the invocation of multiple IN services associated with the MT call and some of these multiple trigger elements are used for the invocation of multiple IN services associated with the roaming leg.

8) Certain IN services for MT calls are required only when a roaming leg is established. The present invention offers the tools to accomplish this.

9) The present invention may be used to route a roaming leg through an ISUP service node on a subscription basis or generically for all served subscribers.

CLAIMS

1. A method for handling Intelligent Network services associated with a call to a subscriber of a mobile telecommunications network, the network comprising a control node (110), a Home Location Register (111) and one or more Service Control Points (121, 122, 123) , the method comprising the steps of:
   a. said control node (110) sending (101) to said Home Location Register (111), one or more requests for routing information associated with said call;
   b. said control node (110) receiving (102) from said Home Location Register (111) service trigger elements associated with said services;
   c. said control node (110) using said trigger elements for invoking (103) said services in said one ore more Service Control Points (121, 122, 123);
   d. said control node (110) receiving (104) from said one or more Service Control Points (121, 122, 123) information related to said services associated with said trigger elements.

2. The method according to claim 1, wherein said Home Location Register (111) sends a first service trigger element of said multiple service trigger elements in response to a first request for routing information and a second service trigger element of said multiple service trigger elements in response to a second request for routing information.

3. The method according to claim 1, wherein said Home Location Register (111) sends said multiple service trigger elements in response to a first request for routing information.

4. The method according to claim 2 or 3, wherein said Home Location Register (111) sends the requested routing information in response to a second request for routing information.

5. The method according to any of the claims 2-4, wherein said second request for routing information is associated with the establishment of a signalling

connection between said control node (110) and a Visited Mobile services Switching Center (112).

6. The method according to any one of the preceding claims, wherein said requested routing information comprises a Mobile Station Roaming Number to be used for the call to said subscriber.

7. The method according to any one of the preceding claims, wherein a plurality of said service trigger elements is comprised in one Mobile Application Part message.

8. The method according to claim 7, wherein said one Mobile Application Part message is sent from said Home Location Register (111) to said Control Node in multiple Signalling Connection Control Part messages, due to Mobile Application Part segmentation.

9. The method according to any of the claims 1-6, wherein one or more of said service trigger elements is included in a Mobile Station Roaming Number as a prefix or a suffix.

10. The method according to any of the claims 1-6, wherein said service trigger elements comprise separate parameters.

11. The method according to any one of the preceding claims, wherein a first service of said services is executed in a first Service Control Point (121) of said one or more Service Control Points (121, 122, 123) and a second service of said services is executed in a second Service Control Point (122) of said one or more Service Control Points (121, 122, 123).

12. The method according to claim 11, wherein a first service of said services is a pre-paid charging service.

13. The method according to claim 11 or 12, wherein a second service of said services is a mobile terminating service such as a personal greeting service.

14. The method according to any one of the preceding claims, wherein said control node (110) is a Gateway Mobile Switching Centre (110).

15. The method according to any of the claims 2-14, wherein said first request contains a Mobile Station ISDN number of said subscriber.

16. The method according to any of the claims 2-15, wherein said second request contains a Mobile Station ISDN number of said subscriber and a "Suppress T-CSI" parameter.

17. The method according to any one of the preceding claims, wherein a first or a second request of said one or more requests for routing information comprises a Mobile Application Part Send Routing Information message.

18. A control node (110) for handling Intelligent Network services associated with a call to a subscriber of a mobile telecommunications network, the network comprising said control node (110), a Home Location Register (111) and one or more Service Control Points (121, 122, 123); the control node (110) configured to send to said Home Location Register (111) one or more requests for routing information associated with said call; the control node (110) further configured to receive from said Home Location Register (111) multiple service trigger elements associated with said services, and for invoking said services in said one ore more Service Control Points (121, 122, 123) by using said trigger elements; the control node further configured to receive from said one or more Service Control Points (121, 122, 123) information related to said services associated with said trigger elements.

19. A computer program comprising program instructions for causing a computer to perform the method according to of any of the claims 1-17.

20. A computer program on a carrier and comprising computer executable instructions for causing a computer to perform the method according to claims 1-17.

21. A computer program according to claim 19, wherein said carrier is a record medium, computer memory, read-only memory or an electrical carrier signal.

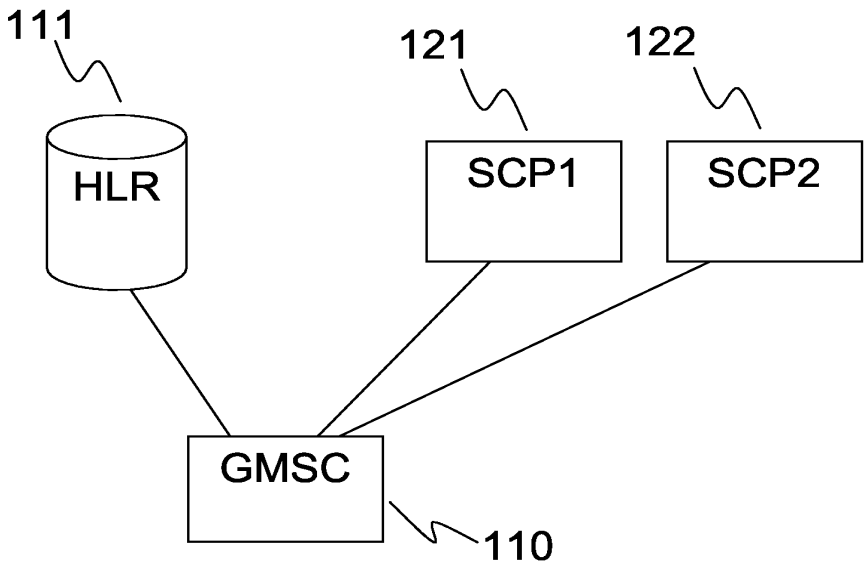


Fig. 1

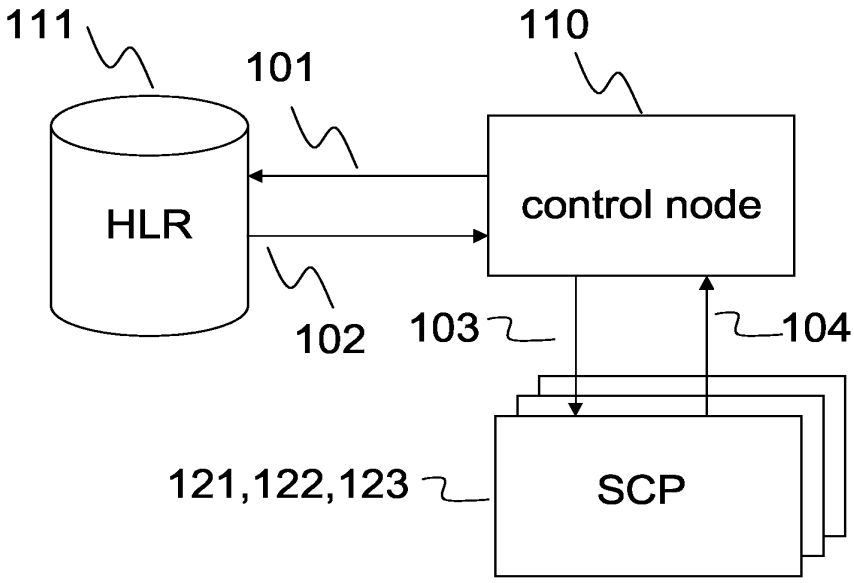


Fig. 2

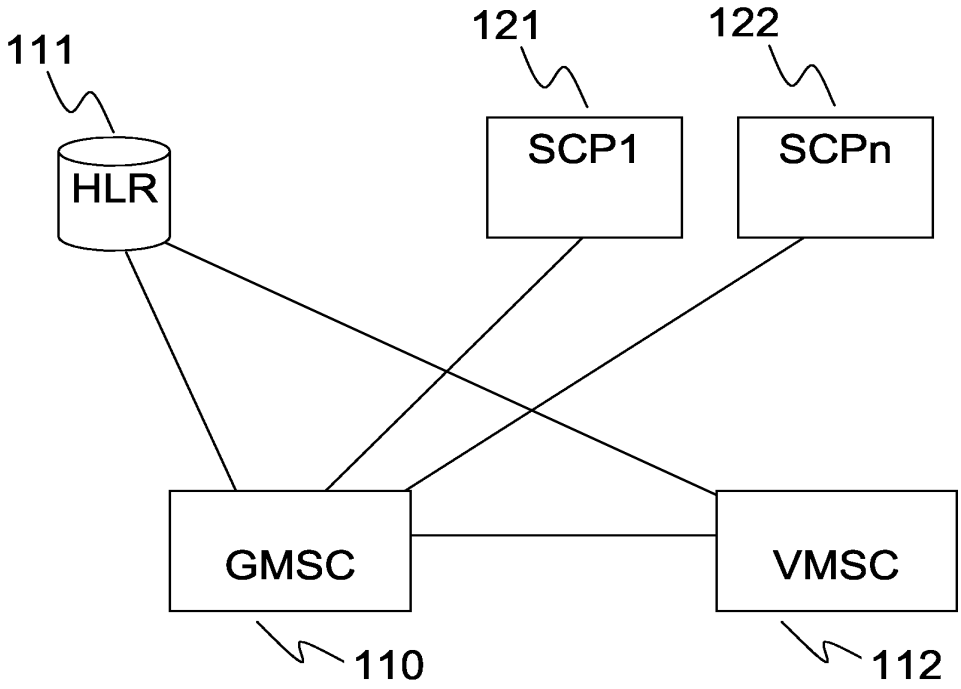


Fig. 3

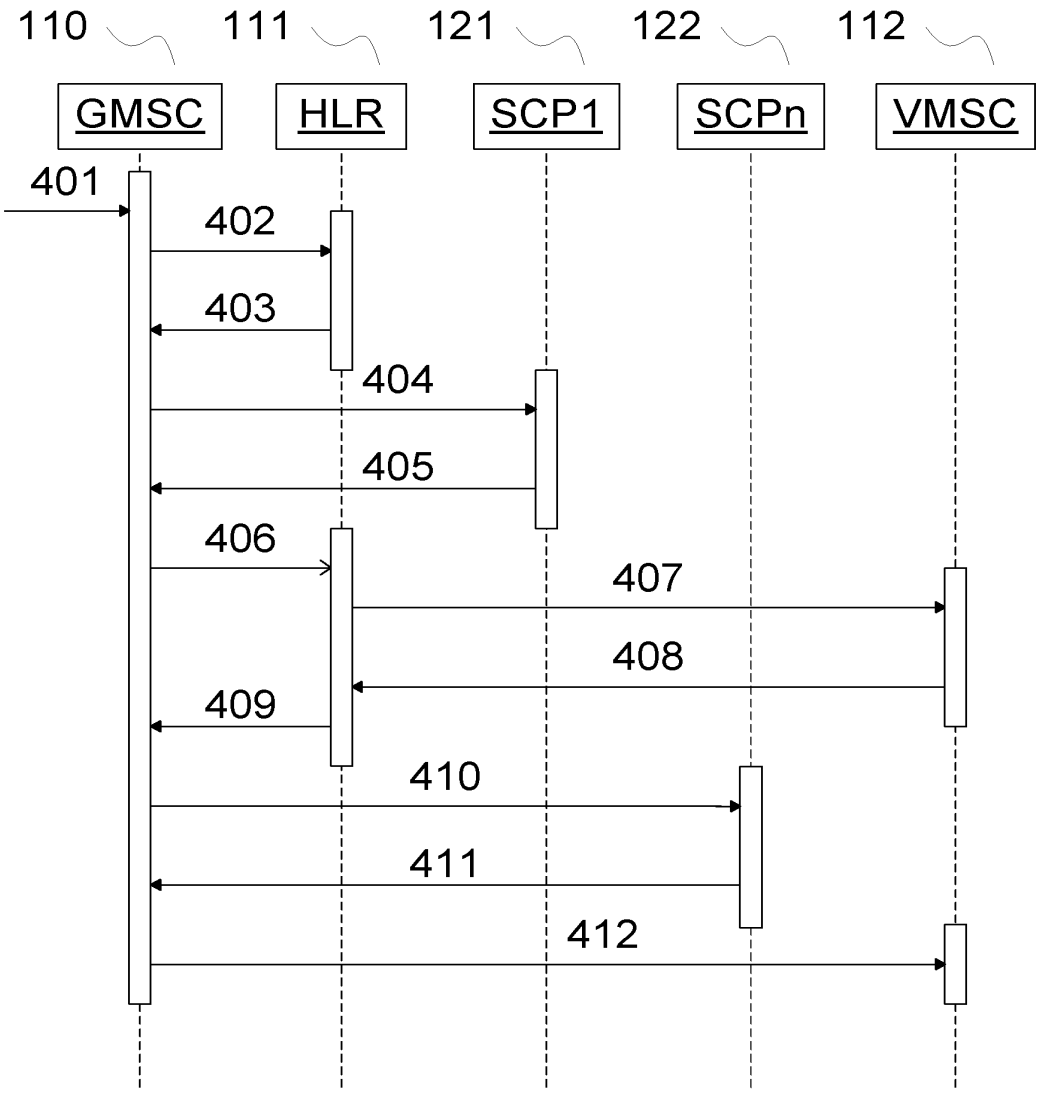

110
111
121
122
112
GMSC
HLR
SCP1
SCPn
VMSC
401
402
403
404
405
406
407
408
409
410
411
412

Fig. 4

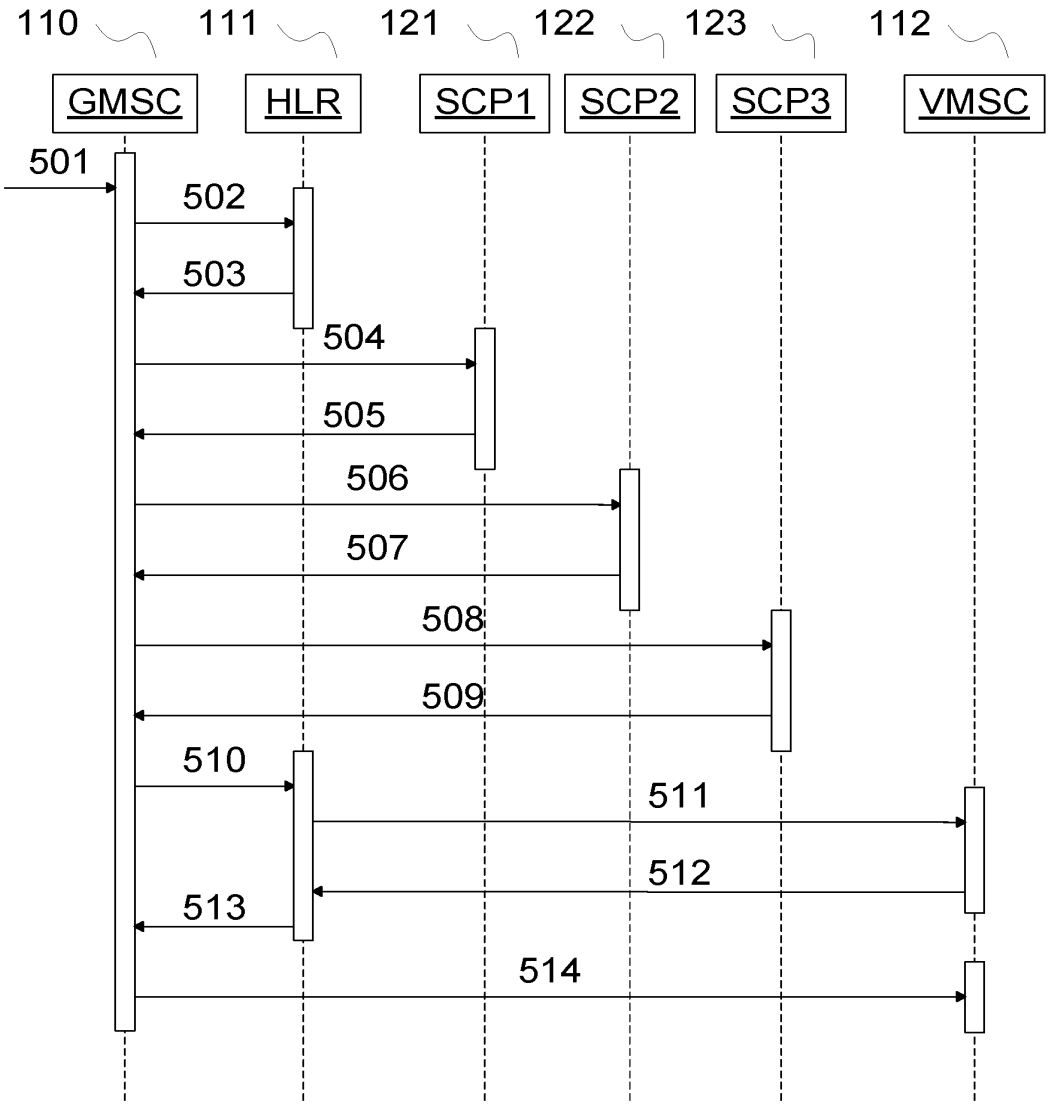

110
111
121
122
123
112
GMSC
HLR
SCP1
SCP2
SCP3
VMSC
501
502
503
504
505
506
507
508
509
510
511
512
513
514

Fig. 5

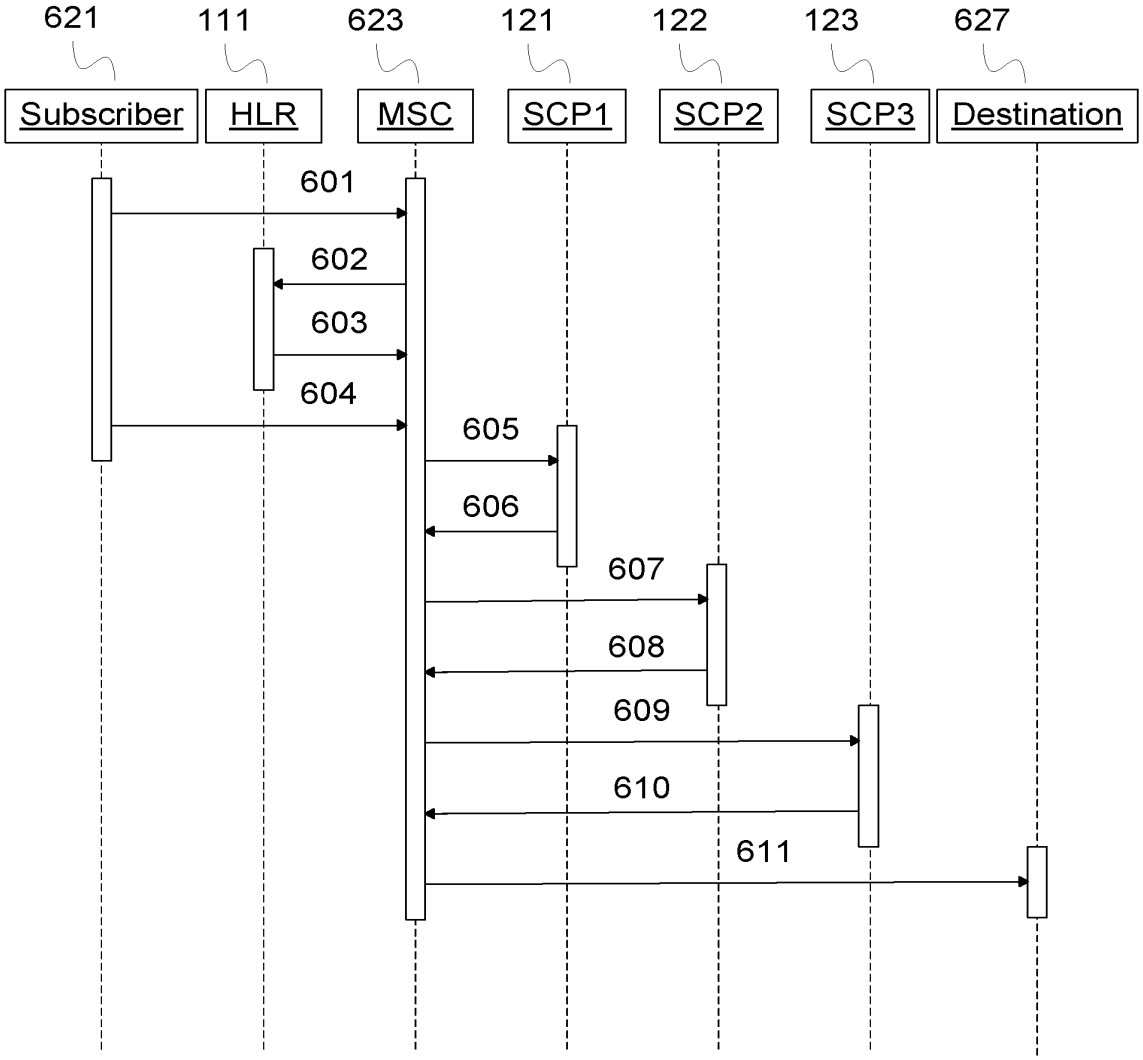

621
111
623
121
122
123
627
Subscriber
HLR
MSC
SCP1
SCP2
SCP3
Destination
601
602
603
604
605
606
607
608
609
610
611

Fig. 6

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2005/056843

A. CLASSIFICATION OF SUBJECT MATTER
H04Q3/00 H04Q7/24

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04Q

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2004/103012 A (SIEMENS AKTIENGESELLSCHAFT; KASTL, PETRA; WOELKNER, CHRISTIAN) 25 November 2004 (2004-11-25) page 9, line 7 - page 10, line 37	1-21
X	WO 97/07637 A (MOTOROLA LTD; CHAMBERS, DAVID; CRICHTON, PAUL; DODD, ADRIAN) 27 February 1997 (1997-02-27) page 3, line 26 - page 5, line 24 figure 1	1-21

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
8 February 2006	27/02/2006

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

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

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2005/056843

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2004103012 A	25-11-2004	AU 2003242558 A1	03-12-2004
WO 9707637 A	27-02-1997	CA 2229447 A1	27-02-1997
		CN 1194079 A	23-09-1998
		DE 69631888 D1	22-04-2004
		DE 69631888 T2	05-08-2004
		EP 0846399 A1	10-06-1998
		GB 2304491 A	19-03-1997
		HK 1016400 A1	01-08-2003
		JP 2000502217 T	22-02-2000

Form PCT/ISA/210 (patent family annex) (April 2005)

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04M 1/66 (2006.01)

[12] 发明专利申请公开说明书

[21] 申请号 200480002062.0

[43] 公开日 2006 年 7 月 12 日

[11] 公开号 CN 1802839A

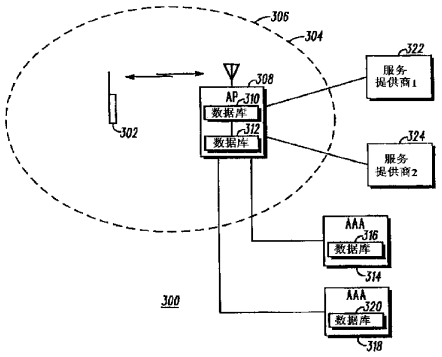
[22] 申请日 2004.1.13
[21] 申请号 200480002062.0
[30] 优先权
[32] 2003.1.13 [33] US [31] 60/439,743
[32] 2004.1.12 [33] US [31] 10/755,800
[86] 国际申请 PCT/US2004/000870 2004.1.13
[87] 国际公布 WO2004/064306 英 2004.7.29
[85] 进入国家阶段日期 2005.7.11
[71] 申请人 摩托罗拉公司（在特拉华州注册的公司）
地址 美国伊利诺斯州
[72] 发明人 约翰纳·维尔德
拉杰什·帕日亚努尔
[74] 专利代理机构 中原信达知识产权代理有限责任公司
代理人 李 涛 钟 强
权利要求书 2 页 说明书 11 页 附图 4 页

[54] 发明名称

通过无线局域网向移动站提供网络服务信息的方法和装置

[57] 摘要

一种无线局域网(WLAN)通信系统(300)，包括与移动站(302)通信的接入点(308)以及至少一个鉴别、授权、结算(AAA)服务器(314、318)，提供鉴别过程，由此移动站用户可以在被鉴别之前从一个或多个 WLAN 服务提供商和/或一个或多个 3GPP 服务提供商(322、324)中选择 WLAN 服务提供商，进而根据与所选服务提供商相关联的、除了服务集标识符(SSID)之外的网络服务信息来作出订制所选服务提供商的服务的决定。



1. 一种用于提供网络服务信息给接入无线局域网的移动站用户的方法，包括：

接收鉴别移动站的请求；和

作为对接收到上述请求的响应，传送关于多个服务提供商中每个服务提供商的网络识别和服务信息到移动站。

2. 如权利要求 1 所述的方法，其中，鉴别移动站的请求与网络识别和服务信息每个都是在媒介接入控制层消息中传送的。

3. 如权利要求 1 所述的方法，进一步包括：

请求鉴别信息；和

接收包括对从多个服务提供商中选择服务提供商的选择的鉴别信息。

4. 如权利要求 3 所述的方法，进一步包括：

根据接收到的鉴别信息来确定鉴别、授权、结算服务器；和

通过确定的鉴别、授权、结算服务器来请求对移动站的授权。

5. 一种用于接入无线局域网的方法，包括：

传送鉴别移动站的请求；

接收关于服务提供商的网络识别和服务信息；和

根据接收到的网络识别和服务信息来确定是否接入无线局域网。

6. 如权利要求 5 所述的方法，其中，鉴别移动站的请求与网络识别和服务信息每个都是在媒介接入控制层消息中传送的。

7. 如权利要求 5 所述的方法，其中，接收关于服务提供商的网络识别和服务信息包括接收关于多个服务提供商中的每个服务提供商

的网络识别和服务信息，并且其中，该方法进一步包括：

接收对鉴别信息的请求；和

传送对从多个服务提供商中选择服务提供商的选择。

8. 一种无线局域网中的接入点，包括：

存储器，储存关联于多个服务提供商中每个服务提供商的服务提供商标识符和网络服务信息；和

处理器，连接到存储器，组装一个或多个消息，所述消息包括与多个服务提供商中每个服务提供商相关联的服务提供商标识符和网络服务信息，并将这一个或多个消息传送到移动站。

9. 如权利要求 8 所述的接入点，其中，所述一个或多个消息包括第一一个或多个消息，并且其中，所述处理器接收鉴别移动站的请求，作为对接收到该请求的响应，组装所述第一一个或多个消息，进而组装包括对鉴别信息的请求的第二消息，然后将所述第二消息传送到移动站。

10. 如权利要求 9 所述的接入点，其中，所述处理器进而响应于传送对鉴别信息的请求，接收所请求的鉴别信息，而且，作为对接收到所请求的鉴别信息的响应，组装请求对移动站的授权的第三消息，然后将所述第三消息传送到服务器。

11. 如权利要求 10 所述的接入点，其中，所述存储器，关联于服务器，储存服务提供商标识符，其中，所接收到的鉴别信息包括服务提供商标识符，并且其中，所述处理器根据所接收到的服务提供商标识符来确定所述服务器。

通过无线局域网向移动站提供网络服务信息的方法和装置

技术领域

本发明一般涉及无线局域网，具体涉及由无线局域网基础设施向移动站提供网络覆盖、网络可接入性和网络服务信息。

背景技术

局域网（LAN）允许组织在高速网络上共享信息，其可以由相对便宜的硬件组件来组装。LAN 还通过允许 LAN 内的多用户通过对所有用户公用的接口连接到 LAN 外多个网络中的每个，来提供相对便宜的硬件连接给超出 LAN 的网络。直到近来，LAN 受限于硬连线的基础设施，需要用户通过有线连接物理上连接到 LAN。但是，随着无线技术和无线消息传递的近来的发展，无线通信也被用于 LAN 领域，导致无线局域网（WLAN）的发展。

图 1 是现有技术的示例无线局域网（WLAN）通信系统 100 的框图。通信系统 100 包括 WLAN，其包括基本服务集（BSS）104，BSS 又包括一个或多个接入点（AP）106、108（示出了两个）。与 BSS 104 相关联的是服务集标识符（SSID），该 SSID 为 BSS 104 中每个 AP 106、108 所公有，并由 BSS 104 中每个 AP 106、108 储存，起到 BSS 的标识符的作用。WLAN，尤其是一个或多个 AP 106、108 中的每个，连接到鉴别（Authentication）、授权（Authorization）、结算（Accounting）（AAA）服务器 110，AAA 服务器 110 向 WLAN 提供鉴别、授权、结算服务。AAA 服务器 110 包括数据库 112，其储存与授权接入 WLAN 的每个移动站（MS）相关联的标识符，并且进一步储存与每个标识符相关联的密码。

当 MS 102 希望接入 WLAN 时，MS 首先必须建立和配置与一个

或多个 AP 106、108 中的一个 AP 的链路，通常通过主动或被动扫描 WLAN 来完成。在主动扫描中，MS 102 通过广播探测请求（Probe Request）来开始建立和配置链路。探测请求包括服务集标识符（SSID）以及 MS 所支持的功能和数据率。一旦接收到探测请求，一个或多个 AP 106、108 中的每个 AP 确定探测请求中包含的 SSID 是否同与 AP 相关联的 SSID 相同。当 SSID 相同时，AP 响应探测请求，发送探测响应回到 MS，其包括与 AP 相关联的 SSID 以及 AP 所支持的功能和数据率。基于接收到的探测响应，MS 102 从一个或多个 AP 106、108 中选择最佳 AP，诸如 AP 106，并且发送关联请求到所选的 AP 106，其包括 SSID，还包括 MS 所支持的功能和数据率。一旦接收到关联请求，AP 106 发送关联响应到 MS 102，其包括唯一关联于 AP 的标识符，即 AP 地址，和 AP 将要支持的功能和数据率，并且建立 MS 和所选 AP 之间的链路。

在被动扫描中，不利用探测请求和探测响应，MS 102 可以选择 AP 并发送关联请求到所选 AP，以响应于接收到一个或多个 AP 106、108 中每个断断续续地发射的信标（Beacon）。类似于探测响应，每个信标包括与 AP 相关联的 SSID 以及 AP 所支持的功能和数据率。

在建立了 MS 102 和 AP 106 之间的链路之后，在对 MS 102 授权发送数据业务到 AP 106（即，不封锁对 WLAN 的接入）之前必须鉴别 MS 102。图 2 是现有技术的 WLAN 鉴别过程的信号流图 200。鉴别过程开始于 MS 102 发送 EAPOL（Extensible Application Protocol Over LAN，局域网可扩展应用协议）-开始消息 202 到 AP 106。响应于接收到 EAPOL-开始消息 202，AP 106 发送 EAPOL-EAP（Extensible Application Protocol，可扩展应用协议）-请求/识别消息 204 到 MS 102。EAPOL-EAP-请求/识别消息 204 从 MS 请求鉴别信息，诸如唯一关联于 MS 的标识符和密码。一旦接收到 EAPOL-EAP-请求/识别消息 204，MS 102 发送 EAPOL-EAP-响应/识别消息 206 到 AP 106，其提供了所请求的信息。

一旦接收到 EAPOL-EAP-响应/识别消息 206，AP 106 将 MS 102 所提供的标识符和密码通过半径（RADIUS）-EAP-响应/识别消息 208 转发到 AAA 服务器。一旦接收到识别消息，AAA 服务器 110 选择 EAP 鉴别方法。该方法包括一轮或多轮的 EAP 鉴别请求消息 210、212，从 AAA 服务器 110 传送到 MS 102，以及作为响应的 EAP 鉴别响应消息 214、216，从 MS 传送到 AAA 服务器。EAP 消息在 AAA 服务器 110 和 AP 106 之间携带在半径消息中，在 AP 106 和 MS 102 之间携带在 EAPOL 消息中。在鉴别请求和鉴别响应的最终交换的结束处，AAA 服务器 110 基于储存在数据库 112 中的一个或多个公知的用户标识符，诸如密码、共享秘密、公钥或数字证书，来鉴别 MS 102。如果 AAA 服务器 110 能够成功地鉴别 MS 102，那么 AAA 110 将半径-EAP-成功消息 218 传送到 AP 106。一旦接收到半径-EAP-成功消息 218，AP 106 将 EAPOL-EAP-成功消息 220 传送到 MS 102，并且不再封锁对 MS 102 的接入。如果 AAA 服务器 110 不能成功鉴别 MS 102，则 AAA 服务器将半径-EAP-失败消息传送到 AP 106，AP 106 继续封锁对 MS 102 的接入。

随着 WLAN 逐渐普及，WLAN 建立在更多数量的商业设施和公共场所中，诸如咖啡馆、机场、图书馆、学校以及会议中心。由于订制不同服务提供商的服务的不同人群在这些场所表达了希望接入 WLAN 服务的需求，因此对于提供商来说，将发展需要以提供交叠服务。但是，当前对于 AP 的共享并没有规定任何过程。相反地，在当前最新技术中，每个提供商提供独立的 AP，其配置以自己的 SSID 并且广播该 SSID。这样的系统十分浪费，因为它迫使服务提供商提供冗余的系统。而且，提供 WLAN 服务的可用带宽是有限的，主要的 WLAN 场所，诸如机场和会议中心，可能不具有足够的带宽来支持多个服务提供商中每个所使用的交叠 AP。

此外，当前最新技术仅仅允许用户根据 SSID 来选择服务提供商。

当用户能够接入多个服务提供商的每个的网络时，SSID 独自不可能向用户提供足够的信息来作出有关使用哪个服务提供商的充分有见识（fully informed）的决定。而且，当用户执行被动扫描时，用户可能不得不在选择与所需服务提供商相关联的 SSID 之前扫描和处理多个信标，消耗了向 MS 供电的有限寿命电池的过多的电量。

因此，需要一种方法和装置，允许接入 WLAN 的 MS 用户根据一个或多个标准，诸如每个服务提供商所支持的服务、服务价格、付费方法、访问的网络提供商和用户的归属网络之间的关系，从多个服务提供商中选择服务提供商，并进一步允许多个服务提供商共享 AP。

附图说明

图 1 是现有技术的示例无线局域网的框图。

图 2 是现有技术鉴别过程的信号流图。

图 3 是根据本发明实施例的无线通信系统的框图。

图 4 是根据本发明实施例的图 3 的移动站的框图。

图 5 是根据本发明实施例的图 3 的无线通信系统所执行的鉴别过程的信号流图。

具体实施方式

为了解决上述需要，即一种方法和装置，用于允许接入无线局域网（WLAN）的 MS 用户根据一个或多个标准，诸如每个服务提供商所支持的服务、服务价格、付费方法、访问的网络提供商和用户的归属网络之间的关系，从多个服务提供商中选择服务提供商，并进一步允许多个服务提供商共享 AP，提供一种 WLAN 通信系统，其包括与移动站通信的接入点，至少一个鉴别、授权、结算（AAA）服务器提供鉴别过程，由此移动站用户可以在被鉴别之前从一个或多个 WLAN 服务提供商和/或一个或多个 3GPP 服务提供商中选择 WLAM 服务提供商，进一步根据与所选服务提供商相关联的、除了服务集标识符（SSID）之外的网络服务信息来作出订制所选服务提供商的服务的决

定。

一般地，本发明的实施例包括一种用于向接入无线局域网的移动站用户提供网络服务信息的方法。该方法包括接收鉴别移动站的请求，作为对接收到请求的响应，传送关于多个服务提供商中每个服务提供商的网络识别和服务信息到移动站。

本发明的另一个实施例包括一种用于接入无线局域网的方法。该方法包括传送鉴别移动站的请求，接收关于服务提供商的网络识别和服务信息，以及根据接收到的网络识别和服务信息来确定是否接入该无线局域网。

本发明又一个实施例包括一种无线局域网中的接入点。接入点包括存储器和连接到存储器的处理器。存储器储存与多个服务提供商中的每个服务提供商相关联的标识符和网络服务信息，并将一个或多个消息传送到移动站。

通过参考图 3-5 可更加全面地描述本发明。图 3 是根据本发明实施例的无线通信系统 300 的框图。通信系统 300 包括无线局域网（WLAN）304，其包括具有一个或多个接入点（AP）308（示出了一个）的基本服务集（BSS）306。AP 308 提供无线通信服务给用户设备（UE），也就是，移动站（MS），诸如 MS 302，其位于 AP 所服务的覆盖区域内。优选地，MS 302 是便携、移动、或蜂窝通信设备，诸如但不限于蜂窝电话、无线电话、或无线调制解调器，其包括在数据终端设备内或连接到数据终端设备，诸如个人电脑、笔记本电脑、工作站、打印机、或传真机，其能够在 WLAN 通信系统中工作。BSS 306 和 AP 308 是由能够与 WLAN 网络交互的多个公共和/或专用网络服务提供商 322、324（示出了两个）所共享的，也就是说，代表这多个公共和/或专用网络服务提供商 322、324 来提供无线通信服务，这些服务提供商诸如但不限于，3GPP（第三代合作项目）、3GPP2、和企业

网络服务提供商，其允许 MS 与有效连接到 AP 的相应的外部网络进行通信。

通信系统 300 还包括一个或多个鉴别、授权、结算（AAA）服务器 314、318（示出了两个），其有效连接到 WLAN 304，具体连接到 AP 308，并且提供鉴别、授权和结算服务给 WLAN。多个 AAA 服务器 314、318 的每个 AAA 服务器都与关联于 BSS 306 和 AP 308 的多个服务提供商 322、324 之一相关联。每个 AAA 服务器 314、318 包括各自的数据库 316、320，其储存与被授权接入 WLAN 304 的每个移动站（MS）相关联的标识符，进一步地，关联于每个标识符，储存密码和相关付费信息，诸如与 MS 相关联的归属服务提供商。在本发明的另一实施例中，AP 308，或 BSS 306 和 AP 308，可以仅代表单一的 WLAN 服务提供商，诸如服务提供商 322，来提供无线通信服务。

AP 308 包括处理器 310，诸如一个或多个微处理器、微控制器、数字信号处理器（DSP）、其组合或者本领域普通技术人员已知的这样的其他设备。AP 308 还包括与处理器相关联的一个或多个存储设备 312，诸如随机存取存储器（RAM）、动态随机存取存储器（DRAM）、和/或只读存储器（ROM）或其等价物，其储存可由处理器执行的数据和程序。存储设备 312 还关联于与 AP 相关的每个服务提供商 322、324，储存服务提供商标识符或网络标识符、优选储存服务集标识符（SSID），以及网络服务信息，诸如关于服务提供商所支持的服务的信息、服务提供商所支持的每项服务的价格、为所提供的服务付费的方法、以及每个服务提供商与用户的归属服务提供商之间的关系，诸如其他服务提供商（即，归属网络）的订户使用该服务提供商网络（即访问网络）时该服务提供商所征收的任何额外费用。

图 4 是根据本发明实施例的 MS 302 的框图。MS 302 包括连接到处理器 404 的用户接口 402，处理器 404 诸如一个或多个微处理器、微控制器、数字信号处理器（DSP）、其组合或者本领域普通技术人

员已知的这样的其他设备。用户接口 402 向 MS 的用户提供与 MS 交互的能力，包括输入指令到 MS。在本发明的一个实施例中，用户接口 402 包括显示屏幕，其包括触摸屏，触摸屏能够确定用户在触摸屏上触摸的位置（即 X 坐标和 Y 坐标），并把位置数据传送到处理器 404。根据位置数据，处理器 404 随后将用户的触摸转换成指令。在本发明的另一个实施例中，用户接口 402 可包括显示屏幕和键盘。

MS 302 还包括与处理器 404 相关联的一个或多个存储设备 406，诸如随机存取存储器（RAM）、动态随机存取存储器（DRAM）、和/或只读存储器（ROM）或其等价物，其储存可由处理器执行的数据和程序。存储设备 406 还储存唯一关联于 MS 的 MS 标识符以及 SSID 和相应的鉴别标识符，诸如密码、共享秘密、公钥、数字证书等等，关联于每个服务提供商，诸如 MS 302 所订制的一个或多个服务提供商 322、324。此外，存储设备 406 储存用于组装 MS 与 WLAN 304 所交换的消息的指令。

优选地，通信系统 300 根据用于 WLAN 通信系统的电气电子工程师协会（IEEE）802.11 标准、尤其是根据 IEEE P802.1X/D11 和 802.11i/D2 标准来工作，该标准在此整体结合进来，其可以从 IEEE 行政办公机构（Piscataway, NJ）或者通过 standards.ieee.org 在线获得。此外，通信系统 300 优选还根据第三代合作项目（3GPP）对于 WLAN-蜂窝交互标准（TR 22.934 和 TR 23.934）的要求工作，该标准可从 ETSI 的 3GPP 处（Mobile Competence Centre, 650, route des Lucioles, 06921 Sophia-Antipolis Cedex, France）或通过 3gpp.org 在线获得，还有因特网工程任务组（IETF）RFC（请求注解）2284，其可以从 IETF 办公机构（Reston, VA）或者通过 ietf.org/rfc 在线获得，其描述了媒介接入控制（MAC）层可扩展鉴别协议（EAP），提供了鉴别协议的 MAC 层协商，用于在允许网络层协议通过链路发送之前鉴别对等设备，这些标准和协议，以及 IETF 备忘录“EAP AKA Authentication”，H. Haverinen, February 2002, 和“EAP SIM Authentication”, H. Haverinen,

June 2002 都在这里整体结合进来。

为了让 MS 302 接入 WLAN 304，MS 首先根据公知的链路建立和配置技术建立与 WLAN 的链路。一旦建立了这条链路，通信系统 300 在授权 MS 发送数据业务之前鉴别 MS 302。在现有技术中，为了订制 WLAN 的服务，鉴别过程仅仅允许 MS 用户根据相关服务提供商的 SSID 作出订制决定。跟现有技术不同，通信系统 300 提供了鉴别过程，从而 MS 302 的用户可以在被鉴别之前从一个或多个 WLAN 服务提供商和/或一个或多个 3GPP 服务提供商中选择 WLAN 服务提供商，进而根据与所选服务提供商相关联的、除了服务集标识符（SSID）之外的网络服务信息作出订制所选服务提供商的服务的决定。

图 5 是根据本发明实施例的通信系统 300 所执行的鉴别过程的信号流图 500。鉴别过程开始于 MS 发送鉴别步骤开始消息 502，优选为 EAPOL（局域网可扩展应用协议）-开始消息，到 WLAN 304，具体是到 AP 308。一旦接收到鉴别步骤开始消息 502，AP 308，具体是 AP 的处理器 310，从存储器 312 中提取关于与 AP 相关联的每个服务提供商（诸如服务提供商 322 和 324）的网络识别和服务信息。AP 308 随后在网络识别和服务信息消息 504、优选为 EAPOL-EAP-请求/信息消息中将提取的网络识别和服务信息传送到 MS 302。

一旦接收到网络识别和服务信息消息 504，MS 302 在用户接口 402 的显示屏幕中显示 508 关联于相应服务提供商 322、324 的至少一部分的接收到的网络识别和服务信息。通过显示网络识别和服务信息，MS 302 允许 MS 用户作出关于订制服务提供商用于特定通信会话的有见识的（informed）选择，而不是局限于仅仅根据 SSID 就作出选择。而且，通过在鉴别过程的开始处向 MS 302 提供对应于与 AP 308 相关联的每个服务提供商 322、324 的网络识别和服务信息，系统 300 减少了 MS 302 通过向 AP 提供单一 SSID 并反过来接收对应于所提供的 SSID 的网络服务信息而单独恳请与 BSS 相关联的每个服务提供商的

网络服务信息的需要。

根据在 MS 302 的用户接口 402 上显示的信息，MS 用户随后能够决定是否接入 WLAN 304。一旦确定接入 WLAN，用户向 MS 302 输入，同时 MS 从用户接收 508，对服务提供商的选择。例如，用户可能通过选择用户接口的显示屏幕上显示的软按键或者文本消息或者通过按下用户接口的键盘上的按键来输入他或她的选择。在本发明的另一个实施例中，其中，AP 308 只代表单一的服务提供商提供无线通信服务，MS 302 用户可能不需要输入服务提供商的选择，而是输入希望接入 WLAN 304 的指示。在本发明又一个实施例中，MS 的用户或卖家可能在 MS 302 的存储设备 406 中储存服务偏好。储存的偏好可能随后由 MS 302 用于自动选择服务提供商或根据 MS 从 AP 308 所接收到的网络和服务信息确定是否接入 WLAN 304。

一旦接收到网络服务信息消息 504，MS 302 通过传送确认 510、优选为 EAPOL-EAP-响应/信息/ACK 消息回到 AP 308 来确认消息的接收。一旦接收到确认 510，AP 308 将消息 512 传送到 MS 302，从 MS 请求鉴别信息，诸如唯一关联于 MS 的标识符、与所选服务提供商相关联的 SSID、和密码。优选地，请求鉴别信息的消息 512 是 EAPOL-EAP-请求/识别消息。一旦接收到请求鉴别信息的消息 512 并且一旦从 MS 用户接收到对服务提供商的选择、接收到用户希望接入 WLAN 304 的指示、或自动选择了服务提供商或确定接入 WLAN 304，MS 302 就发送提供请求的鉴别信息的消息 514，优选为 EAPOL-EAP-响应/识别消息，其包括所选网络的标识符、即 SSID，以及至少一部分的接收到的网络识别和服务信息。通过提供 SSID 和至少一部分的接收到的网络识别和服务信息，MS 302 向 WLAN 304、具体是 AP 308 提供所选的服务提供商。根据从 MS 接收的 SSID 和信息，WLAN 能够确定合适的 AAA 服务器 314、318 用于鉴别 MS。

一旦接收到请求的鉴别信息，AP 308 能够确定合适的 AAA 服务

器 314、318 来进行鉴别。AP 308 随后在鉴别信息消息 516、优选为半径-EAP-响应/识别消息中将 MS 302 所提供的标识符和密码转发给与所选服务提供商相关联的 AAA 服务器，诸如 AAA 服务器 314。类似于通信系统 100，一旦接收到鉴别信息消息 516，AAA 服务器 314 就选择 EAP 鉴别方法，AAA 服务器就要通过该方法鉴别 MS 302。EAP 鉴别方法包括一轮或多轮的 EAP 鉴别请求消息 518、520，其分别从 AAA 服务器 314 传送到 AP 308 和从 AP 308 传送到 MS 302，而作为响应，还包括 EAP 鉴别响应消息 522、524，分别从 MS 到 AP 和从 AP 到 AAA 服务器。在本发明的一个实施例中，EAP 消息是 MAC 层消息或数据链路层消息，其携带在 AAA 服务器 314 和 AP 308 之间的半径协议消息以及 AP 308 和 MS 302 之间的 EAPOL 消息中。在本发明的另一实施例中，在 AAA 服务器 314 和 AP 308 之间交换的 EAP 消息是 MAC 层消息或数据链路层消息，其携带在直径（Diameter）协议消息中。

在鉴别请求和鉴别响应的最终交换的结尾处，AAA 服务器 314 根据储存在 AAA 数据库 316 中的一个或多个公知鉴别标识符，诸如密码、共享秘密、公钥、或数字证书，来鉴别 MS 302。如果 AAA 服务器 314 能够成功鉴别 MS 302，则 AAA 服务器 314 传送授权消息 526、优选为半径-EAP-成功消息，到 AP 308，用于授权 AP 不再封锁对 MS 302 的接入。一旦接收到授权消息 526，AP 308 传送授权消息 528、优选为 EAPOL-EAP-成功消息，到 MS 302，用于授权 MS 接入 WLAN 304 并解除对 MS 302 的接入的封锁。如果 AAA 服务器 314 不能成功鉴别 MS 302 的话，则 AAA 服务器传送授权失败消息 532、优选为半径-EAP-失败消息，到 AP 308。在此情况下，AP 308 继续到框 534 接入 MS 302。

总而言之，WLAN 通信系统 300 提供了鉴别过程，由此 MS 302 用户可以在被鉴别之前从共享 WLAN 的一个或多个 WLAN 服务提供商和/或一个或多个 3GPP 服务提供商 322、324 中选择 WLAN 服务提

供商，进而根据与所选服务提供商相关联的、除服务集标识符（SSID）之外的网络服务信息，作出订制所选服务提供商的服务的决定。作为鉴别过程的一部分，WLAN 304 向 MS 提供关于一个或多个服务提供商的网络识别和服务信息，诸如每个服务提供商所支持的服务、服务价格、付费方法、以及访问的网络提供商和用户的归属网络之间的关系，从而允许 MS 用户作出关于 WLAN 服务提供商的有见识的选择。MS 可随后从这一个或多个服务提供商中选择服务提供商并且通过向 WLAN 传送相关 SSID 和至少一部分的接收到的网络识别和服务信息来通知 WLAN 所选的服务提供商。根据从 MS 接收到的 SSID 和信息，WLAN 能够确定合适的 AAA 服务器 314、318，用于鉴别 MS。

尽管本发明具体通过结合特定其实施例而显示和描述，但本领域技术人员将理解，可以作出各种变化以及进行要素的等价替换，这并不偏离本发明如权利要求所述的范围。因此，说明书和附图都应被视为说明性的而非限制性的，所有这样的变化和替换都包括在本发明的范围之内。

上面已经关于特定实施例描述了益处、其他优点、和问题的解决方案。但是，益处、优点、问题的解决方案，以及任何能够引起任何益处、优点或解决方案，或者使之出现或变得更显著的要素都不应被视作是任意或所有权利要求的决定性的、必需的或者关键的特征或要素。如这里所使用的，术语“包括、包含”或其任何变形，都意欲覆盖非排他性的包含，因此，包括一系列要素的过程、方法、物品或装置不仅仅包括那些列出的要素，还有可能包括其他未明确列出或者这样的过程、方法、物品或装置所固有的其他要素。还应当理解，关系术语的使用（如果有的话），诸如第一和第二、顶和底等等，都仅仅是用来区分一个实体或行为与另一个实体或行为，而不必要求或暗示这样的实体或行为之间的任何实际的这样的关系或顺序。

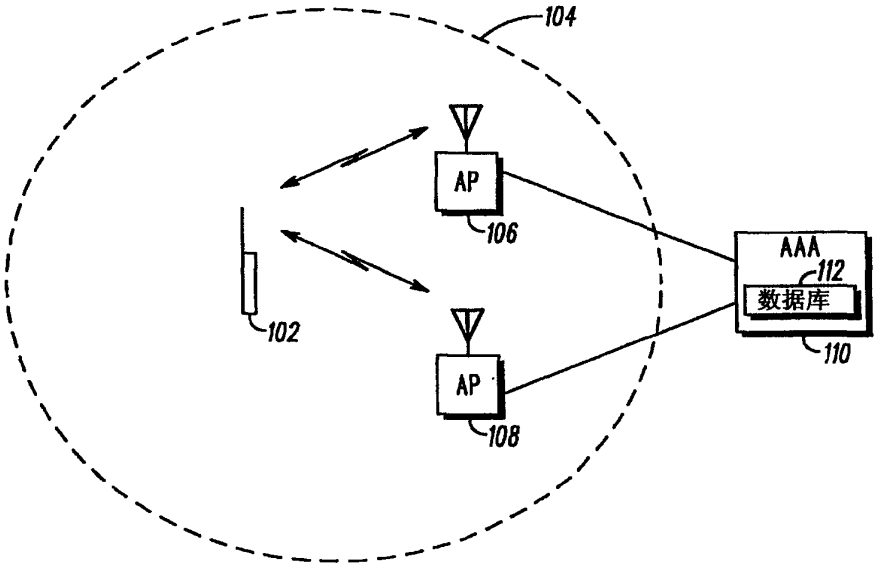


图1
现有技术

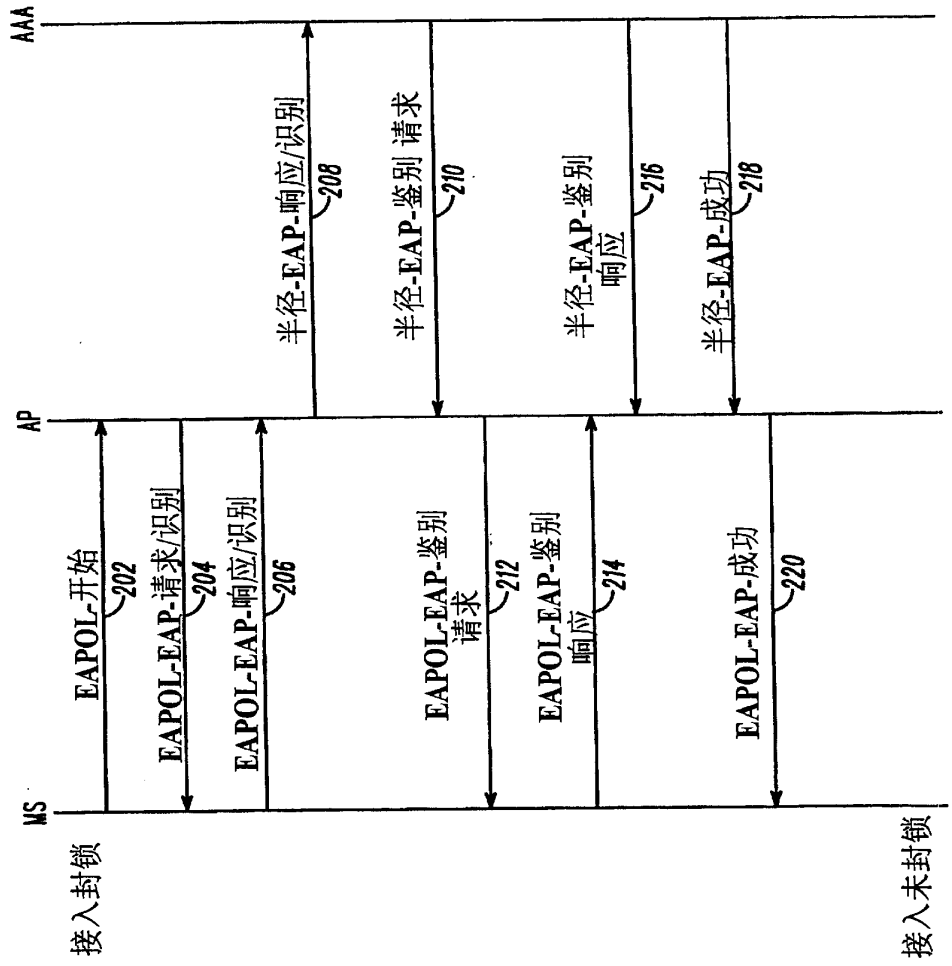

AAA
AP
MS
EAPOL-开始
202
EAPOL-EAP-请求/识别
204
EAPOL-EAP-响应/识别
206
半径-EAP-响应/识别
208
半径-EAP-鉴别 请求
210
EAPOL-EAP-鉴别
请求
212
EAPOL-EAP-鉴别
响应
214
半径-EAP-鉴别
响应
216
半径-EAP-成功
218
EAPOL-EAP-成功
220
接入封锁
接入未封锁
200

图2
现有技术

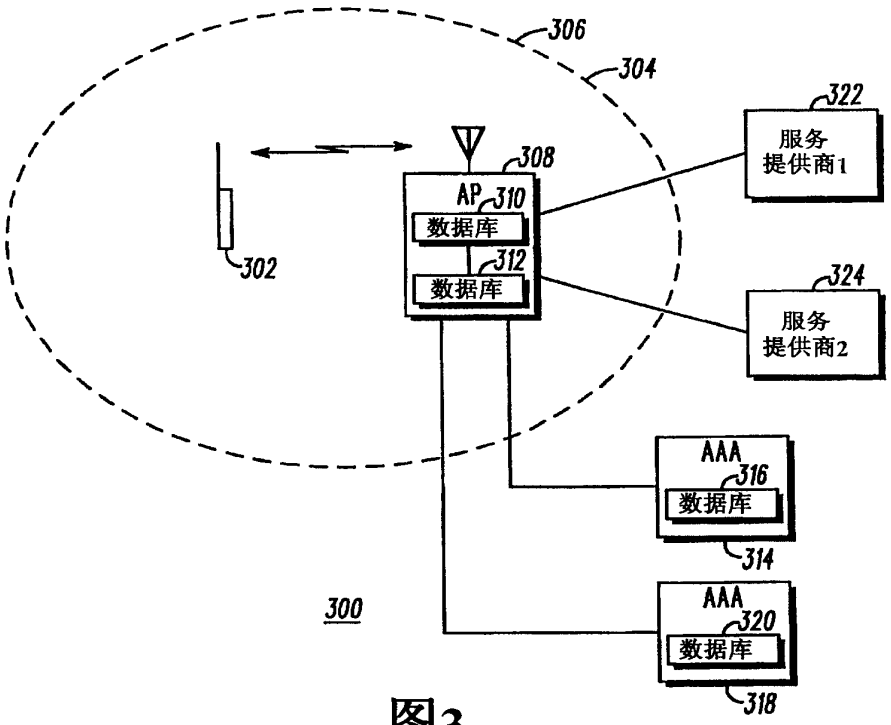

306
304
322
服务
提供商1
308
AP
310
数据库
312
数据库
302
324
服务
提供商2
AAA
316
数据库
314
300
AAA
320
数据库
318

图3

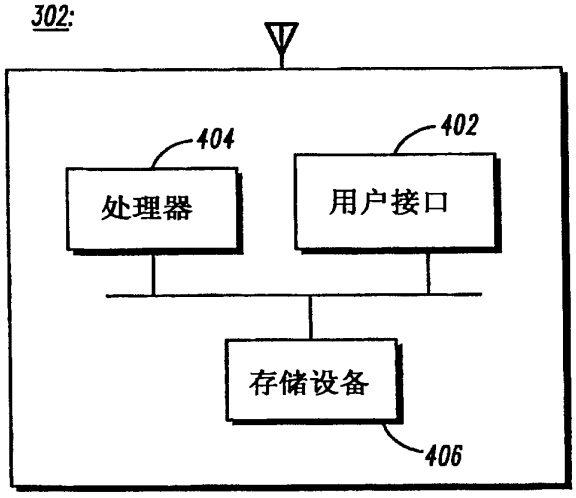

302:
404
处理器
402
用户接口
存储设备
406

图4

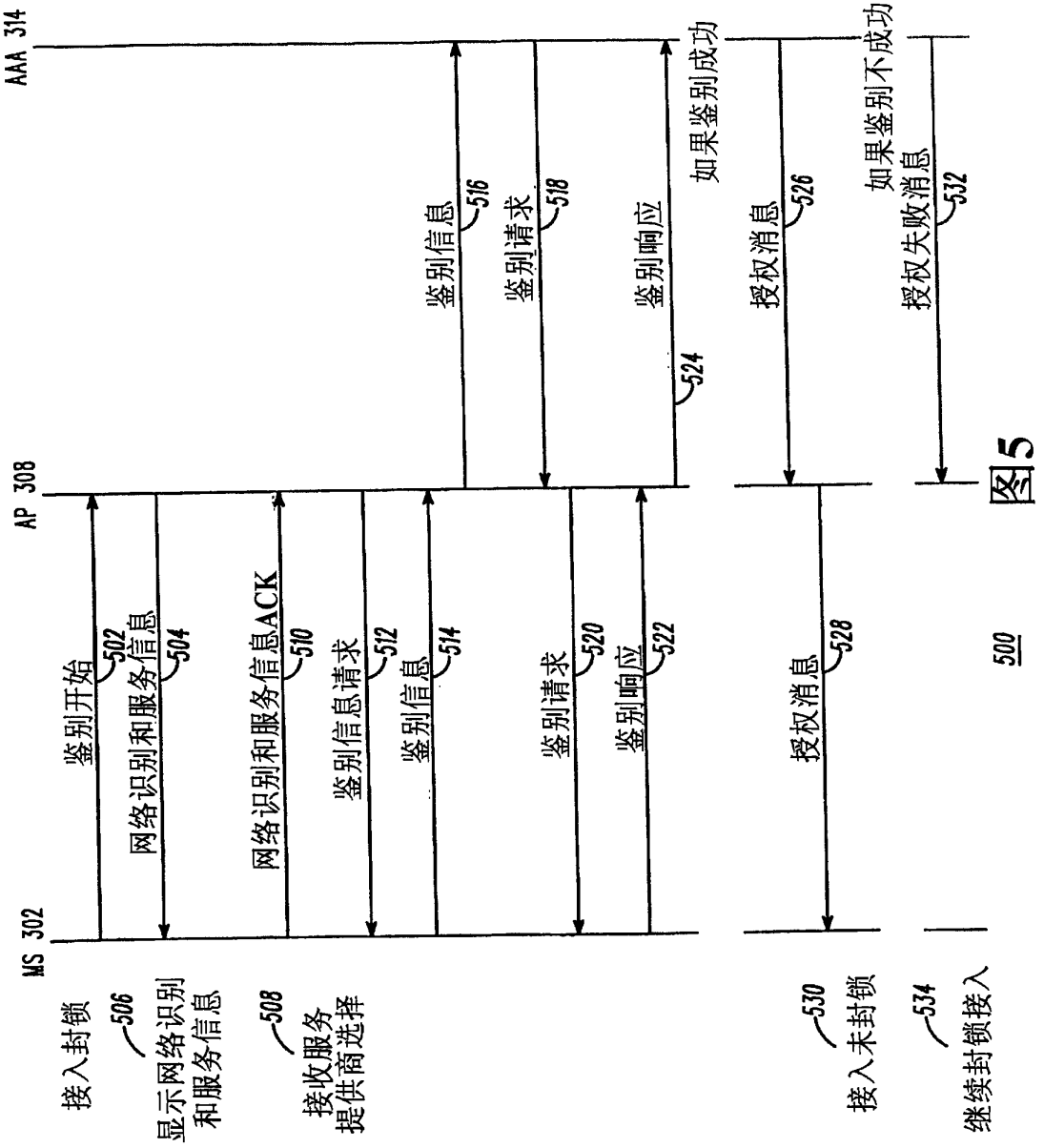

MS 302
AP 308
AAA 314
接入封锁
鉴别开始 502
网络识别和服务信息 504
显示网络识别和服务信息 506
网络识别和服务信息ACK 510
接收服务提供商选择 508
鉴别信息请求 512
鉴别信息 514
鉴别信息 516
鉴别请求 518
鉴别请求 520
鉴别响应 522
鉴别响应 524
如果鉴别成功
授权消息 526
授权消息 528
接入未封锁 530
如果鉴别不成功:
授权失败消息 532
继续封锁接入 534
500

图5

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 July 2004 (29.07.2004)

PCT

(10) International Publication Number
WO 2004/064306 A2

(51) International Patent Classification[7]: H04L

(21) International Application Number: PCT/US2004/000870

(22) International Filing Date: 13 January 2004 (13.01.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/439,743 13 January 2003 (13.01.2003) US
10/755,800 12 January 2004 (12.01.2004) US

(71) Applicant *(for all designated States except US)*: **MOTOROLA INC. A CORPORATION OF THE STATE OF DELAWARE** [US/US]; 1303 East Algonquin Road, Schaumburg, Illinois 60196 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **WILD, Johanna,** [DE/DE]; Seitzstr. 17, Bavaria, 80538 Muenchen (DE). **PAZHYANNUR, Rajesh,** [IN/US]; 1204 East Algonquin Road, Schaumburg, Illinois 60173 (US).

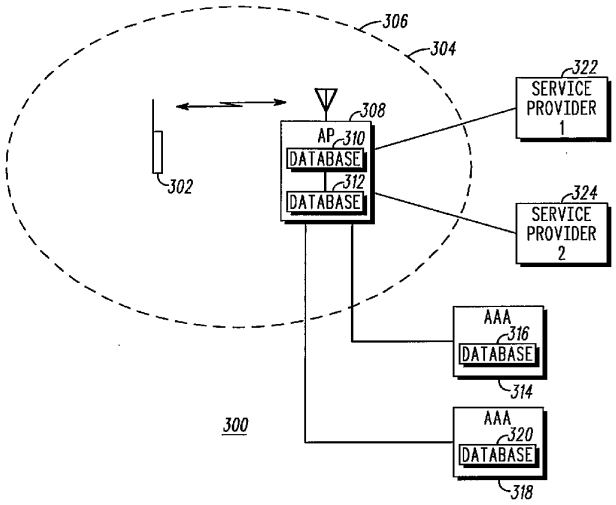
(74) Agents: **MAY, Steven A.,** et al.; 1303 East Algonquin Road, Schaumburg, Illinois 60196 (US).

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

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

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR PROVIDING NETWORK SERVICE INFORMATION TO A MOBILE STATION BY A WIRELESS LOCAL AREA NETWORK



(57) Abstract: A wireless local area network (WLAN) communication system (300) that includes an access point (308) in communication with a mobile station (302) and at least one Authentication, Authorization, and Accounting (AAA) server (314, 318) provides an authentication process whereby a user of the mobile station may select a WLAN service provider from among one or more WLAN service providers and/or one or more 3GPP service providers (322, 324) before being authenticated and further to make a decision to subscribe to the services of the selected service provider based on network service information, other than or in addition to an Service Set Identifier (SSID), associated with the selected service provider.

WO 2004/064306 A2

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

METHOD AND APPARATUS FOR PROVIDING NETWORK SERVICE INFORMATION TO A MOBILE STATION BY A WIRELESS LOCAL AREA NETWORK

Field of the Invention

The present invention relates generally to wireless local area networks and, in particular, to provision of network coverage, network accessibility, and network service information by a wireless local area network infrastructure to a mobile station.

Background of the Invention

Local area networks (LANs) allow organizations to share information over a high speed network that may be assembled with relatively inexpensive hardware components. LANs also provide for relatively inexpensive hardware connections to networks beyond the LAN by allowing multiple users within the LAN to connect to each of multiple networks outside of the LAN through an interface common to all users. Until recently, LANs were limited to hardwired infrastructure, requiring the user to physically connect to the LAN via a wired connection. However, with the recent growth of wireless telephony and wireless messaging, wireless communications have also been applied to the realm of LANs, resulting in the development of wireless local area networks (WLANs).

FIG. 1 is a block diagram of an exemplary wireless local area network (WLAN) communication system 100 of the prior art. Communication system 100 includes a WLAN that comprises a Basic Service Set (BSS) 104, which BSS in turn comprises one or more Access Points (APs) 106, 108 (two shown). Associated with BSS 104 is a Service Set Identifier (SSID), which SSID is common to, and stored by, each AP 106, 108 in BSS 104 and functions as an identifier of the BSS. The WLAN, and in particular each of the one or more APs 106 and 108, is coupled to an Authentication, Authorization, and Accounting (AAA) server 110 that provides authentication, authorization, and

accounting services to the WLAN. AAA server 110 includes a database 112 that stores identifiers associated with each mobile station (MS) that is authorized to access the WLAN and further stores a password in association with each identifier.

When an MS 102 wishes to access the WLAN, the MS must first establish and configure a link with an AP of the one or more APs 106, 108, typically by actively or passively scanning the WLAN. In an active scan, MS 102 initiates the establishment and configuration of a link by broadcasting a Probe Request. The Probe Request includes a Service Set Identifier (SSID) and capabilities and data rates supported by the MS. Upon receiving the Probe Request each AP of the one or more APs 106, 108 determines whether the SSID included in the Probe Request is the same as the SSID associated with the AP. When the SSIDs are the same, the AP responds to the Probe Request by transmitting a Probe Response back to the MS that includes the SSID associated with the AP and capabilities and data rates supported by the AP. Based on the received Probe Responses, MS 102 selects a best AP, such as AP 106, of the one or more APs 106, 108 and transmits an Association Request to the selected AP 106 that includes the SSID and further includes the capabilities and data rates supported by the MS. Upon receiving the Association Request, AP 106 transmits an Association Response to MS 102 that includes an identifier uniquely associated with the AP, that is, an AP address, and the capabilities and data rate that will be supported by the AP, and establishes a link between the MS and the selected AP.

In a passive scan, instead of utilizing a Probe Request and a Probe Response, MS 102 may select an AP and transmit an Association Request to the selected AP in response to receiving a Beacon that is intermittently transmitted by each of the one or more APs 106, 108. Similar to the Probe Response, each Beacon includes the SSID associated with the AP and capabilities and data rates supported by the AP.

After a link is established between MS 102 and AP 106, MS 102 must be authenticated before the MS is authorized to transmit data traffic to AP 106, that is, is access to the WLAN is unblocked. FIG. 2 is a signal flow diagram 200 of a WLAN authentication process of the prior art. The authentication process begins when MS 102 transmits an EAPOL (Extensible Application Protocol Over LAN)-Start message 202 to

the AP 106. In response to receiving EAPOL-Start message 202, AP 106 transmits an EAPOL-EAP (Extensible Application Protocol)-Request/Identity message 204 to the MS 102. EAPOL-EAP-Request/Identity message 204 requests authentication information from the MS, such as an identifier uniquely associated with the MS and a password. Upon receiving EAPOL-EAP-Request/Identity message 204, MS 102 transmits an EAPOL-EAP-Response/Identity message 206 to AP 106 that provides the requested information.

Upon receiving EAPOL-EAP-Request/Identity message 206, AP 106 forwards the identifier and password provided by MS 102 to AAA server 110 in a RADIUS-EAP-Response/Identity message 208. On receiving the identity message AAA server 110 chooses an EAP authentication method. The method involves one or more rounds of EAP authentication request messages 210, 212 that are conveyed from AAA server 110 to MS 102 and, in response, EAP authentication response messages 214, 216 that are conveyed from the MS to the AAA server. The EAP messages are carried in RADIUS messages between AAA server 110 and AP 106 and in EAPOL messages between AP 106 and MS 102. At the end of the final exchange of authentication requests and authentication responses, AAA server 110 authenticates MS 102 based on one or more well known user identifiers, such as a password, a shared secret, a public key, or a digital certificate, that is stored in database 112. If AAA server 110 can successfully authenticate MS 102, then AAA 110 conveys a RADIUS-EAP-Success message 218 to AP 106. Upon receiving the RADIUS-EAP-Success message 218, AP 106 conveys an EAPOL-EAP-Success message 220 to MS 102 and unblocks access to the MS 102. If AAA server 110 cannot successfully authenticate MS 102, then the AAA server conveys a RADIUS-EAP-Failure message to the AP 106. In this case, AP 106 continues to block access to MS 102.

With the increasing popularity of WLANs, WLANs are being set up in an increasing number of commercial establishments and public places, such as coffee houses, airports, libraries, schools, and convention centers. As diverse groups of people who subscribe to the services of a diversity of service providers express their desire to access WLAN services in such places, the need will evolve for the providers to provide overlapping services. However, currently no process is prescribed for a sharing of an AP.

Instead, in the current state of the art, each provider provides a separate AP that is configured with, and broadcasts, its own SSID. Such a system is wasteful in that it forces service providers to provide redundant systems. Furthermore, the bandwidth available for provision of WLAN services is limited and prime WLAN locations, such as airports and convention centers, may not have sufficient bandwidth to support overlapping APs employed by each of multiple service providers.

In addition, the current state of the art permits a user to select a service provider based only on SSID. When a user is capable of accessing the networks of each of multiple service providers, the SSID alone may not provide the user with sufficient information to make a fully informed decision concerning which service provider to use. Furthermore, when the user performs a passive scan, the user may have to scan and process multiple beacons before selecting an SSID associated with a desired service provider, consuming an excessive amount of power of a limited life battery powering an MS.

Therefore a need exists for a method and apparatus that permits a user of an MS accessing a WLAN to select a service provider from among multiple service providers based on one or more criterion, such as services supported by each service provider, service costs, methods of billing, and a relationship between the visited network provider and the user's home network, and that further allows multiple service providers to share an AP.

Brief Description of the Drawings

FIG. 1 is a block diagram of an exemplary wireless local area network of the prior art.

FIG. 2 is a signal flow diagram of a prior art authentication process.

FIG. 3 is a block diagram of a wireless communication system in accordance with an embodiment of the present invention.

FIG. 4 is a block diagram of the mobile station of FIG. 3 in accordance with an embodiment of the present invention.

FIG. 5 is a signal flow diagram of an authentication process performed by the wireless communication system of FIG. 3 in accordance with an embodiment of the present invention.

Detailed Description of the Invention

To address the need for a method and an apparatus that that permits a user of an MS accessing a wireless local area network (WLAN) to select a service provider from among multiple service providers based on one or more criterion, such as services supported by each service provider, service costs, methods of billing, and a relationship between the visited network provider and the users home network, and that further allows multiple service providers to share an AP, a WLAN communication system that includes an access point in communication with a mobile station and at least one Authentication, Authorization, and Accounting (AAA) server provides an authentication process whereby a user of the mobile station may select a WLAN service provider from among one or more WLAN service providers and/or one or more 3GPP service providers before being authenticated and further to make a decision to subscribe to the services of the selected service provider based on network service information, other than or in addition to an Service Set Identifier (SSID), associated with the selected service provider.

Generally, an embodiment of the present invention encompasses a method for providing network service information to a user of a mobile station accessing a wireless local area network. The method includes receiving a request to authenticate the mobile station and, in response to receiving the request, conveying network identification and service information with respect to each service provider of a plurality of service providers to the mobile station.

Another embodiment of the present invention encompasses a method for accessing a wireless local area network. The method includes conveying a request to authenticate a mobile station, receiving network identification and service information with respect to a service provider, and determining whether to access the wireless local area network based on the received network identification and service information.

Yet another embodiment of the present invention encompasses an Access Point in a wireless local area network. The Access Point includes a memory and a processor coupled to the memory. The memory stores an identifier and network service information in association with each service provider of a plurality of service providers. The processor assembles one or more messages comprising the service provider identifier and the network service information associated with each service provider of a plurality of service providers and conveys the one or more messages to a mobile station.

The present invention may be more fully described with reference to FIGs. 3-5. FIG. 3 is a block diagram of a wireless communication system 300 in accordance with an embodiment of the present invention. Communication system 300 comprises a wireless local area network (WLAN) 304 that includes a Basic Service Set (BSS) 306 comprising one or more Access Points (APs) 308 (one shown). AP 308 provides wireless communication services to user equipment (UEs), that is, mobile stations (MSs), such as MS 302, located in a coverage area serviced by the AP. Preferably MS 302 is a portable, mobile, or cellular communication device, such as but not limited to a cellular telephone, a radiotelephone, or a wireless modem that is included in or coupled to data terminal equipment, such as a personal computer, a laptop computer, a workstation, a printer, or a facsimile machine, that is capable of operating in a WLAN communication system. BSS 306 and AP 308 are shared by, that is, provide wireless communication services on behalf of, multiple public and/or private network service providers 322, 324 (two shown) capable of interworking with a WLAN network, such as but not limited to 3GPP (Third Generation Partnership Project), 3GPP2, and enterprise network service providers, that allow the MS to communicate with a corresponding external network operably coupled to the AP.

Communication system 300 further includes one or more Authentication, Authorization, and Accounting (AAA) servers 314, 318 (two shown) that are operably coupled to WLAN 304, and in particular to AP 308, and that provide authentication, authorization, and accounting services to the WLAN. Each AAA server of the multiple AAA servers 314, 318 is associated with one of the multiple service providers 322, 324 associated with BSS 306 and AP 308. Each AAA server 314, 318 includes a respective database 316, 320 that stores identifiers associated with each mobile station (MS) that is

authorized to access WLAN 304 and further stores, in association with each identifier, a password and related billing information, such as a home service provider associated with the MS. In another embodiment of the present invention, AP 308, or BSS 306 and AP 308, may provide wireless communication services on behalf of only a single WLAN service provider, such as service provider 322.

AP 308 includes a processor 310, such as one or more microprocessors, microcontrollers, digital signal processors (DSPs), combinations thereof or such other devices known to those having ordinary skill in the art. AP 308 further includes one or more memory devices 312 associated with processor such as random access memory (RAM), dynamic random access memory (DRAM), and/or read only memory (ROM) or equivalents thereof, that store data and programs that may be executed by the processor. Memory devices 312 further store, in association with each service provider 322, 324 associated with the AP, an address of an AAA server 314, 318 associated with the service provider, a service provider identifier or network identifier, preferably a Service Set Identifier (SSID), and network service information, such as information concerning services supported by the service provider, a cost of each service supported by the service provider, methods of billing for the provided services, and a relationship between each service provider and users' home service providers, such as any extra fees the service provider may assess for use of the service provider's network, that is, a visited network, by subscribers to other service providers, that is, a home network.

FIG. 4 is a block diagram of MS 302, in accordance with an embodiment of the present invention. MS 302 includes a user interface 402 coupled to a processor 404, such as one or more microprocessors, microcontrollers, digital signal processors (DSPs), combinations thereof or such other devices known to those having ordinary skill in the art. User interface 402 provides a user of the MS with the capability of interacting with the MS, including inputting instructions into the MS. In one embodiment of the present invention, user interface 402 includes a display screen that comprises a touch screen that is able to determine a position (i.e., an X-coordinate and a Y-coordinate) of a user's touch on the touch screen and convey the position data to processor 404. Based on the position data, processor 404 then translates the user's touch into an instruction. In another embodiment of the present invention, user interface 402 may include a display screen and

a keypad.

MS 302 further includes one or more memory devices 406 associated with processor 404, such as random access memory (RAM), dynamic random access memory (DRAM), and/or read only memory (ROM) or equivalents thereof, that store data and programs that may be executed by the processor. Memory devices 406 further store an MS identifier that is uniquely associated with the MS and an SSID and a corresponding authentication identifier, such as a password, a shared secret, key, a digital certificate, etc., associated with each service provider, such as one or more of service providers 322, 324, subscribed to by MS 302. In addition, memory devices 406 store instructions for assembling messages that are exchanged by the MS with WLAN 304.

Preferably, communication system 300 operates in accordance with the Institute for Electrical and Electronic Engineers (IEEE) 802.11 standards for WLAN communication systems, and in particular the IEEE P802.1X/D11 and 802.11i/D2 standards, which standards are hereby incorporated herein in their entirety and are available from the IEEE administrative offices in Piscataway, NJ, or on-line at standards.ieee.org. In addition, communication system 300 preferably further operates in accordance with the Third Generation Partnership Project (3GPP) requirements for WLAN-Cellular Interworking standards (TR 22.934 and TR 23.934), which standards are available from the 3GPP at ETSI, Mobile Competence Centre, 650, route des Lucioles, 06921 Sophia-Antipolis Cedex, France, or on-line at 3gpp.org, the Internet Engineering Task Force (IETF) RFC (Request For Comments) 2284, which is available from the IETF offices in Reston, VA, or on-line at ietf.org/rfc and describes a medium access control (MAC) layer Extensible Authentication Protocol (EAP) that provides for MAC layer negotiation of an Authentication Protocol for authenticating a peer before allowing Network Layer protocols to transmit over a link, which standards and protocols are hereby incorporated herein in their entirety, and the IETF memoranda "EAP AKA Authentication," by H. Haverinen, dated February 2002, and "EAP SIM Authentication," by H. Haverinen, dated June 2002.

In order for MS 302 to obtain access to WLAN 304, the MS first establishes a communication link with the WLAN in accordance with well known link establishment

and configuration techniques. Upon establishing the link, communication system 300 authenticates MS 302 before authorizing the MS to transmit data traffic. In the prior art, in order to subscribe to the services of a WLAN, the authentication process merely allowed a user of an MS to make a subscription decision on a basis of an SSID of an associated service provider. Unlike the prior art, communication system 300 provides an authentication process whereby a user of MS 302 may select a WLAN service provider from among one or more WLAN service providers and/or one or more 3GPP service providers before being authenticated and further to make a decision to subscribe to the services of the selected service provider based on network service information, other than or in addition to an Service Set Identifier (SSID), associated with the selected service provider.

FIG. 5 is a signal flow diagram 500 of an authentication process executed by communication system 300 in accordance with an embodiment of the present invention. The authentication process begins when the MS transmits an authentication procedure start message 502, preferably an EAPOL (Extensible Application Protocol Over LAN)-Start message, to WLAN 304, and in particular to AP 308. Upon receiving authentication procedure start message 502, AP 308, an in particular processor 310 of the AP, retrieves from memory 312 network identification and service information concerning each service provider associated with the AP, such as service providers 322 and 324. AP 308 then conveys the retrieved network identification and service information to MS 302 in a network identification and services information message 504, preferably an EAPOL-EAP-Request/Information message.

Upon receiving network identification and services information message 504, MS 302 displays 508, in the display screen of user interface 402, at least a portion of the received network identification and service information in association with the corresponding service provider 322, 324. By displaying the network identification and services information, MS 302 permits a user of the MS to make an informed selection of the service provider subscribed to for a particular communication session instead of being limited to making a selection merely based on SSIDs. Furthermore, by providing MS 302 with network identification and service information corresponding to each service provider 322, 324 associated with AP 308 at the outset of the authentication process,

system 300 reduces the need for MS 302 to individually solicit the network service information of each service provider associated with a BSS by providing an AP with a single SSID and receiving, in return, the network service information corresponding to the provided SSID.

Based on the information displayed on user interface 402 of MS 302, a user of the MS is then able to decide whether to access WLAN 304. Upon determining to access the WLAN, the user inputs to MS 302, and the MS receives 508 from the user, a selection of a service provider. For example, the user may input his or her selection by selecting a softkey or a text message displayed on the display screen of the user interface or by depressing a key in a keypad of the user interface. In another embodiment of the present invention, wherein AP 308 provides wireless communication services on behalf of only a single service provider, the user of MS 302 may not need to input a selection of a service provider and may instead input an indication of a desire to access WLAN 304. In yet another embodiment of the present invention, the user or a vendor of the MS may store service preferences in memory devices 406 of MS 302. The stored preferences may then be used by MS 302 to automatically select a service provider or determine whether to access WLAN 304 based on the network and services information received by the MS from AP 308.

Upon receiving network services information message 504, MS 302 acknowledges receipt of the message by conveying an acknowledgment 510, preferably an EAPOL-EAP-Response/Information/ACK message, back to AP 308. Upon receiving acknowledgment 510, AP 308 conveys a message 512 to MS 302 requesting authentication information from the MS, such as an identifier uniquely associated with the MS, an SSID associated with a selected service provider, and a password. Preferably the message 512 requesting authentication information is an EAPOL-EAP-Request/Identity message. Upon receiving message 512 requesting authentication information and upon receiving a selection of a service provider from a user of the MS, receiving an indication of the user's desire to access WLAN 304, or automatically selecting a service provider or determining to access WLAN 304, MS 102 transmits a message 514 providing the requested authentication information, preferably an EAPOL-EAP-Response/Identity message that includes the identifier of the selected network, that

is, the SSID, and at least a portion of the received network identification and services information. By providing the SSID and the at least a portion of the received network identification and services information, MS 302 provides WLAN 304, and in particular AP 308, with the selected service provider. Based on the SSID and information received from the MS, the WLAN is able to determine an appropriate AAA server 314, 318 for authenticating the MS.

Upon receiving the requested authentication information, AP 308 is able to determine an appropriate AAA server 314, 318 for performing authentication. AP 308 then forwards the identifier and password provided by MS 302 to the AAA server associated with the selected service provider, such as AAA server 314, in an authentication information message 516, preferably a RADIUS-EAP-Response/Identity message. Similar to communication system 100, upon receiving authentication information message 516, AAA server 314 then chooses an EAP authentication method by which the AAA server authenticates MS 302. The EAP authentication method involves one or more rounds of EAP authentication request messages 518, 520 that are respectively conveyed from AAA server 314 to AP 308 and from AP 308 to MS 302 and, in response, EAP authentication response messages 522, 524 that are respectively conveyed from the MS to the AP and from the AP to the AAA server. In one embodiment of the present invention, the EAP messages are MAC layer messages or data link layer messages that are carried in RADIUS protocol messages between AAA server 314 and AP 308 and in EAPOL messages between AP 308 and MS 302. In another embodiment of the present invention, the EAP messages exchanged between AAA server 314 and AP 308 are MAC layer messages or data link layer messages that are carried in Diameter protocol messages.

At the end of the final exchange of authentication requests and authentication responses, AAA server 314 authenticates MS 302 based on one or more well known authentication identifiers, such as a password, a shared secret, a public key, or a digital certificate, that is stored in the AAA's database 316. If AAA server 314 can successfully authenticate MS 302, then AAA server 314 conveys an authorization message 526, preferably RADIUS-EAP-Success message, to AP 308 authorizing the AP to unblock access to MS 302. Upon receiving authorization message 526, AP 308 conveys an

authorization message 528, preferably an EAPOL-EAP-Success message, to MS 302 authorizing the MS to access WLAN 304 and unblocks 530 access to MS 302. If AAA server 314 cannot successfully authenticate MS 302, then the AAA server conveys an authorization failure message 532, preferably a RADIUS-EAP-Failure message, to the AP 308. In this case, AP 308 continues to block 534 access to MS 302.

In summary, WLAN communication system 300 provides an authentication process whereby a user of MS 302 may select a WLAN service provider from among one or more WLAN service providers and/or one or more 3GPP service providers 322, 324 sharing the WLAN before being authenticated and further to make a decision to subscribe to the services of the selected service provider based on network service information, other than or in addition to an Service Set Identifier (SSID), associated with the selected service provider. As part of the authentication process, WLAN 304 provides to the MS network identification and services information concerning the one or more service providers, such as services supported by each service provider, service costs, methods of billing, and a relationship between the visited network provider and the user's home network, thereby allowing the user of the MS to make an informed selection of a WLAN service provider. The MS may then select a service provider from among the one or more service provider and inform the WLAN of the selected service provider by conveying to the WLAN an associated SSID and at least a portion of the received network identification and services information. Based on the SSID and information received from the MS, the WLAN is able to determine an appropriate AAA server 314, 318 for authenticating the MS.

While the present invention has been particularly shown and described with reference to particular embodiments thereof, it will be understood by those skilled in the art that various changes may be made and equivalents substituted for elements thereof without departing from the scope of the invention as set forth in the claims below. Accordingly, the specification and figures are to be regarded in an illustrative rather then a restrictive sense, and all such changes and substitutions are intended to be included within the scope of the present invention.

Benefits, other advantages, and solutions to problems have been described above with regard to specific embodiments. However, the benefits, advantages, solutions to problems, and any element(s) that may cause any benefit, advantage, or solution to occur or become more pronounced are not to be construed as a critical, required, or essential feature or element of any or all the claims. As used herein, the terms "comprises," "comprising," or any variation thereof, are intended to cover a non-exclusive inclusion, such that a process, method, article, or apparatus that comprises a list of elements does not include only those elements but may include other elements not expressly listed or inherent to such process, method, article, or apparatus. It is further understood that the use of relational terms, if any, such as first and second, top and bottom, and the like are used solely to distinguish one entity or action from another entity or action without necessarily requiring or implying any actual such relationship or order between such entities or actions.

What is claimed is:

1. A method for providing network service information to a user of a mobile station accessing a wireless local area network comprising:

receiving a request to authenticate the mobile station; and

in response to receiving the request, conveying network identification and service information with respect to each service provider of a plurality of service providers to the mobile station.

2. The method of claim 1, wherein the request to authenticate the mobile station and the network identification and service information are each conveyed in a medium access control layer message.

3. The method of claim 1, further comprising:

requesting authentication information; and

receiving authentication information comprising a selection of a service provider from among the plurality of service providers.

4. The method of claim 3, further comprising:

determining an Authentication, Authorization, and Accounting server based on the received authentication information; and

requesting authorization of the mobile station by the determined Authentication, Authorization, and Accounting server.

5. A method for accessing a wireless local area network comprising:

conveying a request to authenticate a mobile station;

receiving network identification and service information with respect to a service provider; and

determining whether to access the wireless local area network based on the received network identification and service information.

6. The method of claim 5, wherein the request to authenticate the mobile station and the network identification and service information are each conveyed in a medium access control layer message.

7. The method of claim 5, wherein receiving network identification and service information with respect to a service provider comprises receiving network identification and service information with respect to each service provider of a plurality of service providers and wherein the method further comprises:

receiving a request for authentication information; and

conveying a selection of a service provider from among the plurality of service providers.

8. An Access Point in a wireless local area network comprising:

a memory that stores a service provider identifier and network service information in association with each service provider of a plurality of service providers; and

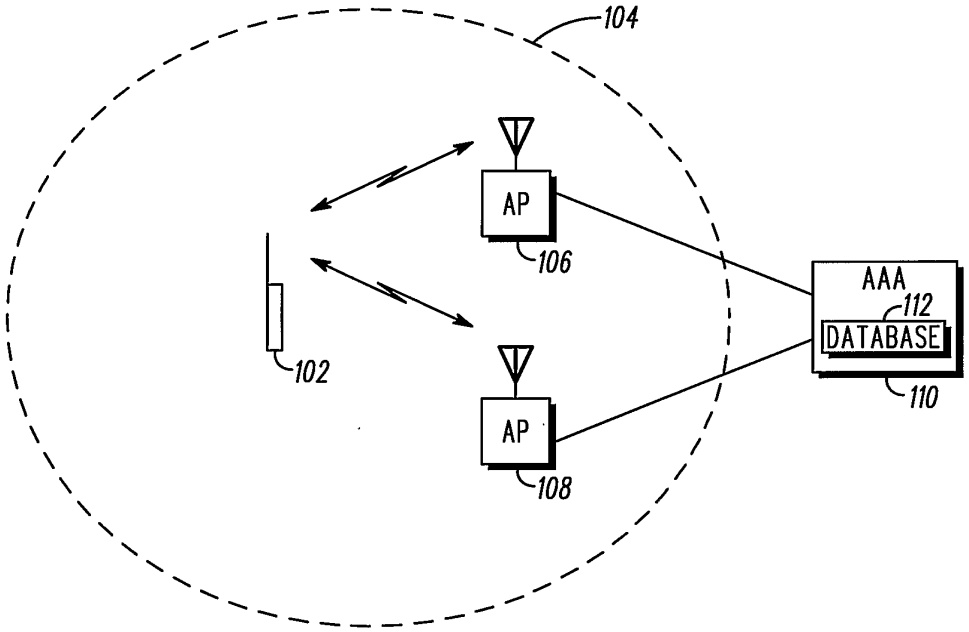
a processor coupled to the memory that assembles one or more messages comprising the service provider identifier and the network service information associated with each service provider of a plurality of service providers and conveys the one or more messages to a mobile station.

9. The Access Point of claim 8, wherein the first one or more messages comprises a first one or more messages and wherein the processor receives a request to authenticate the mobile station, in response to receiving the request, assembles the first one or more messages, and further assembles a second message comprising a request for authentication information and conveys the second message to the mobile station.

10. The Access Point of claim 9, wherein the processor further, in response to conveying the request for authentication information, receives the requested authentication information and, in response to receiving the requested authentication information, assembles a third message requesting authorization of the mobile station and conveys the third message to a server.

11. The Access Point of claim 10, wherein the memory stores, in association with the server, a service provider identifier, wherein the received authentication information comprises the service provider identifier, and wherein the processor determines the server based on the received service provider identifier.

5



100

FIG. 1
—PRIOR ART—

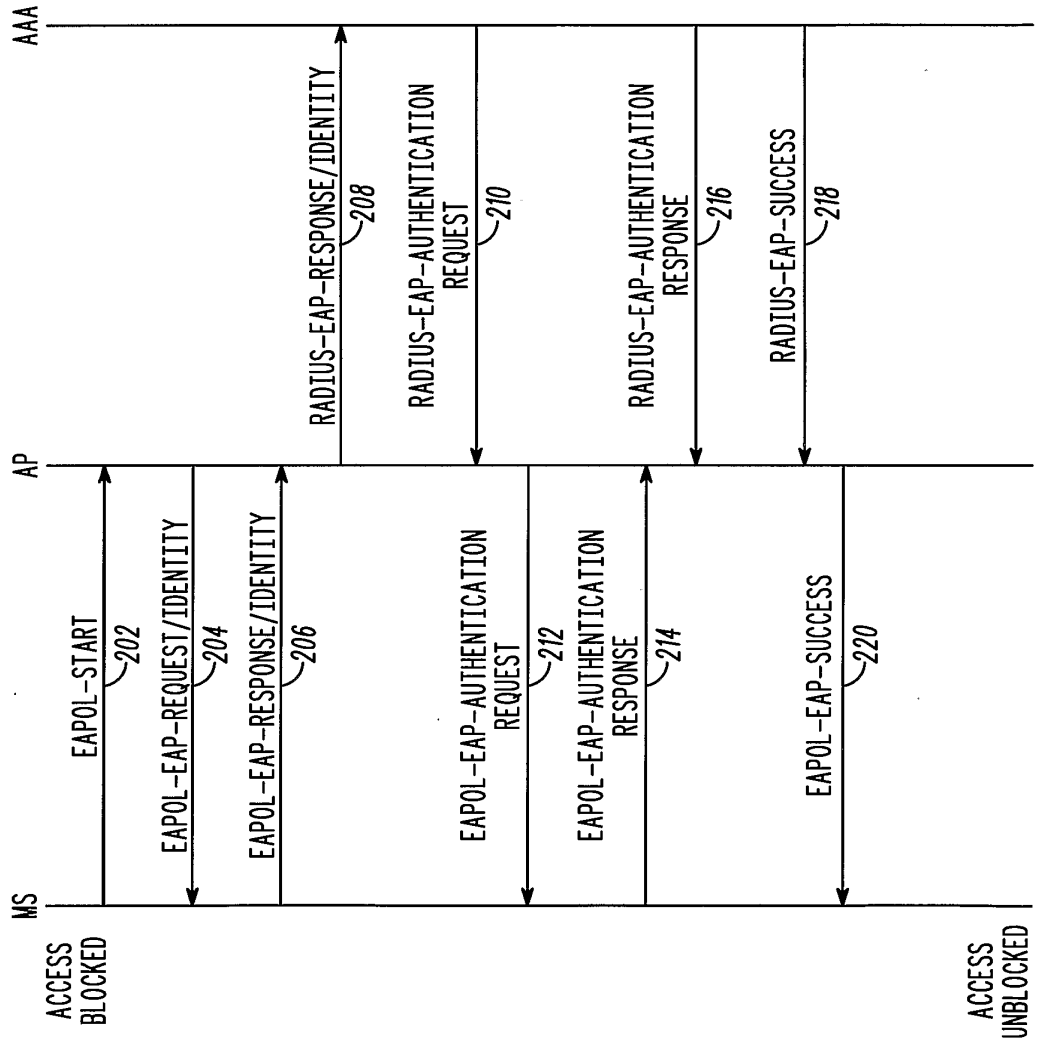


FIG. 2 200
—PRIOR ART—

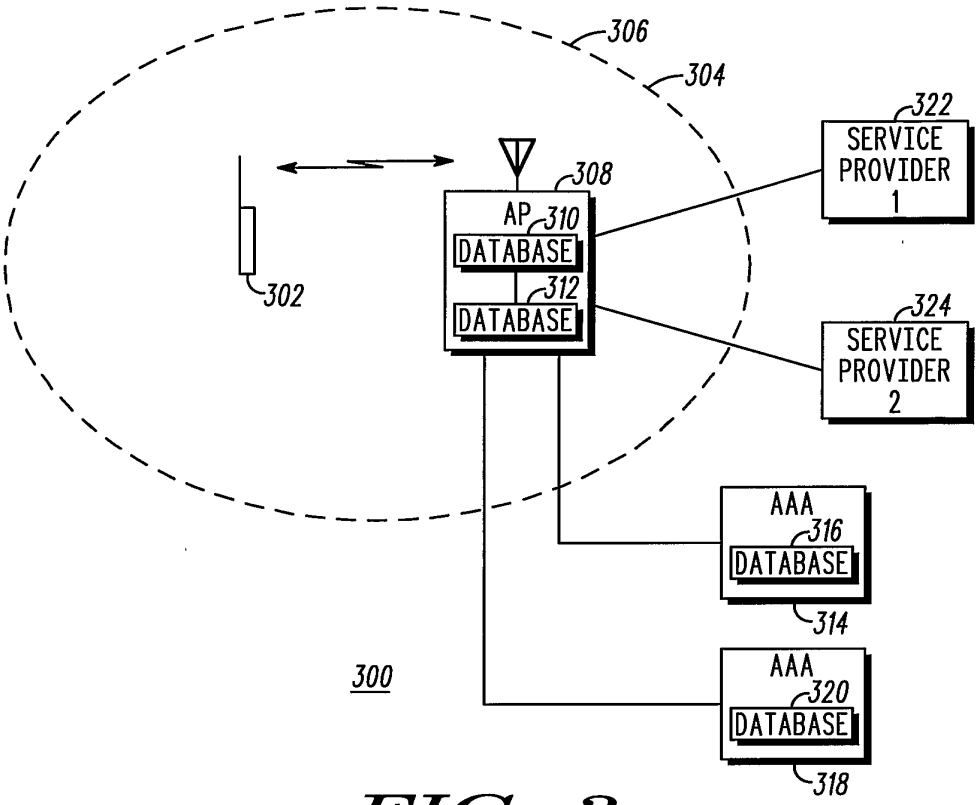

306
304
322
SERVICE PROVIDER 1
308
AP
310
DATABASE
312
DATABASE
302
324
SERVICE PROVIDER 2
AAA
316
DATABASE
314
300
AAA
320
DATABASE
318

FIG. 3

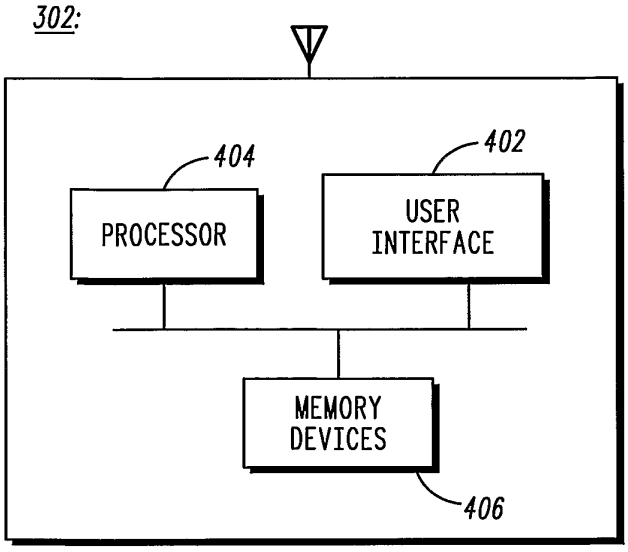

302:
404
PROCESSOR
402
USER INTERFACE
MEMORY DEVICES
406

FIG. 4

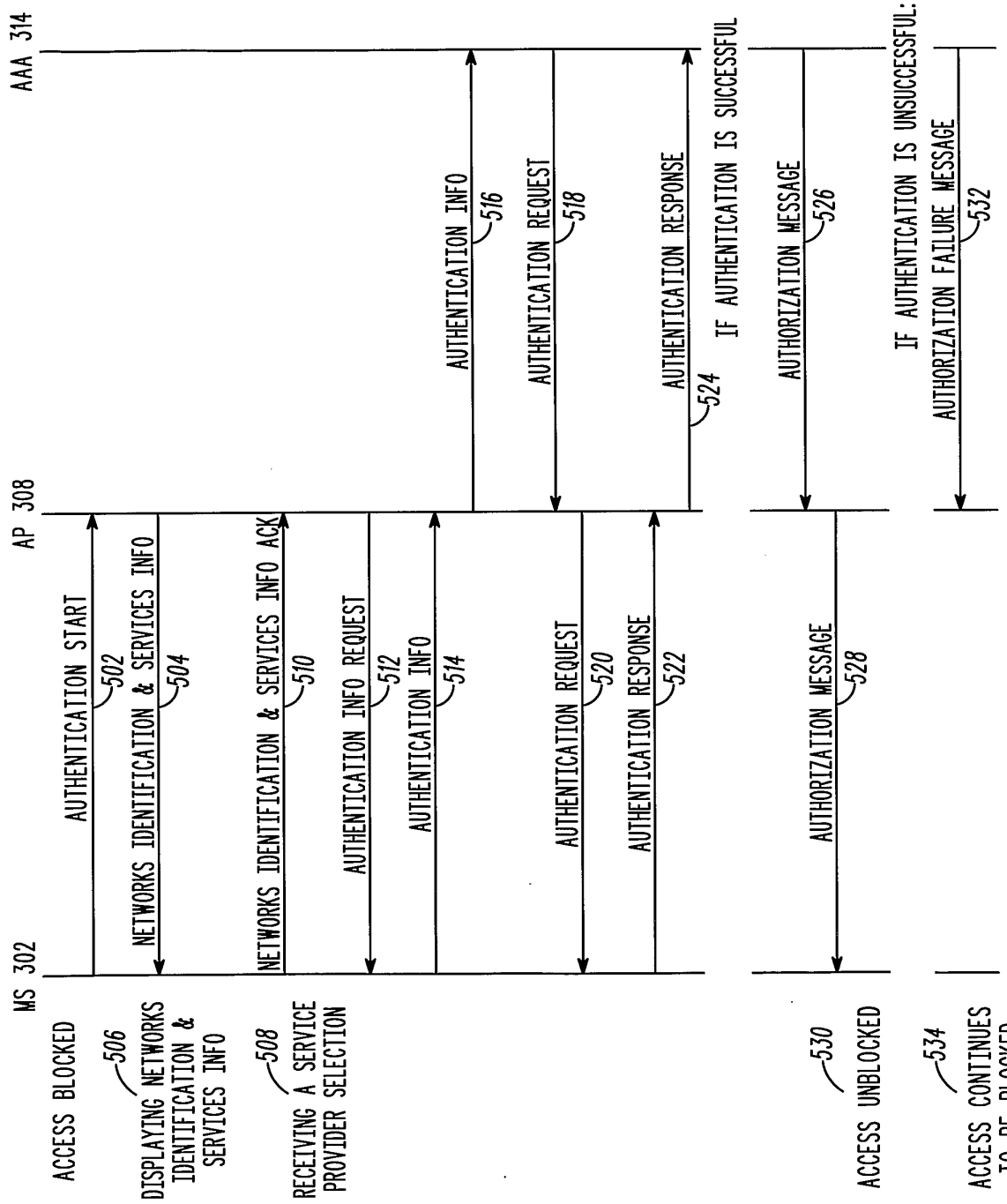

MS 302
AP 308
AAA 314
ACCESS BLOCKED
AUTHENTICATION START
502
NETWORKS IDENTIFICATION & SERVICES INFO
504
DISPLAYING NETWORKS IDENTIFICATION & SERVICES INFO
506
NETWORKS IDENTIFICATION & SERVICES INFO ACK
510
RECEIVING A SERVICE PROVIDER SELECTION
508
AUTHENTICATION INFO REQUEST
512
AUTHENTICATION INFO
514
AUTHENTICATION INFO
516
AUTHENTICATION REQUEST
518
AUTHENTICATION REQUEST
520
AUTHENTICATION RESPONSE
522
AUTHENTICATION RESPONSE
524
IF AUTHENTICATION IS SUCCESSFUL
AUTHORIZATION MESSAGE
528
ACCESS UNBLOCKED
530
AUTHORIZATION MESSAGE
526
IF AUTHENTICATION IS UNSUCCESSFUL:
AUTHORIZATION FAILURE MESSAGE
532
ACCESS CONTINUES TO BE BLOCKED
534
500

FIG. 5

Electronic Acknowledgement Receipt

EFS ID:	17502026
Application Number:	14082040
International Application Number:	
Confirmation Number:	1015
Title of Invention:	Device-Assisted Services for Protecting Network Capacity
First Named Inventor/Applicant Name:	
Customer Number:	106963
Filer:	Krista Susan Jacobsen/Ann Taylor
Filer Authorized By:	Krista Susan Jacobsen
Attorney Docket Number:	RALEP032C1
Receipt Date:	26-NOV-2013
Filing Date:	
Time Stamp:	00:06:17
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	P032C1IDS1.pdf	623638 8c663ced4337b03467e9f7f72aee3ebcaa602d98	no	37

Warnings:	
Information:	

2	Information Disclosure Statement (IDS) Form (SB08)	P032C1IDS2.pdf	618104 7944f5d52227ad88233048a66777fd0a181a8f66	no	22
Warnings:					
Information:					
3	Information Disclosure Statement (IDS) Form (SB08)	P032C1IDS3.pdf	619078 fb6d14ab18852239c29695e1e89d2477a10702f9	no	30
Warnings:					
Information:					
4	Transmittal Letter	P032C1TransLtr.pdf	313627 8cebbc7e2ab95a9a2f1ea83129509b891302b656	no	2
Warnings:					
Information:					
5	Foreign Reference	2037_CN1538730A.pdf	550169 2e3e24baa9d5890cdf219fc4a3d0303062aeda8c	no	11
Warnings:					
Information:					
6	Foreign Reference	2038_CN101115248B.pdf	798834 75acfe730044fed57cd917c2eae4f33b5e7d5028	no	15
Warnings:					
Information:					
7	Foreign Reference	2039_CN101341764A.pdf	1138895 2e2dbcd7a125a434c6548925e43e263bfbdc4a20	no	25
Warnings:					
Information:					
8	Foreign Reference	2039_WO2007068288A1.pdf	216996 5471cebc5a9ee9308c5123883f1aef1064b81f4f	no	32
Warnings:					
Information:					
9	Foreign Reference	2040_CN1802839A.pdf	891159 52b2d7b964ee757bb22239fc56aa4b0e6b82ac84	no	18
Warnings:					
Information:					
10	Foreign Reference	2040_WO2004064306A2.pdf	510026 4efd4e07b8efec25946c766ec966cd4a4accab55	no	22
Warnings:					
Information:					

11	Non Patent Literature	3032_Verizon.pdf	80548 984c09646690e8def9b16a30b9eef2c953a6263d	no	2
Warnings:					
Information:					
12	Non Patent Literature	3033_ChineseLit.pdf	692944 27c80a849cc8dbc81b552f052687e58018a96512	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	7054018		

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

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

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

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

Doc Code: PD.TO.AUTH
Document Description: Authorization to access Appl. by Trilateral Office

PTO/SB/39 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

AUTHORIZATION TO PERMIT ACCESS TO APPLICATION BY PARTICIPATING OFFICES

Send completed form to: Commissioner for Patents
P.O. Box 1450, Alexandria, VA 22313-1450

COMPLETE IF KNOWN	
Application Number	
Filing Date	November 15, 2013
First Named Inventor	Raleigh
Attorney Docket Number	RALEP032C1
Title (Required)	DEVICE-ASSISTED SERVICES FOR PROTECTING NETWORK CAPACITY

The undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the above-identified patent application is filed access to the above-identified patent application. See 37 CFR 1.14(c) and (h).

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

In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date of filing the Authorization to Permit Access to Application by Participating Offices.

This written authorization should be submitted prior to the filing of a subsequent foreign application, in which priority is claimed to the above-identified patent application, with any intellectual property office (e.g., the EPO, JPO, KIPO, or DAS Accessing Office). However, if applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the above-identified patent application is filed to have access to the above-identified patent application, this written authorization should not be filed.

No fee will be charged under 37 CFR 1.19(b)(1) for providing a participating intellectual property office with an electronic copy of the above-identified patent application.

This form must be signed by an authorized party in accordance with 37 CFR 1.14(c).

/Krista S. Jacobsen/	November 15, 2013
Signature	Date
Krista S. Jacobsen	650-517-2798
Printed or Typed Name	Telephone Number
Head Counsel	59374
Title	Registration Number, if applicable

This collection of information is required by 37 CFR 1.14(h). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process an application). Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 6 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

Privacy Act Statement

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

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

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

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	Device-Assisted Services for Protecting Network Capacity
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Filer:	Krista Susan Jacobsen/Ann Taylor
Attorney Docket Number:	RALEP032D1

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility filing Fee (Electronic filing)	4011	1	70	70
Utility Search Fee	2111	1	300	300
Utility Examination Fee	2311	1	360	360
Pages:				
Utility Appl Size fee per 50 sheets >100	2081	1	200	200
Claims:				
Claims in excess of 20	2202	3	40	120
Miscellaneous-Filing:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Publ. Fee- Early, Voluntary, or Normal	1504	1	300	300
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**1350**

Electronic Acknowledgement Receipt

EFS ID:	17421797
Application Number:	14082040
International Application Number:	
Confirmation Number:	1015
Title of Invention:	Device-Assisted Services for Protecting Network Capacity
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	Krista Susan Jacobsen/Ann Taylor
Filer Authorized By:	Krista Susan Jacobsen
Attorney Docket Number:	RALEP032D1
Receipt Date:	15-NOV-2013
Filing Date:	
Time Stamp:	20:39:34
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$1350
RAM confirmation Number	7668
Deposit Account	505876
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

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

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

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

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Application Data Sheet	P032C1ADS.pdf	139319 c8e807614ec2cc2111501da61305d9d6b25c41f1	no	12
Warnings:					
Information:					
This is not an USPTO supplied ADS fillable form					
2		P032C1Application.pdf	721108 2873d8374877384ba025e4924417e554f3dbfee1	yes	158

Multipart Description/PDF files in .zip description

Document Description	Start	End
Specification	1	152
Claims	153	157
Abstract	158	158

Warnings:					
Information:					
3	Drawings-only black and white line drawings	P032C1Drawings.PDF	149242 ff64930648ecaad1f4c61a7ef0a822f2acc416a3	no	29
Warnings:					
Information:					
4	Oath or Declaration filed	P032C1Decl_Ali.pdf	328519 f6668a607c81a8ab900630a87e08b97f21b79461	no	1
Warnings:					
Information:					
5	Oath or Declaration filed	P032C1Decl_Greg.pdf	320676 17690dab2fef99c7dbe660bd9fbcca18afb1f7cc	no	1
Warnings:					
Information:					
6	Oath or Declaration filed	P032C1Decl_Lavine.pdf	574436 d0e5c3946d8084e0f5e7b354ad4ec23598c7e119	no	2

Warnings:					
Information:					
7	Authorization to access Appl. by Trilateral Office	P032C1Authorize.pdf	80642 f5b5c22f475f5051c3bed8c9335d74bd29914c67	no	2
Warnings:					
Information:					
8	Fee Worksheet (SB06)	fee-info.pdf	39939 778253ca935f9bb488b04d420e1576d33098727d	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	2353881		

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

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

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

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

Application Data Sheet	Attorney Docket No.	RALEP032C1
	Application Number	
Title of Invention	DEVICE-ASSISTED SERVICES FOR PROTECTING NETWORK CAPACITY	

Inventor Information:

Inventor 1 -

Legal Name:

First Name:	Gregory
Middle Name:	G.
Family Name:	Raleigh

Residence Information:

City:	Woodside
State:	CA
Country of Residence:	USA

Mailing Address of Inventor: 350 Marine Parkway, Suite 300
Redwood Shores, CA 94065
USA

Inventor 2 -

Legal Name:

First Name:	Alireza
Middle Name:	
Family Name:	Raissinia

Residence Information:

City:	Monte Sereno
State:	CA
Country of Residence:	USA

Mailing Address of Inventor: 350 Marine Parkway, Suite 300
Redwood Shores, CA 94065
USA

Application Data Sheet	Attorney Docket No.	RALEP032C1
	Application Number	
Title of Invention	DEVICE-ASSISTED SERVICES FOR PROTECTING NETWORK CAPACITY	

Inventor 3 -

Legal Name:

First Name:	James
Middle Name:	
Family Name:	Lavine

Residence Information:

City:	Corte Madera
State:	CA
Country of Residence:	USA

Mailing Address of Inventor: 350 Marine Parkway, Suite 300
Redwood Shores, CA 94065
USA

Correspondence Information:

Correspondence Address:	Customer Number 106963
E-mail address:	patent@headwaterllc.com

Application Information:

Title of Invention:	DEVICE-ASSISTED SERVICES FOR PROTECTING NETWORK CAPACITY
Attorney Docket Number:	RALEP032C1
Small Entity Status Claimed:	Yes
Application Type:	Nonprovisional
Subject Matter:	Utility
Total Number of Drawing Sheets:	29

Application Data Sheet		Attorney Docket No.	RALEP032C1
		Application Number	
Title of Invention	DEVICE-ASSISTED SERVICES FOR PROTECTING NETWORK CAPACITY		

Suggested Drawing Figure for Publication: ——

Representative Information:

Customer Number: 106963

Domestic Benefit/National Stage Information:

This application is a DIV of Application No. 13/134,028, filed 05/25/2011

and said Application No. 13/134,028, filed 05/25/2011
is a CIP of Application No. 12/380,759, filed 03/02/2009 (PAT 8270310)
and is a CIP of Application No. 12/380,779, filed 03/02/2009
and is a CIP of Application No. 12/380,758, filed 03/02/2009
and is a CIP of Application No. 12/380,778, filed 03/02/2009 (PAT 8321526)
and is a CIP of Application No. 12/380,768, filed 03/02/2009
and is a CIP of Application No. 12/380,767, filed 03/02/2009 (PAT 8355337)
and is a CIP of Application No. 12/380,780, filed 03/02/2009
and is a CIP of Application No. 12/380,755, filed 03/02/2009 (PAT 8331901)
and is a CIP of Application No. 12/380,756, filed 03/02/2009 (PAT 8250207)
and is a CIP of Application No. 12/380,770, filed 03/02/2009 (ABN)
and is a CIP of Application No. 12/380,772, filed 03/02/2009
and is a CIP of Application No. 12/380,782, filed 03/02/2009 (PAT 8270952)
and is a CIP of Application No. 12/380,783, filed 03/02/2009
and is a CIP of Application No. 12/380,757, filed 03/02/2009 (PAT 8326958)
and is a CIP of Application No. 12/380,781, filed 03/02/2009 (PAT 8229812)
and is a CIP of Application No. 12/380,774, filed 03/02/2009
and is a CIP of Application No. 12/380,771, filed 03/02/2009 (PAT 8023425)
and is a CIP of Application No. 12/380,773, filed 03/02/2009
and is a CIP of Application No. 12/380,769, filed 03/02/2009
and is a CIP of Application No. 12/380,777, filed 03/02/2009 (PAT 8583781)
and is a CIP of Application No. 12/695,019, filed 01/27/2010 (PAT 8275830)
and is a CIP of Application No. 12/695,020, filed 01/27/2010 (PAT 8406748)
and is a CIP of Application No. 12/694,445, filed 01/27/2010 (PAT 8391834)
and is a CIP of Application No. 12/694,451, filed 01/27/2010 (PAT 8548428)

and is a CIP of Application No. 12/694,455, filed 01/27/2010 (PAT 8402111)
and is a CIP of Application No. 12/695,021, filed 01/27/2010 (PAT 8346225)
and is a CIP of Application No. 12/695,980, filed 01/28/2010 (PAT 8340634)
and is a CIP of Application No. 13/134,005, filed 05/25/2011
and claims benefit of Application No. 61/348,022, filed 05/25/2010
and claims benefit of Application No. 61/381,159, filed 09/09/2010
and claims benefit of Application No. 61/381,162, filed 09/09/2010
and claims benefit of Application No. 61/384,456, filed 09/20/2010
and claims benefit of Application No. 61/385,020, filed 09/21/2010
and claims benefit of Application No. 61/387,243, filed 09/28/2010
and claims benefit of Application No. 61/387,247, filed 09/28/2010
and claims benefit of Application No. 61/389,547, filed 10/04/2010
and claims benefit of Application No. 61/407,358, filed 10/27/2010
and claims benefit of Application No. 61/418,507, filed 12/01/2010
and claims benefit of Application No. 61/418,509, filed 12/01/2010
and claims benefit of Application No. 61/420,727, filed 12/07/2010
and claims benefit of Application No. 61/422,565, filed 12/13/2010
and claims benefit of Application No. 61/422,572, filed 12/13/2010
and claims benefit of Application No. 61/422,574, filed 12/13/2010
and claims benefit of Application No. 61/435,564, filed 01/24/2011
and claims benefit of Application No. 61/472,606, filed 04/06/2011

and said Application No. 12/380,759, filed 03/02/2009 (PAT 8270310)
claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,779, filed 03/02/2009
claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,758, filed 03/02/2009
claims benefit of Application No. 61/206,354, filed 01/28/2009

and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,778, filed 03/02/2009 (PAT 8321526)
claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,768, filed 03/02/2009
claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,767, filed 03/02/2009 (PAT 8355337)
claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,780, filed 03/02/2009
claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,755, filed 03/02/2009 (PAT 8331901)
claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,756, filed 03/02/2009 (PAT 8250207)
claims benefit of Application No. 61/206,354, filed 01/28/2009

and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,770, filed 03/02/2009 (ABN)
claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,772, filed 03/02/2009
claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,782, filed 03/02/2009 (PAT 8270952)
claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,783, filed 03/02/2009
claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,757, filed 03/02/2009 (PAT 8326958)
claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,781, filed 03/02/2009 (PAT 8229812)
claims benefit of Application No. 61/206,354, filed 01/28/2009

and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,774, filed 03/02/2009
claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,771, filed 03/02/2009 (PAT 8023425)
claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,773, filed 03/02/2009
claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,769, filed 03/02/2009
claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/380,777, filed 03/02/2009 (PAT 8583781)
claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009

and said Application No. 12/695,019, filed 01/27/2010 (PAT 8275830)
is a CIP of Application No. 12/380,778, filed 03/02/2009 (PAT 8321526)

and is a CIP of Application No. 12/380,771, filed 03/02/2009 (PAT 8023425)
and claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009
and claims benefit of Application No. 61/270,353, filed 07/06/2009
and claims benefit of Application No. 61/264,126, filed 11/24/2009

and said Application No. 12/695,020, filed 01/27/2010 (PAT 8406748)
is a CIP of Application No. 12/380,780, filed 03/02/2009
and claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009
and claims benefit of Application No. 61/275,208, filed 08/25/2009
and claims benefit of Application No. 61/237,753, filed 08/28/2009

and said Application No. 12/694,445, filed 01/27/2010 (PAT 8391834)
is a CIP of Application No. 12/380,780, filed 03/02/2009
and claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009
and claims benefit of Application No. 61/252,151, filed 10/15/2009

and said Application No. 12/694,451, filed 01/27/2010 (PAT 8548428)
is a CIP of Application No. 12/380,780, filed 03/02/2009
and claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009
and claims benefit of Application No. 61/270,353, filed 07/06/2009
and claims benefit of Application No. 61/252,153, filed 10/15/2009

and said Application No. 12/694,455, filed 01/27/2010 (PAT 8402111)
is a CIP of Application No. 12/380,780, filed 03/02/2009

and claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009
and claims benefit of Application No. 61/264,120, filed 11/24/2009

and said Application No. 12/695,021, filed 01/27/2010 (PAT 8346225)
is a CIP of Application No. 12/380,780, filed 03/02/2009
and claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009
and claims benefit of Application No. 61/252,151, filed 10/15/2009
and claims benefit of Application No. 61/252,153, filed 10/15/2009

and said Application No. 12/695,980, filed 01/28/2010 (PAT 8340634)
is a CIP of Application No. 12/380,780, filed 03/02/2009
and is a CIP of Application No. 12/695,019, filed 01/27/2010 (PAT 8275830)
and is a CIP of Application No. 12/695,021, filed 01/27/2010 (PAT 8346225)
and claims benefit of Application No. 61/206,354, filed 01/28/2009
and claims benefit of Application No. 61/206,944, filed 02/04/2009
and claims benefit of Application No. 61/207,393, filed 02/10/2009
and claims benefit of Application No. 61/207,739, filed 02/13/2009
and claims benefit of Application No. 61/270,353, filed 07/06/2009

and said Application No. 13/134,005, filed 05/25/2011
is a CIP of Application No. 12/380,759, filed 03/02/2009 (PAT 8270310)
and is a CIP of Application No. 12/380,779, filed 03/02/2009
and is a CIP of Application No. 12/380,758, filed 03/02/2009
and is a CIP of Application No. 12/380,778, filed 03/02/2009 (PAT 8321526)
and is a CIP of Application No. 12/380,768, filed 03/02/2009
and is a CIP of Application No. 12/380,767, filed 03/02/2009 (PAT 8355337)
and is a CIP of Application No. 12/380,780, filed 03/02/2009
and is a CIP of Application No. 12/380,755, filed 03/02/2009 (PAT 8331901)
and is a CIP of Application No. 12/380,756, filed 03/02/2009 (PAT 8250207)
and is a CIP of Application No. 12/380,770, filed 03/02/2009 (ABN)

and is a CIP of Application No. 12/380,772, filed 03/02/2009
and is a CIP of Application No. 12/380,782, filed 03/02/2009 (PAT 8270952)
and is a CIP of Application No. 12/380,783, filed 03/02/2009
and is a CIP of Application No. 12/380,757, filed 03/02/2009 (PAT 8326958)
and is a CIP of Application No. 12/380,781, filed 03/02/2009 (PAT 8229812)
and is a CIP of Application No. 12/380,774, filed 03/02/2009
and is a CIP of Application No. 12/380,771, filed 03/02/2009 (PAT 8023425)
and is a CIP of Application No. 12/380,773, filed 03/02/2009
and is a CIP of Application No. 12/380,769, filed 03/02/2009
and is a CIP of Application No. 12/380,777, filed 03/02/2009 (PAT 8583781)
and is a CIP of Application No. 12/695,019, filed 01/27/2010 (PAT 8275830)
and is a CIP of Application No. 12/695,020, filed 01/27/2010 (PAT 8406748)
and is a CIP of Application No. 12/694,445, filed 01/27/2010 (PAT 8391834)
and is a CIP of Application No. 12/694,451, filed 01/27/2010 (PAT 8548428)
and is a CIP of Application No. 12/694,455, filed 01/27/2010 (PAT 8402111)
and is a CIP of Application No. 12/695,021, filed 01/27/2010 (PAT 8346225)
and is a CIP of Application No. 12/695,980, filed 01/28/2010 (PAT 8340634)
and claims benefit of Application No. 61/348,022, filed 05/25/2010
and claims benefit of Application No. 61/381,159, filed 09/09/2010
and claims benefit of Application No. 61/381,162, filed 09/09/2010
and claims benefit of Application No. 61/384,456, filed 09/20/2010
and claims benefit of Application No. 61/385,020, filed 09/21/2010
and claims benefit of Application No. 61/387,243, filed 09/28/2010
and claims benefit of Application No. 61/387,247, filed 09/28/2010
and claims benefit of Application No. 61/389,547, filed 10/04/2010
and claims benefit of Application No. 61/407,358, filed 10/27/2010
and claims benefit of Application No. 61/418,507, filed 12/01/2010
and claims benefit of Application No. 61/418,509, filed 12/01/2010
and claims benefit of Application No. 61/420,727, filed 12/07/2010
and claims benefit of Application No. 61/422,565, filed 12/13/2010
and claims benefit of Application No. 61/422,572, filed 12/13/2010
and claims benefit of Application No. 61/422,574, filed 12/13/2010
and claims benefit of Application No. 61/435,564, filed 01/24/2011
and claims benefit of Application No. 61/472,606, filed 04/06/2011

Application Data Sheet		Attorney Docket No.	RALEP032C1
		Application Number	
Title of Invention	DEVICE-ASSISTED SERVICES FOR PROTECTING NETWORK CAPACITY		

Foreign Priority Information:

None.

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications:

☐	This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013. NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Authorization to Permit Access:

Applicant's completed Authorization to Permit Access to Application by Participating Offices, Form PTO/SB/39, accompanies this filing.

Applicant Information:

Assignee is:	The Assignee, which is an Organization
Organization Name:	Headwater Partners I LLC
Mailing Address Information for Applicant:	Headwater Partners I LLC 350 Marine Parkway, Suite 300 Redwood Shores, CA 94065 U.S.A. (650) 517-2786
E-mail Address:	patent@headwaterllc.com

Application Data Sheet		Attorney Docket No.	RALEP032C1
		Application Number	
Title of Invention	DEVICE-ASSISTED SERVICES FOR PROTECTING NETWORK CAPACITY		

Signature:

Signature: /Krista S. Jacobsen/

Date: November 15, 2013

Printed/Typed Name: Krista S. Jacobsen

Registration Number: 59,374

UNITED STATES PATENT APPLICATION

FOR

DEVICE-ASSISTED SERVICES FOR PROTECTING NETWORK CAPACITY

INVENTORS:

GREGORY G. RALEIGH

ALI RAISSINIA

JAMES LAVINE

PREPARED BY:

HEADWATER PARTNERS I LLC
350 MARINE PARKWAY, SUITE 300
REDWOOD SHORES, CA 94065
650-517-2798

ATTORNEY DOCKET NO.: RALEP032C1

DEVICE-ASSISTED SERVICES FOR PROTECTING NETWORK CAPACITY

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application is a divisional of co-pending nonprovisional U.S. Patent Application No. 13/134,028, which is hereby incorporated by reference for all purposes. This application also incorporates by reference the following published U.S. pending nonprovisional patent applications: U.S. publication No. 2010/0188975, filed March 2, 2009, entitled "Verifiable Device Assisted Service Policy Implementation," U.S. publication No. 2010/0192170, filed March 2, 2009, entitled "Device Assisted Service Profile Management with User Preference, Adaptive Policy, Network Neutrality, and User Privacy," U.S. publication No. 2010/0191612, filed March 2, 2009, entitled "Verifiable Device Assisted Service Usage Monitoring with Reporting, Synchronization, and Notification," U.S. publication No. 2010/0191576, filed March 2, 2009, entitled "Verifiable Device Assisted Service Usage Billing with Integrated Accounting, Mediation Accounting, and Multi-Account," U.S. publication No. 2010/0188991, filed March 2, 2009, entitled "Network Based Service Policy Implementation with Network Neutrality and User Privacy," U.S. publication No. 2010/0188990, filed March 2, 2009, entitled "Network Based Service Profile Management with User Preference, Adaptive Policy, Network Neutrality and User Privacy," U.S. publication No. 2010/0192212, filed March 2, 2009, entitled "Automated Device Provisioning and Activation," U.S. publication No. 2010/0191604, filed March 2, 2009, entitled "Device Assisted Ambient Services," U.S. publication No. 2010/0191575, filed March 2, 2009, entitled "Network Based Ambient Services," U.S. publication No. 2010/0188993, filed March 2, 2009, entitled "Network Tools for Analysis, Design, Testing, and Production of Services," U.S. publication No. 2010/0190470, filed March 2, 2009, entitled "Roaming Services Network and Overlay Networks," U.S. publication No. 2010/0192120, filed March 2, 2009, entitled "Open Development System for Access Service Providers," U.S. publication No. 2010/0192207, filed March 2, 2009, entitled "Virtual Service Provider Systems," U.S. application serial No. 12/380,757, filed March 2, 2009, and entitled "Service Activation Tracking System," U.S. publication No. 2010/0191613, filed March 2, 2009, entitled "Open Transaction Central Billing System," U.S. publication No. 2010/0188995, filed March 2, 2009, entitled "Verifiable and Accurate Service Usage Monitoring for Intermediate Networking Devices," U.S. publication No. 2010/0188994, filed March 2, 2009, entitled "Verifiable Service

Billing for Intermediate Networking Devices," U.S. publication No. 2010/0191846, filed March 2, 2009, entitled "Verifiable Service Policy Implementation for Intermediate Networking Devices," U.S. publication No. 2010/0188992, filed March 2, 2009, entitled "Service Profile Management with User Preference, Adaptive Policy, Network Neutrality and User Privacy for Intermediate Networking Devices," U.S. publication No. 2010/0191847, filed March 2, 2009, entitled "Simplified Service Network Architecture," U.S. publication No. 2010/0197266, filed January 27, 2010, entitled "Device Assisted CDR Creation, Aggregation, Mediation, and Billing," U.S. publication No. 2010/0198698, filed January 27, 2010, entitled "Adaptive Ambient Services," U.S. publication No. 2010/0199325, filed January 27, 2010, entitled "Security Techniques for Device Assisted Services," U.S. publication No. 2010/0197267, filed January 27, 2010, entitled "Device Group Partitions and Settlement Platform," U.S. publication No. 2010/0198939, filed January 27, 2010, entitled "Device Assisted Services Install," U.S. publication No. 2010/0195503, filed January 27, 2010, entitled "Quality of Service for Device Assisted Services," U.S. publication No. 2010/0197268, filed January 28, 2010, entitled "Enhanced Roaming Services and Converged Carrier Networks with Device Assisted Services and a Proxy," and U.S. application serial No. 13/13/134,005, filed May 25, 2011, and entitled "System and Method for Wireless Network Offloading."

[0002] This application also incorporates by reference the following U.S. pending provisional patent applications: U.S. provisional application serial No. 61/348,022, filed May 25, 2010, entitled "Device Assisted Services for Protecting Network Capacity," U.S. provisional application serial No. 61/381,159, filed September 9, 2010, entitled "Device Assisted Services for Protecting Network Capacity," U.S. provisional application serial No. 61/381,162, filed September 9, 2010, entitled "Service Controller Interfaces and Workflows," U.S. provisional application serial No. 61/384,456, filed September 20, 2010, entitled "Securing Service Processor with Sponsored SIMs," U.S. provisional application serial No. 61/389,547, filed October 4, 2010, entitled "User Notifications for Device Assisted Services," U.S. provisional application serial No. 61/385,020, filed September 21, 2010, entitled "Service Usage Reconciliation System Overview," U.S. provisional application serial No. 61/387,243, filed September 28, 2010, entitled "Enterprise and Consumer Billing Allocation for Wireless Communication Device Service Usage Activities," U.S. provisional application serial No.

61/387,247, filed September 28, 2010, entitled "Secured Device Data Records," U.S. provisional application serial No. 61/407,358, filed October 27, 2010, entitled "Service Controller and Service Processor Architecture," U.S. provisional application serial No. 61/418,507, filed December 1, 2010, entitled "Application Service Provider Interface System," U.S. provisional application serial No. 61/418,509, filed December 1, 2010, entitled "Service Usage Reporting Reconciliation and Fraud Detection for Device Assisted Services," U.S. provisional application serial No. 61/420,727, filed December 7, 2010, entitled "Secure Device Data Records," U.S. provisional application serial No. 61/422,565, filed December 13, 2010, entitled "Service Design Center for Device Assisted Services," U.S. provisional application serial No. 61/422,572, filed December 13, 2010, entitled "System Interfaces and Workflows for Device Assisted Services," U.S. provisional application serial No. 61/422,574, filed December 13, 2010, entitled "Security and Fraud Detection for Device Assisted Services," U.S. provisional application serial No. 61/435,564, filed January 24, 2011, entitled "Framework for Device Assisted Services," and U.S. provisional application serial No. 61/472,606, filed April 6, 2011, entitled "Managing Service User Discovery and Service Launch Object Placement on a Device."

[0003] Further, this application incorporates by reference the following U.S. provisional patent applications: U.S. provisional application serial No. 61/206,354, filed January 28, 2009, entitled "Services Policy Communication System and Method," U.S. provisional application serial No. 61/206,944, filed February 4, 2009, entitled "Services Policy Communication System and Method," U.S. provisional application serial No. 61/207,393, filed February 10, 2009, entitled "Services Policy Communication System and Method," U.S. provisional application serial No. 61/207,739, filed February 13, 2009, entitled "Services Policy Communication System and Method," U.S. provisional application serial No. 61/270,353, filed July 6, 2009, entitled "Device Assisted CDR Creation, Aggregation, Mediation and Billing," U.S. provisional application serial No. 61/275,208, filed August 25, 2009, entitled "Adaptive Ambient Services," U.S. provisional application serial No. 61/237,753, filed August 28, 2009, entitled "Adaptive Ambient Services," U.S. provisional application serial No. 61/252,151, filed October 15, 2009, entitled "Security Techniques for Device Assisted Services," U.S. provisional application serial No. 61/252,153, filed October 15, 2009, entitled "Device Group Partitions and Settlement Platform," U.S. provisional application serial No. 61/264,120, filed November 24, 2009, entitled "Device

Assisted Services Install," and U.S. provisional application serial No. 61/264,126, filed November 24, 2009, entitled "Device Assisted Services Activity Map."

BACKGROUND

[0004] With the advent of mass market digital communications, applications and content distribution, many access networks such as wireless networks, cable networks and Digital Subscriber Line (DSL) networks are pressed for user capacity, with, for example Evolution-Data Optimized (EVDO), High Speed Packet Access (HSPA), Long Term Evolution (LTE), Worldwide Interoperability for Microwave Access (WiMax), DOCSIS, DSL, and Wireless Fidelity (Wi-Fi) becoming user capacity constrained. In the wireless case, although network capacity will increase with new higher capacity wireless radio access technologies, such as Multiple-Input Multiple-Output (MIMO), and with more frequency spectrum and cell splitting being deployed in the future, these capacity gains are likely to be less than what is required to meet growing digital networking demand.

[0005] Similarly, although wire line access networks, such as cable and DSL, can have higher average capacity per user compared to wireless, wire line user service consumption habits are trending toward very high bandwidth applications and content 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.

[0006] The foregoing example of trends and issues is intended to be illustrative and not exclusive. Other limitations of the art will become apparent to those of skill in the relevant art upon a reading of the specification and a study of the drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] FIG. 1 illustrates a functional diagram of a network architecture for providing quality of service (QoS) for device assisted services (DAS) and/or for providing DAS for protecting network capacity in accordance with some embodiments.

[0008] FIG. 2 illustrates another functional diagram of another network architecture for providing quality of service (QoS) for device assisted services (DAS) and/or for providing DAS for protecting network capacity in accordance with some embodiments.

[0009] FIG. 3 illustrates a functional diagram of an architecture including a device based service processor and a service controller for providing quality of service (QoS) for device assisted services (DAS) and/or for providing DAS for protecting network capacity in accordance with some embodiments.

[0010] FIGS. 4A through 4C illustrates a functional diagram for providing quality of service (QoS) for device assisted services (DAS) in accordance with some embodiments.

[0011] FIG. 5 illustrates a functional diagram for generating a QoS activity map for quality of service (QoS) for device assisted services (DAS) in accordance with some embodiments.

[0012] FIG. 6 illustrates a functional diagram for quality of service (QoS) for device assisted services (DAS) for an end to end coordinated QoS service channel control in accordance with some embodiments.

[0013] FIG. 7 illustrates a flow diagram for quality of service (QoS) for device assisted services (DAS) in accordance with some embodiments.

[0014] FIGS. 8A through 8C each illustrate another flow diagram for quality of service (QoS) for device assisted services (DAS) in accordance with some embodiments.

[0015] FIG. 9 illustrates another flow diagram for quality of service (QoS) for device assisted services (DAS) in accordance with some embodiments.

[0016] FIG. 10 illustrates another flow diagram for quality of service (QoS) for device assisted services (DAS) in accordance with some embodiments.

[0017] FIG. 11 illustrates another flow diagram for quality of service (QoS) for device assisted services (DAS) in accordance with some embodiments.

[0018] FIG. 12 illustrates a device stack for providing various service usage measurement techniques in accordance with some embodiments.

[0019] FIG. 13 illustrates another device stack for providing various service usage measurement techniques in accordance with some embodiments.

[0020] FIG. 14 illustrates a flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments.

[0021] FIG. 15 illustrates another flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments.

[0022] FIG. 16 illustrates another flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments.

[0023] FIG. 17 illustrates another flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments.

[0024] FIG. 18 illustrates another flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments.

[0025] FIG. 19 illustrates another flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments.

[0026] FIG. 20 illustrates another flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments.

[0027] FIG. 21 illustrates another flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments.

[0028] FIG. 22 illustrates another flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments.

[0029] FIG. 23 illustrates a network capacity controlled services priority level chart for device assisted services (DAS) for protecting network capacity in accordance with some embodiments.

[0030] FIG. 24 depicts a diagram of a network capacity protection system utilizing device-assisted services (DAS).

[0031] FIG. 25 depicts a diagram an example of a differential access control notification system.

[0032] FIG. 26 depicts an example of a computer system on which techniques described in this paper can be implemented.

[0033] FIG. 27 depicts a diagram of an example of a system for application-specific differential network access control.

DETAILED DESCRIPTION

[0034] 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.

[0035] 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.

[0036] As the network capacity gains are less than what is required to meet growing digital networking demand, a network capacity crunch is developing due to increasing network congestion on various wireless networks, such as mobile networks. The increasing popularity of various smart phone devices, net book devices, tablet computing devices, and various other wireless mobile computing devices, which are becoming increasingly popular on 3G, 4G, and other advanced wireless networks, is contributing to the network capacity crunch. Some network carriers have indicated that a relatively small number of users on such devices demand a

disproportionately significant amount of their network capacity. For example, AT&T has recently indicated that about 3 percent of its smart phone device users (e.g., Apple iPhone® users) are generating approximately 40 percent of the operator's data traffic.

[0037] For example, in wireless networks, managing the wireless access connection capacity and network access connection resources is important to maintain network performance as network resources/capacity demand increases. Many network performance measures can be advantageously maintained or improved as network loading increases if capacity management and/or network resource management is employed. For example, these performance measures include network availability; the ability to deliver connections to all devices, users and/or applications seeking connections and enabled for service on the network; network access attempt success rate; the transmission speed experienced by one or more devices, users or applications; the average transmission speed experienced by all devices, users and/or applications; network bit error rate or packet error rate; the time delay from network access request to delivered access connection; the one-way delay or round-trip delay for a transmission; the delay timing jitter for a transmission; the time variation in transmission speed for one or more connections; the ability of the network to deliver various requested/needed levels of Quality of Service (QoS) to devices, users or applications that require differentiated connection QoS classes; the ability of the network to maintain efficiency (e.g., aggregated service throughput measured across all devices, users, and/or applications); the ability of the network to share or distribute a performance measure (e.g., the performance measures listed above) uniformly or fairly across multiple devices, users, and/or applications that all have the same service quality class or the same service plan performance parameters.

[0038] For example, if there is a limited amount of shared bandwidth for a set of user devices (e.g., a set of devices on a wireless network, such as a given base station or base station controller or femto cell or pico cell; or a set of devices on a cable modem networks, etc.), and if multiple and/or all devices allow all applications to indiscriminately access or attempt to access network resources or transmit/receive traffic, then the network can generally become overloaded. As a result, a subset of users/devices or in some cases most or all users/devices obtain poor network performance. As another example, if one or more devices forming a subset of devices on the network allow multiple and/or all applications to indiscriminately access or attempt to access network resources or transmit/receive traffic, then the network can become overloaded.

As a result, a subset of users/devices or in some cases most or all users/devices obtain poor network performance.

[0039] Traditionally, mobile devices typically have specialized designs that are optimized to preserve network capacity and protect network resources from being over taxed. For example, wireless devices that browse the Internet often use specialized protocols such as WAP and data traffic compression or low resolution techniques rather than standard HTTP protocols and traffic used in wired Internet devices.

[0040] However, the wireless devices that implement specialized methods for accessing the Internet and/or other networks often implement complex specifications provided by one or more wireless carriers that own the networks that the device is designed to connect to. Such complex specifications often require time consuming design, testing, and certification processes. These processes in part have the effect of narrowing the base of device suppliers to those qualified and willing to perform the specialized design work required, slowing time to market for new devices, increasing the expense to develop new devices and reducing the types of applications that are supported.

[0041] Device OEMs have recently created wireless devices that are designed more like standard Internet devices and not fully optimized to preserve network capacity and resources. Many wireless service customers desire this type of device, and the OEMs generally want to reduce the complexity and time to market to deliver such devices. In addition, new market needs and new government requirements sometimes require that carriers offer a more open process for bringing new devices onto their network, in which the process does not require all of the specialized design and certification described above. These and various other factors are driving a growing need and trend for less complex and time consuming wireless device design and certification processes.

[0042] This trend has led many carriers to begin selling devices that are designed more as standard Internet service devices that connect to the Internet and other data networks through carrier wireless networks. As the cellular network is opened up to more and more new devices, applications and markets, there is a growing demand to allow general purpose Internet devices and applications to gain access to wireless networks without necessarily going through

specialized design and certification process requirements to make the devices and applications efficient and authorized for access to such wireless networks.

[0043] However, general purpose Internet devices are not as frugal or sparing with wireless network access bandwidth. Moreover, with the advent of always on wide area network connections to the Internet has led to popular Internet services and applications that typically assume very inexpensive access and generally heed no attention to, for example, network busy state. As more general purpose Internet devices are provided for us on various wireless networks (e.g., mobile wireless networks), a high frequency of inefficient wireless network accesses continue to rise, which can reduce network capacity sometimes to levels that hinder access to service for that device (e.g., user, device, software demand) and/or other devices on that wireless network and/or that wireless network segment. As discussed above, judicious use of wireless network bandwidth, capacity, and resources generally results in better service for all users, but at present, device manufacturers and wireless network providers (e.g., wireless network carriers or carriers) have not provided or implemented more intelligent bandwidth usage techniques. These factors generally result in less carrier control of device design, which poses a threat to longer term network capacity and performance preservation as the volume of devices with less optimized wireless designs continues to grow.

[0044] There are many network performance and user performance factors that are impacted by the efficiency of the network, including, for example, overall network congestion; the access network performance experienced by one or more groups of users, devices, applications, network service sources, communication protocols, and/or operating system functions; and/or the performance experienced by a given user, device, application, network service source, communication protocol, and/or operating system function. Under a relatively low capacity demand of a wireless network, network performance as experienced by a group of devices, applications, network service sources, communication protocols, operating system functions, and/or users or by a single device, application, network service source, communication protocol, operating system function, and/or user can degrade somewhat proportionally (e.g., aggregate traffic delivered by the network may be roughly proportional to the peak available network traffic) with incremental increases in network access and/or traffic demand from one or more groups of users, devices, applications, network service sources, communication protocols and/or operating system functions. However, as network resources/network capacity demand increases

(e.g., more wireless network data traffic is demanded in aggregate; more devices are serviced by the network; more users are serviced by the network; more applications are serviced by the network; more network service sources are serviced by the network; more operating system functions are serviced by the network; and/or more differentiated QoS sessions are serviced by the network), network availability/performance can decrease and/or the network may not adequately service one or more users, devices, applications, network service sources, communication protocols, and/or operating system functions, or may not service one or more groups of users, devices, applications, network service sources, communication protocols, and/or operating system functions.

[0045] There are many examples of how increasing network capacity demand can decrease network performance, including for example, to a decrease in average bandwidth offered per device (e.g., one or more users on a device, application, network service source, communication protocol, and/or operating system function executed/implemented on the device); an increase in traffic delivery latency; an increase in traffic delivery latency jitter; insufficient guaranteed or differentiated bandwidth for one or more differentiated QoS and/or dynamic QoS services (e.g., as described herein) to one or more devices, users, applications, network service sources, communication protocols, and/or operating system functions; increased latency for bandwidth reservation services; increased latency for QoS reservation services; performance problems with one or more communication protocols; unacceptable delays in user experience, and/or various other or similar consequences and device or user impacts resulting from reduced network availability and/or reduced network capacity. Examples of network communication protocols that can have degraded performance with excessive network loading or degraded network performance include, for example, Internet protocol (IP), HTML protocols, voice communication protocols including VOIP protocols, real-time video communication protocols, streaming media protocols (e.g., audio, video, etc), gaming protocols, VPN protocols, file download protocols, background service protocols, software update protocols, and/or various other network communication protocols. Thus, is it important to preserve/protect network capacity.

[0046] It is also important to control the number of transactions demanded from a given network resource (e.g., edge network segment, base station, base station controller, MAC resources, pico cell, femto cell, etc.) in a given period of time so that demand does not overcome the transaction servicing ability of that network resource. For example, network resources that

should not be subjected to excess transaction demand can include base station or base station controller resources, media access control (MAC) resources, traffic transport resources, AAA resources, security or authentication resources, home agent (HA) resources, DNS resources, resources that play a part in network discovery, gateway or router resources, data session reservation or establishment resources (e.g., network resources required to manage, set up, conduct, and/or close service sessions, PPP sessions, communication flows, communication streams, QoS flows, radio access bearer reservation resources , tunnels, VPNs, APNs, special service routing, etc.), bandwidth reservation resources, QoS reservation or coordination resources, QoS transport resources, service charging resources, traffic analysis resources, network security resources, and/or various other or similar network resources. In some networks, the network performance degradation due to a given measure of incremental increase in network resource/capacity demand can become relatively large as various network resources become increasingly taxed due to either limited transaction processing capability or limited traffic bandwidth for one or more of the network resources that participate in establishing, servicing, conducting, maintaining, and/or closing the necessary network service connections and/or information exchanges required to conduct a service activity. For example, if the equipment required to establish a PPP session can only handle a certain number of new PPP session openings and/or closings per given period of time, and if device behavior is such that PPP sessions are often opened and/or closed, then the rate of PPP session transactions (e.g., openings and/or closings) can exceed the transaction capacity of the PPP session management resources. This is sometimes referred to as "flooding" or "overloading" a network resource with excess demand or excess connections, and, in such cases, the network resource may begin falling behind in servicing transaction demand in a well controlled manner (e.g., the network resource may continue processing transactions at or near a maximum rate for that network resource), or in some cases, the resource may fall behind transaction demand in a less well controlled manner (e.g., the network resource may become overwhelmed such that its processing rate not only falls below aggregate transaction demand, but the transaction rate processing capability decreases under overload as well). In the PPP session establishment resource example, once the rate of requested transactions exceeds the resource maximum transaction rate, then unmet device demand can grow to a point where one or more devices experiences delays in connecting to and/or communicating (e.g., sending/receiving data) with the network.

[0047] As another example, in any type of random access bandwidth reservation protocol, MAC protocol, or bandwidth delivery protocol, in a network without proper management and/or control of traffic access reservations and/or transmissions, as the network demand increases there may be more collisions between reservation requests, traffic transmissions, application demands, network service source demands, communication protocol demands, and/or operating system function demands causing a decreasing network efficiency that can degrade user, device, application and/or network service performance so that performance falls below acceptable levels. As another example, in systems in which there is a QoS service session reservation system, uncontrolled and/or unmanaged QoS reservation requests and/or reservation grants can lead to a situation where the QoS reservation resources and/or QoS service delivery resources are over taxed to the point where QoS service performance falls below desired levels. As another example, in networks that require some form of minimum resource allocation for transmissions, reservations, or network resource transactions, the network can become inefficient if one or more devices, applications, network service sources, operating system functions, and/or communication protocols have a relatively high rate of network resource access attempts, network accesses or data transmissions for small transmission payloads (e.g., minimum MAC reservation factors, minimum security overhead factors, minimum QoS reservation factors, minimum time responses for establishing a base station connection, minimum time responses for establishing or closing/being released from a session, etc). Even if the data packet comprising the access event is small, the network resources required to complete the access event are often busy servicing the access event for much longer periods of time than are required for the actual data transmission.

[0048] Another example of device service activity behavior that can have an impact on network performance is the way the device, device subsystem, and/or modem subsystem power cycling or transitions from one power save state to another. For example, establishing a basic connection from a device to a wireless base station consumes base station resources for a period of time and in some cases can also consume other network resources such as AAA, HLR, HA, gateway, billing, and/or charging gateway resources. If a device terminates the connection to the base station when the modem subsystem (e.g., or some other portion of the device) goes from active connection state to a power save state, then each time the device enters power save state and then exits power save state network resources are consumed, sometimes for time periods

measured on the order of seconds or in extreme cases even minutes. If such a device has an aggressive power save algorithm that enters power save state after a short idle period, then the device behavior can consume a proportionally large amount of resources such that the network ability to support multiple devices is diminished, or such that the network cannot support very many similar devices on the network. Another similar example is the establishment of network sessions once the base station connection is established (e.g., establishing a PPP session between the device and a home agent (HA) or other gateway), in which network resources required to open and/or close the network session are ignorantly consumed if a device exhibits aggressive power save state cycling or frequently terminates the data session for other reasons.

[0049] Another example of device service activity behavior that can impact network performance is applications that maintain persistent network communication that generates a relatively high frequency of network data packets. Some applications have persistent signaling that falls into this category. Specific examples include frequent device signaling sequences to update widgets on a desktop; synchronize user data such as calendars, contacts, email, and/or other information/content; check or update email or RSS feeds; access social networking websites or tools; online text, voice or video chat tools; update real-time information; and conduct other repetitive actions. Additional application behavior that can significantly tie up network resources and capacity include, for example, conference meeting services, video streaming, content update, software update, and/or other or similar application behavior. For example, even when the user is not directly interacting with or benefiting from this type of application, the application can be running in the background and continuing to consume potentially significant network resources.

[0050] For example, the types of service activities and/or device behavior that can reduce network capacity and/or network resource availability include software updates for OS and applications, frequent OS and application background network accesses and signaling, frequent network discovery and/or signaling (e.g., EtherType messages, ARP messages, and/or other messaging related to network access), cloud synchronization services, RSS feeds and/or other background information feeds, application (e.g., web browser) or device behavior reporting, background email downloads, content subscription service updates and downloads (e.g., music/video downloads, news feeds, etc.), text/voice/video chat clients, virus updates, peer to peer networking applications, inefficient network access sequences during frequent power

cycling or power save state cycling, large downloads or other high bandwidth accesses, and/or greedy application programs that continually and/or frequently access the network with small transmissions or requests for information. Various other examples will now be apparent to one of ordinary skill in the art.

[0051] Thus, not only can network capacity, network performance, and/or network resource availability be degraded by high device transmission bandwidth demand, but other types of persistent or frequent traffic resulting from network resource requests, network data accesses or other network interaction can also degrade network capacity, network performance, and/or network resource whether or not the aggregate bandwidth demand as measured by the total data throughput is high or not. Thus, techniques are needed to preserve network capacity by, for example, differentially controlling these types of network service usage activities in various ways depending on the type of service activity requesting network access and/or requesting transactions with network resources.

[0052] Smart phones and similar devices are exacerbating the problem by making frequent queries of the wireless network as such devices move among cell sites to, while in transit, for example, push email, access social networking tools, and/or conduct other repetitive actions. While data traffic is also growing, signaling traffic is outpacing actual mobile data traffic by 30 percent to 50 percent by some estimates. For example, a Yahoo IM user may send a message but then wait a couple of seconds between messages. To preserve battery life, the smart phone typically moves into an idle mode. When the user pushes another message seconds later, the device has to set up a signaling path again, and even when the signaling resource is released by the smart phone, the network typically does not react fast enough to allow for the next station to use resources until several seconds and sometimes minutes. As a result, the base station controller in this example is spending a lot of its resources trying to process the signaling so it cannot perform other tasks, such as allocate additional resources for data network usage, and such inefficiencies exacerbate the data network capacity crunch and dropped calls on such wireless networks.

[0053] One approach used by smart phone vendors to address this problem and save battery life on their devices is to implement a fast dormancy feature, which allows the mobile device to quickly make a query to the radio network controller to release the connection so that it can

return to the idle state faster. In other words, the device is relaying the fact that the phone is going dormant saving device resources (e.g., signaling channel) rather than network resources. However, the fast dormancy feature can exacerbate this problem by prematurely requesting a network release only to follow on with a request to connect back to the network or by a request to re-establish a connection with the network.

[0054] Network carriers have typically attempted to manage network capacity using various purely central/core network based approaches. For example, some carriers have indicated a robust capacity planning process and sufficient investment is needed to alleviate this growing capacity crunch. Purely centralized network solutions with no assistance from a device based software agent (or service processor) can have several limitations. For example, for some device applications, OS functions or other service usage activities, if the activity is blocked somewhere in the network behind the base station after over the air (OTA) spectrum bandwidth is consumed to open or begin to open a communication socket, then there can still be an appreciable amount of network capacity or resources consumed even though the data transfer is not allowed to complete. In addition, if the service usage activity is aggressive in re-attempting to establish the network connection to transfer the data, and the network continues to allow the OTA portion of the connection establishment but blocks the connection somewhere in the network, then a large amount of capacity can be consumed by many devices exhibiting such behavior even though no useful service is being allowed. Accordingly, some embodiments for protecting network capacity include controlling network service usage activities at the source of the demand – the device. Furthermore, in some embodiments, service usage is controlled in a manner that delays, prevents, or reduces the frequency of service usage activity re-try attempts to connect to the network.

[0055] In some cases, an additional drawback of purely centralized network solutions to protect network capacity arises when service usage activities are controlled, blocked, throttled, and/or delayed by central network equipment with no mechanisms or support to link to a device user interface (UI) to inform the user what is happening and why it is happening. This can lead to a frustrating user experience and reduced carrier customer satisfaction. Accordingly, in some embodiments, a device based UI is provided to provide the user with real time or near real time information regarding why a service usage activity is being controlled, blocked, throttled, and/or otherwise controlled in order to protect network capacity. In some embodiments, a UI is

provided that also informs the user when there are options to set, control, override, or modify service usage controls for the purpose of protecting network capacity. In some embodiments, such user preference inputs also correspond to a change in service usage billing. In some embodiments, such changes in service usage billing due to capacity sparing service control changes by the user are communicated to the user via a UI notification sequence. In some embodiments, techniques for protecting network capacity employ user warnings when a service usage activity classified for differential user notification policies is likely to cause the user to go over service plan caps (e.g., total data byte count usage caps).

[0056] What is needed is intelligent network monitoring to provide real-time traffic monitoring network service usage (e.g., at the packet level/layer, network stack application interface level/layer, and/or application level/layer) of the wireless network (e.g., radio access networks and/or core networks) and to effectively manage the network service usage for protecting network capacity (e.g., while still maintaining an acceptable user experience). Using Device Assisted Services (DAS) techniques, and in some cases, network assisted/based techniques, to provide for network service usage monitoring of devices, network carriers/operators would be provided greater insight into what devices, which users and what applications, and when and where network congestion problems occur, enabling operators to intelligently add additional resources to certain areas when necessary (e.g., offloading data traffic onto femto cells or WiFi hotspots and adding more network resources), to differentially control network service usage, and/or to differentially charge for network service usage based on, for example, a network busy state, for protecting network capacity.

[0057] Intelligent network monitoring of the wireless network to effectively manage network service usage for protecting network capacity can include providing Device Assisted Services (DAS) for protecting network capacity in accordance with various embodiments described herein. For example, intelligent network monitoring of the wireless network to effectively manage network service usage for protecting network capacity can include differentially controlling over the air software updates and/or performing software updates via wired connections only. As another example, intelligent network monitoring of the wireless network to effectively manage network service usage for protecting network capacity can include differentially controlling various applications that demand significant network resources or network capacity. As another example, intelligent network monitoring of the wireless network

to effectively manage network service usage for protecting network capacity can include managing network access connection requests resulting from repeated power down modes in the modem, which can cause resource intensive re-connection and/or re-authentication processes. As another example, intelligent network monitoring of the wireless network to effectively manage network service usage for protecting network capacity can include techniques for keeping PPP sessions alive to avoid the need to consume network resources to re-establish PPP sessions (e.g., unless the application behavior analysis predicts that a mean access time is long enough for the PPP session to be dropped off and yet not causing overall network resource limitations).

[0058] Unlike traditional QoS techniques, which are used to establish a single end or end to end guaranteed service level(s) on a network, techniques disclosed herein for protecting network capacity facilitate implementation of services on a network to facilitate differential control of certain services to protect network capacity (e.g., to reduce network congestion, network capacity demand, network resource demand; and/or to increase network availability). As also disclosed herein, techniques disclosed herein for protecting network capacity facilitate implementation of services on a network to facilitate differential control of certain services to protect network capacity can also facilitate QoS implementations by maintaining needed levels of network capacity/availability to facilitate delivery of certain QoS levels/classes. For example, techniques disclosed herein for protecting network capacity can aggregate across multiple services and/or devices to facilitate differential control of certain services to protect network capacity. As another example, techniques disclosed herein for protecting network capacity can be used to provide for dynamic QoS classifications (e.g., dynamically assigning/classifying and reassigning/reclassifying (based on various criteria, events, and/or measures) network service usage activities to various QoS levels/classes, such as described herein) to facilitate differential control of certain services to protect network capacity.

[0059] Accordingly, Device Assisted Services (DAS) for protecting network capacity is provided. In some embodiments, DAS for protecting network capacity provides for protection of network capacity (e.g., network congestion and/or network access/resource demand and/or network availability on an edge element of the network, such as on the Radio Access Network (RAN) of a wireless network, and/or from a device to a base station/base station controller), such as by controlling network service activity usage activities of a device in wireless communication

with the network to reduce demands on the network. For example, controlling network service usage activities can include classifying and/or controlling network access requests (e.g., IP address requests), network access reservation requests (e.g., a QoS reservation/sequence), network capacity/resources usage (e.g., bandwidth usage), and/or any other network service usage activities. In some embodiments, applications, OS functions, and/or other network service usage activities that request IP addresses from network address server resources are classified and/or controlled so that the IP address requests are withheld, delayed, time windowed, reduced in frequency, aggregated or otherwise controlled. In some embodiments, such "IP address request control policies" for one or more applications, OS functions, and/or other network service usage activities are set, updated, and/or modified before communicating it over a network connection to a network element (e.g., a service controller or another network element/function). In some embodiments, network service usage activities are generated/requested by applications, operating system (OS) functions, and/or other software/functions executed on a device in communication with the network. In some embodiments, it is desirable to apply a service usage control policy for the network service usage activities to protect network capacity (e.g., reduce network capacity demand). For example, some applications and/or OS functions have limited capabilities to defer certain traffic types based on fixed settings in the application, and such applications and/or OS functions typically cannot optimize network service usage activities based on a current network busy state (e.g., based on changing levels of network capacity and/or network performance available to the device). In some embodiments, the network busy state (e.g., or conversely the network availability state) is a characterization of the congestion (e.g., or conversely available capacity) of the network for one or more device connections. For example, the network busy state can provide a measure of how busy or congested the network or a network segment (e.g., network edge element) is for one or more device connections. As another example, network availability state can provide a measure of what network connection resources are available to one or more device connections. Thus, network busy state and network availability state can be viewed as converse ways of providing similar information, and as described herein with respect to various embodiments, these terms can be used interchangeably.

[0060] In some embodiments, techniques are provided for assigning a priority to a network service usage activity and controlling traffic associated with the network services usage activity based on the assigned priority. In some embodiments, techniques are provided for a

implementing a differentiated and dynamic background services classification, for example, as a function of network availability state and/or network busy state.

[0061] In some embodiments, a service usage control policy is used for assisting in network access control of network service usage activities (e.g., deferring some or all of the network capacity demand from these source activities). In some embodiments, some or all of the network capacity demand is satisfied at a point where the network resources or capacity are more available or less busy. In some embodiments, techniques are provided for classifying network service activities associated with one or more applications or OS functions to a background service class and differentially controlling the background service class traffic. In some embodiments, techniques are provided for classifying one or more network service activities associated with an application or OS function to a background service class, while other network service activities associated with that application or OS function are classified to other service classes (e.g., or to different background service class priority levels).

[0062] In some embodiments, techniques are provided for determining a network busy state (e.g., for a network edge element connection to a device, such as for a RAN for the device's current wireless network access and/or to the current base station/base station controller in wireless communication with the device). In some embodiments, techniques are provided for implementing a service usage control policy to differentially control network services traffic based on a network busy state for an activity, a group of activities, or for a service class.

[0063] In some embodiments, DAS for protecting network capacity includes monitoring a network service usage activity of the communications device in network communication; classifying the network service usage activity for differential network access control for protecting network capacity; and associating the network service usage activity with a network service usage control policy based on a classification of the network service usage activity to facilitate differential network access control for protecting network capacity.

[0064] In some embodiments, a network service usage activity is any activity by the device that includes wireless network communication. In some embodiments, an application, an operating system (OS), and/or other device function generates a network service usage activity. In some embodiments, an application, an operating system (OS), and/or other device function generates one or more network service usage activities. Examples of a network service usage

activity include the following: a voice connection (e.g., coded voice connection or voice over IP (VOIP) connection), a device application or widget connection, a device OS function connection, an email text connection, an email download connection, a file download connection, a streaming media connection, a location service connection, a map services connection, a software update (e.g., application, operating system, and/or antimalware software update) or firmware update connection, a device backup connection, an RSS feed connection, a website connection, a connection to a server, a web browser connection, an Internet connection for a device based service activity, establishing a sync service account, a user data synchronization service, a device data synchronization service, a network connection flow or stream, a socket connection, a TCP connection, a destination/port assigned connection, an IP connection, a UDP connection, an HTTP or HTTPS connection, a TLS connection, an SSL connection, a VPN connection, a general network services connection (e.g., establishing a PPP session, authenticating to the network, obtaining an IP address, DNS service), and various other types of connections via wireless network communication as will be apparent to one of ordinary skill in the art.

[0065] In some embodiments, a network service usage activity is classified, associated with, and/or assigned to a background class (e.g., a background service or QoS class) to facilitate differential network service usage control to protect network capacity. In some embodiments, differential network service usage control includes one or more of the following: monitoring network service usage activity; accounting for network service usage activity; reporting network service usage activity; generating a user notification for a network service usage activity; requesting a user preference for control of network service usage activity; accepting a user preference for network service usage activity; implementation of a network service usage activity policy (e.g., block/allow; traffic control techniques, such as throttle, delay, priority queue, time window, suspend, quarantine, kill, remove, and other well known traffic control techniques); implementing UI intercept procedures; generating a network busy state notification; generating a background class notification; generating a user notification for differential network service usage control of a network service usage activity; and various other techniques as described herein.

[0066] In some embodiments, a network availability state includes a state or measure of availability/capacity of a segment of a network (e.g., a last edge element of a wireless network).

In some embodiments, a network busy state includes a state or measure of the network usage level or network congestion of a segment of a network (e.g., a last edge element of a wireless network). In some embodiments, network availability state and network busy state are inverse measures. As used herein with respect to certain embodiments, network availability state and network busy state can be used interchangeably based on, for example, a design choice (e.g., designing to assign background policies based on a network busy state or a network availability state yields similar results, but they are different ways to characterize the network performance and/or capacity and/or congestion). In some embodiments, network availability state and network busy state are dynamic measures as such states change based on network usage activities (e.g., based on a time of day, availability/capacity level, congestion level, and/or performance level). In some embodiments, differential network service usage control of a network service usage activity is based on a network busy state or network availability state.

[0067] In some embodiments, certain network service usage activities are classified as background services. In some embodiments, lower priority and/or less critical (and/or based on various other criteria/measures) network service usage activities are classified as background services based on a network busy state and differentially controlled based on a network busy state to protect network capacity. In some embodiments, differential network service usage control policies are based on a time of day, a network busy state, background services and/or QoS class changes based on a time of day and/or a network busy state, a random back-off for access for certain network service usage activities, a deterministic schedule for certain network service usage activities, a time windowing in which network service usage control policies for one or more service activities or background/QoS classes changes based on time of day, network busy state, a service plan, and various other criteria, measures, and/or techniques as described herein.

[0068] In some embodiments, a network capacity controlled service or network capacity controlled services class includes one or more network services (e.g., background download services and/or various other types or categories of services as described herein) selected for differential network service usage control for protecting network capacity. In some embodiments, a network capacity controlled services classification includes one or more network services associated with a network capacity controlled service/class priority setting for differential network service usage control for protecting network capacity. In some

embodiments, a network capacity controlled service or network capacity controlled services class includes one or more network services associated with a QoS class for differential network service usage control for protecting network capacity. In some embodiments, a network capacity controlled service or network capacity controlled services class includes one or more network services associated with a dynamic QoS class for differential network service usage control for protecting network capacity.

[0069] For example, differentially controlling network service usage activities based on network capacity controlled services or dynamic QoS or QoS classifications can protect network capacity by, for example, improving network performance, increasing network availability, reducing network resources demand, and/or reducing network capacity demand (e.g., based on an individual device, aggregate devices connected to an edge element, and/or aggregate devices connected to many edge elements). In some embodiments, differentially controlling network service usage activities based on network capacity controlled services or dynamic QoS or QoS classifications can protect network capacity while maintaining proper device operation. In some embodiments, differentially controlling network service usage activities based on network capacity controlled services or dynamic QoS or QoS classifications can protect network capacity while maintaining an acceptable user experience (e.g., proper and/or expected device operation, proper and/or software/application/OS/function operation, avoiding (whenever possible) significant adverse impact on device functions, and/or user notifications to keep the user informed of various differential control implemented on the device).

[0070] In some embodiments, dynamic QoS classifications include QoS classifications that can be dynamically modified (e.g., reclassified, reprioritized, upgraded, and/or downgraded) based on various criteria, measures, settings, and/or user input as described herein (e.g., based on a time of day and/or day of week, based on a network busy state, based on a user preference, and/or based on a service plan). In some embodiments, the various techniques described herein related to DAS for providing network capacity and/or QoS for DAS are applied to dynamic QoS related techniques.

[0071] As wireless networks, such as mobile networks, evolve towards higher bandwidth services, which can include or require, for example, various levels of Quality of Service (QoS) (e.g., conversational, interactive data, streaming data, and/or various (end-to-end) real-time

services that may benefit from QoS), demands will increase for converged network services to facilitate such services for end-to-end services between networks (e.g., to allow for control and/or support for such services, for example, QoS support, across network boundaries, such as between wireless networks (such as various service provider networks) and IP networks (such as the Internet), and/or other networks). While various efforts have attempted to address such QoS needs, such as policy management frameworks for facilitating QoS end-to end solutions, there exists a need to facilitate various QoS requirements using Device Assisted Services (DAS).

[0072] Accordingly, Quality of Service (QoS) for Device Assisted Services (DAS) is provided. In some embodiments, QoS for DAS is provided.

[0073] To establish a QoS channel, differentiated services are typically available, in which one class/level of service has a higher priority than another to provide for differentiated services on a network, such as a wireless network. For example, in a wireless network, various network elements/functions can be provisioned and controlled to establish a single end or end to end QoS channel. In some embodiments, a centralized QoS policy coordination and decision function using DAS techniques to assist in coordinating the QoS channel setup and control among the various elements of a wireless network is provided.

[0074] In some embodiments, QoS channel refers to the logical communication channel connected to a device that provides a desired level of QoS service level. For example, the QoS channel can be created with one or more QoS links, in which each link represents a QoS enabled connection that spans a portion of the total end to end network communication path from a near end device to a far end device. For example, the far end device can be on the same network or on a different network, potentially with different access technology and/or a different access network carrier. In some embodiments, the QoS channel includes one or more QoS links in which each link in the channel is QoS enabled, or one or more of the links in the channel is QoS enabled and others are not. As an example, a QoS channel can include the following links: a first device traffic path link, a first device to access network equipment element link (e.g., 2G/3G/4G wireless base station, WiFi access point, cable network head end, DSLAM, fiber aggregation node, satellite aggregation node, or other network access point/node), a first carrier core network, a long haul IPX network, a second carrier core network, a second device to access

network equipment element link, and a second device traffic path link as similarly described herein with respect to various embodiments.

[0075] In some embodiments, each of the links described above has the ability to provide QoS services for that segment of an overall QoS channel. In some embodiments, the device traffic path link and/or the device to access network equipment element link are QoS enabled, but the carrier core network and/or IPX network links are not QoS enabled. In some embodiments, the core network and/or IPX network have sufficient over-provisioning of bandwidth that QoS is not limited by these network elements and, for example, can be limited by the device traffic link and/or the device to access network equipment element link do not have sufficient excess bandwidth making it desirable to QoS enable these QoS channel links. A common example is a 2G/3G/4G wireless network in which a device traffic path link and the device to access network element link (e.g., Radio Access Bearer (RAB)) are QoS enabled while the carrier core network and IPX network links are not (e.g., are provided at a best effort service level or other service levels).

[0076] In some embodiments, a QoS session refers to the QoS enabled traffic for a given device that flows over a QoS channel or QoS link. This QoS traffic supports a QoS service activity. In some embodiments, a QoS service activity includes a device service usage that is requested, configured, or preferably serviced with a given level of QoS. In some embodiments, a device QoS activity is a combination of one or more of the following: application, destination, source, socket (e.g., IP address, protocol, and/or port), socket address (e.g., port number), URL or other similar service identifier, service provider, network type, traffic type, content type, network protocol, session type, QoS identifier, time of day, network capacity (e.g., network busy state), user service plan authorization or standing, roaming/home network status, and/or other criteria/measures as similarly described herein. For example, QoS service activities that are supported by QoS sessions can include VOIP traffic, streaming video traffic, differentiated access bandwidth during busy network periods, real-time interactive traffic, such as network connected multimedia meetings (e.g., shared presentations, picture, video, voice, and/or other such applications/services), best effort interactive, such as Internet browsing, time sensitive services, such as email message body delivery, near real-time interactive services, such as SMS or push to talk, background download services, such as email downloads and other file transfers

(e.g., FTP), and/or truly background download services, such as software updates (e.g., OS or application software updates and/or antimalware updates including content/signature updates).

[0077] In some embodiments, various QoS levels or classes are supported. For example a conversation class can provide for real-time traffic, which is typically very delay sensitive but can tolerate bit errors and packet losses. The conversational class is typically used for Voice Over IP (VOIP) and video telephony, in which users of such services benefit from the short delay features of the conversational class. A streaming class is similar to the conversational class except that the streaming class typically can tolerate more delay than the conversational class. The streaming class is generally used for when one end of the connection is a user (e.g., human user) and the other end is a machine/computer (e.g., for streaming content applications, such as streaming of video, such as movies or other video content). An interactive class is generally intended for traffic that allows delay variation while requiring reasonably low response time (e.g., web browsing or other applications in which the channel can be unused for long periods of time but when a user makes a request for a new page/data, the response time should be reasonably low). A background class is generally used for lowest priority service usages (e.g., typically used for e-mail with and without downloads/attachments, application software updates, OS software updates, and/or other similar applications/functions). In some embodiments, various QoS classes or services are applicable to the conversational class. In some embodiments, various QoS classes or services are also applicable to the streaming class. In some embodiments, various QoS classes or services are also applicable to the interactive class but typically not applicable to the background class. As will now be apparent to one of ordinary skill in the art, various other classes can be provided with lower or higher granularity based on service usage/channel requirements and/or network architectures.

[0078] In some embodiments, a QoS link or a QoS channel supports one QoS session. In some embodiments, a QoS link or a QoS channel supports multiple QoS sessions. In some embodiments, QoS link provisioning is provided to setup the QoS traffic level for a given QoS session or group of QoS sessions.

[0079] In some embodiments, a QoS channel is a single ended QoS channel or an end to end QoS channel. For example, if a QoS channel is end to end, then the QoS channel provisioning is accomplished in a coordinated manner for each QoS enabled link in the QoS channel. If a QoS

channel is single ended, then the network elements and/or device participate in provisioning as much of one end of the QoS channel as possible, leaving provisioning of the QoS for the other end of the channel as the responsibility of the device and/or network elements that handle the traffic at the other end of the QoS channel. In some embodiments, a single ended QoS channel includes another single ended QoS channel at the other end. In some embodiments, only one end has single ended QoS channel enablement while the other end of the channel is a best effort service level, which, for example, can be used where one end of the QoS channel has tighter constraints on traffic capacity or quality than the other end (e.g., a VOIP call with one end that is QoS enabled on a 3G wireless network that has relatively tight bandwidth compared to a lightly loaded cable modem network device on the other end which may not need to be QoS enabled in order to achieve adequate voice quality).

[0080] In some embodiments, a QoS request (e.g., a QoS channel request or QoS service request) is a request for a QoS provisioning event to enable a QoS channel for one or more QoS service activities. In some embodiments, QoS availability assessment includes determining whether one or more of the links in a possible QoS channel are available (e.g., based on network capacity and transmission quality) to provision the necessary level of QoS for a requested QoS channel. In some embodiments, a QoS request is initiated by a device, a user, an application, and/or a network element/function as similarly described herein.

[0081] In some embodiments, a service plan refers to the collection of access service capabilities, QoS capabilities, and/or network capacity controlled services that are associated with a communications device. In some embodiments, the access service capabilities, QoS capabilities, and/or network capacity controlled services are determined by the collection of access service control policies for the device. In some embodiments, these service control policies are implemented in the network equipment. In some embodiments, these access service control policies are implemented both in the device and in the network equipment. In some embodiments, these access service control policies are implemented in the device. In some embodiments, there are different levels of service control capabilities (e.g., policies) based on different levels of service plan payments or device standing or user standing. In some embodiments, there are different levels of service control policies based on network type, time of day, network busy status, and/or other criteria/measures as similarly described herein with respect to various embodiments. In some embodiments, the access control and QoS control

policies are based on the type of service activity being sought. In some embodiments, the QoS level and access level available for a given service activity for a given device or user is determined by the policies associated with the service plan. In some embodiments, a QoS authorization assessment is performed to determine whether a device or user has sufficient service plan standing to allow the requested level of QoS.

[0082] In some embodiments, before a QoS channel or link is provisioned (or before a QoS request is responded to or filled), a QoS availability assessment is performed to determine whether sufficient communication channel resources are available to provision the necessary level of QoS for the QoS channel or link. In some embodiments, this QoS availability assessment is determined by assessing the available QoS capacity for one or more necessary QoS links in the channel. For example, the available QoS link capacity can be assessed for one or more of a device traffic path, a device to access network equipment element link, a core network link, and/or an IPX network link. If the QoS assessment shows that the necessary channel capacity and quality are available for the desired QoS level for one or more desired QoS service activities, then a QoS channel request or QoS service request can be granted. In some embodiments, a QoS link or QoS channel reservation process is provided to reserve QoS capacity and quality in advance of link or channel provisioning to ensure that the available QoS resources are not assigned between the time of QoS availability assessment and QoS channel provisioning.

[0083] In some embodiments, the QoS availability assessment is performed after QoS authorization assessment. This prevents the unnecessary exercising of network elements when the device or user does not have sufficient service plan standing to receive the desired level of QoS even if it is available. This can be an important screening function performed on the device in the service processor, or by a centralized network function such as the service controller (e.g., or interchangeably, the home agent; Home Location Register (HLR); Authentication, Authorization, and Accounting (AAA) server/gateway/function; base station; one of the gateways, policy and charging rules function (PCRF), or other network element/function). In some embodiments, QoS availability is assessed without conducting a QoS authorization assessment or before receiving the response to a QoS authorization assessment.

[0084] In some embodiments, a QoS channel is provisioned to create the QoS channel to support a QoS session (e.g., a QoS service activity). In some embodiments, QoS channel provision includes assigning, routing, and/or otherwise causing the QoS session traffic to flow over one or more QoS links in the assigned QoS channel.

[0085] In some embodiments, device assisted service traffic control and QoS apply readily and directly to the problems of managing a QoS device link for QoS channel provisioning. Accordingly, in some embodiments, a service processor is provided to assist in provisioning the device portion of the QoS channel. In some embodiments, the service processor provisions the device link portion of the QoS channel by placing a higher priority on higher QoS level traffic. In some embodiments, this QoS priority is implemented in a number of ways, including routing the higher priority QoS traffic into first priority in the downstream and/or upstream traffic queues. Upstream traffic queuing is performed directly in some embodiments by transmitting guaranteed bit rate traffic first at higher available throttling rates, differentiated QoS traffic second with a controlled throttling rate, best effort traffic third with possibly lower controlled throttled rates, and/or background traffic fourth when/if bandwidth not needed by the higher levels of QoS traffic and at lower controlled throttling rates. For example, downstream traffic can be handled by queuing traffic and delaying or preventing TCP acknowledgements to be returned for the lower levels of QoS priority, while immediately passing the traffic and TCP acknowledgements for higher levels of QoS priority. The device link portion of the QoS channel is thus provisioned by assigning policies for the queuing priority, delay, throttle rate, and TCP acknowledgement return rate for device traffic in accordance with the bandwidth that is available at any point in time for the device. In some embodiments, various device service processor traffic control capabilities regulate or partially regulate QoS in accordance with a set of network policy instructions, including, in some embodiments, a service plan policy set.

[0086] In some embodiments the device service processor establishes multiple QoS channels through the device traffic path with each QoS channel having traffic control policies as described herein, with each QoS channel policy set creating a different class of QoS. In some embodiments, employing this multiple QoS channel approach, QoS for a given service activity is provided by routing the traffic for that QoS activity to the appropriate QoS channel with the appropriate QoS policy settings. The routing to the appropriate QoS channel can be provided using various techniques. For example, the routing can be provided by applying a common

service traffic control policy set to traffic associated with all QoS service activities that require or request the QoS provided by the common service traffic control policy set. The application of the service traffic control policy set can be accomplished in a number of ways utilizing the embodiments described for the policy implementation agent and the policy control agent described herein. In such embodiments, the problem of assigning a QoS channel to a number of QoS service activities is reduced to applying a pre-determined set of service traffic control policies to each of the QoS service activities, with each pre-determined set of service traffic control policies representing a different QoS class. The device can then manage the overall QoS for all traffic based on the available traffic capacity and quality, the total aggregate traffic demand for each QoS traffic class and the policy rules that determine how each traffic class is provided with differential bit rate and traffic quality as compared to the other traffic classes for a given level of available traffic capacity and quality.

[0087] Based on the aggregate demand for each traffic QoS class, and the traffic capacity and quality level available to the device, the service processor can adjust the total available bit rate or percentage of available traffic capacity for each QoS class. For example, in some embodiments, the aggregate demand for the real-time interactive traffic control class (e.g., services, such as VOIP, emergency communication services or high performance real-time competitive gaming) can be determined, and the QoS routing function on the device (e.g., a QoS router agent/function) can first allocate enough constant bit rate traffic capacity from the available traffic capacity to satisfy these services, with each QoS service activity that requires this QoS class being assigned to this QoS channel. As more QoS service activities require this traffic class, the capacity allocated to the QoS channel out of the available device capacity is increased, and when fewer QoS service activities require this traffic class the capacity for this QoS channel is released. In the event that the device does not have any more available capacity with a guaranteed bit rate QoS level, then additional QoS service activities that desire, require or request this QoS level will not be provided this QoS level, and instead will either be provided with a lower QoS level or will not be allowed to connect to the access network. In some embodiments, there can be a hierarchy among the possible QoS service activities so that if there is no more capacity available at a given service QoS level, then the available capacity for that QoS class is provided to the service activities requiring that QoS from highest priority to lowest, until the available QoS class capacity is consumed, and then one or more QoS service activities

that are too low on the priority list to obtain service with that QoS class are either bumped to a lower QoS class or are denied access. In some embodiments, once the required capacity to satisfy the real-time constant rate traffic needs is satisfied, the remaining capacity available to the device is then divided among the other QoS channel classes in accordance with a priority policy, with the priority policy being based on the relative priority of each service class, the relative priority of each QoS service activity, or a combination of the relative priority of each QoS service class and each QoS service activity. For example, these relative priority policies can vary from device to device based on service plan selection, device type, user standing, user group, device location, device network connection, type of network, time of day, network busy state, and/or other criteria/measures.

[0088] In some embodiments, a QoS link is established between the device and an access network equipment element. For example, such equipment element embodiments can include a 2G/3G/4G wireless base station, a wireless access point, a cable network head end, a DSL network DSLAM, a fiber network device traffic aggregator, a satellite network device traffic aggregator, a frame relay aggregation node, an ATM aggregation node, and/or other network equipment. In some embodiments, a logical communication channel is created between the device and the network equipment element, with the logical communication channel supporting a given level of QoS or QoS class traffic policy set. For example, the logical channel can include a RAB formed between a 2G/3G/4G base station and a wireless end point device. The RAB can be formed by controlling the media access control (MAC) parameters of the base station radio channel so that a given level of QoS class policies can be implemented. For example, the RAB can support constant bit rate, low latency communication traffic for guaranteed bit rate real-time traffic, or a differentiated high priority access channel for streaming traffic, or a best effort random access channel for best effort traffic, or an available unused capacity traffic for background traffic. The QoS channel link created in this manner can be dedicated to a single device, or shared with a subset of devices, or available to all devices. The QoS channel link created in this manner can be used by the device to support a single QoS activity as described herein, or a group of QoS activities as described herein. It will now be apparent to one of ordinary skill in the art that similar settings for cable head end and cable modem MAC can yield similar QoS classes for QoS links for the cable modem case and that similar techniques can be applied for a wireless access point or a satellite system MAC to achieve similar QoS classes for

QoS links. It will also now be apparent to one of ordinary skill in the art that by creating multiple logical channels in the device link, and/or adjusting the available access network capacity and quality for each logical device communication channel in the DSLAM or fiber aggregator, similar QoS class QoS links can be established for the DSL and fiber distribution network cases.

[0089] In some embodiments the device service processor serves to route QoS service activities to the appropriate logical communication channel established for the desired QoS class supported by a QoS link between the device and the access network equipment element. In some embodiments, the device service processor elements (e.g., the policy implementation agent and/or the policy control agent) can be used in some embodiments to assign the same QoS traffic control policies to one or more QoS service activities that require the same QoS level. In a similar manner, in some embodiments, the device service processor elements can be used to assign or route service activity traffic for a given QoS class to the correct logical communication channel between the device and the access network element (e.g., a 2G/3G/4G base station) that supports the traffic control policies for the desired QoS class. For example, a QoS service link that supports guaranteed bit rate and latency can be established with one or more RABs from a base station to the device, and a second QoS service link can be established that supports differentiated preferred access for streaming content using one or more differentiated access RABs, and a third best effort RAB can be used to support best effort traffic. Each of the required RABs is first requested and then provisioned as described herein based on the aggregate required capacity and quality for one or more QoS service activities that require or desire the specific QoS service class associated with the RAB logical channel policy parameters. Once the set of logical QoS channels is thus established, the service processor (e.g., QoS router agent/function) routes the traffic associated with each QoS service activity to the appropriate RAB. In some embodiments, the service processor can detect increases or decreases in aggregate QoS class demand for each QoS class as QoS activities are initiated or terminated for that QoS class, and the service processor can communicate the required increases or decreases in the RAB assignments required to support that logical QoS channel.

[0090] In some embodiments, the access QoS link is established by direct communication from the device in which the device requests the QoS channel or link from the access network equipment element, or the device requests the QoS channel or link from an intermediate

networking device, such as a service controller (e.g., or a readily substituted device with similar features, such as a home agent, an HLR, a mobile switching center, a base station, an access gateway, a AAA system, PCRF, or a billing system). In some embodiments, the device service processor bases the QoS channel or link request on an association the device performs to match a QoS service activity with a desired or required QoS class or QoS traffic control policy set. For example, this association of QoS class or QoS traffic control policy set with QoS service activity can be determined by a predefined policy mapping that is stored on the device and used by the service processor. In some embodiments, this policy mapping store is populated and/or updated by a service controller (e.g., or similar function as described herein). In some embodiments, the mapping is determined by a service controller (e.g., or similar function as described herein) based on a report from the device of the QoS service activity that needs the QoS channel or link.

[0091] In some embodiments, the required or desired QoS level for one or more QoS service activities is determined by a set of QoS service traffic control policies that are pre-assigned to various QoS service activities. For example, a given application can be pre-assigned a QoS class. As another example, a web service destination such as a VOIP service site can be assigned a QoS class. As another example, a given application can have one QoS assignment level for general Internet traffic but have a QoS assignment for real-time gaming traffic. As another example, a real-time broadcasting website can have a best effort QoS level assigned to programming information and general browsing and have a differentiated streaming QoS level for broadcast traffic content. In some embodiments, detection of QoS need or QoS assignment request for a given activity can be assigned by a device service processor according to a pre-defined QoS policy rules table (e.g., QoS activity table), or can be determined by a service controller based on information reported by the device, or can be requested by an application through a QoS application interface (e.g., QoS API), or can be determined by the nature of incoming traffic.

[0092] In embodiments, in which both end points in the QoS channel participate in establishing an end to end QoS channel, the required QoS level is determined and/or communicated by the originating end point. In some embodiments, the required QoS level is determined and/or communicated by the receiving end point. In some embodiments the QoS level is determined and/or communicated by the originating end point service controller (e.g., or the access network element (such as a base station), the HLR, home agent, mobile switching

center, AAA, gateway, or other network element/function). In some embodiments, the QoS level is determined and/or communicated by the receiving end point service controller (e.g., or alternatively the access network element (such as a base station), the HLR, home agent, mobile switching center, AAA, gateway, or other network element/function). In some embodiments, the receiving end point service controller (e.g., or the access network element (such as a base station), the HLR, home agent, mobile switching center, AAA, gateway or other network function) and the originating end point service controller (e.g., or other similar function) communicate with one another to coordinate establishment of the QoS channel between the end points.

[0093] In some embodiments, the near end or originating end device service processor contacts the far end or terminating device service processor to initiate a QoS channel. In some embodiments, the initiation of the QoS channel from the near end or originating device is performed automatically by the far end device when its service processor detects that a given level of QoS is needed for the communication between the two devices. In some embodiments, the near end or originating device service processor detects the need for a QoS channel to the far end or terminating device and contacts a central network resources, such as the service controller (e.g., or other equipment element with similar function for this purpose), and the service controller provisions the far end of the QoS channel, either by communicating directly with the far end device or by communicating with the far end device's service controller (e.g., or other equipment element with similar function for this purpose). In some embodiments, in which the far end device service controller is contacted to assist in provisioning the QoS channel, there is a look up function to determine the address of the far end service controller based on a look up index formed from some aspect of the far end device credentials (e.g., phone number, SIM ID, MEID, IMSI, IP address, user name, and/or other device credentials).

[0094] In some embodiments, the mapping of QoS service activity to the desired level of QoS class or QoS traffic control policies is determined by providing a QoS API in the device service processor that applications use to request a QoS class or QoS channel connection. In some embodiments, an API is provided so that application developers can create application software that uses the standard interface commands to request and set up QoS channels. In some embodiments, the API does one or more of the following: accepts QoS requests from an application, formats the QoS channel request into a protocol appropriate for transmission to

network equipment responsible for assessing QoS channel availability (e.g., including possibly the device traffic control system), coordinates with other network elements (e.g., including possibly the device traffic control system) to reserve a QoS channel, coordinates with other network elements (e.g., including possibly the device traffic control system) to provision a QoS channel, informs the application that the desired QoS channel can be created or not, and/or coordinates with other network elements (e.g., including possibly the device traffic control system) to connect the application with the desired QoS channel class. In some embodiments, the QoS API accepts the application QoS request and communicates and possibly coordinates with one or more QoS network equipment elements, such as a base station, cable head end or access point. In some embodiments, the QoS API accepts the QoS request from the application and communicates and possibly coordinates with an intermediate network element, such as a service processor (e.g., or other similar function as described herein). In some embodiments the QoS API assesses the QoS service plan standing for the device or user before sending QoS channel requests to other network elements, and only initiates the QoS request sequence if required service plan authorization is in place. In this manner, the potentially complex process of establishing a QoS channel with all the specific equipment communication protocols that typically need to be supported to assess QoS channel availability and provision the QoS channel are simplified into a limited set of API commands that are easy for an application development community to learn about and use for QoS differentiated services and applications.

[0095] In some embodiments, local traffic control on the device service processor is combined with traffic control in the link between the device and the access network equipment element. In this manner, both the device traffic control path QoS link and the device to access network element QoS link can be coordinated for best device QoS performance results given the available capacity and quality of the access network traffic for the device. In some embodiments, the policies for how the device manages local traffic control, establishes access network element logical channels (e.g., RABs) and routes traffic to and from the access network element logical channels is all determined by predefined policy rules loaded onto the device by the service controller (or other equivalent network element). In some embodiments, these policies are determined in the service controller itself.

[0096] In some embodiments, a QoS user interface (e.g., QoS UI) is presented to the device user. In some embodiments, the QoS UI notifies the user what level of QoS services the device

is authorized to receive based on the service plan selection. In some embodiments, the QoS UI notifies the user what level of QoS services are available on the present network the device is connected to at the present time. In some embodiments, the QoS UI notifies the user when a level of QoS service that is higher than that authorized by the user service plan is required or desirable for a given service activity that the device has initiated. In some embodiments, the QoS UI provides the user with a set of one or more upgrade options to upgrade the service plan to include a higher level of QoS for one or more service activities. In some embodiments, the QoS UI provides the user with an opportunity to specify what level of QoS the user would like to employ for one or more service usage activities. In some embodiments, the QoS UI allows the user to specify a service plan setting that provides differentiated QoS during times when the network is busy. In some embodiments, the QoS UI allows the user to purchase one or more grades of service QoS with either a post-pay for a pre-defined service period and one or more pre-defined service usage limits by QoS class, a pre-pay for one or more pre-defined service usage limits by QoS class, or another payment system for differentiated QoS services. In some embodiments, the QoS UI provides the user with an opportunity to QoS enable or pay for QoS services for a connection that is initiated by an incoming connection to the device.

[0097] In some embodiments, QoS for DAS techniques include verifying that the device is properly implementing the QoS traffic control policies, for example, in accordance with a service plan. This ensures that errors, hacking, user device software settings manipulations, or other malware events do not result in inappropriate levels of QoS for a given device or group of devices. Accordingly, in some embodiments, the traffic control and QoS verification techniques described herein are employed to verify that the proper level of QoS is applied for a given service usage activity in accordance with a QoS priority policy. For example, verification of QoS channel request policy rules behavior can be implemented in a variety of ways including, as an example, monitoring device QoS channel requests and comparing the level of QoS requested with the level of QoS the device is authorized to receive in the service plan in effect for the device. Verification of proper QoS channel usage behavior by a device can be implemented in a variety of ways including, for example, monitoring network based reports of QoS service usage and comparing the network based reports against the service policy rules that should be in effect given the device service plan. Verification of proper device traffic control to implement a QoS service policy that is in effect can be accomplished in a variety of ways by verifying that the

appropriate traffic control policy rules are being properly implemented as described herein. In some embodiments, DAS for protecting network capacity techniques include various verification techniques (e.g., verifying monitoring, traffic controlling, reporting, and/or other functions implemented or performed by the device), as described herein.

[0098] In some embodiments, the QoS router prioritizes traffic on the device. In some embodiments, the QoS router connects the QoS enabled session to the RAB that has the proper QoS level. In some embodiments, one session is routed to the RAB. In some embodiments, more than one session can be routed to an RAB. In some embodiments, multiple RABs providing multiple QoS levels are created to the device, and the QoS router routes each service activity to the RAB dictated by the QoS policy rules in effect on the device.

[0099] In some embodiments, the network collects service usage charges for different QoS classes. In some embodiments, there is differentiated service charging for the different classes of QoS service usage. As an example, since guaranteed bit rate traffic consumes network resources whether the traffic capacity is used or not, there can be a time element involved in the charging calculations. As a more detailed example, guaranteed bit rate services can be charged by the total bandwidth provisioned to the device at a given time multiplied by the amount of time that that bandwidth is made available. In some embodiments, differentiated access traffic that has higher QoS than best effort traffic but is not guaranteed bit rate can be charged at a higher rate than best effort traffic but lower than guaranteed bit rate. In some embodiments, such traffic can be charged based on the time the QoS channel is made available and the total amount of data transmitted over the channel, or can only be based on the total amount of data transmitted over the channel. Best effort traffic is charged in some embodiments based only on the total amount of data used, with the data charges being less than differentiated streaming access services. Background data services in some embodiments are charged at the lowest rate, possibly with only certain times of the day or periods of low network traffic demand being available for such services, and with the service being based on total data transmitted. In some embodiments, all QoS service levels can be charged based on a fixed price for a fixed charging period, possibly with a service usage cap with additional charges if the service cap is exceeded. In such fixed price scenario embodiments, the price charged is again higher for higher levels of QoS. In some embodiments, the network collects service usage charges for different network capacity

controlled service classes. In some embodiments, there is differentiated service charging for the different classes of network capacity controlled service usage, as described herein.

[00100] In some embodiments, the network equipment (e.g., access network element, gateways, AAA, service usage storage systems, home agent, HLR, mobile data center, and/or billing systems) record and report service usage for one or more of the QoS service classes used by the device. In some embodiments, the device service processor records and reports service usage for one or more of the QoS service classes used by the device and reports the QoS service class usage to the service controller (e.g., or another substitute network element). In some embodiments, in which the device is recording reporting usage for one or more QoS service classes, it is important to verify the device service usage reports to ensure that the device usage reports are not distorted, tampered with, and/or otherwise in error. In some embodiments, verifying service usage reports against service usage that should be occurring given the service control policies in place on the device, service processor agent functional operation verification, test service usage events, agent query response sequences, device service processor software protection techniques, device service processor software environment checks, and several other techniques are provides as described herein. For example, using one or more of these verification techniques can provide a verifiable device assisted QoS service usage charging system. As another example, using one or more of these verification techniques can provide a verifiable network capacity controlled service usage charging system. In some embodiments, the network equipment (e.g., access network element, gateways, AAA, service usage storage systems, home agent, HLR, mobile data center, and/or billing systems) record and report service usage for one or more of the network capacity controlled service classes used by the device, as described herein.

[00101] In some embodiments, device assisted traffic control is provided for managing network congestion as follows. For example, when a given base station or group of base stations experience traffic demand that is high relative to the available capacity and/or service quality that can be provided, and such a condition is determined (e.g., detected or reported) based on a network busy state assessment as described below and further herein, then a service controller (e.g., or another network function) can issue, send, and/or implement traffic control throttling policies to/for the devices in accordance with a measure of the excess traffic demand the one or more base stations is experiencing. For example, the device service processors connected to an

overly busy base station can be instructed to reduce the traffic control priority for one or more classes of QoS traffic, reducing the queuing priority, throttling rate, delay and/or access allowance for some or all of one or more classes of traffic. As another example, the device service processors connected to an overly busy base station can be instructed to reduce the traffic control priority for one or more classes of network capacity controlled services traffic, reducing the queuing priority, throttling rate, delay and/or access allowance for some or all of one or more classes of such traffic. As another example, one or more classes of network capacity controlled services traffic, such as background download processes, which can include, for example, software updates can be turned off completely or throttled back significantly. As another example, best effort traffic such as Internet browsing can be throttled or reduced for a group of devices connected to base stations experiencing excess traffic demand. As another example, a policy can be implemented on the devices connected to busy base stations in which the device is allowed to browse or conduct other best effort service activities at a relatively high throttling rate for a period of time, but if the device uses more than a certain amount of service (e.g., total data downloaded and/or uploaded) in a certain period of time then the device may be traffic controlled according to an adaptive throttling policy as described herein. In some embodiments, higher QoS level traffic cannot be throttled in such circumstances, such as VOIP traffic where real-time guaranteed bit rate is important to meet user service needs or expectations, while lower priority traffic such as interactive browsing and/or background download are throttled and/or blocked. In some embodiments, the QoS availability assessment processes described herein are adjusted so that higher QoS channels are not provided and provisioned in times or locations in which a given base station or group of base stations experience excess demand or demand above a given threshold.

[00102] In some embodiments, users or devices that have service plans with higher QoS levels, or service plans with higher priority during busy network periods have different traffic control policies (e.g., for QoS services and/or network capacity controlled services) applied to them that result in a higher level of traffic performance and/or a higher level of QoS service availability. For example, emergency service workers can be given higher traffic control access policies that result in differentiated services during peak busy times on the network or a portion of the network. In some embodiments, users can obtain a premium service plan for differentiated access during peak busy time periods or may use higher levels of QoS service settings and/or

service plans to achieve differentiated service during peak busy periods. As another example, services that demand high levels of QoS classes, such as real-time voice services, instant messaging, push to talk, differentiated video streaming, and/or interactive gaming, are not traffic controlled to the same extent that other lower priority services or lower class service plans are traffic controlled during peak busy times. For example, this type of service differentiation can also be applied based on device type, user group, user standing, user reward zone points, and/or other criteria/measures as similarly described herein.

[00103] In some embodiments, the decision to control (e.g., reduce, increase, and/or otherwise control in some manner) the access traffic control settings as described above is made by the device service processor based on the device's assessment of the network capacity, which can be determined using various techniques as described herein. In some embodiments, the decision to control the access traffic control settings as described above is made by a service controller (e.g., or other interchangeable network equipment element or elements as described herein) connected to the device that provides instructions to the device to adjust the access policy settings. For example, the service controller can obtain the network capacity information from access equipment elements, from device reports of traffic capacity and/or quality as described herein, or from reports on traffic capacity and/or quality obtained from dedicated devices used for the purpose of assessing network capacity. In some embodiments, the decision to control the access traffic control settings as described above is based on the time of day, the day of week, or both to accommodate cyclical patterns in network capacity and traffic demand.

[00104] In some embodiments, a service controller (e.g., or another network equipment element or elements, as described herein) assesses network busy state and then controls device traffic demand by reducing the offered capacity for one or more service classes (e.g., for QoS services and/or network capacity controlled services) supported by the access network equipment elements, such as a wireless base station. In such embodiments, the service controller (e.g., or similar function) gathers the network capacity information with one of the techniques described herein and instructs one or more of the access network equipment elements to reduce the offered capacity for one or more levels of QoS classes and/or network capacity controlled service classes, to one or more of the devices connected to the access network equipment elements. For example, the determination of which devices to throttle back can be made based on an equal throttling of all devices of a given service plan status, or based on the device traffic usage

patterns in the recent past as described herein, or based on a combination of service plan status and recent traffic usage patterns.

[00105] In some embodiments, the device is enabled with ambient services that have differentiated QoS services and/or network capacity controlled services as part of the ambient service offering. For example, ambient QoS techniques can be provided using the pre-assigned QoS policies for a given service activity set within the ambient service, or using an ambient service application that requests QoS through the QoS API. Other embodiments for providing QoS differentiated service activities within ambient service offerings will now be apparent to one of ordinary skill in the art. As another example, ambient network capacity controlled service techniques can be provided using the pre-assigned network capacity controlled policies for a given service activity set within the ambient service, monitoring and dynamically assigned techniques, and/or using an ambient service application that uses API or emulated API techniques, and/or other techniques as described herein.

[00106] In some embodiments, a QoS service control policy is adapted as a function of the type of network the device is connected to. For example, the QoS traffic control policies and/or the QoS service charging policies can be different when the device is connected to a wireless network (e.g., a 3G/4G network where there is in general less available QoS enabled traffic capacity) than when the device is connected to a wired network (e.g., a cable or DSL network where there is in general a higher level of QoS capacity available). In such embodiments, the device service processor and the service controller can coordinate to adapt the QoS service control policies and/or the QoS service charging policies to be different depending on which network the device is connected to. Similarly, the device QoS service control policy and/or QoS service charging policy can also be adapted based on whether the device is connected to a home wireless network or a roaming wireless network. In some embodiments, a network capacity controlled service control policy and/or a network capacity controlled charging policy is adapted as a function of the type of network the device is connected to, as similarly described herein.

[00107] In some embodiments, various of the QoS related techniques and/or network capacity controlled services techniques described herein are performed on the device using DAS techniques and/or on the service controller in secure communication with a verified service processor executed on the device using DAS techniques. In some embodiments, various of the

QoS related techniques and/or network capacity controlled services techniques described herein are performed by/in coordination/communication with one or more intermediate network elements/functions for assisting in various techniques (e.g., functions) for QoS techniques and/or network capacity controlled services techniques as described herein.

[00108] FIG. 1 illustrates a functional diagram of a network architecture for providing quality of service (QoS) for device assisted services (DAS) and/or for providing DAS for protecting network capacity in accordance with some embodiments. In some embodiments, QoS for DAS techniques described herein are implemented using the network architecture shown in FIG. 1. In some embodiments, DAS for protecting network capacity techniques described herein are implemented using the network architecture shown in FIG. 1.

[00109] 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 (e.g., via a firewall 124), 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, one or more of the devices 100 are in communication with other network element(s)/equipment that provides an access point, such as a cable network head end, a DSL network DSLAM, a fiber network aggregation node, and/or a satellite network aggregation node. In some embodiments, each of the wireless devices 100 includes a service processor 115 (as shown) (e.g., executed on a processor of the wireless device 100), and each service processor connects through a secure control plane link to a service controller 122 (e.g., using encrypted communications).

[00110] In some embodiments, service usage information includes network based service usage information (e.g., network based service usage measures or charging data records (CDRs), which can, for example, be generated by service usage measurement apparatus in the network equipment), which is obtained from one or more network elements (e.g., BTS/BSCs 125, RAN Gateways (not shown), Transport Gateways (not shown), Mobile Wireless Center/HLRs 132, AAA 121, Service Usage History/CDR Aggregation, Mediation, Feed 118, or other network equipment). In some embodiments, service usage information includes micro-CDRs. In some embodiments, micro-CDRs are used for CDR mediation or reconciliation that provides for

service usage accounting on any device activity that is desired. In some embodiments, each device activity that is desired to be associated with a billing event is assigned a micro-CDR transaction code, and the service processor 115 is programmed to account for that activity associated with that transaction code. In some embodiments, the service processor 115 periodically reports (e.g., during each heartbeat or based on any other periodic, push, and/or pull communication technique(s)) micro-CDR usage measures to, for example, the service controller 122 or some other network element. In some embodiments, the service controller 122 reformats the heartbeat micro-CDR usage information into a valid CDR format (e.g., a CDR format that is used and can be processed by an SGSN or GGSN or other network elements/equipment used/authorized for generating or processing CDRs) and then transmits it to a network element/function for CDR mediation (e.g., CDR Storage, Aggregation, Mediation, Feed 118).

[00111] In some embodiments, CDR mediation is used to account for the micro-CDR service usage information by depositing it into an appropriate service usage account and deducting it from the user device bulk service usage account. For example, this technique provides for a flexible service usage billing solution that uses pre-existing solutions, infrastructures, and/or techniques for CDR mediation and billing. For example, the billing system (e.g., billing system 123 or billing interface 127) processes the mediated CDR feed from CDR mediation, applies the appropriate account billing codes to the aggregated micro-CDR information that was generated by the device, and then generates billing events in a manner that does not require changes to the existing billing systems (e.g., using new transaction codes to label the new device assisted billing capabilities). In some embodiments, network provisioning system 160 provisions various network elements/functions for authorization in the network, such as to authorize certain network elements/functions (e.g., CDR storage, aggregation, mediation, feed 118 or other network elements/functions) for providing micro-CDRs, reformatted micro-CDRs, and/or aggregated or reconciled CDRs.

[00112] As shown in FIG. 1, a CDR storage, aggregation, mediation, feed 118 is provided. In some embodiments, the CDR storage, aggregation, mediation, feed 118 receives, stores, aggregates and mediates micro-CDRs received from mobile devices 100. In some embodiments, the CDR storage, aggregation, mediation, feed 118 also provides a settlement platform using the mediated micro-CDRs, as described herein. In some embodiments, another network element

provides the settlement platform using aggregated and/or mediated micro-CDRs (e.g., central billing interface 127 and/or another network element/function).

[00113] In some embodiments, various techniques for partitioning of device groups are used for partitioning the mobile devices 100 (e.g., allocating a subset of mobile devices 100 for a distributor, an OEM, a MVNO, and/or another partner or entity). As shown in FIG. 1, a MVNO core network 210 includes a MVNO 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). In some embodiments, the MVNO CDR storage, aggregation, mediation, feed 118 receives, stores, aggregates and mediates micro-CDRs received from mobile devices 100 (e.g., MVNO group partitioned devices).

[00114] Those of ordinary skill in the art will appreciate that various other network architectures can be used for providing device group partitions and a settlement platform, and FIG. 1 is illustrative of just one such example network architecture for which device group partitions and settlement platform techniques described herein can be provided.

[00115] In some embodiments, 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 apparatus/systems 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 provides 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 and embodiments 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 127 (e.g., sometimes referred to as the external billing management interface or billing communication interface), which is in communication with the central billing system 123. As shown in FIG. 1, 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.

[00116] In some embodiments, a service processor download 170 is provided, which provides for periodical downloads/updates of service processors (e.g., service processor 115). In some embodiments, verification techniques include periodically updating, replacing, and/or updating an obfuscated version of the service processor, or performing any of these techniques in response to an indication of a potential compromise or tampering of any service processor functionality (e.g., QoS functionality and/or network capacity controlled services functionality) executed on or implemented on the device 100.

[00117] 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) collects device generated/assisted service usage information (e.g., micro-CDRs) for one or more devices on the wireless network (e.g., devices 100); and provides the device generated service 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, as described herein, the CDR storage, aggregation, mediation, feed 118 collects/receives micro-CDRs for one or more devices on the wireless network (e.g., devices 100). In some embodiments, the CDR storage, aggregation, mediation, feed 118 (e.g., or other network elements and/or various 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 service usage information. In some embodiments, 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 (network based) CDRs and/or micro-CDRs for the one or more devices on the wireless network; applies a set of rules to the aggregated CDRs and/or micro-CDRs using a rules engine (e.g., bill by account, transactional billing, revenue sharing model, 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, a revenue sharing platform is provided using various techniques described herein. In some embodiments, QoS usage accounting/charging and/or network capacity controlled services usage accounting/charging is provided using various techniques described herein.

[00118] 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 (e.g., aggregated and mediated CDRs and/or micro-CDRs that are then translated into standard CDRs for a given wireless network) for the one or more devices on the wireless network to a billing interface (e.g., central billing interface 127) or a billing system (e.g., central billing system 123). 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 (e.g., service controller 122) to collect the device generated service usage information (e.g., micro-CDRs) 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 service usage information 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 transport gateway and/or a Radio Access Network (RAN) gateway to collect the network generated/based service usage information for the one or more devices on the wireless network. In some embodiments, the service controller 122 communicates the device assisted service usage information (e.g., micro-CDRs) to the CDR storage, aggregation, mediation, feed 118 (e.g., or other network elements and/or various combinations of network elements).

[00119] In some embodiments, the CDR storage, aggregation, mediation, feed 118 (e.g., or other network elements and/or various combinations of network elements) performs rules for performing a bill by account aggregation and mediation function. 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 service billing function, as described herein, and/or for performing a service/transactional revenue sharing function, as described herein. 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 assisted service usage information (e.g., micro-CDRs). In some embodiments, a rules engine device in communication with the CDR storage, aggregation, mediation, feed 118 (e.g., or other network elements and/or various combinations of network elements) performs a rules engine for aggregating and mediating the device assisted service usage information (e.g., QOS service usage information and/or network capacity controlled services usage information).

[00120] 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.

[00121] In some embodiments, a settlement platform service is provided. For example, micro-CDRs can be aggregated and mediated to associate service usage for one or more services used by a communications device (e.g., a user of the communications device). A rules engine or another function can determine a revenue share allocation for the service usage for a particular service to determine the settlement for such service usage for the revenue sharing allocation/model and to distribute accounting and settlement information to one or more of carriers, distribution partners, MVNOs, wholesale partners, and/or other partners or entities. In some embodiments, the service is a transactional service.

[00122] 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., 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.

[00123] 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 assisted 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.

[00124] 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 assisted service usage information (e.g., micro-CDRs) includes a transaction type field or transaction code (e.g., indicating a type of service for the associated service usage information). For example, the rules engine can apply a rule or a set of rules based on the identified service associated with the device generated service 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).

[00125] 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).

[00126] In some embodiments, the service controller 122 sends the device generated CDRs to the rules engine (e.g., a service usage data store and rules engine, such as CDR storage, aggregation, mediation, feed 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 (e.g., by network provision system 160) and behaves substantially similar to other CDR generators on the network).

[00127] In some embodiments, the service controller 122 is provisioned as a new type of networking function that is recognized as a valid, authorized, and secure source for CDRs by the other necessary elements in the network (e.g., CDR storage, aggregation, mediation, feed 118). In some embodiments, if the necessary network apparatus only recognize CDRs from certain types of networking equipment (e.g., a RAN gateway or transport gateway), then the service controller 122 provides authentication credentials to the other networking equipment that indicate that it is one of the approved types of equipment for 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.

[00128] 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 provides the device assisted service usage information (e.g., device based CDRs or micro-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), as it is not required to mediate network based CDRs and device assisted CDRs), and the device based service usage information is provided to the central billing interface 127 or the central billing system 123.

[00129] In some embodiments, the device based CDRs (e.g., micro-CDRs) and/or new CDRs generated based on execution of a rules engine as described herein are provided only for devices that are managed and/or based on device group, service plan, or any other criteria, categorization, and/or grouping, such as based on ambient service or ambient service provider or transactional service or transactional service provider.

[00130] In some embodiments, QoS for DAS includes a service processor (e.g., any device assisted element/function) that facilitates coordination for and/or provisions wireless access/radio access bearers (e.g., RABs). In some embodiments, the service processor determines whether a request for QoS is authorized (e.g., according to QoS service level, user standing, available local network capacity (e.g., as reported by other device(s) and/or network)). In some embodiments, device QoS capacity demand reports provide and/or augment network capacity demand reports.

[00131] In some embodiments, QoS for DAS includes a service controller (e.g., any network device based service control element/function) that facilitates coordination for and/or provisions wireless access/radio access bearers (e.g., RABs) on a device (e.g., a communications device, such as a mobile wireless communications device and/or an intermediate networking device), on network, and/or on device plus network. In some embodiments, the service controller provides device QoS capacity demand reports to other network equipment/elements/functions, and then also provisions the RAB channel based on various criteria and determinations.

[00132] In some embodiments, QoS for DAS provides for device assisted monitoring, information, and/or functionality to facilitate QoS without and/or to assist network based

monitoring, information, and/or functionality (e.g., Deep Packet Inspection (DPI) and/or provides such monitoring, information, and/or functionality that may not be available via network based monitoring, information, and/or functionality (e.g., encrypted activities on the device may not be accessible by DPI or other network based techniques). For example, QoS for DAS can assist in the QoS setup to facilitate the QoS setup and provide such information that may not otherwise be available using network based only techniques. For example, device assisted activity and/or service monitoring techniques can assist in classifying the QoS for the monitored activity and/or service using, for example, a QoS activity map (e.g., as described herein or other similar techniques). For example, using such device assisted techniques eliminates and/or minimizes DPI or other network based techniques that can give rise to privacy concerns/issues, network neutrality concerns/issues, and/or otherwise may not be able to provide similar or equivalent granular service/activity monitoring, as discussed above, and/or also off loads such processing from the network (e.g., network elements/devices/functionality) to the communications devices (e.g., at least for such communications devices that can perform such functions, based on their processing and/or memory capabilities, as would be apparent to one of ordinary skill in the art). In some embodiments, QoS for DAS includes the service provider for providing an initial authorization/clearance for a QoS request (e.g., using various techniques described herein), and the service controller determines if the QoS request should be authorized (e.g., based on various QoS authorization/clearance/approval criteria (e.g., QoS activity maps and/or QoS request rule) and/or network capacity, as described herein). In some embodiments, QoS for DAS includes the service provider for providing a QoS request including a QoS class to the service controller, and the service controller determines if the QoS request should be authorized, as described herein. In some embodiments, DAS for protecting network capacity provides for device assisted monitoring, information, and/or functionality to facilitate protecting network capacity without and/or to assist network based monitoring, information, and/or functionality (e.g., Deep Packet Inspection (DPI) and/or provides such monitoring, information, and/or functionality that may not be available via network based monitoring, information, and/or functionality (e.g., encrypted activities on the device may not be accessible by DPI or other network based techniques). In some embodiments, DAS for protecting network capacity provides for device assisted monitoring, information, and/or functionality to facilitate protecting network capacity without solely relying upon DPI and/or without any use or any significant use

of DPI wireless network, which conserves network resources and network capacity by controlling device network access behavior at the device instead of deep in the core network at a DPI gateway (e.g., DPI based techniques consume over the air wireless network capacity even if chatty device behavior is blocked at a DPI gateway; in contrast, DAS for protecting network capacity techniques that do not use DPI based techniques for controlling device service usage can, for example, provide a device based usage notification and service selection UI that does not consume over the air wireless network capacity).

[00133] In some embodiments, QoS for DAS and/or DAS for protecting network capacity includes providing or facilitating reports for base station (BTS) for network capacity (e.g., sector, channel, busy state information or network capacity usage/availability, and/or network capacity expected demand) based on, for example, one or more of the following: monitored application usage on the communications device, monitored user activity on the communications device, location of the communications, other available networks, and/or other monitored or determined activity, service usage measure, and/or metric. In some embodiments, at or after execution of an application that is determined to require network service usage (e.g., may require increased wireless network bandwidth, such as based on a service usage activity map), QoS for DAS sends information to the network (e.g., a network controller or other network device element/function) that capacity demand is forthcoming for the communications device (e.g., potentially initiating a provisioning of a QoS radio access bearer (RAB) or other type of RAB).

[00134] In some embodiments, network capacity (e.g., busy state information) is collected from one or more communications devices in communication with a wireless network (e.g., network capacity/usage information measured from each respective communications device's perspective is determined and stored by the service processor on each respective communications device) and reported to the service controller, and the service controller (e.g., or another network element/function) uses this information to determine what resources are available for allocation to various levels of QoS (e.g., to respond to/facilitate various QoS requests) and/or to workload balance across multiple base stations and/or networks (e.g., wired networks, cellular, Wi-Fi, and/or other wireless networks).

[00135] In some embodiments, the service processor executed on the communications device sends a QoS request (e.g., a wireless network bearer channel reservation request or Radio Access

Bearer (RAB) request) to the service controller. The service controller verifies the request using various verification techniques as described herein. In some embodiments, the service controller facilitates coordination of various device QoS requests with one or more base stations (BTSs) in communication with the communications device to provide for the requested QoS reservation to facilitate the new QoS session. In some embodiments, the service controller provides a QoS routing function by, for example, providing various QoS routing instructions to a device service processor (e.g., aggregating, prioritizing, queuing, authorizing, allocating reservations/RABs, denying, re-routing (such as to other BTSs and/or other networks) and/or otherwise managing QoS requests), in which the BTS may or may not be QoS aware. For example, QoS priority can be based on activity (e.g., service usage and/or application), service level, user standing, network capacity, time of day, and/or QoS priority can be purchased on a transaction basis, a session basis, a pre-pay basis or a plan basis. As another example, QoS priority can also vary by device type, user within a group, group, application type, content type, or any other criteria or measure and/or any combination thereof. In some embodiments, the service controller also facilitates coordination of various device QoS requests with other network elements/functions for QoS implementation and management to provide for an end to end QoS solution.

[00136] In some embodiments, QoS can be symmetric for two mobile devices or asymmetric. In some embodiments, QoS resource availability can be from communications devices, BTS(s), other network functions (e.g., service control, service controller and/or any other network elements/functions) or any combination thereof. In some embodiments, the service controller provides QoS demand information to another network element/function. In some embodiments, the service controller provides the central aggregator and policy decision point (PDP). In some embodiments, the service controller controls (e.g., at least in part) QoS related functions for communications devices, BTS(s), and/or a combination of both.

[00137] In some embodiments, charging (e.g., monitoring and/or determining associating charging or billing) for QoS service usage/transactions and/or network capacity controlled services usage/transactions is determined using various techniques described herein. For example, the service processor can assist in charging for QoS and/or network capacity controlled activities. In some embodiments, the service processor uses device assisted Charging Data Records (CDRs) or micro-CDRs to assist in charging for QoS and/or network capacity controlled activities (e.g., using QoS class related transaction codes and/or network capacity controlled

related transaction codes), as described herein with respect to various embodiments. In some embodiments, charging for QoS and/or network capacity controlled services is performed in whole or in part by one or more network elements/functions (e.g., service controller, SGSN/GGSN/other gateways, and/or billing interfaces/servers).

[00138] In some embodiments, service usage information includes network based service usage information. In some embodiments, the network based service usage information includes network based CDRs. In some embodiments, service usage information includes device based service usage information. In some embodiments, device based service usage information includes device assisted CDRs, also referred to herein as micro-CDRs, as described herein. In some embodiments, micro-CDRs are used for CDR mediation or reconciliation that provides for service usage accounting on any device activity that is desired (e.g., providing granular service usage information, such as based on application layer service usage monitoring, transaction service usage monitoring, QoS activities/sessions/transactions, network capacity controlled activities/sessions/transactions, and/or other types of service usage information). In some embodiments, each device includes a service processor (e.g., a service processor executed on a processor of a communications device, such as a mobile device or an intermediate networking device that can communicate with a wireless network).

[00139] In some embodiments, each device activity that is desired to be associated with a billing event (e.g., for a QoS related billing event) is assigned a micro-CDR transaction code, and the service processor is programmed to account for that activity associated with that transaction code (e.g., various transaction codes can be associated with service usage associated with certain services, applications, and/or based on QoS classes or priorities, respectively, which can be used for providing granular service usage for these various Internet/network based services/sites/transactions and/or any other Internet/network based services/sites, which can include transactional based services). For example, using these techniques, as described herein, essentially any type of device activity (e.g., including QoS classes and prioritization and/or network capacity controlled classes and prioritization) can be individually accounted for and/or controlled (e.g., throttled, restricted, and/or otherwise controlled as desired). In some embodiments, the service processor periodically reports (e.g., during each heartbeat or based on any other periodic, push, and/or pull communication technique(s)) micro-CDR usage measures to, for example, a service controller or some other network element/function. In some

embodiments, the service controller reformats the heartbeat micro-CDR usage information into a valid CDR format (e.g., a CDR format that is used and can be processed by an SGSN or GGSN or some other authorized network element/function for CDRs) and then transmits the reformatted micro-CDRs to a network element/function for performing CDR mediation.

[00140] In some embodiments, CDR mediation is used to properly account for the micro-CDR service usage information by depositing it into an appropriate service usage account and deducting it from the user device bulk service usage account. For example, this technique provides for a flexible service usage billing solution that uses pre-existing solutions for CDR mediation and billing. For example, the billing system can process the mediated CDR feed from CDR mediation, apply the appropriate account billing codes to the aggregated micro-CDR information that was generated by the device, and then generate billing events in a manner that does not require changes to existing billing systems, infrastructures, and techniques (e.g., using new transaction codes to label the new device assisted billing capabilities).

[00141] In some embodiments, the various QoS techniques performed on or by the communications device (e.g., using a service processor to provide or assist in providing QoS session provisioning, QoS policy management, QoS policy enforcement, and/or QoS accounting/charging, such as QoS charging records and reports) are verified (e.g., using various verification techniques described herein). In some embodiments, the various network capacity controlled services techniques performed on or by the communications device (e.g., using a service processor to provide or assist in providing network capacity controlled services policy management, network capacity controlled services policy enforcement, and/or network capacity controlled services charging, such as network capacity controlled services charging records and reports) are verified (e.g., using various verification techniques described herein).

[00142] For example, a QoS request, QoS related policy rules (e.g., QoS activity map, QoS related service plan and/or service policy settings) and implementation, QoS policy enforcement, and QoS charging are verified (e.g., periodically, per transaction, and/or based on some other criteria/metric). In some embodiments, verification techniques include one or more of the following: compare a network based service usage measure with a first service policy associated with the communications device, compare a device assisted service usage measure with the first service policy, compare the network based service usage measure to the device assisted service

usage measure, perform a test and confirm a device assisted service usage measure based on the test, perform a User Interface (UI) notification (e.g., which can include a user authentication, password, question/answer challenge, and/or other authentication technique), and/or other similar verification techniques as will now be apparent to one of ordinary skill in the art. Accordingly, in some embodiments, QoS for DAS "closes the loop" for verification of various QoS related techniques, such as QoS requests, QoS grants, QoS usage, and/or QoS charging. In some embodiments, the service processor and the service controller serve as a verifiable QoS management/coordination system for other QoS elements/functions in network. In some embodiments, if such or other verification techniques determine or assist in determining that a QoS request, QoS report, and/or QoS policy behavior (e.g., or similarly, network capacity controlled services monitoring, reporting, and/or policy behavior) does not match expected requests, reports, and/or policy, then responsive actions can be performed, for example, the communications device (e.g., and/or suspect services) can be suspended, quarantined, killed/terminated, and/or flagged for further analysis/scrutiny to determine whether the device is malfunctioning, needs updating, has been tampered with or compromised, is infected with malware, and/or if any other problem exists.

[00143] In some embodiments, the communications device (e.g., the service processor) maintains a QoS flow table that associates or maps device activity to QoS level/class to RAB/QoS channel, and in some embodiments, the communications device also informs a QoS management network function/element of the relative priority of the QoS flows for the communications device (e.g., based on or using the QoS flow table). In some embodiments, the service controller receives or collects information from the communications device and maintains such a QoS flow table for the communications device and, in some embodiments, the service controller also informs a QoS management network function/element of the relative priority of the QoS flows for the communications device (e.g., based on or using the QoS flow table). In some embodiments, flows can be assigned to activities originating at the communications device in a transparent way, or simply by activity class or user preference, or using other techniques.

[00144] In some embodiments, the communications device maintains a table of QoS billing rates, scheduled transmission times, and/other QoS related information to implement an overlay MAC at the data networking level to manage QoS on legacy networks that are not QoS MAC

enabled and/or do not have the various functionality to support QoS controls (e.g., and such techniques can also be used to provide for QoS functionality across different networks). In some embodiments, QoS related policies are exchanged between roaming and home service controllers to facilitate QoS support while roaming on a non-home network(s).

[00145] In some embodiments, the communications device serves as a network capacity indicator (e.g., collecting network capacity information for a local cell and communicating or reporting that network capacity information to the service controller). For example, permanent local cell communications devices can be placed in local cell areas to augment legacy equipment for such network capacity indicator/reporting functions. Various other techniques for determining network capacity and/or network availability are described herein.

[00146] In some embodiments, service partners and/or service providers can subsidize in whole or in part to upgrade a given user or group of users to better QoS related service level agreement (SLA)/class for a preferred destination. In some embodiments, based on monitored service usage and/or other monitored behavior of the communications device, such subsidized QoS upgrade/offers can be presented to a user of the communications device (e.g., as an incentive/reward for desired or preferred user behavior or for other reasons). Similarly, in some embodiments, these techniques are also applied to network capacity controlled services.

[00147] In some embodiments, QoS charging is based on QoS channel/reservation, service flow, or RAB charging (e.g., single flow per RAB, multi-flow per RAB, multi-RAB per flow). In some embodiments, charging (e.g., for QoS and/or for network capacity controlled services) is based on one or more of the following: network busy state, time criteria, user service class request, traffic volume and class, time and class, network capacity (e.g., network busy state) and class, time of day and class, location, traffic type, application type, application class, destination, destination type, partner service, and/or other criteria/measures. In some embodiments, QoS charging is verified using the various verification techniques described herein (e.g., test charging events). In some embodiments, network capacity controlled services charging is verified using the various verification techniques described herein (e.g., test charging events). In some embodiments, QoS charging is by data usage (e.g., by Megabyte (MB)), service flow by time by QoS class, speed by time, network busy state, time of day/day of week, service plan, current network, and/or other criteria/measures. In some embodiments, network capacity controlled

services charging is by data usage (e.g., by Megabyte (MB)), service flow by time by network capacity controlled services class, speed by time, network busy state, time of day/day of week, service plan, current network, and/or other criteria/measures.

[00148] In some embodiments, QoS for DAS includes coordinating functions with one or more of the following: DAS elements/functions, Radio Access Network (RAN), Transport network, Core network, GRX network, IPX network, and/or other networks/elements/functions.

[00149] FIG. 2 illustrates another functional diagram of another network architecture for providing quality of service (QoS) for device assisted services (DAS) and/or for providing DAS for protecting network capacity in accordance with some embodiments. In some embodiments, QoS for DAS techniques described herein are implemented using the network architecture shown in FIG. 2. In some embodiments, DAS for protecting network capacity techniques described herein are implemented using the network architecture shown in FIG. 2.

[00150] As shown, FIG. 2 includes various devices 100 including service processors 115. For example, devices 100 can include various types of mobile devices, such as phones, PDAs, computing devices, laptops, net books, tablets, cameras, music/media players, GPS devices, networked appliances, and any other networked device; and/or devices 100 can include various types of intermediate networking devices, as described herein. The devices 100 are in communication with service control 210 and central provider access and core networks 220. Service policies and accounting functions 230 are also provided in communication with the central provider access and core networks 220. For example, devices 100 can communicate via the central provider access and core networks 220 to the Internet 120 for access to various Internet sites/services 240 (e.g., Google sites/services, Yahoo sites/services, Blackberry services, Apple iTunes and AppStore, Amazon.com, FaceBook, and/or any other Internet service or other network facilitated service).

[00151] In some embodiments, FIG. 2 provides a wireless network architecture that supports various DAS for protecting network capacity techniques as described herein. Those of ordinary skill in the art will appreciate that various other network architectures can be used for providing various DAS for protecting network capacity techniques as described herein, and FIG. 2 is

illustrative of just another such example network architecture for which DAS for protecting network capacity techniques as described herein can be provided.

[00152] FIG. 3 illustrates another functional diagram of an architecture 300 including a device based service processor 115 and a service controller 122 for providing quality of service (QoS) for device assisted services (DAS) and/or for providing DAS for protecting network capacity in accordance with some embodiments. In some embodiments, QoS for DAS techniques described herein are implemented using the functions/elements shown in FIG. 3. In some embodiments, DAS for protecting network capacity techniques described herein are implemented using the functions/elements shown in FIG. 3.

[00153] For example, the architecture 300 provides a relatively full featured device based service processor implementation and service controller implementation. As shown, this corresponds to a networking configuration in which the service controller 122 is connected to the Internet 120 and not directly to the access network 1610. As shown, a data plane (e.g., service traffic plane) communication path is shown in solid line connections and control plane (e.g., service control plane) communication path is shown in dashed line connections. As will be apparent to one of ordinary skill in the art, 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. 3 are described below with respect to, for example, FIGS. 4, 12, and 13 as well as FIGS. 5 through 11 (e.g., QoS for DAS related embodiments) and FIGS. 14 through 23 (e.g., DAS for protecting network capacity related embodiments).

[00154] As shown in FIG. 3, 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.

[00155] As shown in FIG. 3, 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. 3, 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.

[00156] In some embodiments, the service control server link 1638 provides for securing, signing, encrypting and/or otherwise protecting the communications before sending such communications over the service control link 1653. For example, the service control server link 1638 can send to the transport layer or directly to the link layer for transmission. In another example, the service control server link 1638 further secures the communications with transport layer encryption, such as TCP TLS or another secure transport layer protocol. As another example, the service control server link 1638 can encrypt at the link layer, such as using IPSEC, various possible VPN services, other forms of IP layer encryption and/or another link layer encryption technique.

[00157] As shown in FIG. 3, the service controller 122 includes an access control integrity server 1654 (e.g., service policy security server). 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 (e.g., QoS policy violation and/or a network capacity controlled services policy violation) or a system integrity breach is suspected.

[00158] 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 (e.g., service policy security agent) reports and error conditions. Many of the access control integrity agent 1654 checks can be accomplished by the server. For example, the access control integrity agent 1654 checks include one or more of the following: service usage measure against usage range consistent with policies (e.g., usage measure from the network and/or from the device); configuration of agents; operation of the agents; and/or dynamic agent download.

[00159] 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 (e.g., a QoS policy and/or a network capacity controlled services policy). For example, device service policy implementations can include measuring total QoS data passed, QoS 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.

[00160] In some embodiments, the access control integrity server 1654 (e.g., and/or some other agent of service controller 122) verifies device service policy, and the verification error conditions that can indicate a mismatch in QoS service measure and QoS 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 QoS 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 (e.g., a QoS policy and/or a network capacity controlled services policy).

[00161] As shown in FIG. 3, service controller 122 includes a service history server 1650 (e.g., charging server). 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 (e.g., CDR feed and CDR mediation). 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.

[00162] As shown in FIG. 3, service controller 122 includes a policy management server 1652 (e.g., policy decision point (PDP) server) for managing service usage policies, such as QoS policies and/or a network capacity controlled services policies. 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.

[00163] 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 the 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, and/or other sensitive information) 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, and/or otherwise obtains a measure of network availability/capacity and adjusts traffic shaping policy and/or other policy settings based on available network availability/capacity (e.g., a network busy state).

[00164] As shown in FIG. 3, 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 some embodiments, the network traffic analysis server 1656 estimates the service quality and/or service usage for the network under variable settings on potential service policies. In some 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. In some embodiments, the network traffic analysis server 1656 estimates the network availability/capacity for the network under variable settings on potential service policies. In some embodiments, the network traffic analysis server 1656 identifies actual or

potential service behaviors by one or more devices that are impacting and/or causing problems for overall network availability/capacity.

[00165] As shown in FIG. 3, Service Analysis, Test & Download 122B includes a beta test server 1658 (e.g., policy creation point and beta test server). 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, such as for protecting network capacity.

[00166] As shown in FIG. 3, service controller 122 includes a service download control server 1660 (e.g., a service software download control server). In some embodiments, the service download control server 1660 provides a download function to install and/or update service software elements (e.g., the service processor 115 and/or agents/components of the service processor 115) on the device, as described herein.

[00167] As shown in FIG. 3 service controller 122 includes a billing event server 1662 (e.g., micro-CDR server). 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.

[00168] As shown in FIG. 3, the Access Network HLR 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 the device service history 1618).

[00169] As shown in FIG. 3, 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 (e.g., to verify service usage charging). In some embodiments, the device service history 1618 is used to synchronize and/or verify the local service usage counter (e.g., to verify service usage accounting).

[00170] As shown in FIG. 3, the central billing 1619 (e.g., central provider billing server) 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.

[00171] As shown in FIG. 3, in some embodiments, modem selection and control 1811 (e.g., in communication with connection manager 1804 as shown) 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 (e.g., 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 (e.g., potentially for higher service payments) than other users). As another example, ambient services (e.g., as similarly described herein) can be provided for the hotspot for verified service processors.

[00172] 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 (e.g., or 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.

[00173] As shown in FIG. 3, 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. 3, 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.

[00174] As shown in FIG. 3, service processor 115 includes an API and OS stack interface 1693. In some embodiments, the API and OS stack interface 1693 provides the QoS API functionality as similarly described herein with respect to various embodiments. In some embodiments, a QoS API is used to report back QoS availability to applications. In some

embodiments, the API and OS stack interface 1693 provides the network capacity controlled API and/or emulated API functionality as similarly described herein with respect to various embodiments. As shown, service processor 115 also includes a router 1698 (e.g., a QoS router agent/function and/or a network capacity controlled services router agent/function) and a policy decision point (PDP) agent 1692. In some embodiments, the router 1698 provides QoS router functionality as similarly described herein with respect to various embodiments. In some embodiments, the router 1698 provides network capacity controlled services router functionality as similarly described herein with respect to various embodiments. In some embodiments, the QoS router supports multiple QoS channels (e.g., one or more provisioned/allocated QoS links forming a QoS channel between the device and the desired end point, such as an access point/BTS/gateway/network for a single ended QoS channel or other communication device for an end to end QoS channel, depending on the QoS connection/network support/availability/etc.). In some embodiments, the QoS router supports multiple QoS channels, which can each have different QoS classes/levels. In some embodiments, the QoS router routes application/service usage traffic to an appropriate QoS channel. In some embodiments, the QoS router determines the routing/mapping based on, for example, one or more of the following: a QoS API request, a QoS activity map, a user request, a service plan, a service profile, service policy settings, network capacity, service controller or other intermediate QoS network element/function/device, and/or any other criteria/measure, as similarly described herein with respect to various embodiments. In some embodiments, multiple different applications/services are routed to a particular QoS channel using various techniques described herein. In some embodiments, different applications/services are routed to different QoS channels using various techniques described herein. In some embodiments, the QoS router assists in managing and/or optimizing QoS usage for the communications device. In some embodiments, the QoS router assists in managing and/or optimizing QoS usage across multiple communications devices (e.g., based on network capacity for a given cell area/base station or other access point). In some embodiments, PDP agent 1692 provides the PDP agent functionality as similarly described herein with respect to various embodiments. As shown, architecture 300 also includes a suspend resume interface 320, network QoS provisioning interfaces 330 (e.g., for providing the various QoS techniques described herein), and an activation/suspend resume server 340 and billing interface server 350 in the service controller 122A.

[00175] 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 (e.g., charging agent), 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 (not shown), 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 socket (such as by IP address, protocol, and/or port), by socket id (such as port address/number), by port number, by content type, by application or application type, and/or any other service usage activity classification/categorization) with associated IP addresses and/or other criteria/measures. 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 for providing QoS for DAS and/or for providing DAS for protecting network capacity. 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, and/or any of the various other DAS related techniques as described herein with respect to various embodiments.

[00176] 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 (e.g., 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 (e.g., 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 (e.g., security credentials). In some embodiments, the ability to load at least a portion of service processor 115 software into protected non-volatile memory also requires a secure key and/or signature and/or requires that the service processor 115 software components being loaded into non-volatile memory are also securely encrypted and appropriately signed by an authority that is trusted by a secure software downloader function, such as service downloader 1663 as shown in FIG. 3. 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.

[00177] FIGS. 4A through 4C illustrates a functional diagram for providing quality of service (QoS) for device assisted services (DAS) in accordance with some embodiments. In some

embodiments, QoS for DAS techniques described herein are implemented using the network architecture shown in FIGS. 4A through 4C.

[00178] Referring to FIG. 4A, in some embodiments, QoS functionality is performed at the communications device 100 using service processor 115 as similarly described herein. For example, the service processor 115 determines whether or not a QoS request is authorized (e.g., based on the associated service plan and/or other criteria/measures). If the QoS request is authorized, then the service processor 115 communicates with the base station (BTS) 125 to send the QoS request (e.g., a RAB or multi-RAB reservation request) to the local BTS. The BTS determines whether to accept or deny the QoS request (e.g., based on network capacity, such as using a first come first service QoS/network bandwidth or best effort access policy or other techniques, and/or other criteria/measures). The BTS responds to the QoS request accordingly. If the QoS request is granted, the QoS session can be initiated as similarly described herein. In some embodiments, the service processor 115 also performs various QoS charging functions using various techniques described herein, and the service processor 115 periodically sends QoS charging records or reports to the service controller 122 (e.g., and/or another network element/function). In some embodiments, the service processor 115 and the QoS related functions performed by the service processor 115 are periodically verified using the various techniques described herein.

[00179] Referring to FIG. 4B, FIG. 4B is similar to FIG. 4A except that the service controller 122 is also shown to be in communication with the service processor 115 of the communications device 100, which can provide for the download and periodically updating of the QoS rules and/or other service plan/profile/policy information that can include QoS related information. In some embodiments, the service processor 115 also performs various QoS charging functions using various techniques described herein, and the service processor 115 periodically sends QoS charging records or reports to the service controller 122 (e.g., and/or another network element/function). In some embodiments, the service processor 115 and the QoS related functions performed by the service processor 115 are periodically verified using the various techniques described herein.

[00180] Referring to FIG. 4C, at 410, the service processor 115 sends a QoS request to the service controller 122 (e.g., the service processor can also (at least in part) determine whether the

QoS request is authorized as similarly described with respect to FIG. 4A). At 420, the service controller 122 sends the QoS request to the BTS 125 if it is determined that the QoS request is authorized using various techniques described herein and/or whether the BTS 125 has network capacity for the QoS request. For example, the service controller can provide a central policy decision point function for QoS related activities (e.g., based on QoS prioritization, network capacity, and/or other criteria/measures/policies). At 430, the service controller 122 communicates the response to the QoS request accordingly. At 440, if the QoS request was approved, the device 100 initiates the QoS session (e.g., using a RAB or multi-RAB reservation) via the BTS 125. In some embodiments, the service processor 115 also performs various QoS charging functions using various techniques described herein, and the service processor 115 periodically sends QoS charging records or reports to the service controller 122 (e.g., and/or another network element/function). In some embodiments, the service processor 115 and the QoS related functions performed by the service processor 115 are periodically verified using the various techniques described herein.

[00181] In some embodiments, QoS techniques as described herein are implemented in the device (e.g., using the service processor 115) and one or more other network elements/functions, such as the BTS 125, service controller 125, RAN, SGSN/GGSN/other gateways and/or other network elements/functions, in which various of the QoS related functions can be distributed or allocated to such network elements/functions based on various design/network architecture approaches as will now be apparent to one of ordinary skill in the art, in which QoS related activities and/or functions at the device 100 are verified using various verification techniques described herein.

[00182] In some embodiments, the device determines QoS availability by directly querying QoS link reservation equipment in the network (e.g., an access point, such as the BTS 125). In some embodiments, the device determines QoS availability based on an intermediate network function that coordinates QoS requests with one or more network QoS link resources. In some embodiments, the device requests a QoS reservation in advance of QoS link establishment with one or more QoS network link resources. In some embodiments, in response to a QoS request, a QoS channel is reported as available only if/after it is determined that the necessary one or more QoS links required to create the QoS channel are available, and, for example, the QoS channel

can then be reserved based on a confirmation or automatically be reserved in response to the QoS request.

[00183] FIG. 5 illustrates a functional diagram for generating a QoS activity map for quality of service (QoS) for device assisted services (DAS) in accordance with some embodiments. In particular, FIG. 5 illustrates techniques for mapping a service plan or a set of service plan policies/rules for QoS 510 to a set of QoS activity rules 530. As shown, a set of QoS rules/QoS related device state information 510 (e.g., a set of associated service plan, service plan usage, other state such as network capacity or forecasted demand or time of day/day of week, activity usage, QoS level, and/or user preferences) is mapped using a QoS mapping function to a set of QoS activity rules 530 using various techniques described herein. At 530, activity rules (e.g., activity policy rules instructions) 530 are determined using the mapping function 520. In some embodiments, DAS for network capacity controlled services techniques can similarly be implemented using the techniques described with respect to FIG. 5 (e.g., for generating and implementing a network capacity controlled services activity map).

[00184] In some embodiments, the service plan includes a list of activity policies, and each activity policy in the service plan specifies how the activity policy is modified by rules state information. In some embodiments, each activity policy then becomes the instruction for the engine (e.g., QoS mapping function 520) that maps the activity policy to QoS activity rules 530. In some embodiments, service controller 122 downloads QoS mapping function 520, which is implemented by service processor 115.

[00185] In some embodiments, the service processor determines (e.g., and classifies) application/service usage activity demand with or without granular application/service usage activity (e.g., depending on various user/service plan/service provider/network/legal and/or other privacy restrictions and/or any other related requirements or settings). For example, policies (e.g., service policy settings and/or service profile settings) can be downloaded to provide such application/service usage activity monitoring rules and a QoS activity map for assigning such monitored activities to various QoS classes or priorities, and, in some embodiments, such monitoring and the QoS activity map can also be implemented using various verification techniques described herein (e.g., periodically audited, tested, compared with network service usage information). In some embodiments, the QoS activity map is based on a service plan,

service profile, and/or service policy settings associated with the communications device. In some embodiments, the QoS activity map is based on a device group and/or user group. In some embodiments, the QoS activity map is based on user input (e.g., a user of the communications device can identify QoS classes/service levels for various applications and/or service activities, in response to requests for user input, based on user configurations, user defined rules (e.g., to eliminate or mitigate privacy and/or net neutrality concerns/issues), and/or confirmed monitored user behavior QoS related patterns or preferences). In some embodiments, the QoS activity map includes mappings/associations based on one or more of the following: a user preference for a given destination, destination class, application, application class (e.g., by application class instead of with respect to a specific application can also eliminate or mitigate privacy and/or net neutrality concerns/issues), flow, traffic or flow class, time period, time of day, location, network busy state (e.g., provide QoS when you can, then charge more when busy, notify user of busy state), device type, user type, user plan, user group, user standing, partner service, tokens, service type, and/or other criteria or measures.

[00186] In some embodiments, various techniques described herein are managed for device 100 for incoming and/or outgoing QoS requests. In some embodiments, as shown in FIG. 6, QoS for DAS includes establishing an end to end coordinated QoS service channel control.

[00187] FIG. 6 illustrates a functional diagram for quality of service (QoS) for device assisted services for an end to end coordinated QoS service channel control in accordance with some embodiments. As shown in FIG. 6, a wireless communications device 100A includes a service processor 115A in secure communication with service controller 122A. A wireless communications device 100B includes a service processor 115B in secure communication with service controller 122B. In some embodiments, when, for example, device 100A initiates a QoS request for a QoS class session in communication with device 100B (e.g., a VOIP call or another application service requiring or possibly using a QoS class/level session, such as a conversational or other QoS type of class/level), as sequence of actions are performed using service controller 122A and service controller 122B to facilitate/setup an end to end coordinated QoS service channel control. In some embodiments, as similarly described herein, assuming that service processor 115A and service controller 122A determine that the QoS request from device 100A is authorized for that device, then the service controller 122A contacts registry 650 (e.g., a device registry, such as an HLR, mobile services center, or other central database or registry including,

for example, service controller mappings by device/IP address/other) to determine the service controller associated with/responsible for managing QoS/service control for device 100B. The registry 650 provides the service controller 122B information (e.g., IP address/other address) based on this lookup determination. In some embodiments, service controller 122A then initiates the QoS request with service controller 122B to determine if the device 100B is authorized and/or available for the QoS session requested by device 100A. In some embodiments, service controllers 122A/B communicate with BTSs 125A/B to determine whether the QoS request can be facilitated (e.g., based on network capacity) as similarly described herein. In some embodiments, the service controllers 122A and 122B provide the central QoS coordination function and can request appropriate QoS channels directly from the respective local BTSs. In some embodiments, the service controllers 122A and 122B also communicate with one or more of the following network elements/functions as shown in FIG. 6 in order to facilitate an end to end coordinated QoS service channel control: RAN 610/670, Core Network 620/660, and IPX network 630. In some embodiments, service controllers 122A and 122B communicate with various necessary network elements for provisioning to facilitate session provisioning through the carrier core network as similarly discussed above. In some embodiments, service controllers 122A and 122B communicate with various necessary network elements for provisioning to facilitate session provisioning through the IPX network as similarly discussed above. As will be apparent to one of ordinary skill in the art, QoS for DAS techniques as described herein can be similarly implemented using these or similar techniques to various other network architectures.

[00188] FIG. 7 illustrates a flow diagram for quality of service (QoS) for device assisted services (DAS) in accordance with some embodiments. At 702, the process begins. At 704, QoS rules are received or determined (e.g., a service processor receives or requests the QoS rules, which may be included in service plan, service profile, and/or service policy settings associated with the communications device). In some embodiments, the QoS rules are verified using various techniques as described herein (e.g., periodically updated, replaced, downloaded, obfuscated, and/or tested using by a service controller and/or using other verification techniques). In some embodiments, a QoS API is also used by various applications to initiate a QoS request, as described herein with respect to various embodiments. In some embodiments, the QoS rules are implemented in the form of a QoS activity map in accordance with various embodiments described herein. At 706, the communications device's standing for QoS is

determined using various techniques described herein (e.g., based on the service plan, service profile, service policy settings, QoS rules, based on QoS class, current service usage, current billing standing, and/or any other criteria/measure). In some embodiments, in addition to verifying the device/user standing for the QoS request, whether the device is following or in compliance with an assigned QoS reservation request policy is also verified using various techniques described herein. If the device is determined to not be eligible for QoS, then at 708, the device User Interface (UI) provides information concerning the denial/ineligibility for QoS session(s) (e.g., denial/ineligibility explanation and/or options for providing for one or more QoS options, such as a service plan upgrade or payment for a certain/set of/period of time for QoS session(s) access). If the device is determined to be eligible for QoS, then at 710, QoS availability is determined (e.g., based on network capacity, which may be determined at the device, via communication with the service controller, via communication with the BTS, and/or any combination thereof, using the various techniques described herein). If QoS is determined to not be available, then at 712, the UI provides information and/or options concerning the QoS availability (e.g., unavailability explanation and/or options for providing for one or more QoS options, such as a service plan upgrade or payment for a certain/set of/period of time for QoS session(s) access). If QoS is determined to be available, then at 714, a request for network resources for the QoS session is sent to one or more network resources (e.g., service controller, BTS, gateway, core/transport network, IPX/GRX networks, and/or other network elements/functions/resources). At 716, a confirmation of the approved QoS session is received to close the loop for the QoS for DAS (e.g., a QoS schedule is received that provides the QoS session confirmation information, such as a scheduled RAB/multi-RAB and/or other reserved network resource(s) by schedule/other criteria). At 718, one or more verification techniques are performed to verify the QoS for DAS implementation on the device using various verification techniques described herein (e.g., comparing QoS service usage reports from a network source with the associated device policy; comparing QoS service usage reports from a network source with the QoS service usage reports from the device, and/or using other verification techniques as similarly described herein). At 720, the process is completed.

[00189] FIGS. 8A through 8C each illustrate another flow diagram for quality of service (QoS) for device assisted services (DAS) in accordance with some embodiments. FIG. 8A illustrates another flow diagram for quality of service (QoS) for device assisted services (DAS) in

accordance with some embodiments. At 802, the process begins. In some embodiments, the QoS policies are implemented on the device (e.g., service processor collects/receives an associated service plan that defines/specifies basic policies for QoS, which can include a QoS activity map, which, for example, maps QoS classes based on application, service usage, flow type, destination, time of day, network capacity, and/or other criteria/measures, as similarly described herein). In some embodiments, a QoS API is also used by various applications to initiate a QoS request, as described herein with respect to various embodiments. In some embodiments, the QoS rules are implemented in the form of a verified QoS activity map in accordance with various embodiments described herein. At 804, a QoS request is determined (e.g., by QoS class for a particular associated service/application). In some embodiments, the QoS request is determined at least in part by using the QoS activity map using various techniques described herein, for example, based on service/application usage monitoring on the device (e.g., by the service processor service usage monitoring agent). In some embodiments, the QoS request is determined based on the QoS API. In some embodiments, the QoS request is determined to be associated with an outgoing connection or an incoming connection. At 806, whether the QoS request is authorized is determined (e.g., whether the QoS request supported by the service plan, sufficient charging credit exists for this QoS request, and/or other criteria/measures). If not, then at 808, the UI provides a responsive notification and/or option as similarly described herein. If the QoS request is approved, then at 810, a request for network resources for the QoS session is sent to one or more network resources (e.g., service controller, BTS, gateway, core/transport network, IPX/GRX networks, a/another service controller in communication with another communications device such as for setting up a conversational class QoS connection with the other communications device, and/or other network elements/functions/resources). If the device is determined to be eligible for QoS, then at 810, QoS availability is determined (e.g., based on network capacity, which may be determined at the device, via communication with the service controller, via communication with the BTS or another network element/function, and/or any combination thereof, using the various techniques described herein). If QoS is determined to not be available, then at 812, the UI provides information and/or options concerning the QoS availability (e.g., unavailability explanation and/or options for providing for one or more QoS options, such as a service plan upgrade or payment for a certain/set of/period of time for QoS session(s) access). If QoS is determined to

be available, then at 814, a request for network resources for the QoS session is sent to one or more network resources (e.g., service controller, BTS, gateway, core/transport network, IPX/GRX networks, and/or other network elements/functions/resources, to setup, for example, a QoS end to end connection – coordinate all resources end to end for the approved and verified QoS flow). At 816, a confirmation of the approved QoS session is received to close the loop for the QoS for DAS (e.g., a QoS schedule is received that provides the QoS session confirmation information, such as a scheduled RAB/multi-RAB and/or other reserved network resource(s) by schedule/other criteria). At 818, a QoS router is executed/performed on the communications device to assist in implementing QoS for DAS using various verification techniques described herein (e.g., to perform QoS queuing, throttling, and/or other QoS router related functions as described herein). At 820, verified QoS charging is performed (e.g., at least in part) on the device using various techniques described herein (e.g., using the service processor, such as the charging/service usage monitoring and/or other agents as described herein). In some embodiments, QoS charging records and/or reports are provided to one or more network elements for managing QoS billing and/or other QoS management/billing related service control functions (e.g., to the service controller and/or the billing interface or billing server). In some embodiments, QoS for DAS also facilitates reestablishing the QoS session/connection/channel/stream if the QoS session/connection/channel/stream is lost or goes down, using similar techniques to those described herein as would be apparent to one of ordinary skill in the art. At 822, the process is completed. In some embodiments, the QoS provisioning channel is closed when the device session is over to, for example, free up various resources.

[00190] FIG. 8B illustrates another flow diagram for quality of service (QoS) for device assisted services (DAS) in accordance with some embodiments. In some embodiments, QoS for DAS includes identifying the QoS requirements (e.g., QoS level or QoS class) for a service activity. At 824, the process begins. In some embodiments, the QoS policies are implemented on the device (e.g., service processor collects/receives an associated service plan that defines/specifies basic policies for QoS, which can include a QoS activity map, which, for example, maps QoS classes based on application, service usage, flow type, destination, time of day, network capacity, and/or other criteria/measures, as similarly described herein). In some embodiments, the QoS rules are implemented in the form of a verified QoS activity map in accordance with various embodiments described herein. At 826, the device monitors device activity, such as

service/application usage activities. In some embodiments, the device detects the relevant activities based on various service usage monitoring techniques described herein. At 828, a QoS request is determined, for example, using various techniques described herein. At 830, a QoS level is determined based on the application and/or various device monitored service usage/application activities associated with the QoS request using various techniques described herein. For example, the QoS level can be determined using the QoS activity map, which provides a QoS policy defined by a table associating various QoS levels with a variety of activities that include various device monitored service usage/application activities. In some embodiments, the QoS activity map includes QoS level mappings based on one or more of the following: application, destination/source, traffic type, connection type, content type, time of day/day of week, network capacity, activity usage, service plan selection, current standing, user class, device class, home/roaming, network capabilities, and/or other criteria/measures as similarly described herein. In some embodiments, at 832, if the QoS level cannot be determined and/or in order to confirm a QoS level or selection among multiple potential appropriate/approved QoS levels, the UI presents options for a user to select the QoS level. At 834, the QoS request is initiated for the determined QoS level (e.g., QoS class and/or priorities). At 836, the process is completed.

[00191] FIG. 8C illustrates another flow diagram for quality of service (QoS) for device assisted services (DAS) in accordance with some embodiments. In some embodiments, QoS for DAS includes determining whether the network should grant the QoS request for a given device activity. At 842, the process begins. At 844, QoS request is determined. At 846, the communications device's standing for QoS is determined using various techniques described herein (e.g., a service processor in combination with a service controller or based on a communication for authorization of the QoS request sent to the service controller determines whether the QoS request is authorized, which can be based on the service plan, service profile, service policy settings, QoS rules, based on QoS class, current service usage, current billing standing, and/or any other criteria/measure). If the device is determined to not be eligible for QoS, then at 848, the device User Interface (UI) provides information concerning the denial/ineligibility for QoS session(s) (e.g., denial/ineligibility explanation and/or options for providing for one or more QoS options, such as a service plan upgrade or payment for a certain/set of/period of time for QoS session(s) access). If the device is determined to be eligible

for QoS, then at 850, QoS availability is determined (e.g., based on network capacity, which may be determined at the device, via communication with the service controller, via communication with the BTS or another network element/function, and/or any combination thereof, using the various techniques described herein). If QoS is determined to not be available, then at 852, the UI provides information and/or options concerning the QoS availability (e.g., unavailability explanation and/or options for providing for one or more QoS options, such as a service plan upgrade or payment for a certain/set of/period of time for QoS session(s) access). If QoS is determined to be available, then at 854, a request for network resources for the QoS session is sent to one or more network resources (e.g., service controller, BTS, gateway, core/transport network, IPX/GRX networks, and/or other network elements/functions/resources can be queried directly and/or a centralized QoS resource/network function/element/database can be queried for determining such network resources and coordinating such scheduling). At 856, a confirmation of the approved QoS session is received to close the loop for the QoS for DAS (e.g., a QoS schedule is received that provides the QoS session confirmation information, such as a scheduled RAB/multi-RAB and/or other reserved network resource(s) by schedule/other criteria). At 858, a QoS router is performed. In some embodiments, the QoS router is performed on the device (e.g., service processor), on a network element/function (e.g., service controller), and/or in combinations thereof. In some embodiments, the QoS router prioritizes multiple QoS requests across a given communications device. In some embodiments, the QoS router prioritizes multiple QoS requests across multiple communications devices and/or across multiple BTSs. In some embodiments, the QoS router performs various QoS class degradation, promotion, and/or other throttling related techniques as similarly described herein (e.g., based on session priority, network capacity, workload balancing, QoS priority rules, and/or other criteria/measures/rules). At 860, the process is completed.

[00192] FIG. 9 illustrates another flow diagram for quality of service (QoS) for device assisted services (DAS) in accordance with some embodiments. In some embodiments, QoS for DAS includes QoS session provision for a service activity. At 902, the process begins. At 904, a new QoS session is granted and/or confirmed. At 906, a device service processor (e.g., policy decision point (PDP) agent, also referred to herein as a policy control agent) maps the QoS session grant to a QoS monitoring policy (e.g., based on a service controller provided QoS related policy, based on a service plan associated with the device, user, device/user group, and/or

other criteria/measures, as similarly described herein). At 908, the QoS monitoring policy provides commands/instructions to a policy enforcement point (PEP) (e.g., PEP agent, also referred to herein as a policy implementation agent) for managing/enforcing the new QoS priorities/sessions. At 910, the PEP determines whether to allow, block, throttle, and/or queue priority (e.g., and/or otherwise control using various traffic control related techniques) a session based on the QoS monitoring policy. At 912, the process is completed.

[00193] FIG. 10 illustrates another flow diagram for quality of service (QoS) for device assisted services (DAS) in accordance with some embodiments. In some embodiments, Radio Access Bearer (RAB) support is available, and the following process is performed in accordance with some embodiments. At 1002, the process begins. At 1004, the device service processor detects a QoS request or QoS need (e.g., a QoS API request, a QoS request or need/benefit of QoS session based on service usage monitoring, such as by application and/or another service usage measure/activity). At 1006, the service processor and/or the service processor in communication with the service controller determines if the service plan allows/supports the requested QoS. If not, then at 1008, a UI event is generated (e.g., notifying the device user that such QoS/QoS level/class is not available, and potentially offering a QoS/service plan upgrade/purchase for that QoS/QoS level/class). At 1010, the service processor communicates the QoS request to the service controller (e.g., using a secure service control link or secure communication channel, as similarly described herein) to request the QoS level/class. At 1012, the service controller determines whether network resources are available using various techniques as described herein. In some embodiments, network capacity is determined using various techniques, such as local device measurements; dedicated local device measurement reports; BTS reports; other network element reports; by assessing, for example, a combination of one or more of available bandwidth, traffic delay or latency, available QoS level, variability in available bandwidth, variability in latency, and/or variability in available QoS level; and/or other techniques as described herein. At 1014, the service controller responds to the QoS request (e.g., grants or denies the QoS request). In some embodiments, another UI event is generated if the QoS request is denied as similarly described herein. At 1016 (assuming the QoS request is granted), the device requests a QoS channel from the BTS. In some embodiments, the request includes a QoS request authorization code received from the service controller. In some embodiments, the service controller provides a notification of the QoS request approval for the communications

device to the BTS, so that the BTS can verify the approval of the QoS request. In some embodiments, the BTS confirms the device QoS channel request directly with the service controller. For example, various other techniques for verifying the QoS channel request can also be used as similarly described herein and as would be apparent to one of ordinary skill in the art. In some embodiments, the device service processor and/or service controller provides QoS related reports informing the BTS of how many QoS channels (e.g., RABs) to provision and how many best effort resources to provision based on device demand projections. At 1018 (assuming the QoS channel request is verified), the QoS session is initiated based on an allocated RAB or multi-RAB reservation received from the BTS (e.g., and/or other network elements as similarly described herein). At 1020, the process is completed.

[00194] FIG. 11 illustrates another flow diagram for quality of service (QoS) for device assisted services (DAS) in accordance with some embodiments. In some embodiments, RAB support is not available, and the following process is performed in accordance with some embodiments. At 1102, the process begins. At 1104, the device service processor detects a QoS request or QoS need (e.g., a QoS API request, a QoS request or need/benefit of QoS session based on service usage monitoring, such as by application, or other service usage measure/activity). At 1106, the service processor and/or the service processor in communication with the service controller determines if the service plan allows/supports the requested QoS. If not, then at 1108, a UI event is generated (e.g., notifying the device user that such QoS/QoS level/class is not available, and potentially offering a QoS/service plan upgrade/purchase for that QoS/QoS level/class). At 1110, the service processor communicates the QoS request to the service controller (e.g., using a secure service control link or secure communication channel, as similarly described herein) to request the QoS level/class. At 1112, the service controller determines whether network resources are available using various techniques as described herein. In some embodiments, network capacity is determined using various techniques, such as local device measurements, BTS reports, other network element reports, and/or other techniques as described herein. In some embodiments, the service controller throttles other devices on the link so that the requested QoS level can be achieved (e.g., as RAB support is not available). In some embodiments, the service controller time slots traffic from the device end in synchronization with a BTS clock or absolute clock to facilitate the requested QoS level and to achieve necessary network capacity to support/facilitate the requested QoS level (e.g., minimizing jitter/inter-packet delay variation)

based on current/forecasted network capacity on the link. At 1114, the service controller responds to the QoS request (e.g., grants or denies the QoS request). In some embodiments, another UI event is generated if the QoS request is denied as similarly described herein. At 1116 (assuming the QoS request is granted), the device initiates the QoS session. At 1118, the device service processor and/or the device service processor in secure communication with the service controller monitors and verifies the QoS session using various monitoring and verification techniques described herein (e.g., checks CDRs to determine if the QoS channel is properly implemented by the device). In some embodiments, a UI event is generated to notify the device user if there are potential problems with the QoS session implementation, to periodically inform the user of QoS charging, and/or other events/information related to QoS activities. At 1120, the process is completed.

[00195] FIG. 12 illustrates a device stack for providing various service usage measurement techniques 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 (e.g., for monitoring QoS related activities and/or for monitoring network capacity controlled services as described herein), a billing agent, and an access control integrity agent to assist in verifying the service usage measures, QoS related activities and functions, 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/detect 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 driver/agent 1690 (e.g., policy enforcement point driver/agent), 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.

[00196] 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.

[00197] 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).

[00198] 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 certain embodiments to differentiate the traffic or service activity taking place through one modem from that of one or more of the other modems. In some embodiments, measurement point VI, or another measurement point, is located over, within or below one or more of the individual modem drivers. The respective modem buses for each modem reside between example measurement points V and VI. In the next higher layer, a modem selection & control layer for multimode device based communication is provided. In some embodiments, this layer is controlled by a network decision policy that selects the most desirable network modem for some or all of the data traffic, and when the most desirable network is not available the policy reverts to the next most desirable network until a connection is established provided that one of the networks is available. In some embodiments, certain network traffic, such as verification, control, redundant or secure traffic, is routed to one of the networks even when some or all of the data traffic is routed to another network. This dual routing capability provides for a variety of enhanced security, enhanced reliability or enhanced manageability devices, services or applications. In the next higher layer, a modem firewall is provided. For example, the modem firewall provides for traditional firewall functions, but unlike traditional firewalls, in order to rely on the firewall for verifiable service usage control, such as access control and security protection from unwanted networking traffic or applications, the various service verification techniques and agents described herein are added to the firewall function to verify compliance with service policy and prevent/detect 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 and described herein. 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 (e.g., QoS IP queuing and routing layer and/or a network capacity controlled services 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 QoS IP queuing and routing and/or for network capacity controlled services 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.

[00199] As shown in FIG. 12, the application service interface layer (e.g., QoS application service interface layer and/or network capacity controlled services 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.

[00200] 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.

[00201] FIG. 13 illustrates another device stack for providing various service usage measurement techniques 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. 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 functions on the modem subsystem (e.g., and such an approach can be applied to one or more modems). For example, the service processor can be distributed as a standard

feature set contained in a modem chipset hardware of software package or modem module hardware or software package, and such a configuration can provide for easier adoption or development by device OEMs, a higher level of differentiation for the chipset or modem module manufacturer, higher levels of performance or service usage control implementation integrity or security, specification or interoperability standardization, and/or other benefits.

[00202] 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.

[00203] Additional Embodiments of DAS for Protecting Network Capacity

[00204] In some embodiments, DAS for protecting network capacity includes classifying a service activity as a network capacity controlled service and implementing a network capacity controlled services policy. In some embodiments, DAS for protecting network capacity includes device assisted/based techniques for classifying a service activity as a network capacity controlled service and/or implementing a network capacity controlled services policy. In some embodiments, DAS for protecting network capacity includes network assisted/based techniques (e.g., implemented on a network element/function, such as a service controller, a DPI gateway, a BTS/BTSC, etc., or a combination of network elements) for classifying a service activity as a network capacity controlled service and/or implementing a network capacity controlled services

policy. In some embodiments, DAS for protecting network capacity includes providing a network access API or an emulated or virtual network access API (e.g., such an API can provide network busy state information and/or other criteria/measures and/or provide a mechanism for allowing, denying, delaying, and/or otherwise controlling network access). In some embodiments, DAS for protecting network capacity includes implementing a service plan that includes a network capacity controlled services policy (e.g., for differential network access control and/or differential charging for network capacity controlled services, which can also be based on a network busy state and/or other criteria/measures).

[00205] In some embodiments, DAS for protecting network capacity techniques also provide improved user privacy and facilitate network neutrality requirements. In contrast, network based techniques (e.g., DPI based techniques) can give rise to user privacy and network neutrality concerns and problems as discussed above. In some embodiments, DAS for protecting network capacity techniques include allowing a user to specify (e.g., permit or not permit) whether the network is aware of the user's Internet behavior (e.g., using UI input). In some embodiments, DAS for protecting network capacity techniques include allowing a user to select how they want their traffic usage and service plan costs to be managed.

[00206] FIG. 14 illustrates a flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments. At 1402, the process begins. At 1404, monitoring a network service usage activity of a device in network communication (e.g., wireless network communication) is performed. At 1406, whether the monitored network service usage activity is a network capacity controlled service is determined. At 1408 (the monitored network service usage activity was determined not to be a network capacity controlled service), the network service usage activity is not classified for differential network access control. At 1410, (the monitored network service usage activity was determined to be a network capacity controlled service), the network service usage activity is classified (e.g., into one or more network capacity controlled services) for differential network access control for protecting network capacity. In some embodiments, classifying the network service usage activity includes classifying the network service usage activity into one or more of a plurality of classification categories for differential network access control for protecting network capacity (e.g., one or more network capacity controlled service classifications and/or a priority state classification, such as a background services classification and/or a background priority state classification). At

1412, associating the network service usage activity with a network capacity controlled services control policy based on a classification of the network service usage activity to facilitate differential network access control for protecting network capacity is performed. At 1414, implementing differential network access control for protecting network capacity by implementing different traffic controls for all or some of the network service usage activities (e.g., based on a network busy state or another criteria/measure) is performed. At 1416, the process is completed.

[00207] FIG. 15 illustrates another flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments. At 1502, the process begins. At 1504, monitoring network service usage activities of a device in network communication is performed. At 1506, monitored network service usage activity of the device is reported (e.g., to a network element/function). At 1508, a statistical analysis of a reported network service usage activities across a plurality of devices is performed (e.g., by a network element/function). At 1510, the device receives a network service usage activity classification list (e.g., a network capacity controlled services list, which can be generated, for example, based on the monitored network service usage activities and the statistical analysis as well as other criteria/measures, including, for example, a service plan and/or a network busy state) from the network element. At 1512, implementing differential network access control based on the network service usage activity classification list for protecting network capacity is performed. At 1514, the process is completed. In some embodiments, DAS for protecting network capacity further includes associating the network service usage activity with a network service usage control policy (e.g., a network capacity controlled services policy) based on a classification of the network service usage activity to facilitate differential network access control for protecting network capacity. In some embodiments, DAS for protecting network capacity further includes differentially controlling the network service usage activity (e.g., network capacity controlled service) based on the service usage activity classification list.

[00208] FIG. 16 illustrates another flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments. At 1622, the process begins. At 1624, a first report of network service usage activity of a first device is received (e.g., at a network element/function) from the first device. At 1626, a second report of network service usage activity of a second device (e.g., at a network element/function) from the second device is

received. At 1628, a statistical analysis of a plurality of reported service usage activities across a plurality of devices, including the first device and the second device, is performed (e.g., by a network element/function). At 1630, a network service usage activity classification list (e.g., a network capacity controlled services classification list) is sent to the first device (e.g., from a network element/function) for classifying network service usage activities (e.g., network capacity controlled services) based on the network service usage activity classification list for differential network access control for protecting network capacity. At 1632, a network service usage activity classification list is sent to the second device (e.g., from a network element/function) for classifying network service usage activities based on the network service usage activity classification list for differential network access control for protecting network capacity. At 1634, the process is completed. In some embodiments, DAS for protecting network capacity further includes associating the network service usage activity with a service usage control policy (e.g., a network capacity controlled services policy) based on a classification of the network service usage activity to facilitate differential network access control for protecting network capacity. In some embodiments, DAS for protecting network capacity further includes differentially controlling the network service usage activity (e.g., network capacity controlled service) based on the service usage activity classification list (e.g., network capacity controlled services classification list). In some embodiments, classifying network service usage activities is based on which network to which the device is connected. In some embodiments, the network service usage control policy is based on which network to which the device is connected.

[00209] FIG. 17 illustrates another flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments. At 1702, the process begins. At 1704, monitoring a network service usage activity of a plurality of devices in network communication using network based techniques is performed. At 1706, a statistical analysis of monitored network service usage activities across the plurality of devices is performed. At 1708, a network service usage activity classification list (e.g., a network capacity controlled services classification list) is sent to each of the plurality of devices for classifying network service usage activities (e.g., network capacity controlled services) based on the service usage activity classification list for differential network access control for protecting network capacity. At 1710, the process is completed.

[00210] FIG. 18 illustrates another flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments. At 1802, the process begins. At 1804, monitoring network service usage activities of a device in network communication is performed. At 1806, associating a network service usage activity (e.g., a network capacity controlled service) with a service usage control policy (e.g., a network capacity controlled services policy) based on a classification of the network service usage activity (e.g., a network capacity controlled services classification list) for differential network access control for protecting network capacity is performed. At 1808, a user notification based on the service usage control policy is generated. At 1810, the process is completed.

[00211] In some embodiments, the service usage control policy includes a service usage notification policy. In some embodiments, the user notification includes one or more of the following: a notification that the application to be downloaded and/or launched is a network capacity controlled service; a list of one or more service activities (e.g., applications, OS/other software functions/utilities, and/or other functions/utilities as described herein) that have a network capacity controlled services classification; type of service policy in effect for one or more network capacity controlled services; notification that a service activity belongs to a network capacity controlled services class; notification that a service activity that is classified as network capacity controlled service can have the service class changed; notification that if the service class is changed for a service activity the service charges will change; notification that one or more networks are available (e.g., one or more alternative networks and/or network busy state information and/or charging information and/or incentives associated with such networks), a service plan upgrade/downgrade offer/option; and an offer for a service plan that rewards a user that responds to the notification a service plan is lower cost/discounted for responding to notification to use or not to use service activity based on usage level warning notification. In some embodiments, the user notification includes a user preference selection, including one or more of the following: a provision to associate an access policy control with the application (e.g., allow/block, notify of usage, notify of usage at a given threshold, traffic control settings, allow during certain times, allow when network not busy, and/or other policy controls as described herein), an over-ride option for selecting the service usage control policy; a modify option to select the service usage control policy; a select option to select a new service plan (e.g., an option to review and select alternative/new service plan upgrade/downgrade options), and an

acknowledgement request (e.g., to confirm/acknowledge receipt of the notification, in which the acknowledgement can be transmitted to a network element/function and/or stored locally for later reference/transmission).

[00212] In some embodiments, before a given device application, process, function, OS service or other service activity is allowed to start, the intention to start is intercepted by a launch manager, the background service policy set or the network protection service policy set for the service activity is retrieved, and any necessary user notification or service launch control policies are implemented prior to allowing the service activity to launch. In such embodiments, a launch intercept manager may be used to implement this functionality. In some embodiments, this launch intercept manager is provided with a list identifying the service activities (e.g., application identifiers, OS function identifiers, aggregate service activity identifiers, and/or component service activity identifiers) that have a launch control policy in effect. In some embodiments, the list of launch control policies includes blocking or delaying launch of the one or more service activities. In some embodiments, the launch control policy includes a user notification before, during or after the service activity is launched. In some embodiments, the user is informed that a service activity that has a background service control policy in effect or a network protection service control policy in effect is attempting to launch, is about to launch or has launched. In a further set of embodiments, the launch is held up until the user is notified and is allowed to decide if they would like to launch the service activity. In some embodiments, the user notification includes a message that the service activity attempting to launch consumes a large amount of service usage and asks the user if they would like to continue (e.g., "This application consumes a large amount of data, would you like to continue?", "This application consumes data even when you are not using it, would you like to continue?" "This application consumes data while you are roaming which adds cost to your usage bill, would you like to continue?", etc). In some embodiments, the decision on whether or not to launch a service activity is pre-programmed into the list identifying the service activities (e.g., application identifiers, OS function identifiers, aggregate service activity identifiers, and/or component service activity identifiers) that have a launch control policy in effect. In some embodiments a portion of the list is pre-programmed by the user in accordance with user preference for controlling usage of service activities. In some embodiments, a portion of the list is pre-programmed by a network element (e.g., a service controller) in accordance with network

background service or network protection service policies specified by a service policy design management system operated by a service provider as described herein. In some embodiments, the policy implementation defined by the list identifying the service activities (e.g., application identifiers, OS function identifiers, aggregate service activity identifiers, and/or component service activity identifiers) that have a launch control policy in effect is verified to ensure that the user or malicious software has not defeated the policy enforcement specified in the list. In some embodiments the list identifying the service activities that have a launch control policy in effect includes launch policies that are a function of one or more of: background service state, network busy state (or performance state or QoS state), type of network the device is connected to, home or roaming connection, time of day or day of week.

[00213] In some embodiments, the various design techniques described herein that allow for intercepting a service activity intention to launch, and applying a background service policy set or a network protection service policy set can be designed into the OS itself. For example, the intercept and policy implementation functions can be designed into the activity manager, broadcast intent manger, media service manager, service manager, or other application or service activity management function in the Android OS. One of ordinary skill in the art will recognize that similarly, the various design techniques described herein that allow for intercepting a service activity intention to launch, and applying a background service policy set or a network protection service policy set can be designed into application launch management functions in the iPhone OS, windows mobile OS, windows PC OS, Blackberry OS, Palm OS, and other OS designs.

[00214] In some embodiments, the pre-launch user notification information indicates one or more of: typical service usage or cost, or projected service usage or cost for the service activity attempting to launch. In some embodiments, the user sets limitations on access for one or more service activities and once this limit is hit then when the service activities with exceeded limits attempt to launch the user is notified. In some embodiments, the user chooses from a set of service restrictions rather than simply blocking or allowing service activity launch, with example service restrictions including but not limited to: a pre-configured set of restriction policies to chose from (e.g., full access, limited access, highly restricted access or block access), block, throttle, delay, aggregate and hold, limit amount of usage per unit time, cap usage, set limit for additional notification, specify type of network, specify busy state (performance, QoS) or background state, or choose from pre-configured settings options.

[00215] In some embodiments, the user notification occurs after the user attempts to download or load an application onto the device (e.g., an application downloaded from the web or an online application store for a smart phone or other wireless/network computing device, such as an Apple iPhone or iPad, or Google Android/Chrome based device). In some embodiments, the user notification occurs after the user attempts to run the service activity or to initiate usage of a cloud based service/application (e.g., Google or Microsoft cloud service based apps). In some embodiments, the user notification occurs after one or more of the following: the service usage activity hits a usage threshold event, the service usage activity attempts a network service usage that satisfies a pre-condition, an update to a network capacity protection service activity classification list or policy set, and a network message is sent to the device triggering the notification. In some embodiments, the user notification provides information on the service usage activity that is possible, typical, or likely for the service usage activity. In some embodiments, the user notification includes a user option for obtaining more information about the service usage of the service activity (e.g., a message that the service usage activity may result in a high service usage and/or that the service usage activity may or will result in a high service usage as compared in some way to a limit of the current service plan) to make informed user preference settings.

[00216] In some embodiments, a user notification includes displaying (e.g., and as applicable, allowing users to provide UI input) one or more of the following: current and/or past/historical/logged network service usage activity list, current and/or past/historical/logged network capacity controlled service usage activities, current activity policy settings, current or available networks, service plan options (e.g., for how to treat one or more network capacity controlled service traffic types), selection option(s) to assign a network capacity controlled service activity into a different priority traffic control and/or charging buckets, network service usage by activity (e.g., network capacity controlled services and other services), network busy state (e.g., and with resulting policies in force), service activity policy setting vs. busy state and time/day/week, network service activity priority, network service activity usage statistics (e.g., vs. network busy state and/or network service usage control policy state).

[00217] In some embodiments, a UI notification is displayed when user attempts a network capacity controlled service activity during a network busy state (e.g., that modifies a network capacity controlled services policy). In some embodiments, the UI notification includes

information on service plan choice and a network capacity controlled services policy over-ride option (e.g., one time, time window, usage amount, permanent by activity, and/or all), charging information based on a user selection, and/or service plan upgrade information and options.

[00218] In some embodiments, a UI notification is displayed for user input for preferences/configurations for multiple networks (e.g., WiFi, 4G, 3G, and/or other wired or wireless access networks) including charging policy. In some embodiments, a UI notification is displayed when a specified network traffic service usage activity (e.g., based on network capacity controlled services classification, QoS classification, priority classification, time based criteria, network capacity, service plan, charging criteria, and/or other criteria/measures) is being attempted or is occurring and providing options (e.g., allow, block, delay, throttle, and/or other options).

[00219] In some embodiments, a UI fuel gauge is displayed (e.g., to depict current and/or historical network service usage, for example, relative to a service plan for the device, by network, relative to network busy state, time based criteria, and/or other criteria/measures). In some embodiments, a user notification includes a communication sent to the user (e.g., an email, SMS or other text message, voice message/call, and/or other electronic form of communication). In some embodiments, the communication sent to the user includes network service usage information, network capacity controlled service usage related information, and/or an instruction to log into a web page or send a communication for more information (e.g., regarding an information update and/or alert or warning message, such as related to network service usage and/or charging for network service usage).

[00220] In some embodiments, a notification (e.g., a user or network service cloud notification) is generated based on an aggregate service activity reports usage (e.g., allows network provider to generate user notifications and/or to notify application provider/service activity provider). In some embodiments, a notification (e.g., a user or network service cloud notification) is generated based on a publishing of an updated/new network capacity controlled services list based on an aggregate monitored activity (e.g., based on a service plan, velocity, sockets opening frequency/rate (e.g., messaging layer behavior), total data usage, peak busy time usage to formulate or update black list for monitoring, notifying, and/or controlling, which can be applied to one, multiple, group, or all devices). In some embodiments, a notification (e.g., a user or

network service cloud notification) is generated based on data usage trends for particular device relative to an associated service plan and/or other comparable devices or data usage thresholds/statistical based data usage measures.

[00221] In some embodiments an application is actually composed of several component applications, processes or functions. Examples of this include but are not limited to: the components of a Java application JAR file; applications that use OS functions; applications that use a proxy service function; applications, functions or processes that coordinate with one another to implement a composite process, function or application; and OS process functions that support an application or overall OS function. In such embodiments it is important to be able to categorize all applications, functions and processes on a device that contribute to the service usage of a service activity so that the service activity can be monitored for service usage, have the service usage accounted for, implement the appropriate user notification when one or more service activity components attempts to start or use the network, implement the appropriate user notification when one or more service activity components reaches a pre-determined service usage level that requires user notification, and implement the appropriate background service or network protection service usage controls as specified herein ((including but not limited to for example: block network access, restrict network access, throttle network access, delay network access, aggregate and hold network access, select for time of day network access restrictions, select network type restrictions, select roaming network access restrictions, select service usage restrictions such as a usage limit, select service cost restrictions such as a cost limit or otherwise place on another form of background service status or network usage restriction as described herein). In the case of service activity components that belong exclusively to one aggregate service activity (e.g., an application, application JAR file or OS function), this may be accomplished by including each of the component service activities on a list that identifies the service activity components that belong to the aggregate service activity, and then monitoring, possibly controlling and providing user notifications based on the aggregate or component behavior of each service activity in accordance with the policies specified for the aggregate service activity. For example, it is necessary to group all application launch behavior and/or network access behavior under the monitoring, launch, notification, accounting and background service controls or network protection service controls (or other background or network protection service policies as specified herein) in accordance with the background service or

network protection service policies for the aggregate application that the JAR file supports. As another example, if an OS network synch or update function utilizes various software components or processes to implement the network synch or update function, then each of the software components or process must be monitored and aggregated under the background service policies or network protection service policies for the aggregate OS synch or update function.

[00222] In some embodiments, this ability to group usage for a related set of service activity components dedicated to an aggregate service activity as described herein is used to improve usage reporting of service activities to a service controller for the purpose of statistically identifying service activities that are candidates for background service policy controls or network protections service policy controls.

[00223] In some cases, multiple applications, processes, functions, OS services or other service activities can utilize a common set of component software applications, processes, functions or OS services. In such cases, in order to implement background service policies and/or network protection service policies for service activity monitoring and accounting, service activity launch control, user notification, or network access control as described herein, it is necessary to associate the specific network access data or information flows to and from the common component software applications, processes or functions that belong to the specific initiating application, process, function or other service activity that is to be managed according to a background service or network protection service policy set. In what follows, a specific set of examples is provided on how to map common component service activity for a set of common OS functions referred to as proxy service functions to a specific application, process, function, OS service or other service activity for the purpose of implementing a background service policy set or a network protection service policy set as described herein. Once these examples are reviewed, it will be obvious to one of ordinary skill in the art how to apply similar mapping of service activity for a common set of components to a service activity that is to be managed in accordance with a background service policy set or a network protection service policy set as described herein.

[00224] In some embodiments, this ability to group usage for a common set of service activity components as described herein is used to improve usage reporting of service activities to a

service controller for the purpose of statistically identifying service activities that are candidates for background service policy controls or network protections service policy controls.

[00225] In some embodiments, a proxy network service manager refers to an intermediary data flow function in a device operating system that sits on a data path between a device application and a device networking stack interface to provide a level of network service abstraction from the network stack interface, a higher level service function above the network stack interface, enhanced or special traffic processing functions, media service transfer management, file download service, HTTP proxy service functions, QoS differentiation, or other similar or related higher level traffic processing. Example Proxy Service Managers include the following: media service manager (e.g., android media service library function), email service manager, DNS function, software download service manager, media download manager (e.g., audio player, streaming media player, movie downloader, media service OS function, etc.), data download service manager, Android "media" library function, Android.net library function, Jave.net library function, Apache library function, other similar software/library functions or services in other device operating systems, SMTP/IMAP/POP proxy, HTTP proxy, IM proxy, VPN service manager, SSL proxy, etc. Herein these alternative network access data flows that are initiated by an application are termed application proxy service flows. In such embodiments an app can sometimes simply request a network access service activity from an OS component such as a proxy service component rather than directly accessing the network. In such embodiments, in order to implement background service controls or user notification of application service usage, it is necessary to monitor the application proxy service flows, classify them as being initiated by or belonging to a particular application or service activity, and implement the proper background service classifications, user notifications, application process launch intercept, background service accounting, and background service usage restrictions as described herein in accordance with the policies intended for the initiating application or service activity. This is accomplished by inserting service usage monitors that allow a mapping of (i) the initiating application identifier (e.g., app name, app fingerprint, application identification tag, application process number, application credential, or other secure or non-secure application or process identifier) to (ii) the request to the proxy service and subsequently to (iii) the network service flows between the proxy service and the network elements that service the information communications. Once this mapping is accomplished, the service usage flows of the proxy service can then be accounted

back to the initiating application, device software process or other service activity, the proper policies can then be applied to each service usage flow for user notification, service activity launch control, service activity background accounting (including variable charge rating dependent on background service state and/or sponsored service charging), service activity background service controls or network usage restrictions as described herein (including but not limited to for example: block network access, restrict network access, throttle network access, delay network access, aggregate and hold network access, select for time of day network access restrictions, select network type restrictions, select roaming network access restrictions, select service usage restrictions such as a usage limit, select service cost restrictions such as a cost limit or otherwise place on another form of background service status or network usage restriction as described herein).

[00226] In some embodiments, this ability to track service usage for an service activity through a proxy service as described herein is used to improve usage reporting of service activities to a service controller for the purpose of statistically identifying service activities that are candidates for background service policy controls or network protections service policy controls.

[00227] In some embodiments, the various design techniques described herein that allow for monitoring, accounting for and/or implementing service policy for component service activities that belong to an aggregate service activity can be designed into the OS itself. For example, in certain current mobile OS implementations (e.g., Android, iPhone, Blackberry, etc) there are some applications available in the market that allow a user to get an estimate for how much data a certain subset of applications are consuming on a wireless service provider network, but it is not possible for the user or application to get an indication of the service usage for certain OS functions, whereas the embodiments disclosed herein will allow for this. As another example, in certain current mobile OS implementations it is not possible to associate proxy service usage (e.g., media download and media streaming proxy library software functions) with the specific applications that use the proxy service, so while the user can be informed of generic common OS functions or proxy services (e.g., in the case of Android: "media service," "media," "gallery," "google service framework" and other generic common OS software library functions or proxy services), there is no way for the user to determine what applications widgets or other service activities are actually generating this common service function usage, whereas the invention described herein permits the user full visibility on such usage monitoring examples.

Furthermore, if the OS is retrofitted with the intercept and policy implementation functions can be designed into the activity manager, broadcast intent manger, media service manager, service manager, or other application or service activity management function in the Android OS. One or ordinary skill in the art will recognize that similarly, the various design techniques described herein that allow for intercepting a service activity intention to launch, and applying a background service policy set or a network protection service policy set can be designed into application launch management functions in the iPhone OS, Windows mobile OS, Windows PC OS, Blackberry OS, Palm OS, and other OS designs.

[00228] FIG. 19 illustrates another flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments. At 1902, the process begins. At 1904, determining a network busy state of one or more networks is performed. In some embodiments, the one or more networks are selected from an access network, a wired network, and a wireless network. At 1906, classifying a network service usage activity (e.g., a network capacity controlled service) of a device based on the network busy state determination is performed to facilitate differential network access control for protecting network capacity of the one or more networks. In some embodiments, the network busy state is based on one or more of the following: network performance, network congestion, network availability, network resource availability, network capacity, or any other network service usage measure, and one or more time windows (e.g., time based criteria). In some embodiments, protecting network capacity of the one or more networks includes protecting network capacity of a last edge segment of a wireless network (e.g., RAN, BTS, BTSC, and/or other network elements). In some embodiments, the determining and classifying are performed using device assisted/based techniques. In some embodiments, the determining and classifying are performed using network assisted/based techniques (e.g., implemented on a network element/function, such as a service controller, a DPI gateway, a BTS/BTSC, etc., or a combination of network elements). In some embodiments, the determining and classifying are performed using a combination of device assisted/based techniques and network assisted/based techniques. At 1908, implementing differential traffic controls is performed based on the service usage activity classification for protecting network capacity. At 1910, the process is completed. In some embodiments, a network busy state is determined based on one or more of the following: a time of day, a network reported busy state, and/or a device (e.g., near-end and/or far-end) determined/reported

network busy state. In some embodiments, a network busy state is determined using one or more of the following: a network probe, a device query, a network probe report (e.g., including a BTS and/or BTSC), a network probe analysis, a device analysis based on performance of native traffic without probe such as TCP timeout, UDP retransmissions, a multiple network test, a device monitored network congestion based on network service usage activity (e.g., application based network access performance data) performed for a network to which the device is connected and/or one or more alternative networks. In some embodiments, a network congestion state is associated with a network busy state (e.g., a network busy state setting/level). For example, a network congestion level of 40% of network usage can be associated with a network busy state setting of 4, a network congestion level of 80% of network usage can be associated with a network busy state setting of 8, and so forth.

[00229] FIG. 20 illustrates another flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments. At 2002, the process begins. At 2004, monitoring a network service usage activity of a device in network communication is performed. At 2006, classifying the network service usage activity (e.g., based on a classification of the network service usage activity for protecting network capacity, for example, as a network capacity controlled service) for protecting network capacity is performed. At 2008, accounting for network capacity controlled services (e.g., accounting for the network service usage activity based on a classification of the network service usage activity for protecting network capacity) is performed. At 2010, charging for network capacity controlled services is performed. At 2012, the process is completed. In some embodiments, DAS for protecting network capacity further includes classifying the network service usage activity as a network capacity controlled service. In some embodiments, DAS for protecting network capacity includes differentially accounting and/or differentially charging for network capacity controlled services and foreground services. In some embodiments, the network service usage control policy includes policies for differentially controlling, accounting, and/or charging for network capacity controlled services (e.g., based on a network busy state, a time based criteria, a service plan, network to which the device or network service usage activity is gaining access from, and/or other criteria/measures). In some embodiments, accounting for network capacity controlled services includes differentially collecting service usage for one or more network capacity controlled service classes in which the accounting is modified/varies (e.g.,

dynamically) based on one or more of the following: network busy state (e.g., modify/credit accounting during network congestion not satisfying the user preference), network service activity, access network (e.g., the network to which the device/service activity is currently connected), user preference selection, time based criteria (e.g., current time of day/day of week/month), associated service plan, option to time window. In some embodiments, charging for network capacity controlled services includes mapping an accounting to a charging report. In some embodiments, charging for network capacity controlled services includes sending the charging report to a network element (e.g., a service controller, a service cloud, a billing interface/server, and/or another network element/function). In some embodiments, charging for network capacity controlled services includes mediating or arbitrating CDRs/IPDRs for network capacity controlled service(s) vs. other network service usage activities or bulk network service usage activities. In some embodiments, charging for network capacity controlled services includes converting a charging report to a billing record or billing action. In some embodiments, charging for network capacity controlled services includes generating a user notification of network capacity controlled service charges upon request or based a criteria/measure (e.g., a threshold charging level and/or a threshold network service usage level). In some embodiments, charging for network capacity controlled services includes charge by application based on a charging policy (e.g., bill by application according to billing policy rules, such as for billing to a user or to a sponsored service provider, carrier, and/or other entity).

[00230] FIG. 21 illustrates another flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments. In some embodiments, DAS for protecting network capacity includes providing a device service access API that provides an interface for applications, OS functions, and/or other service usage activities to a network access connection (e.g., or stack) for providing differential network access for protecting network capacity. In some embodiments, the differential network access is determined by one or more of the following: a service priority of the service usage activity and a network busy state. At 2102, the process begins. At 2104, a device service access API request is received. At 2106, the device service access API request is responded to. In some embodiments, the differential network access (e.g., for network capacity controlled services and/or based on network busy state and/or other criteria/measures) is implemented by one or more of the following: providing network busy state information to the service usage activity, receiving

network busy state information, receiving network capacity demands for the service usage activity, receiving a scheduled time/time slot demand from the service usage activity, receiving and/or providing network location and/or physical location information (e.g., base station, communication channel, cell sector, roaming or non-roaming network to which the device is connected, and/or GPS or other physical location data), providing information to the service usage activity informing it when it is allowed to access the network, providing information to the service usage activity informing it what traffic controls must be applied/implemented, providing information to the service usage activity informing it when the network is available to it for access, and providing information to the service usage activity of its scheduled access time/time slot (e.g., based on one or more of the following: priority, network busy state, and time of day) (e.g., with a specified performance level or service level, such as data transfer size, speed, network capacity controlled service priority level, QoS level, data transfer type, scheduling time(s), and/or network connection parameters), and instructing the device and/or service usage activity to transition to a different state (e.g., power save state, sleep state dormant, idle, wait state, and/or an awake state). At 2108, differential network access is implemented. At 2110, the process is completed. In some embodiments, the device service access API is a programmatic interface, a virtual interface, and/or an emulated interface that provides instructions for differential access to a network to protect network capacity, as described herein.

[00231] In some embodiments, the API is served or located on the device, on a network element (e.g., using a secure communication between the device and the network element for the API communication, such as HTTPS, TLS, SSL, an encrypted data connection or SS7 control channel, and/or other well known secure communication techniques), and/or both/partly in both. In some embodiments, a network based API is an API that facilitates an API or other interface communication (e.g., secure communication as discussed above) between an application executing on the device and a network element and/or service cloud for protecting network capacity. For example, a network API can provide an interface for an application to communicate with a service cloud (e.g., network server) for obtaining network access control information (e.g., network busy state, multiple network information based on available networks and/or network busy state information of available networks, network capacity controlled service priorities and availability, scheduled time/time slots for network access based on network busy state, service plan, network capacity controlled service, and/or other criteria/measures). As

another example, a network API can facilitate an application provider, central network/service provider, and/or a third party with access to communicate with the application to provide and/or request information (e.g., physical location of the application, network location of the application, network service usage information for the application, network busy state information provided to the application, and/or other criteria/measures). As yet another example, a network API can facilitate a broadcast to one or more applications, OS functions, and/or devices (e.g., partitioned based on geography, network, application, OS function, and/or any other criteria/measure) with network capacity related information (e.g., network busy state, availability based on network capacity controlled service classification and/or priority level, scheduled time/time slots for certain network capacity controlled service classification and/or priority level, emergency/high priority software/antimalware/vulnerability update and scheduled time/time slots for such software updates, and/or other criteria/measures). In some embodiments, the network access API for protecting network capacity is an open API or standard/required API (e.g., required or standardized for applications for a certain network service provider, such as to be provided via the Verizon application store or the Apple AppStore) published for application and OS developers so that the applications and OS functions are designed to understand and implement the network access API for protecting network capacity. For example, a certification program can be established to provide application and OS developers with test specifications, working implementations, and/or criteria to make sure the network access API is properly implemented and is functioning in accordance with the specified requirements. In some embodiments, the network access API is an interface for communication with a service controller (e.g., service controller 122) or another network element/function (e.g., a service usage API for communication with a service usage server or billing interface/server or another network element/function that facilitates a secure communication for sending/receiving or otherwise communicating network access related information for protecting network capacity). In some embodiments, the network API provides for sponsored billing (e.g., reverse billing) of all, classified, and/or a subset of network service usage charges to a sponsored partner associated with the network service usage activity (e.g., application) that accesses the network API. In some embodiments, the network API provides for a sponsored service in which the network service usage activity (e.g., application) that accesses the network API provides a sponsored service partner credential to the network API, the credential is used as a billing

mechanism to charge the sponsored partner, the user account is mediated to remove the sponsored partner charge, and the network API provides access service and/or information service (e.g., location information, local information, content information, network information, and/or any other information).

[00232] FIG. 22 illustrates another flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments. At 2202, the process begins. At 2204, network service usage activities of a device are monitored (e.g., using a verified/verifiable service processor). At 2206, a network busy state (e.g., a measure of network capacity, availability, and/or performance) is determined based on the monitored network service usage activities (e.g., using various techniques as described herein). In some embodiments, a service processor on the device is used to determine (e.g., measure and/or characterize) a network busy state experienced by the device (e.g., which can be used to determine the network access control policy for one or more network capacity controlled services). At 2208, a network busy state report is sent to a network element/function (e.g., a service controller and/or another network element/function as described herein). At 2210, the process is completed. In some embodiments, the service processor is verified using various techniques described herein. In some embodiments, the network busy state report includes one or more of the following: data rate, latency, jitter, bit error rate, packet error rate, number of access attempts, number of access successes, number of access failures, QoS level availability, QoS level performance, and variability in any of the preceding parameters. In some embodiments, the network busy state report includes one or more of the following: base station ID, cell sector ID, CDMA ID, FDMA channel ID, TDMA channel ID, GPS location, and/or physical location to identify the edge network element that is associated with the network busy state report to a network element. In some embodiments, the monitoring of network service usage activities includes measuring the network performance for traffic the device is transmitting/receiving and/or generating network performance testing traffic. In some embodiments, the network busy state is collected (e.g., and/or used to assist, supplement, and/or verify device based network busy state measures) by one or more network elements that can measure and/or report network busy state (e.g., BTS, BTSC, base station monitor, and/or airwave monitor). For example, airwave monitors and/or base station monitors can be provided to facilitate a reliable characterization of network busy state in a coverage area of one or more base stations and/or base station sectors, such as affixed

mobile terminals (e.g., trusted terminals that can include additional network busy state monitoring and/or reporting functionality) installed (e.g., temporarily or permanently) in the coverage area of one or more base stations and/or base station sectors (e.g., in which a sector is the combination of a directional antenna and a frequency channel) so that the affixed mobile terminals perform network busy state monitoring and reporting to the service controller, the local base station, and/or other network element(s)/function(s) as similarly described herein. In some embodiments, the permanently affixed mobile terminals provide network monitors for reporting, for example, network busy state, to a central network element, such as the service controller, which can, for example, aggregate such network busy state information to determine network busy state for one or more network coverage areas. In some embodiments, the permanently affixed mobile terminals are always present in these locations where installed and always on (e.g., performing network monitoring), and can be trusted (e.g., the permanently affixed mobile terminals can be loaded with various hardware and/or software credentials). For example, using the permanently affixed mobile terminals, a reliable characterization of network busy state can be provided, which can then be reported to a central network element and aggregated for performing various network busy state related techniques as described herein with respect to various embodiments. In some embodiments, the network element/function uses the network busy state report (e.g., and other network busy state reports from other devices connected to the same network edge element) to determine the network busy state for a network edge element connected to the device. In some embodiments, network element/function sends a busy state report for the network edge element to the device (e.g., and to other devices connected to the same network edge element), which the device can then use to implement differential network access control policies (e.g., for network capacity controlled services) based on the network busy state. In some embodiments, a network busy state is provided by a network element (e.g., service controller or service cloud) and broadcast to the device (e.g., securely communicated to the service processor).

[00233] FIG. 23 illustrates a network capacity controlled services priority level chart for device assisted services (DAS) for protecting network capacity in accordance with some embodiments. In some embodiments, various applications, OS functions, and/or other utilities/tools installed/loaded onto and/or launched/executing/active on a communications device (e.g., device 100) are classified as network capacity controlled services for protecting network capacity. In

some embodiments, one or more of the network capacity controlled services are assigned or classified with network capacity controlled service levels or priority levels for protecting network capacity. In some embodiments, one or more of the network capacity controlled services are dynamically assigned or classified with network capacity controlled service levels or priority levels based on one or more criteria/measures (e.g., dynamic criteria/measures), such as network busy state, current access network, time based criteria, an associated service plan, and/or other criteria/measures. In some embodiments, a higher priority level means that the application or utility/function is granted higher relative priority for network access (e.g., a priority level 10 can provide for guaranteed network access and a priority level 0 can provide a blocked network access, while priority levels between 1 through 9 can provide relatively increasing prioritized network access potentially relative to allocated network access and other services requesting network access).

[00234] As shown in FIG. 23, the network capacity controlled services are dynamically assigned or classified with network capacity controlled service levels or priority levels based on the network busy state of the current access network. For example, an email application, Microsoft Outlook, is assigned different priority levels for protecting network capacity based on the network busy state, as shown: a priority level 6 for a network busy state (NBS) level of 10% (e.g., up to about 10% of the network capacity is being utilized based on current or recently/last measured/detected/determined network capacity/resources usage using various techniques as described herein), a priority level 5 for a network busy state (NBS) level of 25%, a priority level 4 for a network busy state (NBS) level of 50%, a priority level 3 for a network busy state (NBS) level of 75%, and a priority level 2 for a network busy state (NBS) level of 90%. As also shown, an antivirus (AV) software update application/utility/function is assigned different priority levels for protecting network capacity based on the network busy state: a priority level 9 for a network busy state (NBS) level of 10%, a priority level 7 for a network busy state (NBS) level of 25%, a priority level 5 for a network busy state (NBS) level of 50%, a priority level 3 for a network busy state (NBS) level of 75%, and a priority level 1 for a network busy state (NBS) level of 90%. Various other applications and utilities/functions are shown with various priority level assignments/classifications based on the network busy state levels shown in the network capacity controlled services priority level chart of FIG. 23. As will be apparent to one of ordinary skill in the art, various assignments and/or techniques for dynamically assigning priority levels for

network access based on network busy state levels can be applied for protecting network capacity (e.g., based on user preferences, service plans, access networks, a power state of device, a device usage state, time based criteria, and various other factors such as higher priority for urgent software and/or security updates, such as a high priority security or vulnerability software patch or update, and/or urgent or high priority emails or other communications, such as a 911 VOIP call).

[00235] Referring again to FIGS. 1 through 3, DAS for protecting network capacity is implemented using a service processor (e.g., a service processor 115) of the device (e.g., a device 100) using various DAS techniques as described herein to facilitate differential network service access control (e.g., for network capacity controlled services) to assist in protecting network capacity in accordance with some embodiments. In some embodiments, the service processor and/or one or more agents of the service processor is/are verified using one or more of the following verification techniques (e.g., and/or to specifically verify monitoring the network service usage activity, classifying one or more service activities into one or more network capacity controlled service classes, associating the one or more network capacity controlled service classes with one or more differential service activity policies, and/or determining a network busy state): compare a network based service usage measure with a service policy and/or service plan associated with the device, compare a device assisted service usage measure with the service policy and/or service plan associated with the device, compare the network based service usage measure to the device assisted service usage measure, compare a first device assisted service usage measure to a second device assisted service usage measure, verify presence of the service processor and/or one or more agents of the service processor, verify configuration of the service processor, verify service usage activities are reported properly (e.g., using test service usages to generate service usage events/reports for analysis and confirmation), verify billing events are reported properly, compare the network based service usage measure with reported device billing data, verify reporting of a test billing event, verify reporting of the communications device reports billing events from a transaction server, verify presence of an activation tracking system, verify device configuration or operation, verify device standing or service plan standing, verify proper operation of the service processor, verify service processor heartbeat response reports, verify monitoring of a test service event, download a new service processor (e.g., and/or one or more agents or new configuration settings of the service processor)

and perform integrity checks, verify a service processor code configuration with agent self-diagnosis checks, verify that the communications device uses the first service only after being authorized, verify user standing, verify a network busy state (e.g., compare and/or statistically process network busy state measures from more than one device in which the network busy state monitoring apparatus, for example, is located in a secure execution environment on the device), verify various differential network access control implementations (e.g., network capacity controlled services are properly monitored/determined/detected, controlled, accounted for, and/or charged for), verify various QoS implementations (e.g., as discussed above), and verify an agent communications log. Various other verification techniques are described herein and similar and other verification techniques for providing DAS for protecting network capacity using device based implementations (e.g., service processors and/or other device based agents or software/hardware techniques) will now be apparent to one of ordinary skill in the art in view of the various embodiments described herein.

[00236] In some embodiments, the service processor is secured using various hardware and software techniques described herein, including, for example, implementing all and/or portions of the service processor in a secure virtual machine, protected execution environment, secure storage (e.g., secure memory), secure modem, and/or other secure implementation techniques as described herein and/or other or similar techniques as will now be apparent to one of ordinary skill in the art in view of the various embodiments described herein. For example, the service processor can be implemented in software and executed in a protected area of an OS executed on the device and/or executed in protected execution partitions (e.g., in CPU, APU, SIM chipset, modem, modem secure execution partition, SIM, other hardware function on the device, and/or any combination of the above).

[00237] In some embodiments, a network service usage counter is embedded into a secure execution environment (e.g., a program store in secure non-volatile memory located on a modem card and/or a modem chip not accessible by device applications, secure CPU environment for executing program and/or secure program operation for data path monitoring and/or control that cannot be bypassed by device applications to get to the modem connection to the network) in a device modem (e.g., using measurement points V, VI, and/or other measurement points of FIG. 12). In some embodiments, the service usage counter counts data traffic (e.g., bytes and/or any other measure of service usage, such as file transactions, message transactions, connection time,

time of connection or duration of connection, and/or traffic passed or transactions passed for a given QoS or network capacity controlled service priority level), traffic as a function of time, traffic according to a network service activity classification (e.g., by application, destination/source, port, traffic type, content type, time of day, network busy state, and/or any other criteria/measure). In some embodiments, the service usage counter counts data traffic (e.g., as discussed above) while coordinating with a VPN layer established, for example, for both layer-III (e.g., IPSEC) and layer-II (e.g., L2TP tunnel) so that precise over the air service usage measure is counted for billing mediation and/or network service usage charging (e.g., customer billing, sponsored service bill by service and/or any other charging or billing). In some embodiments, the service usage counter counts data traffic (e.g., as discussed above) while coordinating with accelerator software (e.g., a compression/decompression engine) which transforms frames for more efficient over the air transmission. As similarly discussed above, service processor coordination with the accelerator layer facilitates a precise over the air service usage measure for billing mediation and/or network service usage charging. In some embodiments, the service usage counter counts data traffic (e.g., as discussed above) while coordinating with both the VPN layer and accelerator software layer to facilitate a precise over the air service usage measure for billing mediation and/or network service usage charging.

[00238] In some embodiments, the service usage counter reports the service usage to a network element (e.g., a service controller, charging gateway, PCRF, AAA, HA, billing system, mediation system, traffic accounting database, base station or base station controller, and/or another network element/function or central network element/function). In some embodiments, the information reported to the network element is encrypted or signed with a corresponding key known by the network element. In some embodiments, the communication link to the network element to pass the service usage count is conducted over a wireless network specific channel such as SMS, MMS, SS-7, or another specialized control channel. In some embodiments, the communications link to the network element to pass the service usage count is conducted over a network channel (e.g., via IP, TCP, UDP, HTTP, HTTPS, TLS, SSL, point to point signed variants of TLS or SSL, or another data network channel via the network control channel connection to the device). In some embodiments, the data network control channel traffic is injected into the PPP stream at the modem. In some embodiments, the data network control channel traffic is passed up to the device networking stack for connection to the network. In

some embodiments, a signed or encrypted service usage count from the modem subsystem is coordinated to provide a service usage count for a time period that also corresponds to a similar time period for a service processor heartbeat report that includes a service usage measure or count. For example, this provides the service controller or another network element with a secondary set of information that can be used to verify and/or secure the service usage measures reported by the service processor. Various techniques can be used to synchronize the time period for the modem service usage count and the service processor service usage count. For example, the service processor can request a latest count message from the modem, in which the modem counts all service usage since the previous request for latest count until the present request for latest count, encrypts the latest count message so that the service processor or other application software or OS software on the device cannot decode and/or tamper with the message, and the modem service usage counter then passes the encrypted message to the service processor. The service processor can then pass the encrypted service usage count message from the modem to the service controller along with the service processor service usage accounting message(s) for the same or similar time period. The service controller can then decode both service count messages from the secure modem subsystem and the service processor and correlate the two measures to verify the service usage reporting by, for example, looking for discrepancies that would indicate service usage control or charging errors or device service processor tampering. In some embodiments, the secure modem subsystem records byte counts for streams (e.g., and/or flows, socket connections, or combinations of IP destination/source/ports), potentially along with time of day, network busy state, QoS level, and/or other criteria/measures, and reports these counts for each stream that had traffic activity during the current reporting interval. For example, the service controller can then correlate the stream service usage information with the service usage information provided by the service processor heartbeat service usage report to verify that the service processor service usage report is consistent with the independent measure made in the modem subsystem. In some embodiments, service usage reports (e.g., certified service usage reports) are correlated on the device and/or in the network (e.g., using one or more network elements/functions, such as the service controller).

[00239] In some embodiments, a deeper analysis of traffic can be conducted in the modem subsystem service usage count. For example, a layer 7 analysis of the service usage can be conducted for HTTP or HTTPS traffic flowing through the modem in which the modem

subsystem service usage counter performs an HTTP level analysis of the traffic to associate web traffic gets and other transfers with a given higher level service classification (e.g., ad server, content server, proxy server, and/or traffic that is referred by the local host serving up a web page). In some embodiments, the modem subsystem service usage count can be augmented for HTTPS, SSL or TLS traffic by including a trusted proxy server embedded in the modem system. For example, the proxy server can be trusted by the device stack so that the encryption keys for HTTPS, TLS or SSL are known by the proxy server allowing the modem based proxy server, located, for example, in a secure execution environment, to perform layer 7 analysis of encrypted traffic in a manner similar to that described above. In some embodiments, the embedded proxy server generates server SSL certificates for each connection to a specific remote host in real time based on a root certificate trusted by the device (e.g., and/or by network service usage activity, such as by application) and also trusted by the embedded proxy server, and the proxy server then becomes a middle man emulating a remote SSL host on one side and emulating the device (e.g., and/or network service usage activity, such as application) on the other side, decrypting the traffic, analyzing it and re-encrypting before forwarding to and from the remote host. Similarly, as in the case of layer 3 and 4 traffic analysis performed by the modem service usage counting subsystem, the layer 7 service usage count messages can be encrypted and passed to the service controller via various channels. In some embodiments, the layer 7 modem subsystem service usage counting system records service usage counts for a reporting time period that is similar to the reporting time period used by the service processor so that the service controller can correlate the service processor accounting messages against the modem accounting messages with layer 7 information.

[00240] In some embodiments, the secure service usage reporting system elements are located in a secure execution environment that includes the modem driver. In some embodiments, all traffic that gets to the modem for the network traffic being controlled or accounted for is required to go through the secure modem driver so that an independent count can be generated and reported to the service controller as described above without the need to embed the secure service usage counting and reporting elements in the modem.

[00241] In some embodiments, the secure service usage reporting system elements are located in a secure execution environment that includes the modem driver and modem hardware interface controller driver (e.g., USB controller for 2/3/4G and SDIO controller for WiFi). In

some embodiments, all traffic that gets to the modem for the network traffic being controlled or accounted for is required to go through the secure modem driver and modem hardware interface controller driver (e.g., USB controller for 2/3/4G and SDIO controller for WiFi) so that precise count can be generated by either the modem driver and/or modem hardware interface controller driver (e.g., USB controller for 2/3/4G and SDIO controller for WiFi) and passed to the secure service usage reporting element to send it to the service controller for customer charging/billing. This scheme provides flexibility (e.g., most of the device software and operation system and its services/applications need not be located/executed in the secure execution environment) while ensuring usage counting to occur securely as it pertains to the customer accounting and billing.

[00242] In some embodiments, the layer 7 proxy server traffic accounting and reporting techniques used for processing HTTPS, TLS, and SSL traffic, as discussed above, are also used in the service processor itself to allow a detailed accounting of encrypted layer 7 traffic by the device. In some embodiments, the information thus obtained is filtered so that private user information is not transmitted to the network (e.g., service controller, PCRF, and/or any other network element/function) but only service usage information sufficient to allow for accounting of service plan usage, to verify service control policy implementation, or to verify service charging policy implementation is transmitted to the network (e.g., service controller, PCRF, and/or any other network element/function). In some embodiments, the layer 7 proxy server for processing secure or in the clear device service usage accounting messages is located in secure hardware execution environments in the device application processor or within secure software partitions in the operating system.

[00243] Various techniques can be used to verify and/or secure service usage controls or service usage charging reports. For example, if the secondary service usage reports indicate that service usage is outside of the service usage policy limits that are intended to be in effect (e.g., based on a service plan and/or service policy associated with the device), then the service controller can indicate an error flag for further analysis and action (e.g., implementing various verification and responsive actions as described herein, such as blocking the activity, throttling the activity, quarantining the device, updating/replacing the service processor, and/or monitoring the device using various additional DAS and/or network assisted monitoring techniques). As another example, if the service usage reports from the service processor do not match up with the secondary service usage reports, then the service controller can indicate an error flag for further

analysis and action. For example, the correlation can be based on bulk measures of service usage (e.g., total bytes over a given period of time), or using finer grain measures of service usage (e.g., verifying the accounting between one group of service usage activities, such as application, destination/source, port, content type, time of day, network busy state, QoS level, and/or other criteria/measures) charged to one service plan charging record versus the accounting for another group of service usage activities charged to another service plan charging record. In some embodiments, the correlation process between the two service usage accounting reports is performed continuously on all device traffic in real time or near real time as the usage accounting reports are received. In some embodiments, the usage accounting reports are stored and analyzed or correlated later (e.g., periodically, based on a request or audit, and/or based on certain events, such as threshold network service usage events and/or any other events based on various criteria/measures). In some embodiments, only an audit of a portion of time is used to correlate the two usage accounting reports, which, for example, can reduce network traffic and/or network processing load in the service controller.

[00244] In some embodiments, correlation techniques are applied by the service controller to compare two different service usage measures as described above based on one or more of the following: total amount of data (e.g., bytes for file transfers, sessions, and/or other measures), amount of data per unit time, total number of accesses, number of accesses per unit time or frequency of accesses, accesses during a time interval (e.g., peak time), accesses during a network busy state, access requests, and individual versus group transmissions at a point in time (e.g., each for a given set of destinations or destinations and traffic types).

[00245] In some embodiments, service usage monitoring includes characterizing service usage activities by streams, flows, destination/port, packet inspection, and/or other criteria/measures using the various techniques as described herein and/or other or similar techniques as would be apparent to one of ordinary skill in the art. In some embodiments, service usage monitoring includes characterizing service usage activities by streams, flows, destination/port, packet inspection, and/or other criteria/measures and then correlating to find network service usage behavior patterns that identify likely association of behavior with one or more service activities being managed.

[00246] In some embodiments, DAS for network capacity control includes classifying traffic to determine which network service usage activity(ies) are causing traffic (e.g., increasing network capacity/resources usage beyond a threshold), and then determining if access network service usage activity(ies) are violating any rules (e.g., service usage policies or service plan settings associated with the device/user). In some embodiments, DAS for network capacity control includes generating a list for network capacity controlled services that specifies behavioral characteristics for one or more network service usage activities with expected access limits based on access control policy for each managed network service usage activity (e.g., based on service usage policies or service plan settings associated with the device/user). In some embodiments, DAS for network capacity control includes monitoring and/or controlling network service usage activities based on limits, which, for example, can be based on one or more of the following: total access traffic counters, counters for different types of access traffic, destinations, ports, frequency of accesses, access behavior during a given time, access behavior during a given busy state, access behavior for groups of activities (e.g., verify clumping), and/or other criteria/measures.

[00247] Accordingly, in some embodiments, a second secure and trusted service usage measure is provided that the service controller (e.g., or another network element/function) can use to verify or secure the service control or service charging reports for the service processor. In some embodiments, the secure and trusted service usage measure also provides for enhanced verification and service security in cases, in which, for example, network based service usage measures are available for additional correlation with the service processor service usage reports. In cases in which network based service usage measures are either not available or are only available at widely spaced time intervals (e.g., roaming networks or other networks with no timely network based service usage measure), these techniques facilitate real time or near real time verification or security for the device assisted service controls and charging.

[00248] In some embodiments, a SIM card performs a portion or all of the secure environment processing described above, with the device modem traffic, or a copy of the device modem traffic, being directed to the SIM secure subsystem for traffic accounting and reporting. In some embodiments, a SIM card is used to store QoS classifications and/or network capacity controlled services classifications for various service usage activities so that the user behavior in using certain network service usage activities and/or the user preferences in controlling certain network

service usage activities do not need to be relearned or redownloaded as the user swaps the SIM between different devices. In some embodiments, the SIM keeps a local record of service usage activity for multiple devices that belong to the user or the user family plan, so that the service usage notification and policies can be immediately updated on a given device as the user swaps the SIM from device to device. In some embodiments, the manner in which this service usage history is stored on the SIM is secure so that it cannot be tampered with. In some embodiments, the SIM card is used to implement various application management and/or traffic control techniques described herein. In some embodiments, the SIM card is used to inspect traffic, classify traffic, create reports (e.g., certified service activity usage reports), encrypt the report, send the report to a network element/function, and the network element/function correlates the reports (e.g., using network assisted measures for comparisons and/or using various other techniques as described herein). In some embodiments, a SIM card performs a portion or all of the secure environment processing described above using one or more modem measurement points. For example, the traffic that is to be classified can be routed through the SIM and correlated with what is measured by the modem. In some embodiments, network assisted/based network service usage activity classifications are compared SIM based/assisted classifications for service usage monitoring/reporting verification (e.g., detected inconsistencies in monitored/reported network service usage activities can be identified, such as based on total traffic, streams/flows/sockets activities, and/or other criteria/measures). In some embodiments, the reports include a verified sequence so that reports cannot be spoofed and/or missing reports can be determined.

[00249] In some embodiments, a portion or all of the secure environment processing described above are applied to implement and/or verify QoS for DAS techniques and/or DAS for network capacity controlled services techniques as described herein.

[00250] In some embodiments, the reports include one or more of the following: a number of times the device is cycled from or to a power cycle state in the modem, a number of times during a time window or network busy state, a power cycle versus number of streams initiated during the cycle, and a power cycle versus the streams that are transmitted during that cycle, In some embodiments, device power cycle events trigger generating of a report.

[00251] In some embodiments, monitoring, reporting, control, accounting, charging, and/or policy implementation for network capacity controlled services is verified (e.g., using various verification techniques described herein). If any of the verification techniques determine or assist in determining that the network capacity controlled services monitoring, reporting, control, accounting, and/or charging, and/or policy implementation has been tampered with, disabled, and/or is not properly implemented or functioning, then responsive actions can be performed, for example, the device (e.g., and/or suspect services) can be suspended, quarantined, killed/terminated, and/or flagged for further analysis/scrutiny to determine whether the device is malfunctioning, needs updating, has been tampered with or compromised, is infected with malware, and/or if any other problem exists.

[00252] In some embodiments, the service processor monitors a network service usage activity of a device. In some embodiments, monitoring of the service usage activity includes monitoring for multiple networks (e.g., to determine which networks are available and/or a network busy state of the available networks). In some embodiments monitoring a network service usage activity is performed by and/or assisted by a service cloud (e.g., one or more network elements that provide such a service). In some embodiments, monitoring the network service usage activity includes identifying the network service usage activity, measuring the network service usage of the network service usage activity, and/or characterizing the network service usage of the network service usage activity (e.g., using device assisted/based techniques, network assisted/based techniques, testing/offline monitoring/analysis techniques, and/or a combination thereof).

[00253] In some embodiments, the service processor implements differential network access service control (e.g., for network capacity controlled services), network service usage accounting, network service usage charging, and/or network service usage notification on the device to facilitate DAS for protecting network capacity.

[00254] In some embodiments, the service processor (e.g., a service processor 115) is updated, communicated with, set, and/or controlled by a network element (e.g., a service controller 122). In some embodiments, the service processor receives service policy information from a network function selected from a base station (e.g., a base station 125), a RAN gateway, a core gateway, a DPI gateway, a home agent (HA), a AAA server (e.g., AAA server 121), a service controller,

and/or another network function or combinations of network functions as described herein and/or as will now be apparent to one of ordinary skill in the art in view of the various embodiments described herein. In some embodiments, the service processor is updated through over the air or over the network OS software updates or application software updates or device firmware updates. In some embodiments, the service processor uses an IP connection, SMS connection, and/or MMS connection, for a control channel with a service controller. In some embodiments, the service processor queries a service controller to determine the association of a monitored network service usage activity with a network service usage control policy. In some embodiments, the device (e.g., service processor) maintains a network capacity controlled services list and/or network capacity controlled services policy for one or more of the active services (e.g., actively executing and/or previously installed/downloaded to the device) that have been classified as a network capacity controlled service (e.g., as the number of applications continues to grow, as hundreds of thousands of applications are already available on certain platforms, maintaining a list specific and/or a set of policies unique or specific to each application is not efficient). In this embodiment, when a new application is active/launched and/or downloaded to the device, the device can request an updated network capacity controlled services list and/or an updated network capacity controlled services policy accordingly (e.g., and/or periodically refresh such lists/policies).

[00255] In some embodiments, differential network access control for protecting network capacity includes controlling network services traffic generated by the device (e.g., network capacity controlled services based on a network service usage control policy (e.g., a network capacity controlled services policy). In some embodiments, differential network access control for protecting network capacity includes providing assistance in control of the distribution of bandwidth among devices, network capacity controlled services (e.g., applications, OS operations/functions, and various other network services usage activities classified as network capacity controlled services), a differentiated QoS service offering, a fair sharing of capacity, a high user load network performance, and/or preventing one or more devices from consuming so much network capacity that other devices cannot receive adequate performance or performance in accordance with various threshold and/or guaranteed service levels. In some embodiments, differential network access control for protecting network capacity includes applying policies to determine which network the service activity should be connected to (e.g., 2G, 3G, 4G, home or

roaming, WiFi, cable, DSL, fiber, wired WAN, and/or another wired or wireless or access network), and applying differential network access control rules (e.g., traffic control rules) depending on which network to which the service activity is connected. In some embodiments, differential network access control for protecting network capacity includes differentially controlling network service usage activities based on the service usage control policy and a user input (e.g., a user selection or user preference). In some embodiments, differential network access control for protecting network capacity includes differentially controlling network service usage activities based on the service usage control policy and the network the device or network service activity is gaining access from.

[00256] In some embodiments, the network service usage control policy is dynamic based on one or more of the following: a network busy state, a time of day, which network the service activity is connected to, which base station or communication channel the service activity is connected to, a user input, a user preference selection, an associated service plan, a service plan change, an application behavior, a messaging layer behavior, random back off, a power state of device, a device usage state, a time based criteria (e.g., time/day/week/month, hold/delay/defer for future time slot, hold/delay/defer for scheduled time slot, and/or hold/delay/defer until a busy state/availability state/QoS state is achieved), monitoring of user interaction with the service activity, monitoring of user interaction with the device, the state of UI priority for the service activity, monitoring the power consumption behavior of the service activity, modem power cycling or power control state changes, modem communication session set up or tear down, and/or a policy update/modification/change from the network. In some embodiments, the network service usage control policy is based on updated service usage behavior analysis of the network service usage activity. In some embodiments, the network service usage control policy is based on updated activity behavior response to a network capacity controlled service classification. In some embodiments, the network service usage control policy is based on updated user input/preferences (e.g., related to policies/controls for network capacity controlled services). In some embodiments, the network service usage control policy is based on updates to service plan status. In some embodiments, the network service usage control policy is based on updates to service plan policies. In some embodiments, the network service usage control policy is based on availability of alternative networks. In some embodiments, the network service usage control policy is based on policy rules for selecting alternative networks. In some

embodiments, the network service usage control policy is based on network busy state or availability state for alternative networks. In some embodiments, the network service usage control policy is based on specific network selection or preference policies for a given network service activity or set of network service activities.

[00257] In some embodiments, associating the network service usage activity with a network service usage control policy or a network service usage notification policy, includes dynamically associating based on one or more of the following: a network busy state, a time of day, a user input/preference, an associated service plan (e.g., 25 MB data plan, 5G data plan, or an unlimited data plan or other data/service usage plan), an application behavior, a messaging layer behavior, a power state of device, a device usage state, a time based criteria, availability of alternative networks, and a set of policy rules for selecting and/or controlling traffic on one or more of the alternative networks.

[00258] In some embodiments, a network service usage control policy (e.g., a network capacity controlled services policy) includes defining the network service usage control policy for one or more service plans, defining network access policy rules for one or more devices or groups of devices in a single or multi-user scenarios such as family and enterprise plans, defining network access policy rules for one or more users or groups of users, allowing or disallowing network access events or attempts, modulating the number of network access events or attempts, aggregating network access events or attempts into a group of access events or attempts, time windowing network access events or attempts, time windowing network access events or attempts based on the application or function being served by the network access events or attempts, time windowing network access events or attempts to pre-determined time windows, time windowing network access events or attempts to time windows where a measure of network busy state is within a range, assigning the allowable types of access events or attempts, assigning the allowable functions or applications that are allowed network access events or attempts, assigning the priority of one or more network access events or attempts, defining the allowable duration of network access events or attempts, defining the allowable speed of network access events or attempts, defining the allowable network destinations for network access events or attempts, defining the allowable applications for network access events or attempts, defining the QoS rules for one or more network access events or attempts, defining or setting access policy rules for one or more applications, defining or setting access policy rules for one or more

network destinations, defining or setting access policy rules for one or more devices, defining or setting access policy rules for one or more network services, defining or setting access policy rules for one or more traffic types, defining or setting access policy rules for one or more QoS classes, and defining or setting access policy rules based on any combination of device, application, network destination, network service, traffic type, QoS class, and/or other criteria/measures.

[00259] In some embodiments, a network service usage control policy (e.g., a network capacity controlled services policy) includes a traffic control policy. In some embodiments, the traffic control policy includes a traffic control setting. In some embodiments, the traffic control policy includes a traffic control/tier, and the traffic control/tier includes the traffic control setting. In some embodiments, the traffic control policy includes one or more of the following: block/allow settings, throttle settings, adaptive throttle settings, QoS class settings including packet error rate, jitter and delay settings, queue settings, and tag settings (e.g., for packet tagging certain traffic flows). In some embodiments, QoS class settings include one or more of the following: throttle level, priority queuing relative to other device traffic, time window parameters, and hold or delay while accumulating or aggregating traffic into a larger stream/burst/packet/group of packets. In some embodiments, the traffic control policy includes filters implemented as indexes into different lists of policy settings (e.g., using cascade filtering techniques), in which the policy filters include one or more of the following: a network, a service plan, an application, a time of day, and a network busy state. For example, a two dimensional traffic control implementation scheme can be provided using a network busy state and/or a time of day as an index into a traffic control setting (e.g., a certain application's priority level can be increased or decreased based on a network busy state and/or time of day). In some embodiments, the traffic control policy is used for selecting the network from a list of available networks, blocking or reducing access until a connection is made to an alternative network, and/or modifying or replacing a network stack interface of the device to provide for intercept or discontinuance of network socket interface messages to applications or OS functions.

[00260] In some embodiments, a traffic control setting is selected based on the network service usage control policy. In some embodiments, the traffic control setting is implemented on the device based on the network service usage control policy. In some embodiments, the implemented traffic control setting controls traffic/traffic flows of a network capacity controlled

service. In some embodiments, the traffic control setting is selected based on one or more of the following: a time of day, a day of week, a special time/date (e.g., a holiday or a network maintenance time/date), a network busy state, a priority level associated with the network service usage activity, a QoS class associated with the network service usage activity (e.g., emergency traffic), which network the network service activity is gaining access from, which networks are available, which network the network service activity is connected to, which base station or communication channel the network service activity is connected to, and a network dependent set of traffic control policies that can vary depending on which network the service activity is gaining access from (e.g., and/or various other criteria/measures as described herein). In some embodiments, the traffic control setting includes one or more of the following: allow/block, delay, throttle, QoS class implementation, queue, tag, generate a user notification, random back off, clear to send received from a network element, hold for scheduled transmission time slot, selecting the network from the available networks, and blocking or reducing access until a connection is made to an alternative network. In some embodiments, the traffic control setting is selected based on a network capacity controlled services priority state of the network service usage activity and a network busy state. In some embodiments, the traffic control setting is selected based on a network capacity controlled services priority state of the network service usage activity and a network busy state and is global (e.g., the same) for all network capacity controlled services activities or varies based on a network service usage activity priority, user preferences or option selection, an application, a time based criteria, a service plan, a network the device or service activity is gaining access from, a redetermination of a network congestion state after adapting to a previously determined network busy state, and/or other criteria/measures as described herein.

[00261] In some embodiments, network capacity controlled services traffic (e.g., traffic flows) is differentially controlled for protecting network capacity. For example, various software updates for an OS and one or more applications on the device can be differentially controlled using the various techniques described herein. As another example, security/antimalware software (e.g., antivirus, firewall, content protection, intrusion detection/prevention, and/or other security/antimalware software) can be differentially controlled using the various techniques described herein. As yet another example, network backups/imaging, content downloads (e.g., exceeding a threshold individually and/or in aggregate, such as for image, music, video, eBook

content, email attachments, content/media subscriptions, RSS/news feeds, text/image/video chat, software updates, and/or other content downloads) can be differentially controlled using the various techniques described herein.

[00262] For example, using the DAS for protecting network capacity techniques described herein an adaptive policy control for protecting network capacity can be provided. A network capacity controlled services list can be generated, updated, reported, and/or received by the device and stored on the device (e.g., the list can be based on adapted to the service plan associated with the device). If a monitored network service usage activity is not on the list, then the device can report the monitored network service usage activity to a network element (e.g., for a monitored network service usage activity that also exceeds a certain threshold, based on a network busy state, based on a time based criteria, and/or other criteria/measure). As an example, monitored network service usage activity can be reported if/when the monitored network service usage activity exceeds a data usage threshold (e.g., 50 MB total data usage per day, a socket opening frequency/rate, velocity of data usage at an instant in time, or more complicated thresholds over time, over peak periods, by content and time, by various other parameters/thresholds). As another example, the monitored network service usage activity can be reported based on testing of the network service usage behavior and/or application developer characterization input. The report can include information that identifies the network service usage activity and various network service usage parameters.

[00263] In some embodiments, a notification setting is selected based on a service usage notification policy. In some embodiments, a notification setting includes a user notification setting (e.g., various user notifications settings as described above with respect to FIG. 18).

[00264] In some embodiments, classifying the network service usage activity further includes classifying the network service usage activity (e.g., using a usage threshold filter and/or cascading filter techniques) into one or more of a plurality of classification categories for differential network access control for protecting network capacity. In some embodiments, classifying the network service usage activity further includes classifying the network service usage activity into one or more network capacity controlled services in which the network capacity controlled services include one or more of the following: applications requiring data network access, application software updates, applications requiring network information,

applications requiring GPS or physical location, operating system software updates, security software updates, network based backups, email downloads, and a set of activities configured as network capacity controlled service activities based on a service profile and/or user input (e.g., and/or various other types of network service usage activities as described herein and as will now be apparent to one of ordinary skill in the art). For example, network capacity controlled services can include software updates for OS and applications, OS background network accesses, cloud synchronization services, RSS feeds and other background information feeds, browser/application/device behavior reporting, background email downloads, content subscription service updates and downloads (e.g., music/video downloads, news feeds), text/voice/video chat clients, security updates (e.g., antimalware updates), peer to peer networking application updates, inefficient network access sequences during frequent power cycling or power save state cycling, large downloads or other high bandwidth accesses, and greedy application programs that constantly/repeatedly access the network with small transmissions or requests for information. In some embodiments, a network capacity controlled services list is static, adaptive, generated using a service processor, received from a network element (e.g., service controller or service cloud), received from a network element (e.g., service controller or service cloud) and based at least in part on device activity reports received from the service processor, based on criteria set by pre-testing, report of behavior characterization performed by the application developer, and/or based at least in part on user input. In some embodiments, the network capacity controlled services list includes one or more network service activity background (QoS) classes.

[00265] In some embodiments, classifying the network service usage activity further includes classifying the network service usage activity based on one or more of the following: application or widget (e.g., Outlook, Skype, iTunes, Android email, weather channel weather widget, iCal, Firefox Browser, etc), application type (e.g., user application, system application/utility/function/process, OS application/utility/function/process, email, browser, widget, malware (such as a virus or suspicious process), RSS feed, device synchronization service, download application, network backup/imaging application, voice/video chat, peer to peer content application or other peer to peer application, streaming media feed or broadcast reception/transmission application, network meeting application, chat application or session, and/or any other application or process identification and categorization), OS/system function

(e.g., any system application/utility/function/process and/or OS application/utility/function/process, such as a OS update and/or OS error reporting), modem function, network communication function (e.g., network discovery or signaling, EtherType messages, connection flow/stream/session set up or tear down, network authentication or authorization sequences, IP address acquisition, and DNS services), URL and/or domain, destination/source IP address, protocol, traffic type, socket (e.g., IP address, protocol, and/or port), socket address/label/identifier (e.g., port address/port number), content type (e.g., email downloads, email text, video, music, eBooks, widget update streams, and download streams), port (e.g., port number), QoS classification level, time of day, on peak or off peak, network time, network busy state, access network selected, service plan selected, user preferences, device credentials, user credentials, and/or status, modem power cycling or power state changes, modem authentication processes, modem link set up or tear down, modem management communications, modem software or firmware updates, modem power management information, device power state, and modem power state. In some embodiments, classifying the network service usage activity further includes associating the classified network service usage activity with an ID (e.g., an application ID, which can be, for example, a unique number, name, and/or signature). In some embodiments, classifying the network service usage activity further includes classifying the network service usage activity using a plurality of classification parameters, including one or more of the following: application ID, remote IP (e.g., URL, domain, and/or IP address), remote port, protocol, content type, a filter action class (e.g., network busy state class, QoS class, time of day, network busy state, and/or other criteria/measures), and access network selected. In some embodiments, classifying the network service usage activity further includes using a combination of parameters as discussed above to determine the classification of the network service usage activity.

[00266] In some embodiments, classifying the network service usage activity further includes classifying the network service usage activity as a network capacity controlled service, a non-network capacity controlled service, a blocked or disallowed service, and/or a not yet classified/identified service (e.g., unknown/yet to be determined classification or pending classification). In some embodiments, an application connection, OS connection, and/or other service activity is classified as a network capacity controlled service activity when the device has been inactive (e.g., or in a power save state) for a period of time (e.g., when the user has not

interacted with it for a period of time, when it has not displayed user notification policy, and/or a user input has not been received for a period of time, and/or when a power save state is entered). In some embodiments, an application connection, OS connection, and/or other service activity is classified as a network capacity controlled service activity when the monitored network service usage activity exceeds a data usage threshold for more than one application connection, OS connection, and/or other service activity (e.g., aggregated data usage exceeds the data usage threshold); or for a specific application connection. In some embodiments, an application connection, OS connection, and/or other service activity is classified as a network capacity controlled service activity when the monitored network service usage activity exceeds a data usage threshold based on a predetermined list of one or more data usage limits, based on a list received from a network element, usage time limit (e.g., based on a period of time exceeding a usage limit), and/or based on some other usage related criteria/measures. In some embodiments, classifying the network service usage activity further includes classifying the network service usage activity as a network capacity controlled service based on a network peak time, a network busy state, or a network connection to the device falls below a certain performance level (e.g., higher/lower priorities assigned based on various such criteria/other input/factors).

[00267] In some embodiments, one or more of the network capacity controlled services are associated with a different network access policy set for one or more networks and/or one or more alternative networks. In some embodiments, one or more of the network capacity controlled services are associated with a different notification policy set for one or more networks and/or one or more alternative networks. In some embodiments, the network capacity controlled services list is stored on the device. In some embodiments, the network capacity controlled services list is received/periodically updated from a network element and stored on the device. In some embodiments, the network capacity controlled services list includes network capacity controlled services, non-network capacity controlled services (e.g., foreground services or services based on various possibly dynamic criteria are not classified as network capacity controlled services), and an unclassified set of services (e.g., grey list including one or more network service activities pending classification based on further analysis and/or input, such as from a network element, service provider, and/or user). In some embodiments, the network capacity controlled services list is based on one or more of the following:

predefined/predesignated (e.g., network, service plan, pre-test and/or characterized by an application developer) criteria; device assisted/based monitoring (e.g., using a service processor); network based monitoring (e.g., using a DPI gateway); network assisted analysis (e.g., based on device reports of DAS activity analysis). For example, the device can report device monitored network service usage activities (e.g., all monitored network service usage activities or a subset based on configuration, threshold, service plan, network, and/or user input) to the network element. As another example, the network element can update the network capacity controlled services list and send the updated list to the device. As yet another example, the network element can perform a statistical analysis of network service activities across a plurality of devices based on the device based and/or network based network service usage activity monitoring/reporting. In some embodiments, a network service usage activity is determined to be an active application or process (e.g., based on a user interaction with the device and/or network service usage activity, such as a pop-up and/or other criteria/measures).

[00268] In some embodiments, implementing traffic control for network capacity controlled services is provided using various techniques. In some embodiments, the device includes a service processor agent or function to intercept, block, modify, remove or replace UI messages, notifications or other UI communications generated by a network service activity that whose network service usage is being controlled or managed (e.g., using various measurement points as shown in and described with respect to FIGS. 12 and 13). For example, this technique can be used to provide for an improved user experience (e.g., to prevent an application that is being controlled for protecting network capacity from generating repeated and/or confusing messages/alerts to the user). In some embodiments, a network stack interface of the device is replaced or modified to provide for intercept or discontinuance of network socket interface messages to applications or OS functions or other functions/software.

[00269] In some embodiments, implementing traffic control for network capacity controlled services using DAS techniques is provided using various techniques in which the network service usage activity is unaware of network capacity control (e.g., does not support an API or other interface for implementing network capacity control). For example, network service application messaging interface based techniques can be used to implement traffic control. Example network service application messaging interfaces include the following: network stack API, network communication stream/flow interface, network stack API messages, EtherType

messages, ARP messages, and/or other messaging or other or similar techniques as will now be apparent to one of ordinary skill in the art in view of the various embodiments described herein. In some embodiments, network service usage activity control policies or network service activity messages are selected based on the set of traffic control policies or service activity messages that result in reduced or modified user notification by the service activity due to network capacity controlled service policies applied to the network service activity. In some embodiments, network service usage activity control policies or network service activity messages are selected based on the set of traffic control policies or service activity messages that result in reduced disruption of device operation due to network capacity controlled service activity policies applied to the network service activity. In some embodiments, network service usage activity control policies or network service activity messages are selected based on the set of traffic control policies or service activity messages that result in reduced disruption of network service activity operation due to network capacity controlled service activity policies applied to the network service activity. In some embodiments, implementing traffic control for network capacity controlled services is provided by intercepting opens/connects/writes. In some embodiments, implementing traffic control for network capacity controlled services is provided by intercepting stack API level or application messaging layer requests (e.g., socket open/send requests). For example, an intercepted request can be copied (e.g., to memory) and queued (e.g., delayed or throttled) or dropped (e.g., blocked). As another example, an intercepted request can be copied into memory and then a portion of the transmission can be retrieved from memory and reinjected (e.g., throttled). As yet another example, intercepting messaging transmissions can be parsed inline and allowed to transmit (e.g., allowed), and the transmission or a portion of the transmission can be copied to memory for classifying the traffic flow. In some embodiments, implementing traffic control for network capacity controlled services is provided by intercepting or controlling or modulating UI notifications. In some embodiments, implementing traffic control for network capacity controlled services is provided by killing or suspending the network service activity. In some embodiments, implementing traffic control for network capacity controlled services is provided by deprioritizing the process(es) associated with the service activity (e.g., CPU scheduling deprioritization).

[00270] In some embodiments, implementing traffic control for network capacity controlled services using DAS techniques for network service usage activities that are unaware of network

capacity control is provided by emulating network API messaging (e.g., effectively providing a spoofed or emulated network API). For example, an emulated network API can intercept, modify, block, remove, and/or replace network socket application interface messages and/or EtherType messages (e.g., EWOULDBLOCK, ENETDOWN, ENETUNREACH, EHOSTDOWN, EHOSTUNREACH, EALRADY, EINPROGRESS, ECONNREFUSED, EINPROGRESS, ETIMEDOUT, and/other such messages). As another example, an emulated network API can modify, swap, and/or inject network socket application interface messages (socket(), connect(), read(), write(), close(), and other such messages) that provide for control or management of network service activity service usage behavior. As yet another example, before a connection is allowed to be opened (e.g., before a socket is opened), transmission, or a flow/stream is initiated, it is blocked and a message is sent back to the application (e.g., a reset message in response to a sync request or another message that the application will understand and can interpret to indicate that the network access attempt was not allowed/blocked, that the network is not available, and/or to try again later for the requested network access). As yet another example, the socket can be allowed to open but after some point in time (e.g., based on network service usage, network busy state, time based criteria, and/or some other criteria/measure), the stream is blocked or the socket is terminated. As yet another example, time window based traffic control techniques can be implemented (e.g., during non-peak, not network busy state times), such as by allowing network access for a period of time, blocking for a period of time, and then repeating to thereby effectively spread the network access out either randomly or deterministically. Using these techniques, an application that is unaware of network capacity control based traffic control can send and receive standard messaging, and the device can implement traffic controls based on the network capacity control policy using messaging that the network service usage activity (e.g., application or OS or software function) can understand and will respond to in a typically predictable manner as would now be apparent to one of ordinary skill in the art.

[00271] In some embodiments, implementing traffic control for network capacity controlled services using DAS techniques is provided using various techniques in which the network service usage activity is aware of network capacity control (e.g., the network service usage activity supports an API or other interface for implementing network capacity control). For example, a network access API as described herein can be used to implement traffic control for

network capacity controlled services. In some embodiments, the API facilitates communication of one or more of the following: network access conditions, network busy state or network availability state of one or more networks or alternative networks, one or more network capacity controlled service policies (e.g., the network service can be of a current network access setting, such as allow/block, throttle, queue, scheduled time/time slot, and/or defer, which can be based on, for example, a current network, a current network busy state, a time based criteria, a service plan, a network service classification, and/or other criteria/measures), a network access request from a network service activity, a query/polled request to a network service activity, a network access grant to a network service activity (e.g., including a priority setting and/or network capacity controlled service classification, a scheduled time/time slot, an alternative network, and/or other criteria/measures), a network busy state or a network availability state or a network QoS state.

[00272] In some embodiments, implementing traffic control for network capacity controlled services using network assisted/based techniques is provided using various techniques in which the network service usage activity is unaware of network capacity control (e.g., does not support an API or other interface for implementing network capacity control). In some embodiments, DPI based techniques are used to control network capacity controlled services (e.g., to block or throttle network capacity controlled services at a DPI gateway).

[00273] In some embodiments, implementing traffic control for network capacity controlled services using network assisted/based techniques is provided using various techniques in which the network service usage activity is aware of network capacity control (e.g., does support an API or other interface for implementing network capacity control). In some embodiments, the application/messaging layer (e.g., a network API as described herein) is used to communicate with a network service activity to provide associated network capacity controlled service classifications and/or priorities, network busy state information or network availability of one or more networks or alternative networks, a network access request and response, and/other criteria/measures as similarly described herein.

[00274] In some embodiments, DAS for protecting network capacity includes implementing a service plan for differential charging based on network service usage activities (e.g., including network capacity controlled services). In some embodiments, the service plan includes

differential charging for network capacity controlled services. In some embodiments, the service plan includes a cap network service usage for network capacity controlled services. In some embodiments, the service plan includes a notification when the cap is exceeded. In some embodiments, the service plan includes overage charges when the cap is exceeded. In some embodiments, the service plan includes modifying charging based on user input (e.g., user override selection as described herein, in which for example, overage charges are different for network capacity controlled services and/or based on priority levels and/or based on the current access network). In some embodiments, the service plan includes time based criteria restrictions for network capacity controlled services (e.g., time of day restrictions with or without override options). In some embodiments, the service plan includes network busy state based criteria restrictions for network capacity controlled services (e.g., with or without override options). In some embodiments, the service plan provides for network service activity controls to be overridden (e.g., one time, time window, usage amount, or permanent) (e.g., differentially charge for override, differentially cap for override, override with action based UI notification option, and/or override with UI setting). In some embodiments, the service plan includes family plan or multi-user plan (e.g., different network capacity controlled service settings for different users). In some embodiments, the service plan includes multi-device plan (e.g., different network capacity controlled service settings for different devices, such as smart phone v. laptop v. net book v. eBook). In some embodiments, the service plan includes free network capacity controlled service usage for certain times of day, network busy state(s), and/or other criteria/measures. In some embodiments, the service plan includes network dependent charging for network capacity controlled services. In some embodiments, the service plan includes network preference/prioritization for network capacity controlled services. In some embodiments, the service plan includes arbitration billing to bill a carrier partner or sponsored service partner for the access provided to a destination, application, or other network capacity controlled service. In some embodiments, the service plan includes arbitration billing to bill an application developer for the access provided to a destination, application or other network capacity controlled service.

[00275] In some application scenarios, excess network capacity demand can be caused by modem power state changes on the device. For example, when an application or OS function attempts to connect to the network for any reason when the modem is in a power save state

wherein the modem is not connected to the network, it can cause the modem to change power save state, reconnect to the network, and then initiate the application network connection. In some cases, this can also cause the network to re-initiate a modem connection session (e.g., PPP session) which in addition to the network capacity consumed by the basic modem connection also consumes network resources for establishing the PPP session. Accordingly, in some embodiments, network service usage activity control policies are implemented that limit or control the ability of applications, OS functions, and/or other network service usage activities (e.g., network capacity controlled services) from changing the modem power control state or network connection state. In some embodiments, a service usage activity is prevented or limited from awakening the modem, changing the power state of the modem, or causing the modem to connect to the network until a given time window is reached. In some embodiments, the frequency a service usage activity is allowed to awakening the modem, changing the power state of the modem, or causing the modem is limited. In some embodiments, a network service usage activity is prevented from awakening the modem, changing the power state of the modem, or causing the modem until a time delay has passed. In some embodiments, a network service usage activity is prevented from awakening the modem, changing the power state of the modem, or causing the modem until multiple network service usage activities require such changes in modem state, or until network service usage activity is aggregated to increase network capacity and/or network resource utilization efficiency. In some embodiments, limiting the ability of a network service usage activity to change the power state of a modem includes not allowing the activity to power the modem off, place the modem in sleep mode, or disconnect the modem from the network. In some embodiments, these limitations on network service usage activity to awaken the modem, change the power state of the modem, or cause the modem to connect to a network are set by a central network function (e.g., a service controller or other network element/function) policy communication to the modem. In some embodiments, these power control state policies are updated by the central network function.

[00276] FIG. 24 depicts a diagram of a network capacity protection system 2400 utilizing device-assisted services (DAS). The system 2400 includes wireless devices 2402-1 to 2402-N (referred to collectively as the wireless devices 2402), wireless networks 2404-1 to 2404-N (referred to collectively as the wireless networks 2404), a network traffic analysis engine 2406, a

network service usage classification engine 2408, and a differential network access control engine 2410.

[00277] The wireless devices 2402 will at a minimum include a processor, memory (though the memory could be implemented in the processor), a radio, and a radio interface (though the radio interface could be implemented as "part of" the radio). In order to make the wireless devices 2402 useful, they will typically have at least one input device and at least one output device, including input and output interfaces, if applicable.

[00278] The wireless devices 2402 can be implemented as stations. A station, as used herein, may be referred to as a device with a media access control (MAC) address and a physical layer (PHY) interface to the wireless medium that comply with, e.g., the IEEE 802.11 standard. A station can be described as "IEEE 802.11-compliant" when compliance with the IEEE 802.11 standard is intended to be explicit. (I.e, a device acts as described in at least a portion of the IEEE 802.11 standard.) One of ordinary skill in the relevant art would understand what the IEEE 802.11 standard comprises today and that the IEEE 802.11 standard can change over time, and would be expected to apply techniques described in this paper in compliance with future versions of the IEEE 802.11 standard if an applicable change is made. IEEE Std 802.11™-2007 (Revision of IEEE Std 802.11-1999) is incorporated by reference. IEEE 802.11k-2008, IEEE 802.11n-2009, IEEE 802.11p-2010, IEEE 802.11r-2008, IEEE 802.11w-2009, and IEEE 802.11y-2008 are also incorporated by reference.

[00279] In alternative embodiments, one or more of the wireless devices 2402 may comply with some other standard or no standard at all, and may have different interfaces to a wireless or other medium. It should be noted that not all standards refer to wireless devices as "stations," but where the term is used in this paper, it should be understood that an analogous unit will be present on all applicable wireless networks. Thus, use of the term "station" should not be construed as limiting the scope of an embodiment that describes wireless devices as stations to a standard that explicitly uses the term, unless such a limitation is appropriate in the context of the discussion.

[00280] The wireless networks 2404 will typically include an internetworking unit (IWU) that interconnects wireless devices on the relevant one of the wireless networks 2404 with another network, such as a wired LAN. The IWU is sometimes referred to as a wireless access point

(WAP). In the IEEE 802.11 standard, a WAP is also defined as a station. Thus, a station can be a non-WAP station or a WAP station. In a cellular network, the WAP is often referred to as a base station.

[00281] The wireless networks 2404 can be implemented using any applicable technology, which can differ by network type or in other ways. The wireless networks 2404 can be of any appropriate size (e.g., metropolitan area network (MAN), personal area network (PAN), etc.). Broadband wireless MANs may or may not be compliant with IEEE 802.16, which is incorporated by reference. Wireless PANs may or may not be compliant with IEEE 802.15, which is incorporated by reference. The wireless networks 2404 can be identifiable by network type (e.g., 2G, 3G, WiFi), service provider, WAP/base station identifier (e.g., WiFi SSID, base station and sector ID), geographic location, or other identification criteria.

[00282] The wireless networks 2404 may or may not be coupled together via an intermediate network. The intermediate network can include practically any type of communications network, such as, by way of example but not limitation, the Internet, a public switched telephone network (PSTN), or an infrastructure network (e.g., private LAN). The term "Internet" as used herein refers to a network of networks which uses certain protocols, such as the TCP/IP protocol, and possibly other protocols such as the hypertext transfer protocol (HTTP) for hypertext markup language (HTML) documents that make up the World Wide Web (the web).

[00283] In the example of FIG. 24, the network traffic analysis engine 2406 is coupled to the wireless device 2402-1. In a specific implementation, the network traffic analysis engine 2406 is implemented on a server and is coupled to the wireless device 2402-1 through the Internet. However, at least a portion of the network traffic analysis engine 2406 can alternatively be implemented on the wireless device 2402-1, with or without a connection to a server that includes another portion (e.g., a server portion) of the network traffic analysis engine 2406.

[00284] As used in this paper, an engine includes a dedicated or shared processor and, typically, firmware or software modules that are executed by the processor. Depending upon implementation-specific or other considerations, an engine can be centralized or its functionality distributed. An engine can include special purpose hardware, firmware, or software embodied in a computer-readable medium for execution by the processor. As used in this paper, a computer-readable medium is intended to include all mediums that are statutory (e.g., in the United States,

under 35 U.S.C. 101), and to specifically exclude all mediums that are non-statutory in nature to the extent that the exclusion is necessary for a claim that includes the computer-readable medium to be valid. Known statutory computer-readable mediums include hardware (e.g., registers, random access memory (RAM), non-volatile (NV) storage, to name a few), but may or may not be limited to hardware.

[00285] The network traffic analysis engine 2406 analyzes a subset of traffic between the wireless device 2402-1 and a source or destination. The analyzed traffic may or may not be limited to a network segment, such as between a cellular phone and a base station. The network traffic analysis engine 2406 can analyze traffic for a subset of devices in the wireless network 2404-1 service area. The analyzed traffic may or may not be limited to subscribers.

[00286] In the example of FIG. 24, the network service usage classification engine 2408 is coupled to the network traffic analysis engine 2406. In a specific implementation, the network service usage classification engine 2408 is implemented on a server, which may or may not be the same server on which the network traffic analysis engine 2406 is implemented. However, at least a portion of the network service usage classification engine 2408 can alternatively be implemented on the wireless device 2402-1, with or without a connection to a server that includes another portion (e.g., a server portion) of the network service usage classification engine 2408.

[00287] The network service usage classification engine 2408 can categorize traffic based upon the service class (e.g., conversational, streaming, interactive, background, or some other service class) requested or needed for a service. The categorization facilitates identification of a snapshot of service class use at a given time, and, in some implementations, predictions of future service class use based upon the snapshot (e.g., making an assumption that future service class use is at least somewhat related to service class use of the snapshot), historical data analysis (e.g., service class usage at certain times of day/days of the week), identification of trends, or the use of some other predictive technology.

[00288] In the example of FIG. 24, the differential network access control engine 2410 is coupled to the network service usage classification engine 2408. In a specific implementation, the network access control engine 2410 is implemented on a server, which may or may not be the same server on which the network traffic analysis engine 2406 and/or the network service usage

classification engine 2408 are implemented. However, at least a portion of the network access control engine 2410 can alternatively be implemented on the wireless device 2402-1, with or without a connection to a server that includes another portion (e.g., a server portion) of the network access control engine 2410.

[00289] The differential network access control engine 2410 uses the predicted service class use from the network service usage classification engine 2408 to dynamically adjust resources allocated to service classes. For example, the differential network access control engine 2410 can perform a service class availability assessment to determine whether service class capacity for service classes on a channel is sufficient for predicted service usage, and either add resources if service class availability is insufficient for predicted service usage or reduce resources if service class availability is more than sufficient for predicted service usage.

[00290] Alternatively, the differential network access control engine 2410 can instead or in addition control applications on devices such that the applications change service usage levels or delay consumption of wireless resources (e.g., by delaying software updates until more resources become available). In an embodiment, a service usage control policy is implemented on the wireless device 2402-1. This may be necessary in some cases to ensure the wireless device 2402-1 can adjust application settings that are normally fixed, optimize network service usage activation based on network state (e.g., if the network is busy), control over-the-air software updates, throttle resource-hungry applications, manage network service usage requests from repeated power down modes, keep PPP sessions active, or otherwise facilitate dynamic service class adjustments or other device behavior.

[00291] In a specific implementation, subscribers can be incented to change service classes by, for example, charging more for higher service classes. The differential network access control engine 2410 can send a notification of differential charges for service classes. Alternatively, the charges could be implemented via subscriber account settings or preferences.

[00292] In the example of FIG. 24, in operation, the network traffic analysis engine 2406 analyzes traffic from one or more devices, including the wireless device 2402-1. The network service usage classification engine 2408 predicts the amount of resources needed for service classes, and the differential network access control engine 2410 dynamically allocates resources on an as-needed basis to adjust the service classes that are available to the one or more devices

and/or adjusts device behavior for a subset of the one or more devices or instructs a subset of the one or more devices to adjust device behavior such that the device consumes service class-specific resources in accordance with an access control policy appropriate for the resources allocated to the applicable service classes.

[00293] FIG. 25 depicts a diagram an example of a differential access control notification system 2500. In the example of FIG. 25, the system 2500 includes a network service usage analysis engine 2502, a network service usage classification engine 2504, a differential network access control engine 2506, a network service usage control policy datastore 2508, a network service usage notification engine 2510, a user interface 2512, and a service plan update engine 2514.

[00294] In the example of FIG. 25, the network service usage analysis engine 2502 analyzes network service usage activity. The analysis can include an analysis of traffic sent to or from a device, an application running on a device, a request for services, or other analysis that is informative of past, current, or future network service usage. For example, the network service usage activity can include an attempt to download or load an application onto the communications device, an attempt to execute the network service activity or the network service usage activity attempts to access the network, meeting or exceeding a network service usage threshold, satisfying a network service usage pre-condition, an update to a network capacity controlled service activity classification list, an update to a network capacity controlled services policy, and a network message is sent to the device triggering the notification, to name several by way of example. The analysis can occur on a non-WAP station, a WAP or base station, a server, or partly on one of these devices or some other device.

[00295] In the example of FIG. 25, the network service usage classification engine 2504 is coupled to the network service usage analysis engine 2502. The network service usage classification engine 2504 classifies the analyzed network service usage into one or more service classes. The classification can occur on a non-WAP station, a WAP or base station, a server, or partly on one of these devices or some other device.

[00296] In the example of FIG. 25, the differential network access control engine 2506 is coupled to the network service usage classification engine 2504. The differential network access control engine 2506 determines network access parameters using the service classes associated

with the network service usage activity and network service usage control policies stored in the network service usage control policy datastore 2508. The determination can occur on a non-WAP station, a WAP or base station, a server, or partly on one of these devices or some other device. The network service usage control policy datastore 2508 can be implemented on a wireless device, but it is also possible to maintain the datastore remotely relative to the device (e.g., on a server). In a specific implementation, even if the network service usage control policy datastore 2508 is maintained remotely relative to the wireless device, the wireless device will still have a network service usage control policy implemented.

[00297] A datastore can be implemented, for example, as software embodied in a physical computer-readable medium on a general- or specific-purpose machine, in firmware, in hardware, in a combination thereof, or in an applicable known or convenient device or system. Datastores in this paper are intended to include any organization of data, including tables, comma-separated values (CSV) files, traditional databases (e.g., SQL), or other applicable known or convenient organizational formats. Datastore-associated components, such as database interfaces, can be considered "part of" a datastore, part of some other system component, or a combination thereof, though the physical location and other characteristics of datastore-associated components is not critical for an understanding of the techniques described in this paper.

[00298] Datastores can include data structures. As used in this paper, a data structure is associated with a particular way of storing and organizing data in a computer so that it can be used efficiently within a given context. Data structures are generally based on the ability of a computer to fetch and store data at any place in its memory, specified by an address, a bit string that can be itself stored in memory and manipulated by the program. Thus some data structures are based on computing the addresses of data items with arithmetic operations; while other data structures are based on storing addresses of data items within the structure itself. Many data structures use both principles, sometimes combined in non-trivial ways. The implementation of a data structure usually entails writing a set of procedures that create and manipulate instances of that structure.

[00299] In the example of FIG. 25, the network service usage notification engine 2510 is coupled to the differential network access control engine 2506 and the network service usage control policy datastore 2508. The network service usage notification engine 2510 is configured

to generate a notification sufficient to indicate relevant access control information. For example, the notification could indicate what network service usage activities are network capacity controlled services, the type of network service policy in effect for one or more network capacity controlled services, that a network service activity belongs to a network capacity controlled services classification, that a service activity that is classified as network capacity controlled services classification can have the classification changed, that if the service class is changed for the network service activity that the associated network service usage charges will change, a service plan upgrade/downgrade offer, and an offer for a service plan that provides discounts and/or incentives for responding to one or more user notifications for protecting network capacity, to name several by way of example.

[00300] The notification may or may not also include a user preference selection. For example, the notification could include a provision to associate a network service usage control policy with the network service usage activity, an over-ride option for selecting the network service usage control policy, a modify option to select the service usage control policy, and a select option to select a new service plan, to name several by way of example. Other examples include network service usage activity information for one or more network capacity controlled services, predicted network service usage activity information for one or more network capacity controlled services, an option for obtaining more information about the network service usage of the network service usage activity, a message that the network service usage activity may result in network service usage that exceeds a threshold for a service plan associated with the device, an option to review or select an alternative service plan, an acknowledgement request, and an option to submit the acknowledgement request, to name several more by way of example.

[00301] In the example of FIG. 25, the user interface 2512 is coupled to the network service usage notification engine 2510. It may be noted that notifications can be disposed of by consulting user preferences (e.g., when a user indicates that maximum performance or minimum cost should be automatically selected). However, unless subscriber preferences are set as a default, a user is likely to have notifications displayed in the UI 2512. The notification can be in an applicable known or convenient form, such as SMS, email, a popup window, or the like. To the extent a response is permitted, a user can input a response to the notification using an input device (not shown).

[00302] In the example of FIG. 25, the service plan update engine 2514 is coupled to the UI 2512. As was previously mentioned, the UI can be bypassed because of, e.g., user preferences that are determinative of a selection provided in the notification. Regardless of how the selection associated with the notification is made, the service plan update engine 2514 can update a service plan, network service usage control policy, user preferences, or other parameters in accordance with the selection. The service plan update engine 2514 can also update accounting if costs accrue.

[00303] FIG. 26 depicts an example of a computer system 2600 on which techniques described in this paper can be implemented. The computer system 2600 may be a conventional computer system that can be used as a client computer system, such as a wireless client or a workstation, or a server computer system. The computer system 2600 includes a computer 2602, I/O devices 2604, and a display device 2606. The computer 2602 includes a processor 2608, a communications interface 2610, memory 2612, display controller 2614, non-volatile storage 2616, and I/O controller 2618. The computer 2602 may be coupled to or include the I/O devices 2604 and display device 2606.

[00304] The computer 2602 interfaces to external systems through the communications interface 2610, which may include a modem or network interface. It will be appreciated that the communications interface 2610 can be considered to be part of the computer system 2600 or a part of the computer 2602. The communications interface 2610 can be an analog modem, ISDN modem, cable modem, token ring interface, satellite transmission interface (e.g., "direct PC"), or other interfaces for coupling a computer system to other computer systems.

[00305] The processor 2608 may be, for example, a conventional microprocessor such as an Intel Pentium microprocessor or Motorola power PC microprocessor. The memory 2612 is coupled to the processor 2608 by a bus 2670. The memory 2612 can be Dynamic Random Access Memory (DRAM) and can also include Static RAM (SRAM). The bus 2670 couples the processor 2608 to the memory 2612, also to the non-volatile storage 2616, to the display controller 2614, and to the I/O controller 2618.

[00306] The I/O devices 2604 can include a keyboard, disk drives, printers, a scanner, and other input and output devices, including a mouse or other pointing device. The display controller 2614 may control in the conventional manner a display on the display device 2606, which can

be, for example, a cathode ray tube (CRT) or liquid crystal display (LCD). The display controller 2614 and the I/O controller 2618 can be implemented with conventional well known technology.

[00307] The non-volatile storage 2616 is often a magnetic hard disk, an optical disk, or another form of storage for large amounts of data. Some of this data is often written, by a direct memory access process, into memory 2612 during execution of software in the computer 2602. One of skill in the art will immediately recognize that the terms "machine-readable medium" or "computer-readable medium" includes any type of storage device that is accessible by the processor 2608 and also encompasses a carrier wave that encodes a data signal.

[00308] The computer system 2600 is one example of many possible computer systems which have different architectures. For example, personal computers based on an Intel microprocessor often have multiple buses, one of which can be an I/O bus for the peripherals and one that directly connects the processor 2608 and the memory 2612 (often referred to as a memory bus). The buses are connected together through bridge components that perform any necessary translation due to differing bus protocols.

[00309] Network computers are another type of computer system that can be used in conjunction with the teachings provided herein. Network computers do not usually include a hard disk or other mass storage, and the executable programs are loaded from a network connection into the memory 2612 for execution by the processor 2608. A Web TV system, which is known in the art, is also considered to be a computer system, but it may lack some of the features shown in FIG. 26, such as certain input or output devices. A typical computer system will usually include at least a processor, memory, and a bus coupling the memory to the processor.

[00310] In addition, the computer system 2600 is controlled by operating system software which includes a file management system, such as a disk operating system, which is part of the operating system software. One example of operating system software with its associated file management system software is the family of operating systems known as Windows® from Microsoft Corporation of Redmond, Washington, and their associated file management systems. Another example of operating system software with its associated file management system software is the Linux operating system and its associated file management system. The file

management system is typically stored in the non-volatile storage 2616 and causes the processor 2608 to execute the various acts required by the operating system to input and output data and to store data in memory, including storing files on the non-volatile storage 2616.

[00311] FIG. 27 depicts a diagram of an example of a system 2700 for application-specific differential network access control. In the example of FIG. 27, the system 2700 includes a network service consuming application 2702, a network service usage analysis engine 2704, an application behavior datastore 2706, a network service usage classification engine 7708, an application traffic prioritization engine 2710, a network service usage control policy datastore 2712, a differential network access control engine 2714, an application traffic cache 2716, an application traffic override engine 2718, and a network interface 2720. The system 2700 is intended to represent a specific implementation of techniques described previously in this paper for illustrative purposes. The techniques may be applicable to an applicable known or convenient (wired or wireless) device for which there is a motivation to control network service usage.

[00312] In the example of FIG. 27, the network service consuming application 2702 is a application that is implemented on a device. In an expected use, the application is a software application stored at least in part in memory on a wireless device, though kernel-level instructions could be implemented as firmware or even hardware. The application can be referred to as "running" on the device or as being "executed" by the device in accordance with known uses of those terms. Wireless media are known to have more bandwidth constraints, which is why a wireless device is an expected use, though the technique may be applicable to wired devices in certain situations.

[00313] In the example of FIG. 27, the network service usage analysis engine 2704 is coupled to the network service consuming application 2702. The network service usage analysis engine 2704 analyzes traffic from the network service consuming application 2702 and stores relevant data in the application behavior datastore 2706. The data can include all traffic that is sent by the application, or a subset of the traffic (e.g., that which has a certain QoS classification or priority, that which has high resource consumption due to frequent transmission from the application, that which is sent to a particular destination, etc.) The data can also include traffic that is received for the application. The application behavior datastore 2706 can alternatively or in addition be

implemented as a traffic source/destination datastore, which can be valuable if differential access control is based upon the source and/or destination of traffic. The application behavior datastore 2706 includes data structures (e.g., records) representative of data that is organized with implementation-specific granularity. For example, the data structures could be representative of frames (L2), packets (L3), or messages. (It may be noted that the term "packets" is often used to mean collections of data that are not limited to L3.) The desired granularity may depend upon where the network service usage analysis engine 2704 is located. Whether the data structures are changed over time (e.g., to change data associated with a record), replaced as records age, or maintained as historical data is also implementation-specific.

[00314] In the example of FIG. 27, the network service usage classification engine 2708 is coupled to the network service usage analysis engine 2704 and the application behavior datastore 2706. The network service usage classification engine 2708 can categorize the traffic stored in the application behavior datastore 2706 based on, e.g., network type, time of day, connection cost, whether home or roaming, network busy state, QoS, and whether the particular service usage activity is in foreground of user interaction or in the background of user interaction, or other characteristics that are obtained from network service usage analysis or through other means. Classification rules can include, for example, examining if one or more of the following has taken place within a specified period of time: user has interacted with the device, user has interacted with the service usage activity, user has picked up the device, service usage activity UI content is in the foreground of the device UI, audio or video information is being played by the service usage activity, a certain amount of data has been communicated by the service usage activity, service usage activity is or is not on a foreground or background service list. Rules that define which service usage activities to classify as, e.g., background service usage activities can be user-selected, set by a service provider, or through some other applicable means.

[00315] Advantageously, the network service usage analysis engine 2704 can examine a particular service usage activity and the network service usage classification engine 2708 can determine if the particular service usage activity fits a set of one or more classification rules that define the particular service usage activity as, e.g., a background service usage activity.

[00316] In the example of FIG. 27, the application traffic prioritization engine 2710 uses a policy stored in the network service usage control policy datastore 2712 to determine an

appropriate prioritization for traffic to and/or from the network service consuming application 2702. Prioritization can enable the system 2700 to fine-tune the amount of network resources consumed by the network service consuming application 2702, or the rate of network resource consumption. The control policy can require applications to throttle network resource consumption, prohibit the use of network resources by certain applications, etc.

[00317] Advantageously, the application traffic prioritization engine 2710 can determine a particular service usage activity has a particular characteristic, such as being a background service usage activity. This can involve checking whether a condition is satisfied.

[00318] In the example of FIG. 27, the differential network access control engine 2714 is coupled to the application traffic prioritization engine 2710 and the network service usage control policy datastore 2712. The differential network access control engine 2714 causes the network service consuming application 2702 traffic to be queued in the application traffic cache 2716. (If no throttling is required to follow the control policy, of course, the traffic need not be cached anywhere other than is typical, such as in an output buffer.) The application traffic cache 2716 is intended to represent a cache that is implemented on top of an output buffer or other standard caching device, and is used by the differential network access control engine 2714 to facilitate control over "rogue" applications, applications having anomalous behavior, or applications that must otherwise be controlled to conform with the control policy.

[00319] Advantageously, the differential network access control engine can restrict network access of a particular service usage activity when a condition is satisfied, such as when the service usage activity is a background activity.

[00320] In the example of FIG. 27, the application traffic override engine 2718 is coupled to the differential network access control engine 2714 and the application traffic cache 2716. The application traffic override engine 2718 enables a user or device to deviate from the control policy. Such deviation can be prompted by, for example, an incentive offer or a notification of cost.

[00321] In an illustrative example, the device 2700 blocks chatter for an application running in the background that is attempting to report device or user behavior. The application traffic prioritization engine 2710 determines that the chatter has zero priority, such that the network service consuming application 2702 is prevented from consuming any resources. The user can

be sent a notification by the application traffic override engine 2718 that their control policy prohibits the application from consuming network resources, but that the user can opt to deviate from the control policy if they are willing to pay for the consumed resources. If the user is willing to pay for the resources, traffic can be sent at a certain rate from the application traffic cache 2716 through the network interface 2720, or perhaps sent without using the application traffic cache 2716.

[00322] As another illustrative example, the device 2700 could identify application traffic as a software update. The differential network access control engine 2714 may determine that software updates can be received at a throttled rate (perhaps even slower than the lowest QoS categorization). The application traffic override engine 2718 can receive an indication from the user, from user preferences, service provider settings, or the like that the updates can ignore the control policy for a particular application (or for all applications).

[00323] Advantageously, the control policy can set up a priority to communicate cached elements, set minimum update frequencies, provide control policy overrides (typically for payment), or the like to fine-tune differential network access control policies. This can enable the system 2700 to encourage certain behavior, such as sending low QoS traffic when it is cheaper (e.g., when the network does not have a busy state, at historically low-use times of day, when on a certain type of network, such as Wi-Fi, as opposed to another, such as cellular, etc.).

[00324] Some portions of the detailed description are presented in terms of algorithms and symbolic representations of operations on data bits within a computer memory. These algorithmic descriptions and representations are the means used by those skilled in the data processing arts to most effectively convey the substance of their work to others skilled in the art. An algorithm is here, and generally, conceived to be a self-consistent sequence of operations leading to a desired result. The operations are those requiring physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical or magnetic signals capable of being stored, transferred, combined, compared, and otherwise manipulated. It has proven convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers, or the like.

[00325] It should be borne in mind, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to

these quantities. Unless specifically stated otherwise as apparent from the following discussion, it is appreciated that throughout the description, discussions utilizing terms such as "processing" or "computing" or "calculating" or "determining" or "displaying" or the like, refer to the action and processes of a computer system, or similar electronic computing device, that manipulates and transforms data represented as physical (electronic) quantities within the computer system's registers and memories into other data similarly represented as physical quantities within the computer system memories or registers or other such information storage, transmission or display devices.

[00326] The present invention, in some embodiments, also relates to apparatus for performing the operations herein. This apparatus may be specially constructed for the required purposes, or it may comprise a general purpose computer selectively activated or reconfigured by a computer program stored in the computer. Such a computer program may be stored in a computer readable storage medium, such as, but is not limited to, read-only memories (ROMs), random access memories (RAMs), EPROMs, EEPROMs, magnetic or optical cards, any type of disk including floppy disks, optical disks, CD-ROMs, and magnetic-optical disks, or any type of media suitable for storing electronic instructions, and each coupled to a computer system bus.

[00327] The algorithms and displays presented herein are not inherently related to any particular computer or other apparatus. Various general purpose systems may be used with programs in accordance with the teachings herein, or it may prove convenient to construct more specialized apparatus to perform the required method steps. The required structure for a variety of these systems will appear from the description below. In addition, the present invention is not described with reference to any particular programming language, and various embodiments may thus be implemented using a variety of programming languages.

[00328] 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.

CLAIMS

We claim:

1. A system, comprising:

a processor of a communications device configured to:

monitor a network service usage activity of the communications device in network communication;

classify the network service usage activity for differential network access control for protecting network capacity; and

associate the network service usage activity with a network service usage control policy based on a classification of the network service usage activity to facilitate differential network access control for protecting network capacity; and

a memory coupled to the processor and configured to provide the processor with instructions.

2. The system recited in claim 1, wherein the communications device is a mobile communications device, and the service includes one or more Internet based services, and wherein the mobile communications device includes one or more of the following: a mobile phone, a PDA, an eBook reader, a music device, an entertainment/gaming device, a computer, laptop, a net book, a tablet, and a home networking system.

3. The system recited in claim 1, wherein the processor of the communications device is further configured to:

implement differential network access for the network service usage activity for protecting network capacity; and

verify implementation of the differential network access for the network service usage activity.

4. The system recited in claim 1, wherein the processor of the communications device is further configured to:

implement differential network access for the network service usage activity for protecting network capacity using a verified service processor.

5. The system recited in claim 1, wherein the processor of the communications device is further configured to:

implement differential network access for the network service usage activity for protecting network capacity using an emulated network access API.

6. The system recited in claim 1, wherein the processor of the communications device is further configured to:

monitor the network service usage activity based on a service profile; and

determine that the network service usage activity is a network capacity controlled service based on the monitored use of the network service usage activity based on the service profile using a verified service processor.

7. The system recited in claim 1, wherein the processor of the communications device is further configured to:

determine if network access for the network service usage activity is authorized based on a service plan associated with the communications device, a network capacity controlled service priority level associated with the network service usage activity, and a network busy state.

8. The system recited in claim 1, wherein the processor is further configured to:

execute a router for dynamically managing one or more network capacity controlled services and/or QoS sessions for the communications device.

9. The system recited in claim 1, wherein the processor is further configured to:

execute a router for dynamically managing one or more network capacity controlled services and/or QoS sessions for the communications device; and

send network busy state information to a service controller, wherein the service controller provides a policy decision point for management for a plurality of communications devices in communication with one or more base stations.

10. The system recited in claim 1, wherein the processor is further configured to:

execute a router for dynamically managing one or more network capacity controlled services and/or QoS sessions for the communications device;

send network busy state information to a service controller, wherein the service controller provides a policy decision point for management for a plurality of communications devices in communication with one or more base stations; and

receive router traffic control instructions from the service controller, wherein the service controller provides the router traffic control instructions to assist in dynamically managing network capacity usage for the plurality of communications devices in communication with the one or more base stations for protecting network capacity of one or more access networks.

11. The system recited in claim 1, wherein the classifying is based on a current access network and/or the network service usage control policy is based on a current access network.

12. The system recited in claim 1, wherein classifying includes dynamically assigning a network capacity controlled services priority level based on a network busy state.

13. The system recited in claim 1, wherein classifying includes querying a network element for determining a network capacity controlled services classification and/or associating includes querying a network element for determining an association with the network service usage control policy.

14. The system recited in claim 1, wherein the network service usage control policy includes one or more of the following: block/allow settings, throttle settings, adaptive throttle settings, QoS class settings, packet error rate, jitter and delay settings, queue settings, and tag settings.

15. The system recited in claim 1, wherein the network service usage control policy includes traffic control policy filters.

16. The system recited in claim 1, wherein the network service usage control policy includes traffic control policy filters implemented as cascading filters.

17. The system recited in claim 1, wherein the network service usage control policy includes traffic control policy filters using a network busy state and/or a time of day as an index into a traffic control setting.

18. The system recited in claim 1, wherein the processor is further configured to:

differentially control the network service usage activity based on the network service usage control policy based on a network busy state, wherein the network service usage activity is classified as a network capacity controlled service.

19. The system recited in claim 1, wherein the processor is further configured to:

differentially control the network service usage activity based on the network service usage control policy based on a user input and/or a current access network, wherein the network service usage activity is classified as a network capacity controlled service.

20. The system recited in claim 1, wherein the processor is further configured to:

modify or replace a network stack interface of the communications device to provide for intercept or discontinuance of network access messaging for implementing traffic control for network capacity controlled services for protecting network capacity.

21. The system recited in claim 1, wherein the processor is further configured to:

store a network capacity controlled service list, wherein the network capacity controlled service list is periodically updated based on monitored network service usage activities.

22. A method, comprising:

monitoring a network service usage activity of the communications device in network communication;

classifying the network service usage activity for differential network access control for protecting network capacity; and

associating the network service usage activity with a network service usage control policy based on a classification of the network service usage activity to facilitate differential network access control for protecting network capacity.

23. A computer program product, the computer program product being embodied in a computer readable storage medium and comprising computer instructions for:

monitoring a network service usage activity of the communications device in network communication;

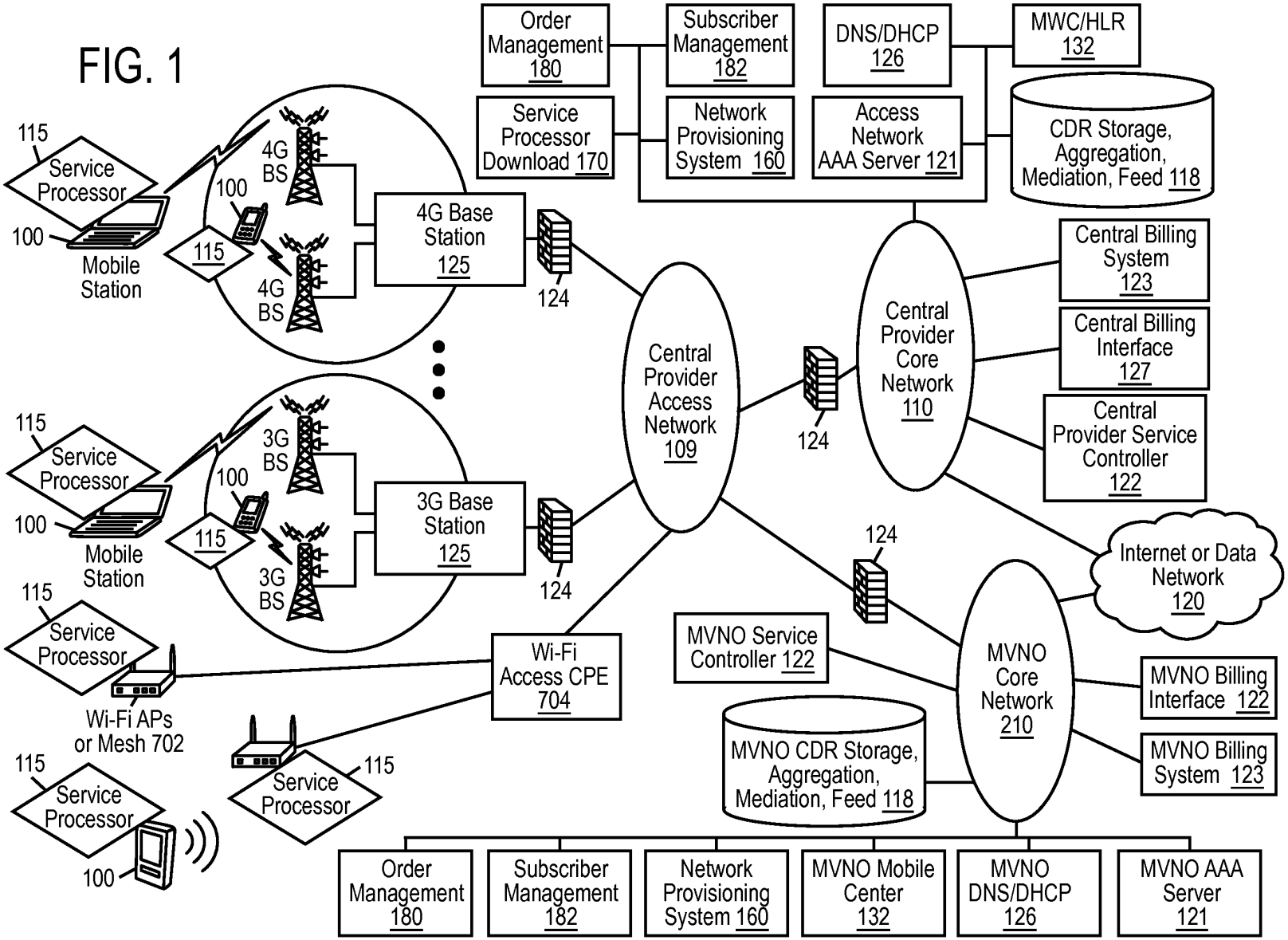
classifying the network service usage activity for differential network access control for protecting network capacity; and

associating the network service usage activity with a network service usage control policy based on a classification of the network service usage activity to facilitate differential network access control for protecting network capacity.

ABSTRACT

A system comprising a processor of a communications device configured to monitor a network service usage activity of the communications device in network communication, classify the network service usage activity for differential network access control for protecting network capacity, and associate the network service usage activity with a network service usage control policy based on a classification of the network service usage activity to facilitate differential network access control for protecting network capacity; and a memory coupled to the processor and configured to provide the processor with instructions.

FIG. 1


Order Management 180
Subscriber Management 182
DNS/DHCP 126
MWC/HLR 132
Service Processor Download 170
Network Provisioning System 160
Access Network AAA Server 121
CDR Storage, Aggregation, Mediation, Feed 118
115
Service Processor
100
Mobile Station
4G BS
100
115
4G BS
4G Base Station 125
124
Central Provider Access Network 109
Central Provider Core Network 110
Central Billing System 123
Central Billing Interface 127
Central Provider Service Controller 122
124
115
Service Processor
100
Mobile Station
3G BS
100
115
3G BS
3G Base Station 125
124
124
Internet or Data Network 120
115
Service Processor
Wi-Fi Access CPE 704
MVNO Service Controller 122
MVNO Core Network 210
MVNO Billing Interface 122
MVNO Billing System 123
Wi-Fi APs or Mesh 702
MVNO CDR Storage, Aggregation, Mediation, Feed 118
115
Service Processor
115
Service Processor
100
Order Management 180
Subscriber Management 182
Network Provisioning System 160
MVNO Mobile Center 132
MVNO DNS/DHCP 126
MVNO AAA Server 121

2566

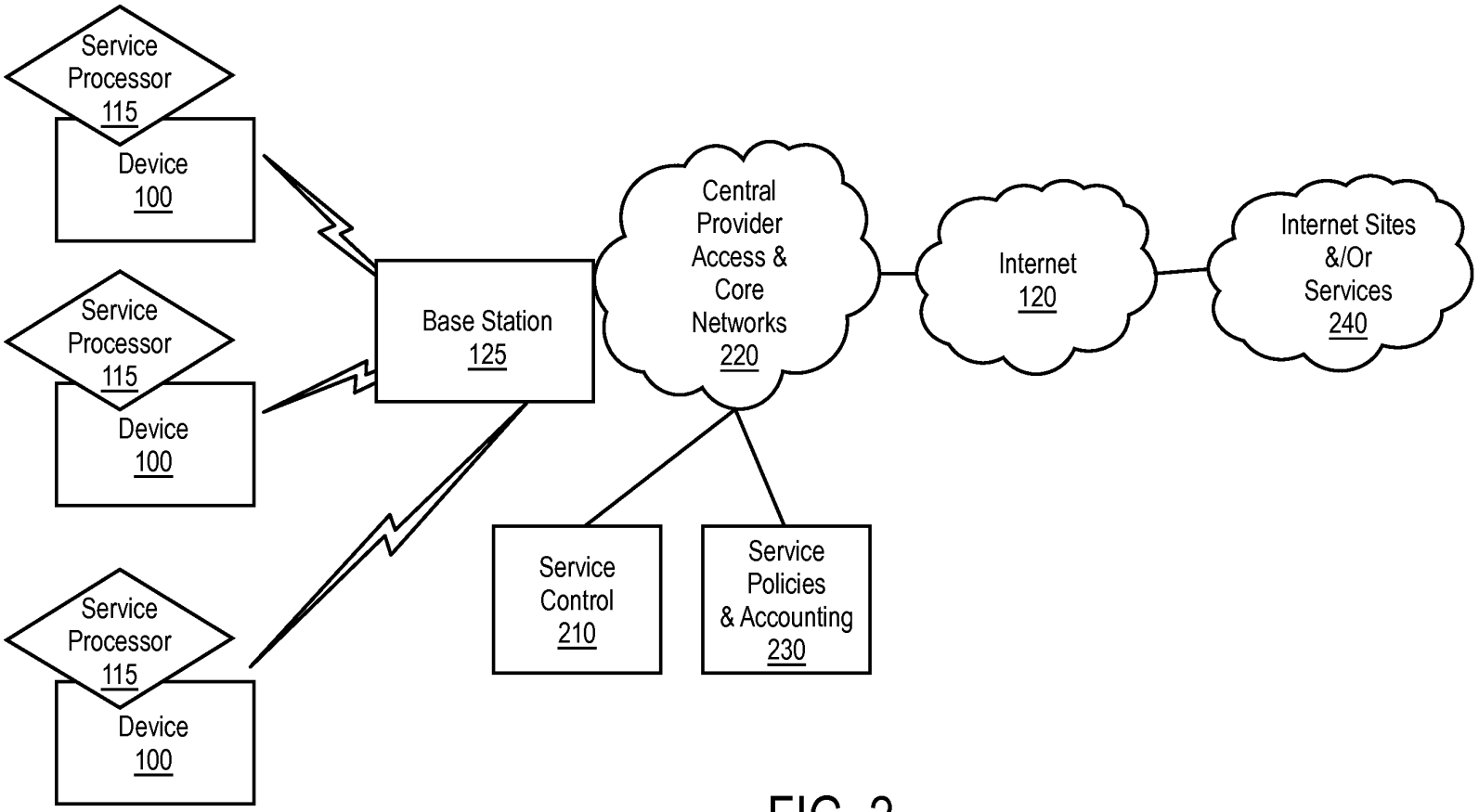

Service Processor 115
Device 100
Service Processor 115
Device 100
Service Processor 115
Device 100
Base Station 125
Central Provider Access & Core Networks 220
Internet 120
Internet Sites &/Or Services 240
Service Control 210
Service Policies & Accounting 230

FIG. 2

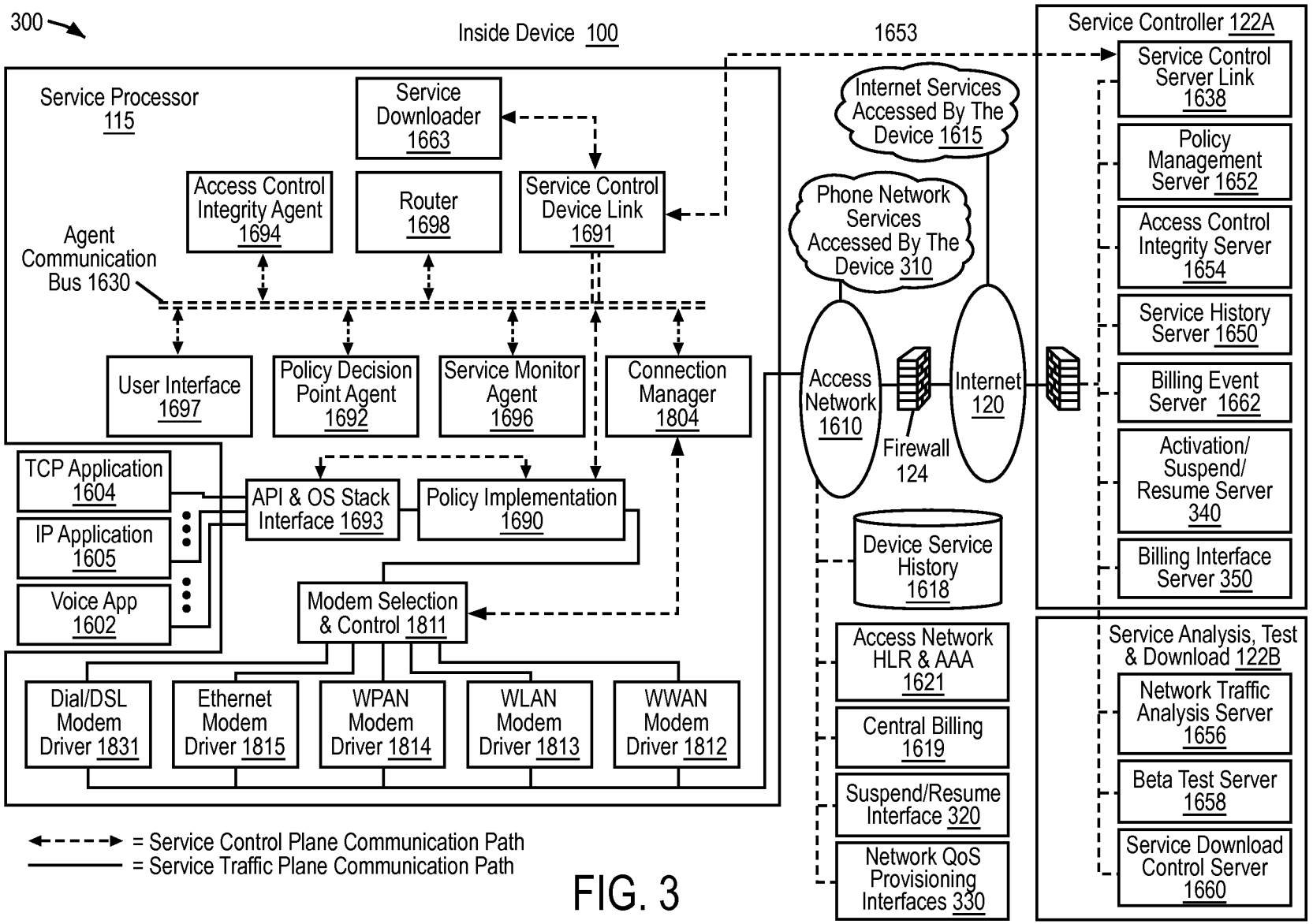

300
Inside Device 100
1653
Service Controller 122A
Service Processor 115
Service Downloader 1663
Access Control Integrity Agent 1694
Router 1698
Service Control Device Link 1691
Agent Communication Bus 1630
User Interface 1697
Policy Decision Point Agent 1692
Service Monitor Agent 1696
Connection Manager 1804
TCP Application 1604
IP Application 1605
Voice App 1602
API & OS Stack Interface 1693
Policy Implementation 1690
Modem Selection & Control 1811
Dial/DSL Modem Driver 1831
Ethernet Modem Driver 1815
WPAN Modem Driver 1814
WLAN Modem Driver 1813
WWAN Modem Driver 1812
Internet Services Accessed By The Device 1615
Phone Network Services Accessed By The Device 310
Access Network 1610
Firewall 124
Internet 120
Device Service History 1618
Access Network HLR & AAA 1621
Central Billing 1619
Suspend/Resume Interface 320
Network QoS Provisioning Interfaces 330
Service Control Server Link 1638
Policy Management Server 1652
Access Control Integrity Server 1654
Service History Server 1650
Billing Event Server 1662
Activation/ Suspend/ Resume Server 340
Billing Interface Server 350
Service Analysis, Test & Download 122B
Network Traffic Analysis Server 1656
Beta Test Server 1658
Service Download Control Server 1660
= Service Control Plane Communication Path
= Service Traffic Plane Communication Path

FIG. 3

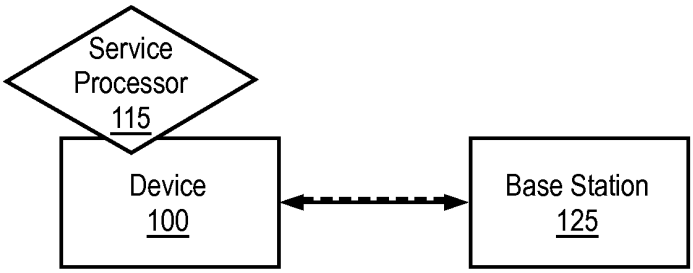


FIG. 4A

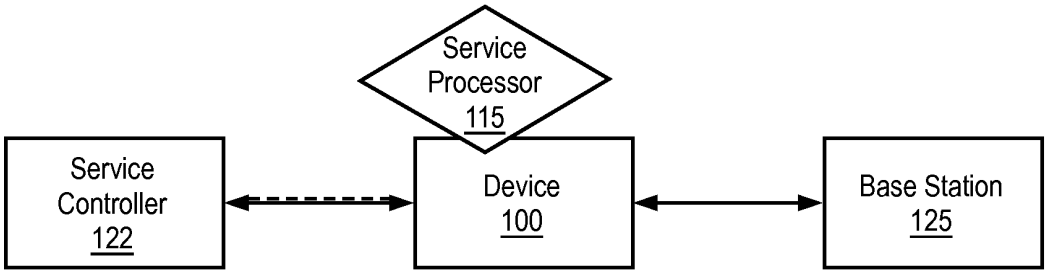


FIG. 4B

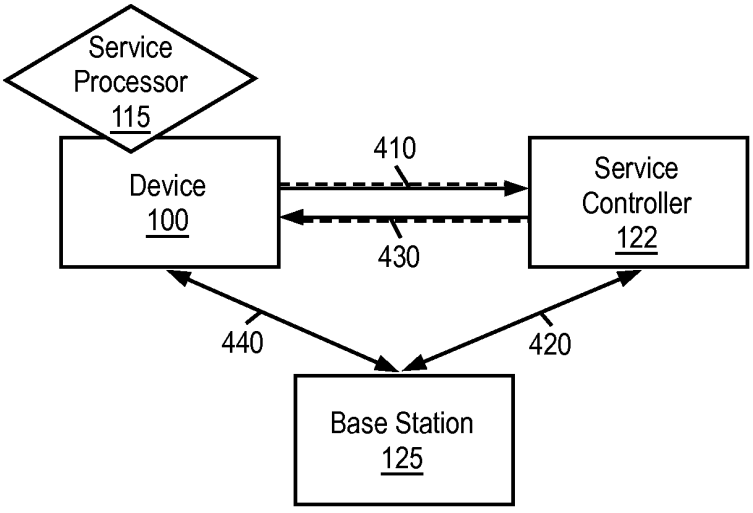


FIG. 4C

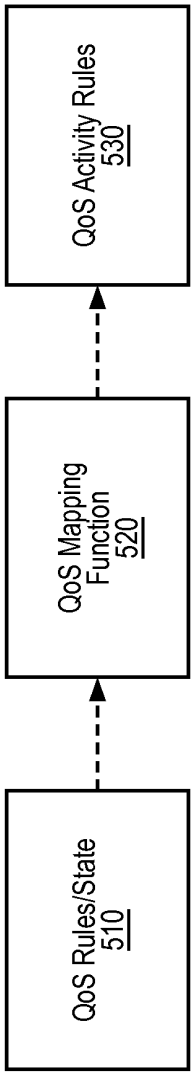

QoS Rules/State
510
QoS Mapping
Function
520
QoS Activity Rules
530

FIG. 5

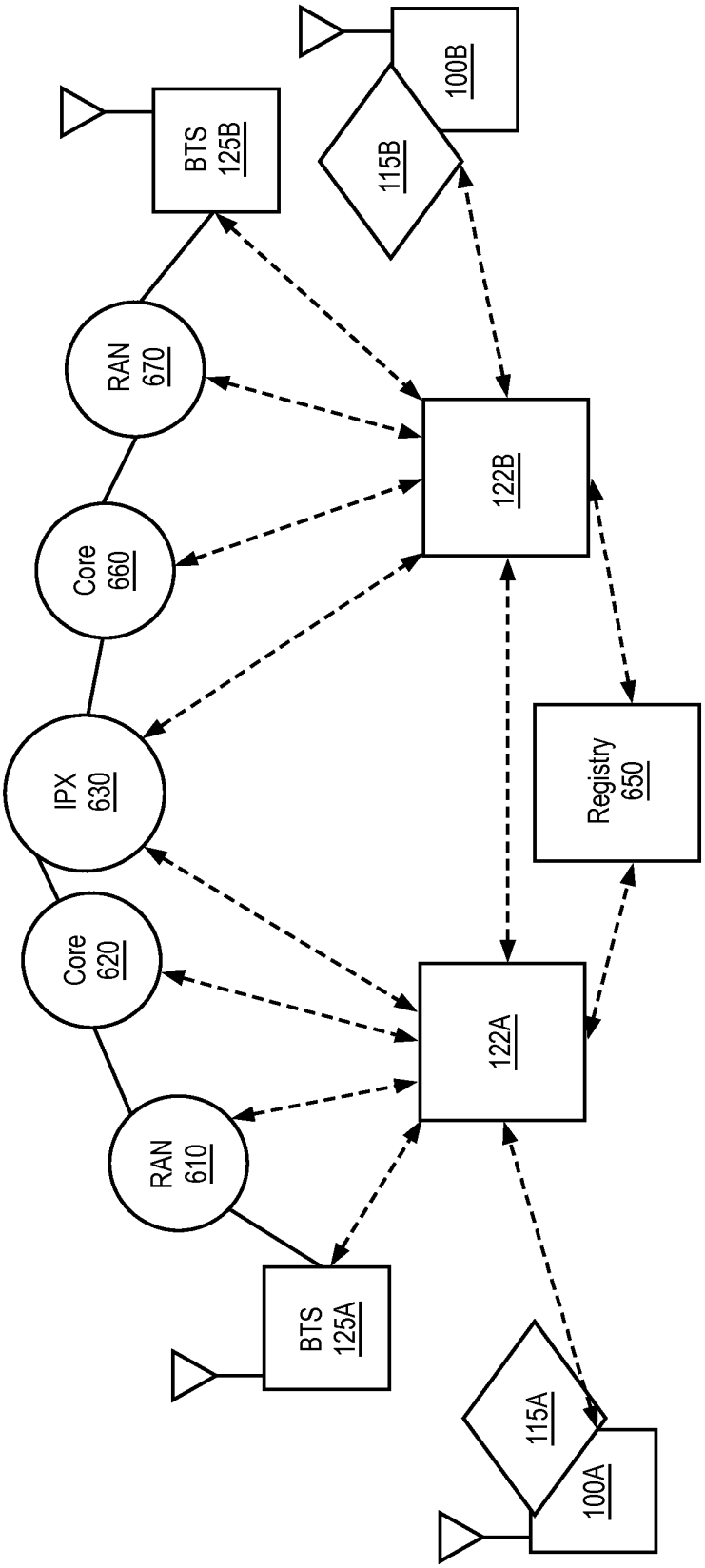

100B
115B
BTS 125B
RAN 670
Core 660
122B
IPX 630
Core 620
RAN 610
BTS 125A
122A
Registry 650
115A
100A

FIG. 6

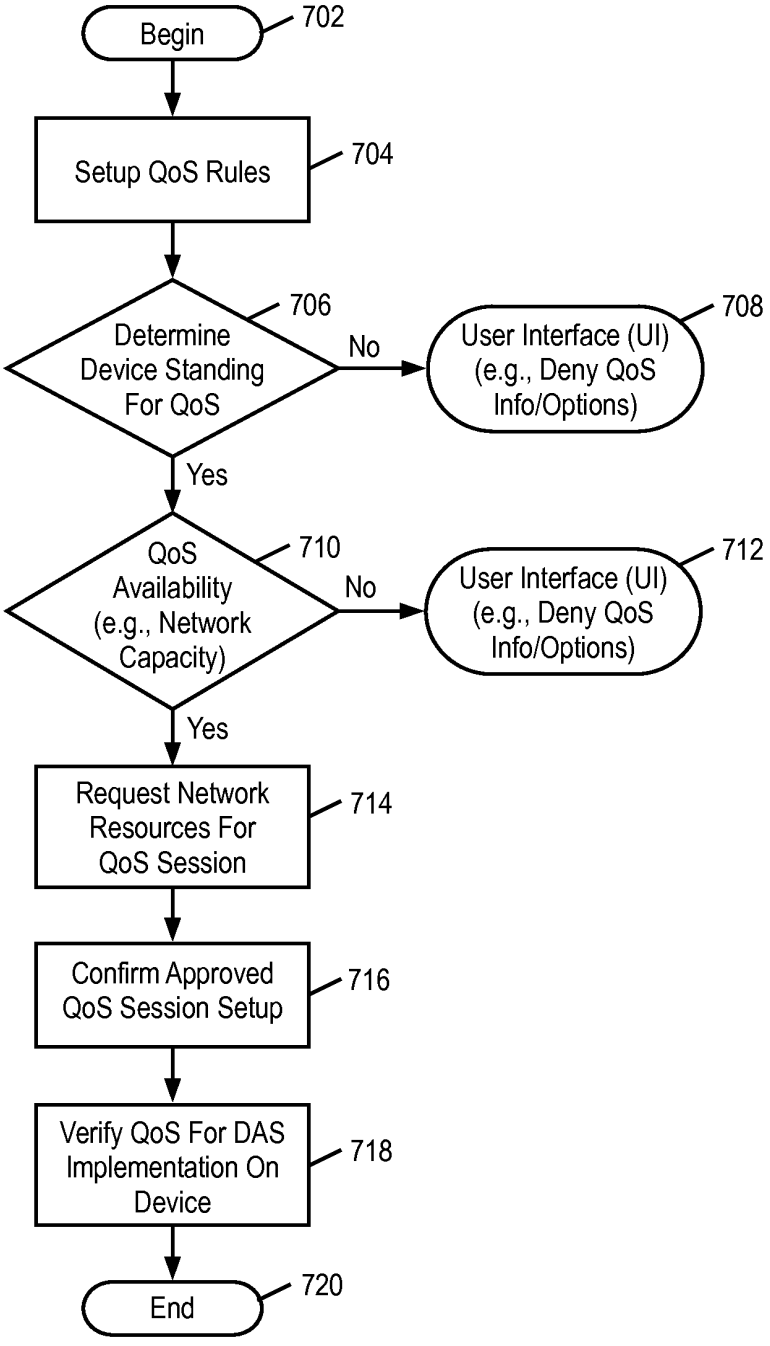

Begin
702
Setup QoS Rules
704
Determine Device Standing For QoS
706
No
User Interface (UI) (e.g., Deny QoS Info/Options)
708
Yes
QoS Availability (e.g., Network Capacity)
710
No
User Interface (UI) (e.g., Deny QoS Info/Options)
712
Yes
Request Network Resources For QoS Session
714
Confirm Approved QoS Session Setup
716
Verify QoS For DAS Implementation On Device
718
End
720

FIG. 7

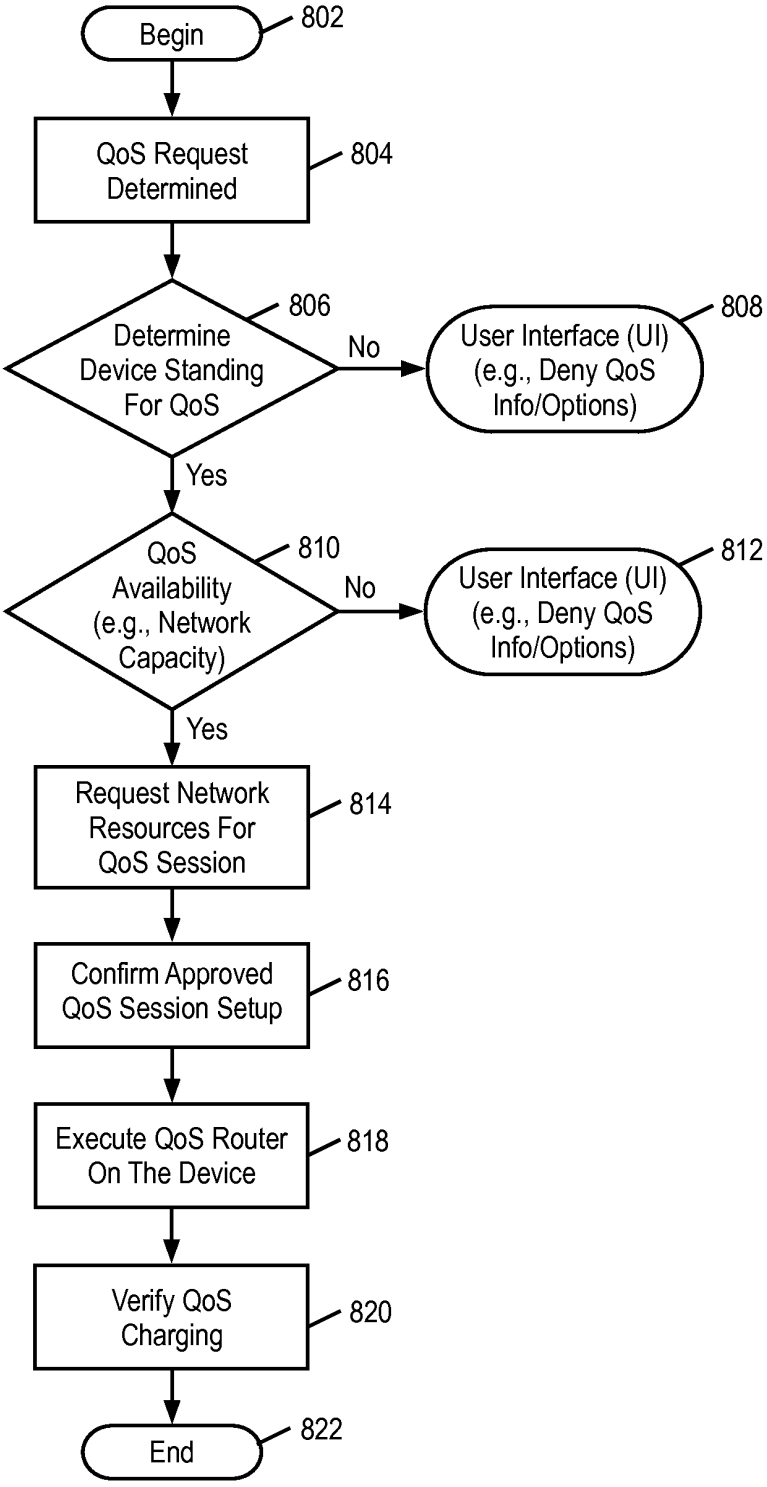

Begin
802
QoS Request Determined
804
Determine Device Standing For QoS
806
No
User Interface (UI) (e.g., Deny QoS Info/Options)
808
Yes
QoS Availability (e.g., Network Capacity)
810
No
User Interface (UI) (e.g., Deny QoS Info/Options)
812
Yes
Request Network Resources For QoS Session
814
Confirm Approved QoS Session Setup
816
Execute QoS Router On The Device
818
Verify QoS Charging
820
End
822

FIG. 8A

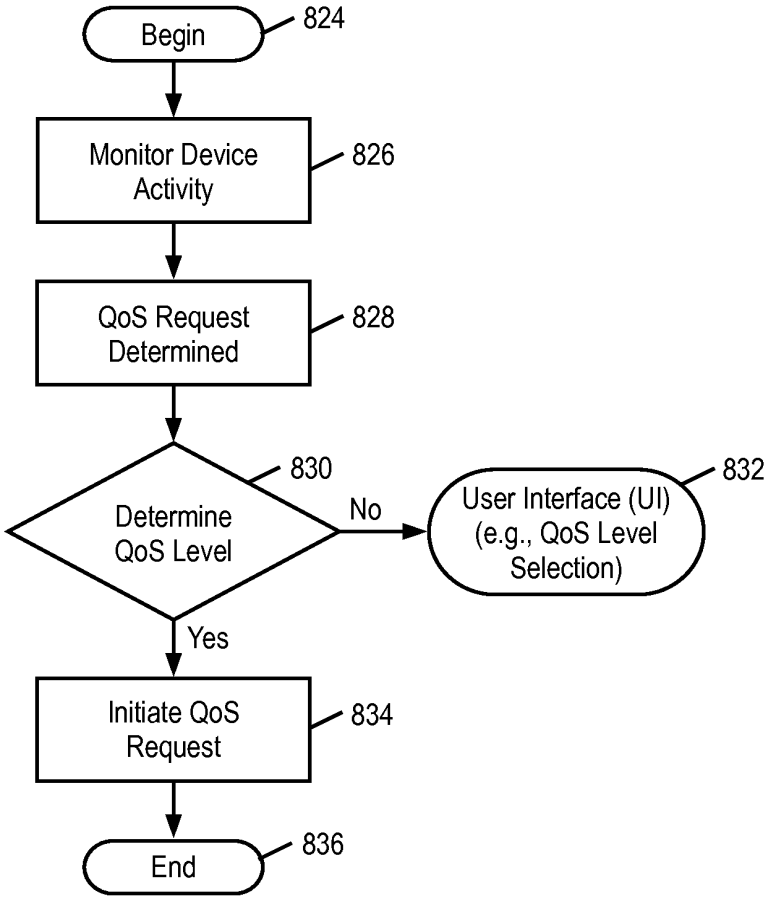

Begin
824
Monitor Device Activity
826
QoS Request Determined
828
Determine QoS Level
830
No
User Interface (UI) (e.g., QoS Level Selection)
832
Yes
Initiate QoS Request
834
End
836

FIG. 8B

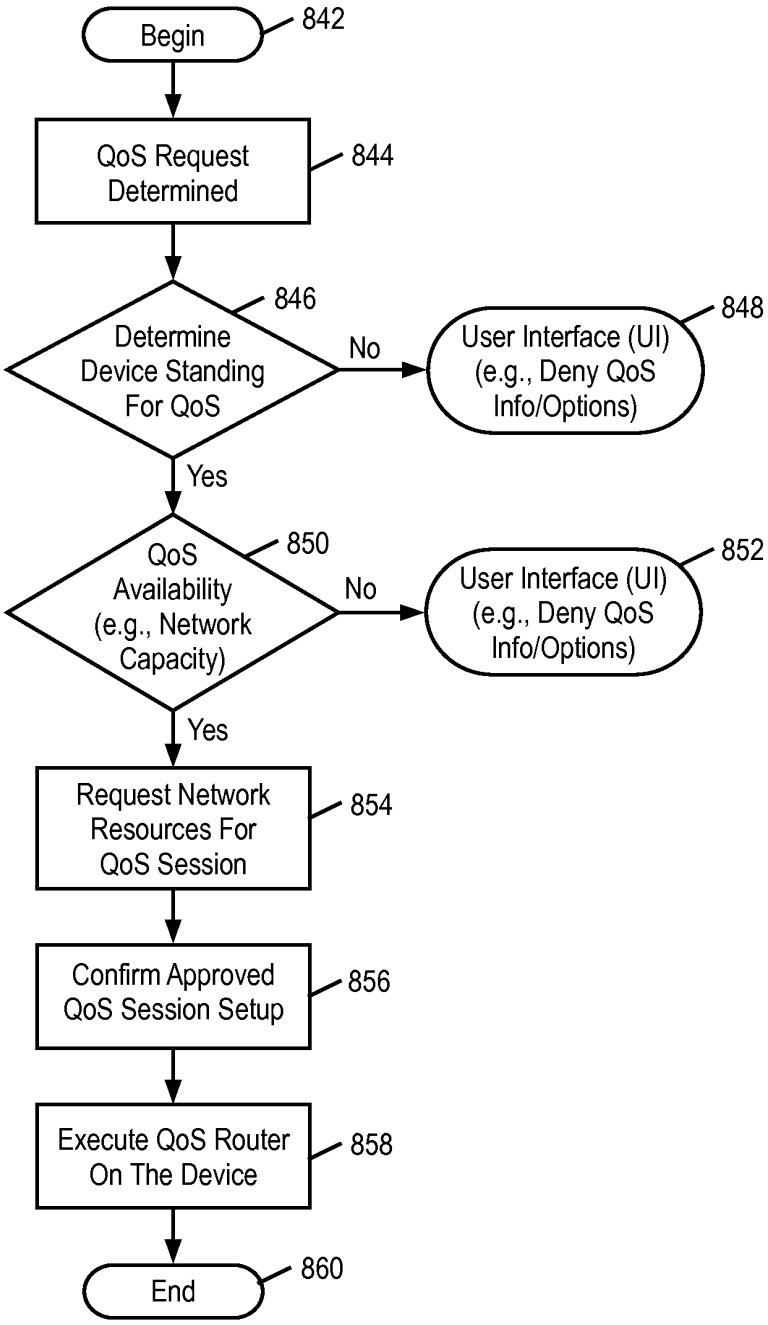

Begin
842
QoS Request Determined
844
Determine Device Standing For QoS
846
No
User Interface (UI) (e.g., Deny QoS Info/Options)
848
Yes
QoS Availability (e.g., Network Capacity)
850
No
User Interface (UI) (e.g., Deny QoS Info/Options)
852
Yes
Request Network Resources For QoS Session
854
Confirm Approved QoS Session Setup
856
Execute QoS Router On The Device
858
End
860

FIG. 8C

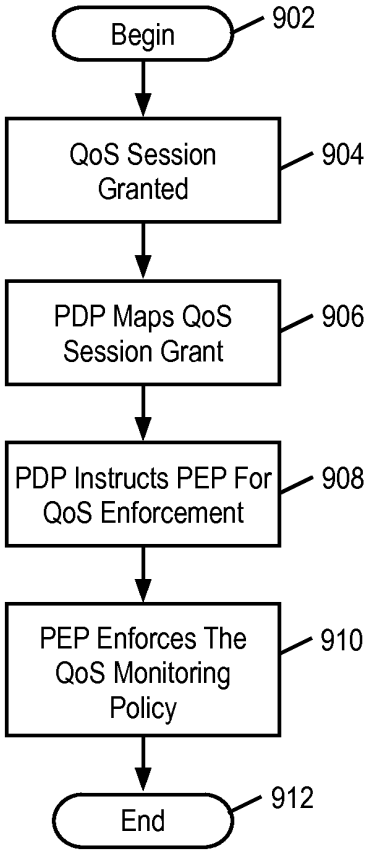

Begin
902
QoS Session Granted
904
PDP Maps QoS Session Grant
906
PDP Instructs PEP For QoS Enforcement
908
PEP Enforces The QoS Monitoring Policy
910
End
912

FIG. 9

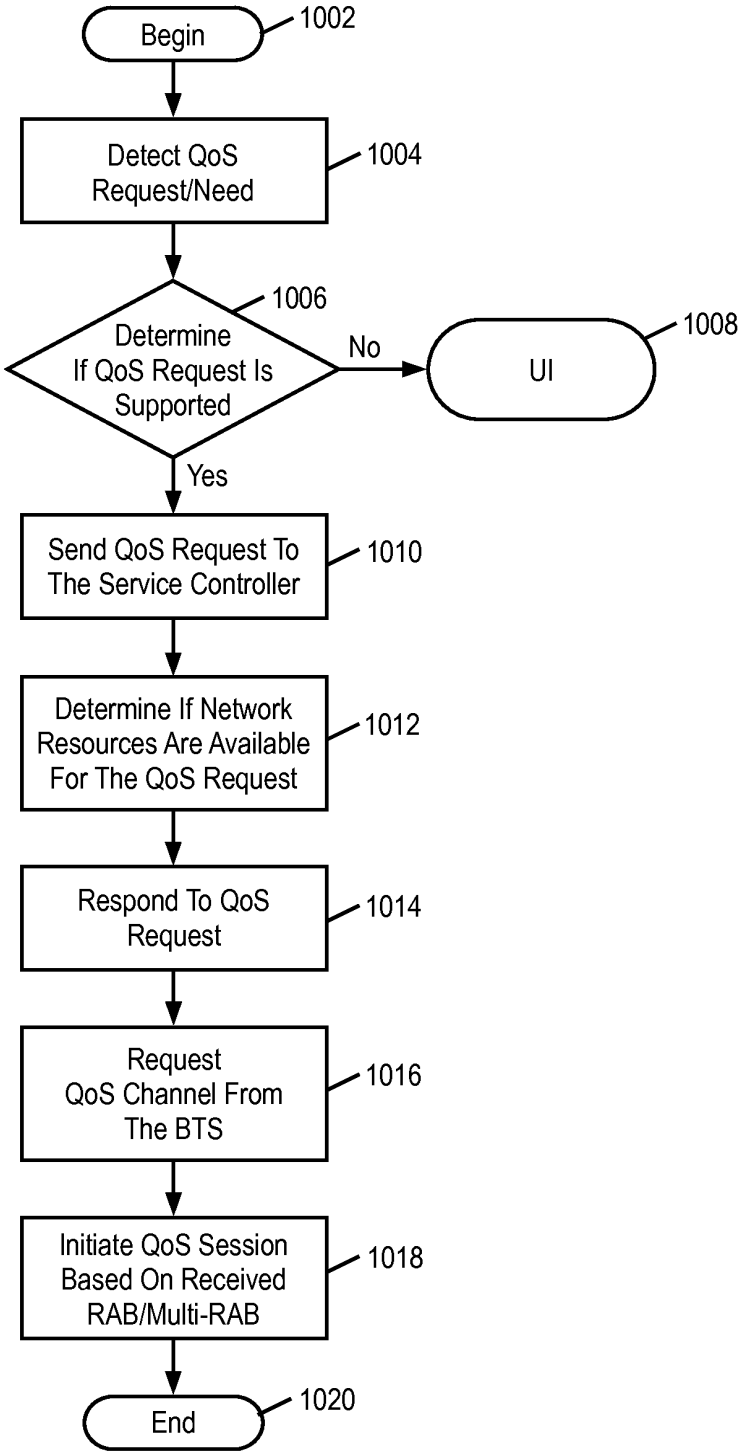

Begin
1002
Detect QoS Request/Need
1004
Determine If QoS Request Is Supported
1006
No
UI
1008
Yes
Send QoS Request To The Service Controller
1010
Determine If Network Resources Are Available For The QoS Request
1012
Respond To QoS Request
1014
Request QoS Channel From The BTS
1016
Initiate QoS Session Based On Received RAB/Multi-RAB
1018
End
1020

FIG. 10

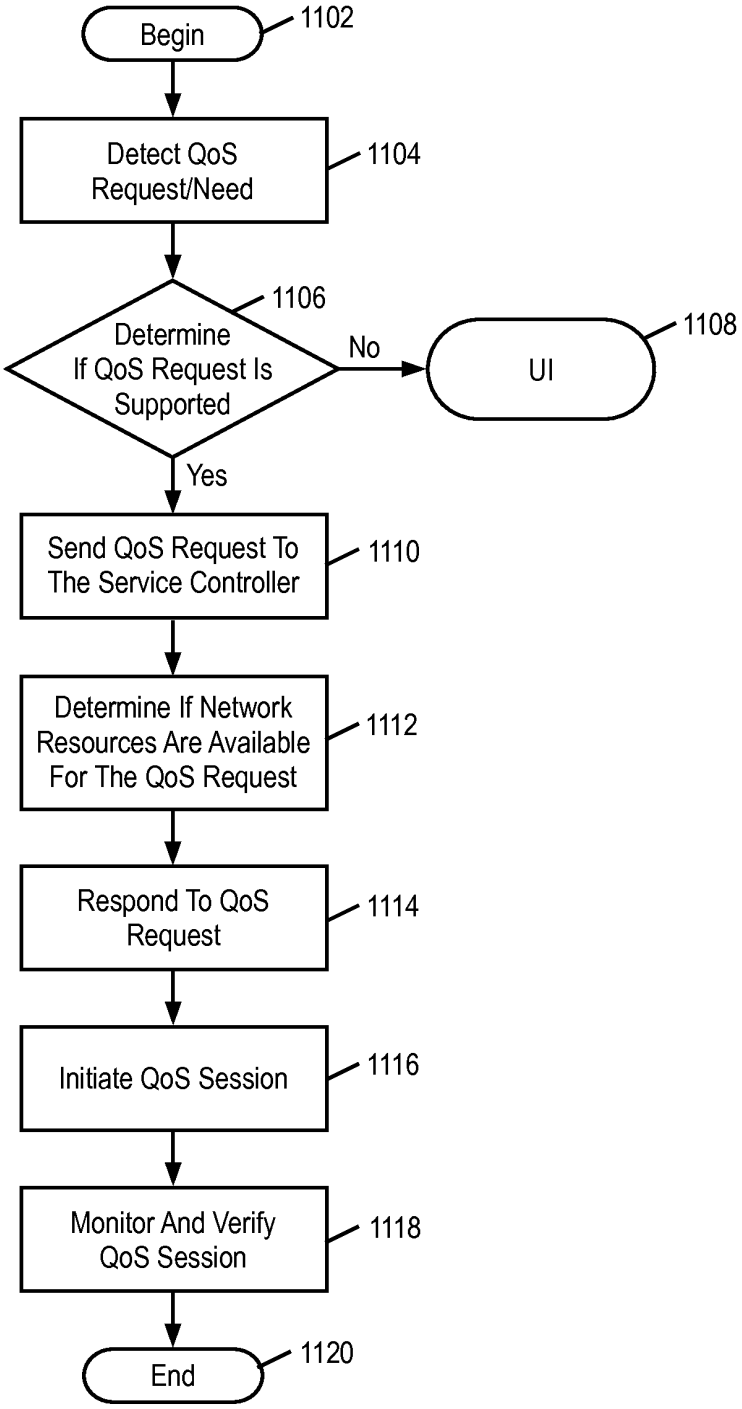

Begin
1102
Detect QoS Request/Need
1104
Determine If QoS Request Is Supported
1106
No
UI
1108
Yes
Send QoS Request To The Service Controller
1110
Determine If Network Resources Are Available For The QoS Request
1112
Respond To QoS Request
1114
Initiate QoS Session
1116
Monitor And Verify QoS Session
1118
End
1120

FIG. 11

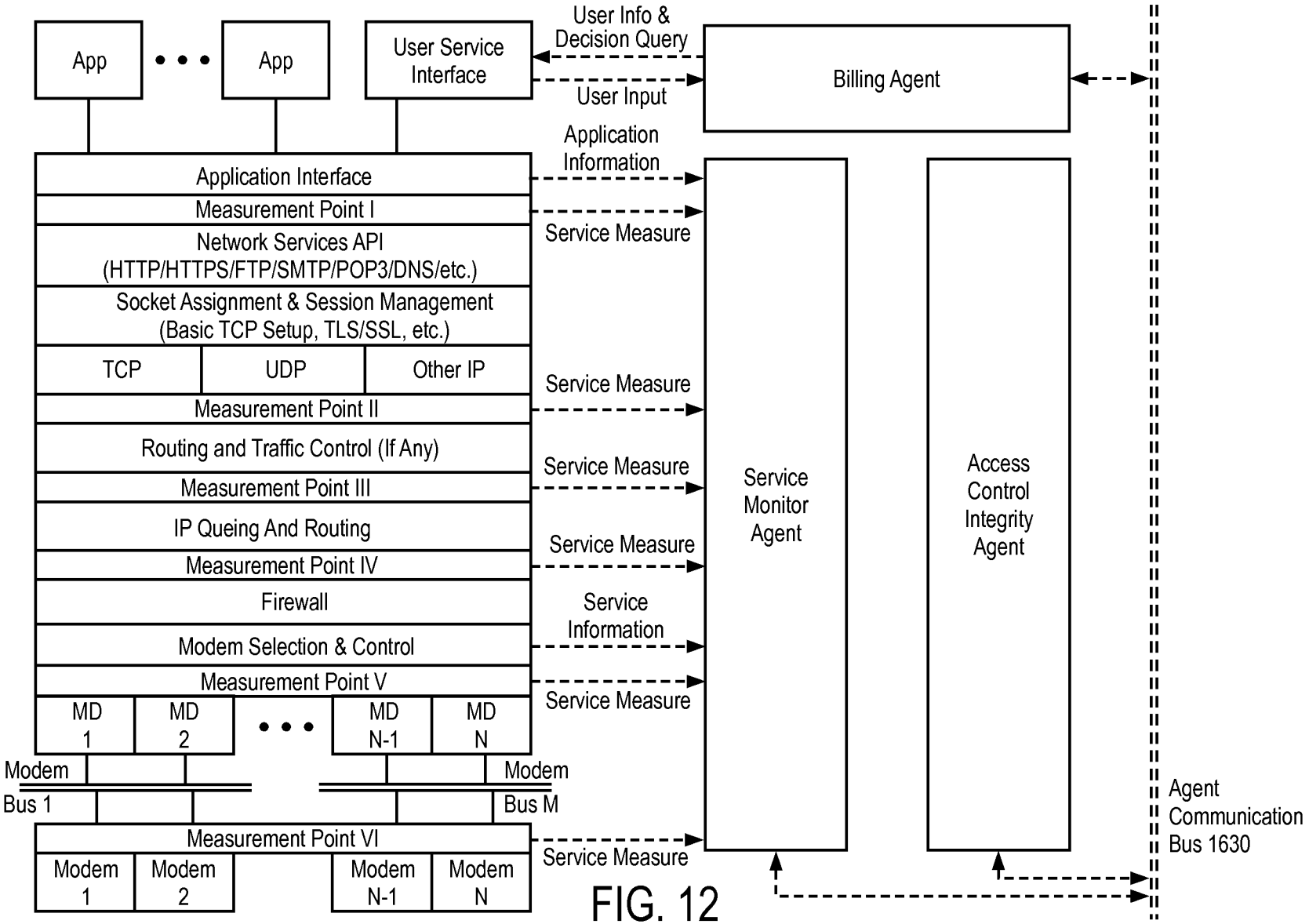

App
App
User Service Interface
User Info & Decision Query
User Input
Billing Agent
Application Information
Application Interface
Measurement Point I
Service Measure
Network Services API (HTTP/HTTPS/FTP/SMTP/POP3/DNS/etc.)
Socket Assignment & Session Management (Basic TCP Setup, TLS/SSL, etc.)
TCP
UDP
Other IP
Service Measure
Measurement Point II
Routing and Traffic Control (If Any)
Service Measure
Measurement Point III
IP Queing And Routing
Service Measure
Measurement Point IV
Firewall
Service Information
Modem Selection & Control
Measurement Point V
Service Measure
MD 1
MD 2
MD N-1
MD N
Modem
Modem
Bus 1
Bus M
Measurement Point VI
Service Measure
Modem 1
Modem 2
Modem N-1
Modem N
Service Monitor Agent
Access Control Integrity Agent
Agent Communication Bus 1630

FIG. 12

2579

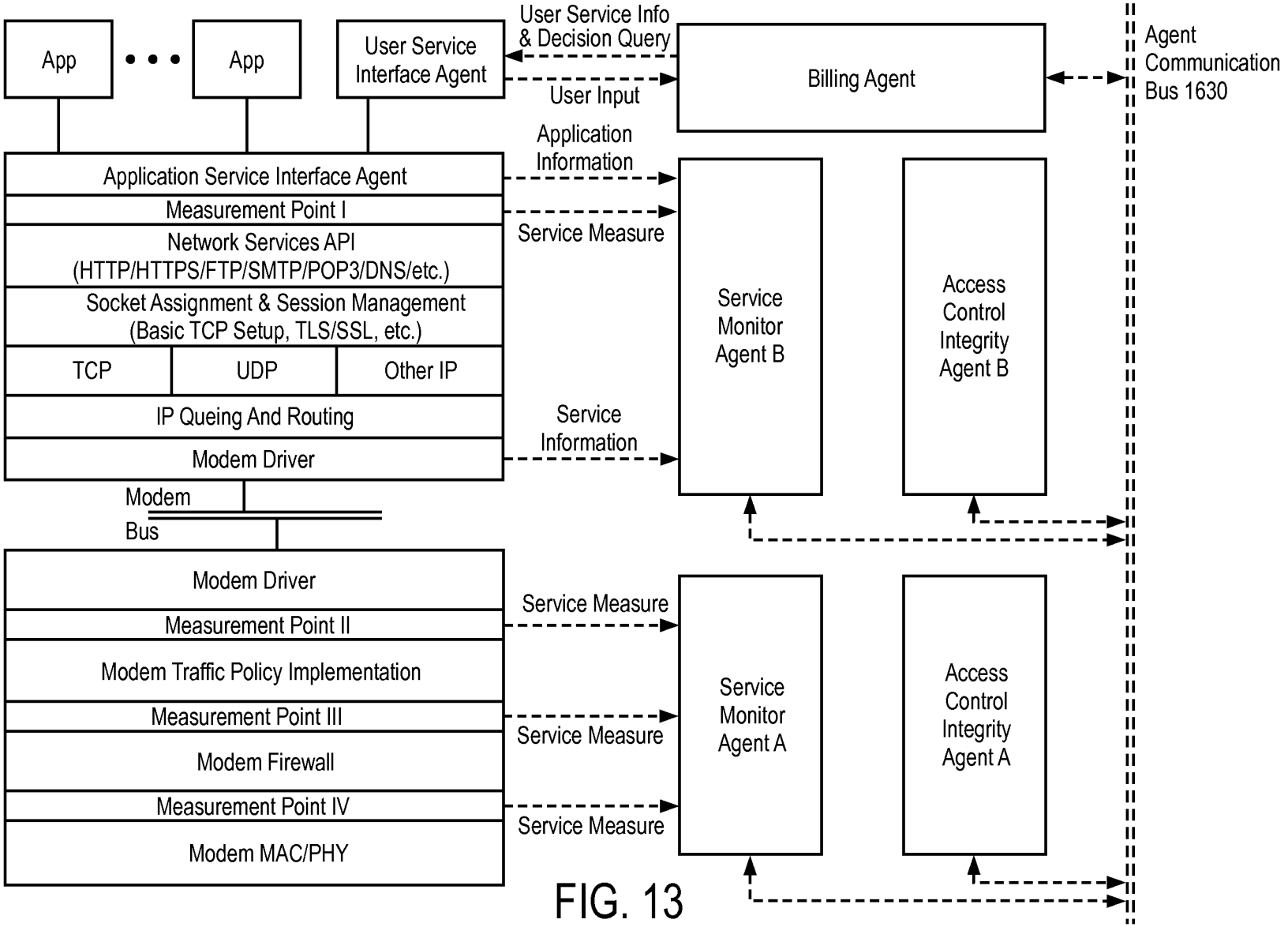

App
App
User Service Interface Agent
User Service Info & Decision Query
User Input
Billing Agent
Agent Communication Bus 1630
Application Information
Application Service Interface Agent
Measurement Point I
Service Measure
Network Services API (HTTP/HTTPS/FTP/SMTP/POP3/DNS/etc.)
Socket Assignment & Session Management (Basic TCP Setup, TLS/SSL, etc.)
TCP
UDP
Other IP
IP Queing And Routing
Service Information
Modem Driver
Service Monitor Agent B
Access Control Integrity Agent B
Modem Bus
Modem Driver
Service Measure
Measurement Point II
Modem Traffic Policy Implementation
Measurement Point III
Service Measure
Modem Firewall
Measurement Point IV
Service Measure
Modem MAC/PHY
Service Monitor Agent A
Access Control Integrity Agent A
2580

FIG. 13

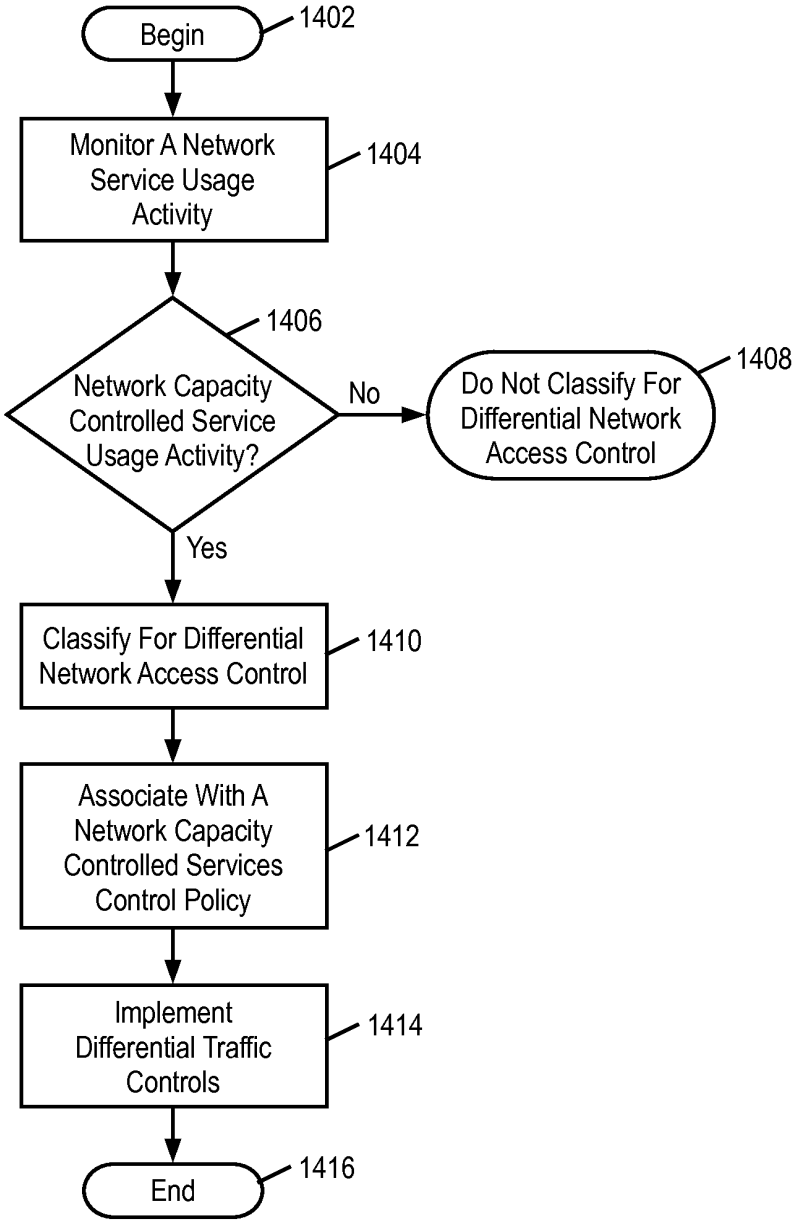

Begin
1402
Monitor A Network Service Usage Activity
1404
Network Capacity Controlled Service Usage Activity?
1406
No
Do Not Classify For Differential Network Access Control
1408
Yes
Classify For Differential Network Access Control
1410
Associate With A Network Capacity Controlled Services Control Policy
1412
Implement Differential Traffic Controls
1414
End
1416

FIG. 14

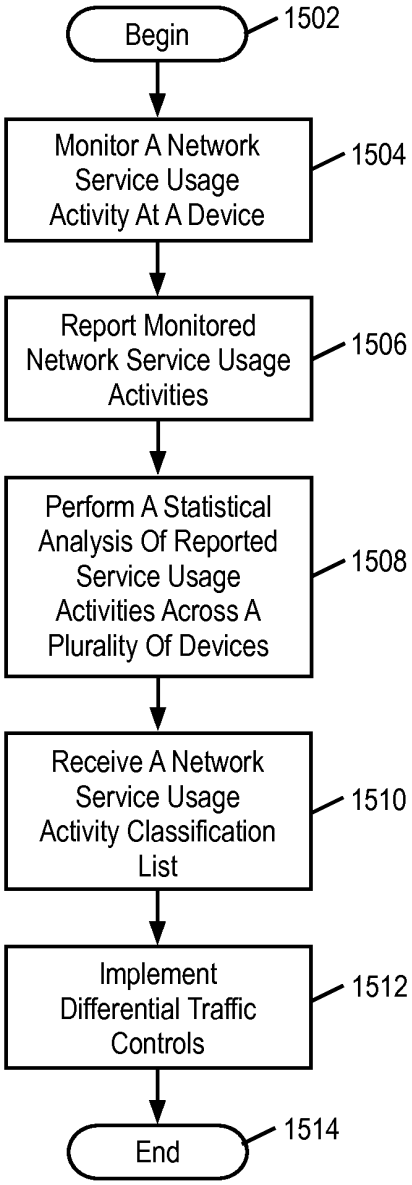

Begin
1502
Monitor A Network Service Usage Activity At A Device
1504
Report Monitored Network Service Usage Activities
1506
Perform A Statistical Analysis Of Reported Service Usage Activities Across A Plurality Of Devices
1508
Receive A Network Service Usage Activity Classification List
1510
Implement Differential Traffic Controls
1512
End
1514

FIG. 15

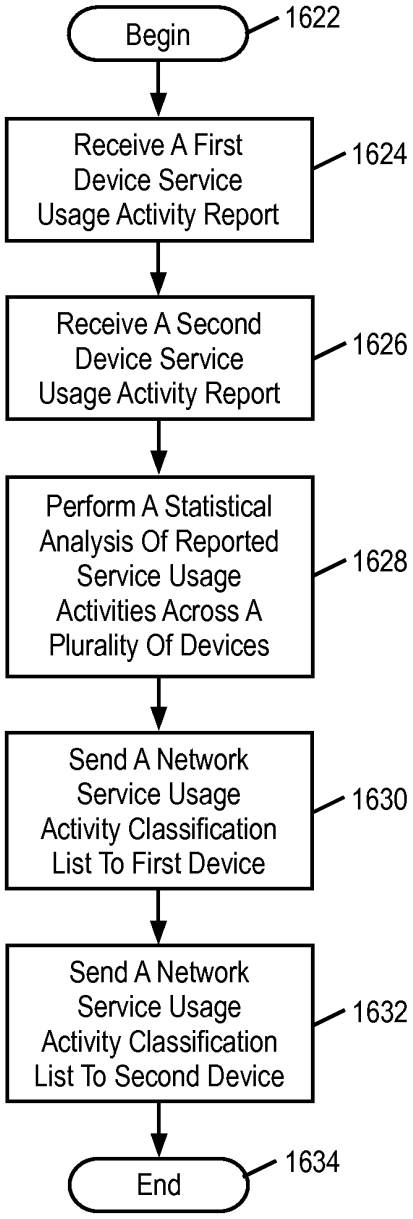

Begin
1622
Receive A First Device Service Usage Activity Report
1624
Receive A Second Device Service Usage Activity Report
1626
Perform A Statistical Analysis Of Reported Service Usage Activities Across A Plurality Of Devices
1628
Send A Network Service Usage Activity Classification List To First Device
1630
Send A Network Service Usage Activity Classification List To Second Device
1632
End
1634

FIG. 16

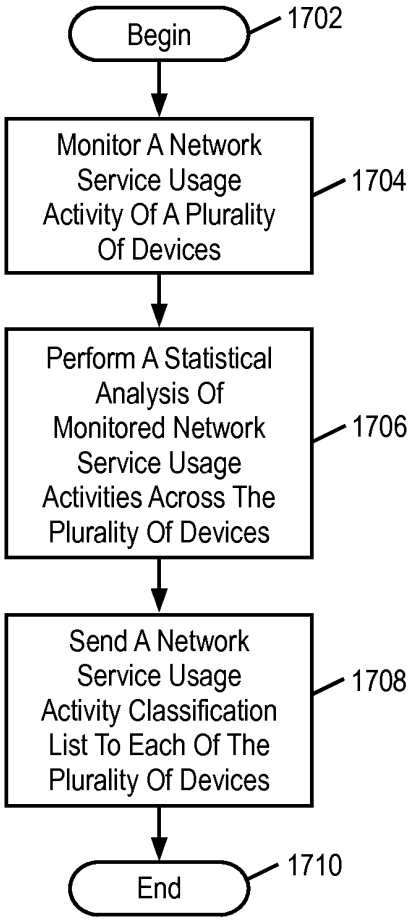

Begin
1702
Monitor A Network Service Usage Activity Of A Plurality Of Devices
1704
Perform A Statistical Analysis Of Monitored Network Service Usage Activities Across The Plurality Of Devices
1706
Send A Network Service Usage Activity Classification List To Each Of The Plurality Of Devices
1708
End
1710

FIG. 17

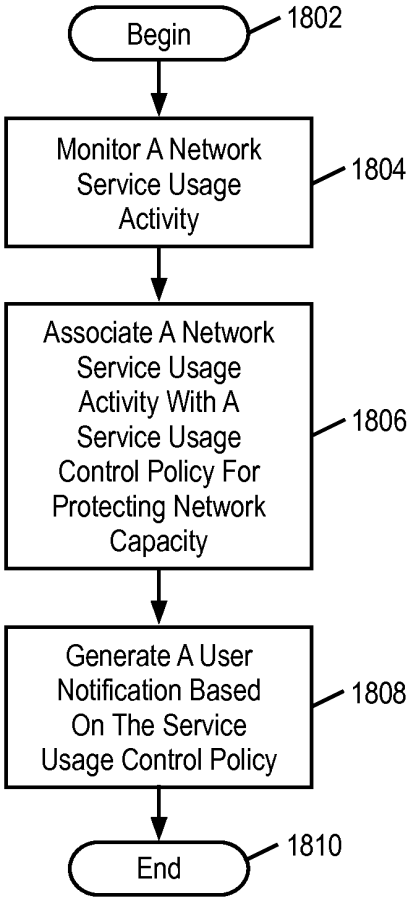

Begin
1802
Monitor A Network Service Usage Activity
1804
Associate A Network Service Usage Activity With A Service Usage Control Policy For Protecting Network Capacity
1806
Generate A User Notification Based On The Service Usage Control Policy
1808
End
1810

FIG. 18

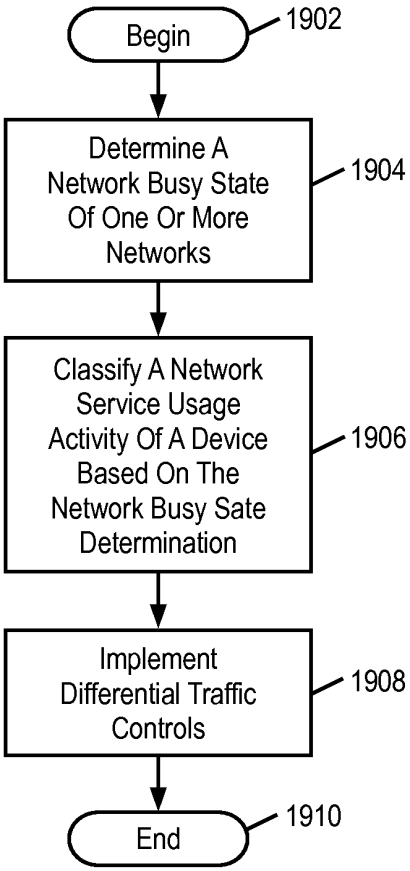

Begin
1902
Determine A Network Busy State Of One Or More Networks
1904
Classify A Network Service Usage Activity Of A Device Based On The Network Busy Sate Determination
1906
Implement Differential Traffic Controls
1908
End
1910

FIG. 19

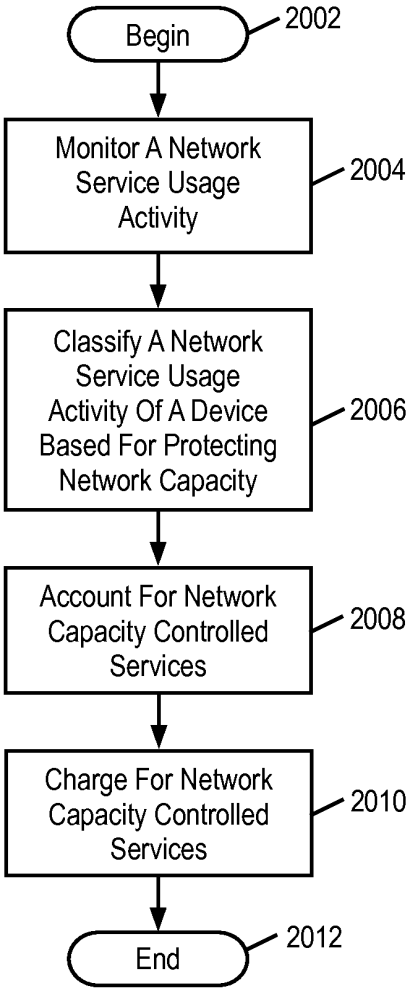

Begin
2002
Monitor A Network Service Usage Activity
2004
Classify A Network Service Usage Activity Of A Device Based For Protecting Network Capacity
2006
Account For Network Capacity Controlled Services
2008
Charge For Network Capacity Controlled Services
2010
End
2012

FIG. 20

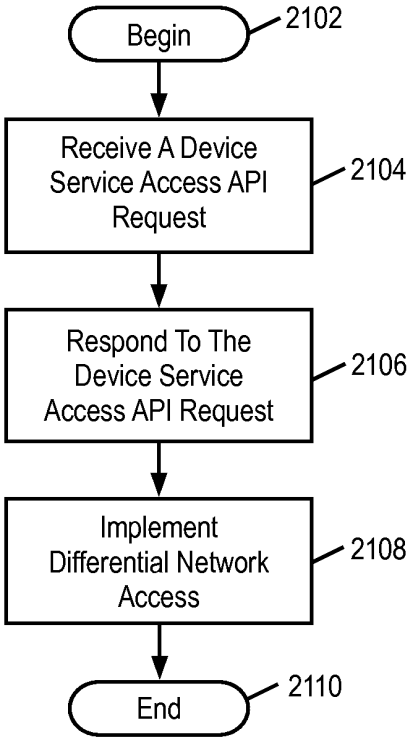

Begin
2102
Receive A Device Service Access API Request
2104
Respond To The Device Service Access API Request
2106
Implement Differential Network Access
2108
End
2110

FIG. 21

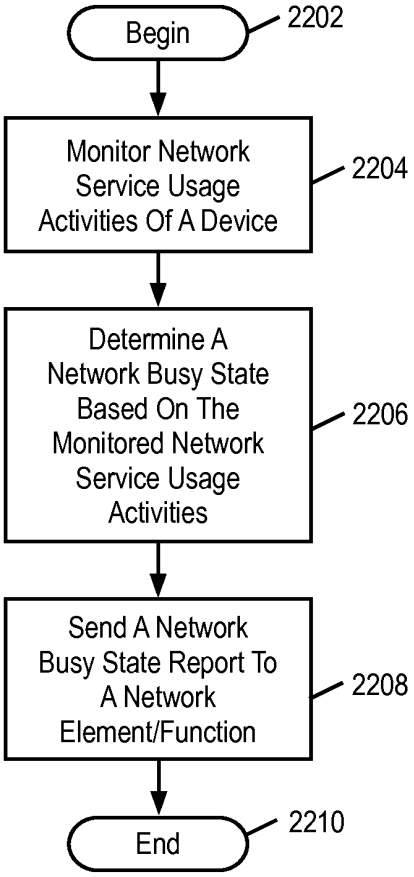

Begin
2202
Monitor Network Service Usage Activities Of A Device
2204
Determine A Network Busy State Based On The Monitored Network Service Usage Activities
2206
Send A Network Busy State Report To A Network Element/Function
2208
End
2210

FIG. 22

	NBS 10%	NBS 25%	NBS 50%	NBS 75%	NBS 90%
Outlook	6	5	4	3	2
Skype	7	6	2	1	0
Safari	5	4	3	2	1
Pandora	5	4	3	2	1
FaceBook	4	3	2	1	0
iTunes	7	6	3	1	0
QuickTime	8	6	4	1	0
AV Software	9	7	5	3	1
Online Backup	3	2	1	1	0
OS Update	2	1	0	0	0

2590

FIG. 23

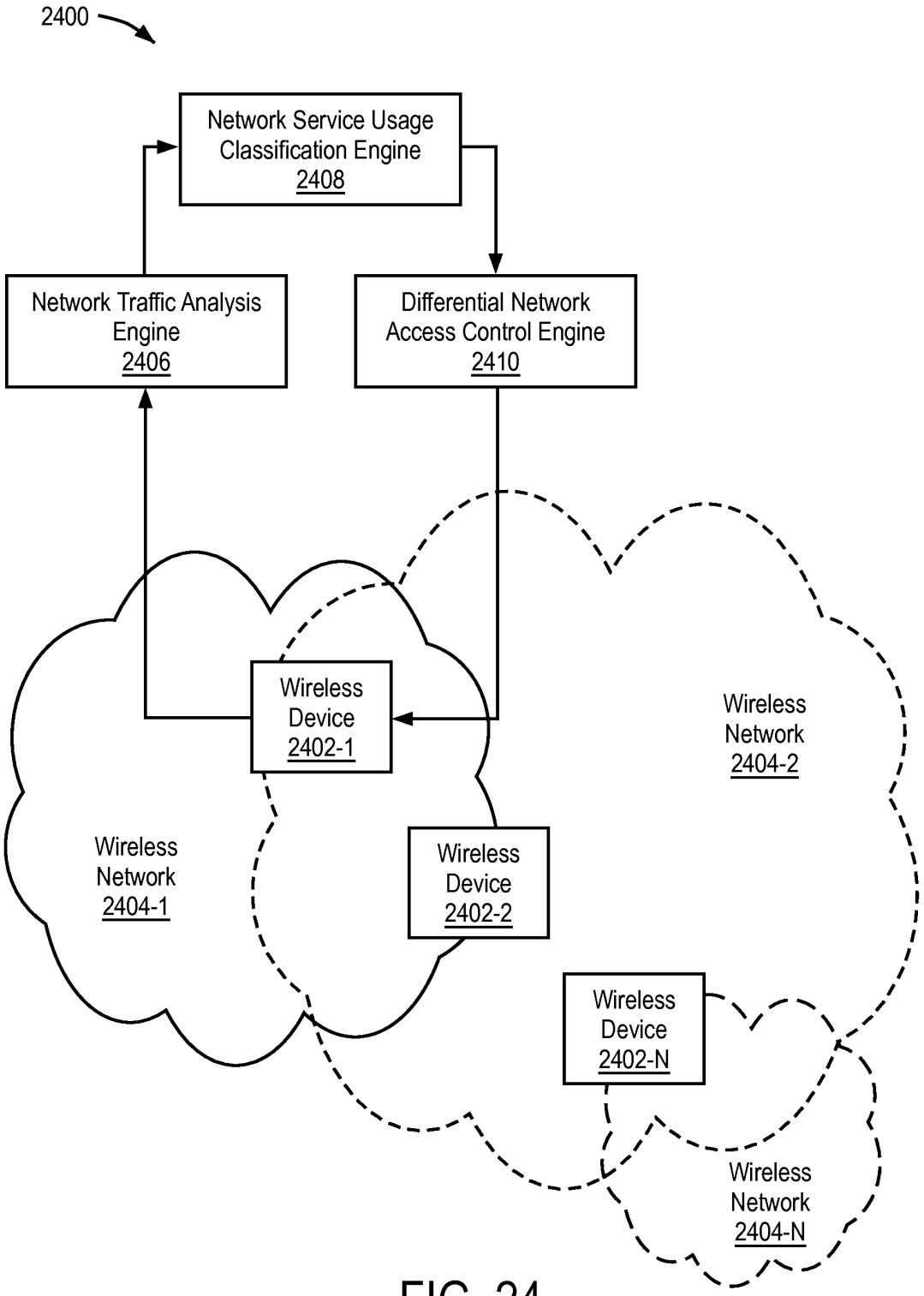

2400
Network Service Usage Classification Engine 2408
Network Traffic Analysis Engine 2406
Differential Network Access Control Engine 2410
Wireless Device 2402-1
Wireless Network 2404-1
Wireless Device 2402-2
Wireless Network 2404-2
Wireless Device 2402-N
Wireless Network 2404-N

FIG. 24

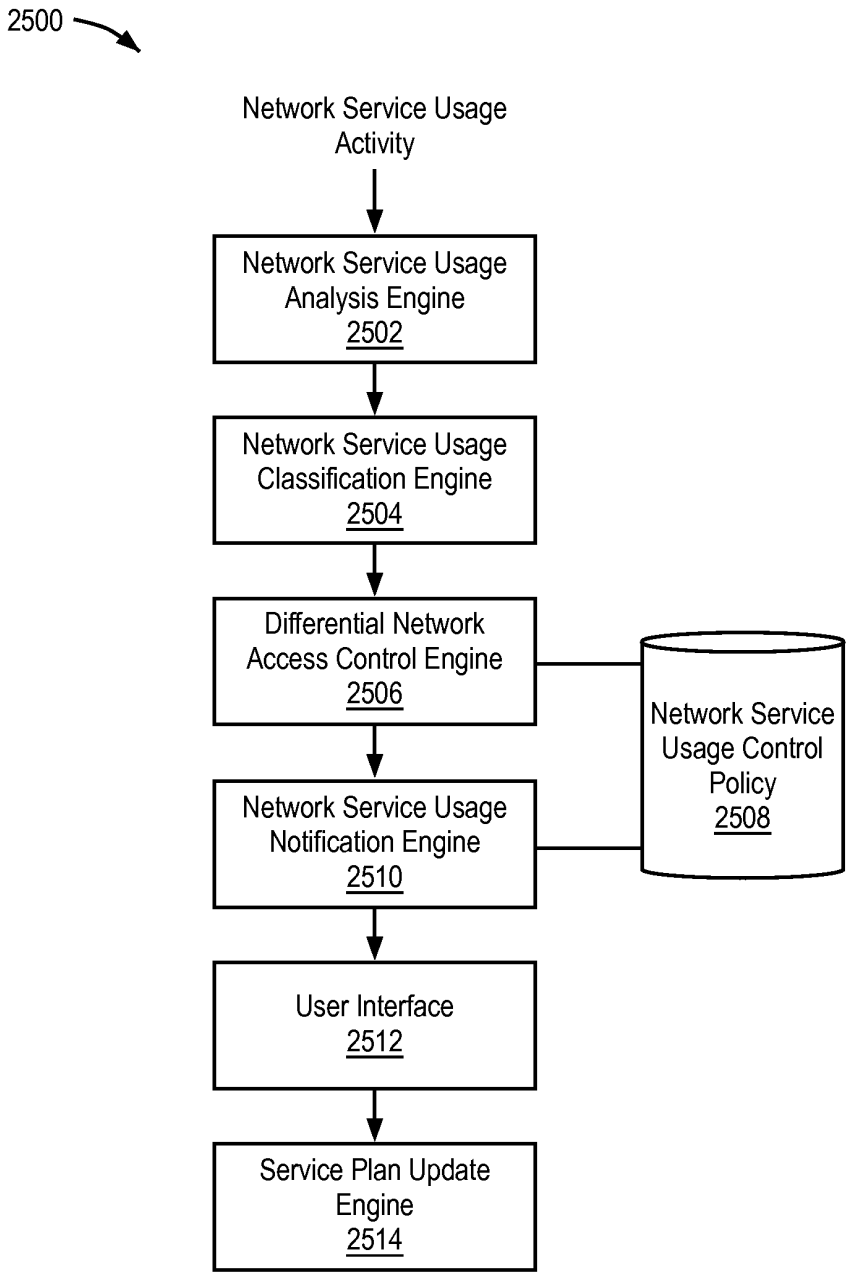

2500
Network Service Usage Activity
Network Service Usage Analysis Engine 2502
Network Service Usage Classification Engine 2504
Differential Network Access Control Engine 2506
Network Service Usage Control Policy 2508
Network Service Usage Notification Engine 2510
User Interface 2512
Service Plan Update Engine 2514

FIG. 25

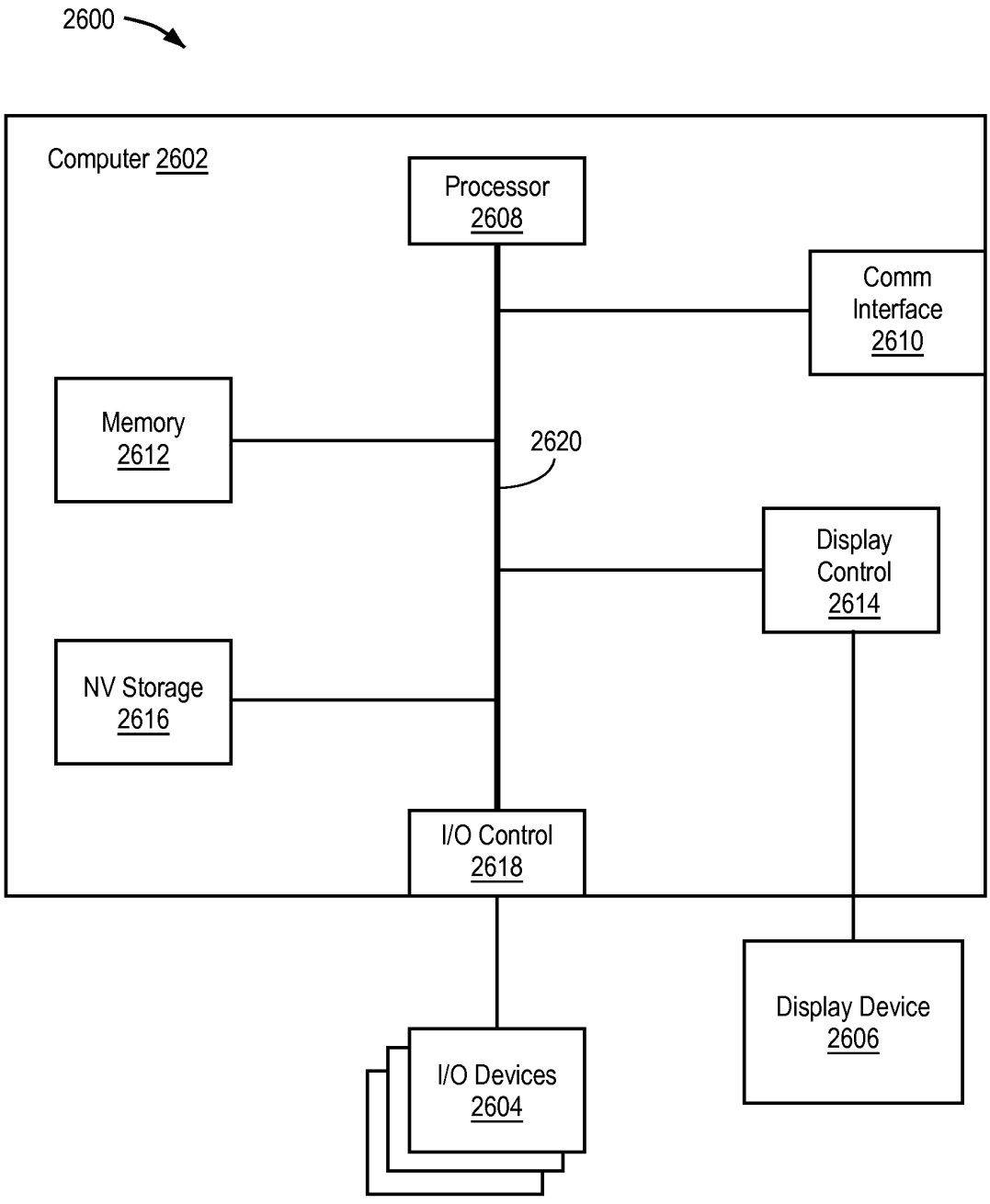

2600
Computer 2602
Processor 2608
Comm Interface 2610
Memory 2612
2620
Display Control 2614
NV Storage 2616
I/O Control 2618
Display Device 2606
I/O Devices 2604

FIG. 26

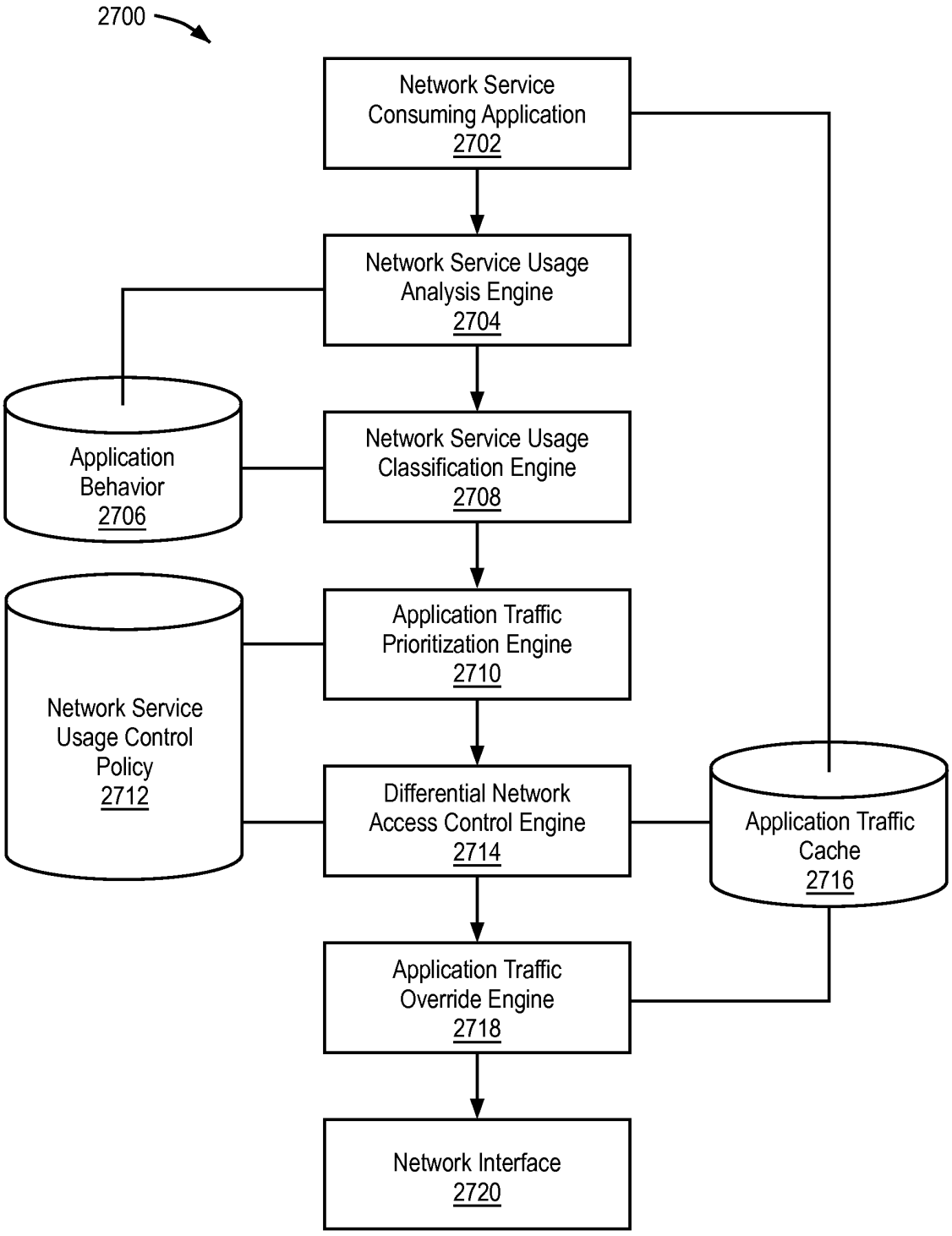

2700
Network Service Consuming Application 2702
Network Service Usage Analysis Engine 2704
Application Behavior 2706
Network Service Usage Classification Engine 2708
Application Traffic Prioritization Engine 2710
Network Service Usage Control Policy 2712
Differential Network Access Control Engine 2714
Application Traffic Cache 2716
Application Traffic Override Engine 2718
Network Interface 2720

FIG. 27

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

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

Title of Invention	Device-Assisted Services for Protecting Network Capacity (RALEP032C1)

As the below named inventor, I hereby declare that:

This declaration is directed to:

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

filed on _____.

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

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

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

WARNING:

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

LEGAL NAME OF INVENTOR

Inventor: Alireza Raissinia Date (Optional): 11/13/2013

Signature: _____

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

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

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

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

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

Title of Invention	Device-Assisted Services for Protecting Network Capacity (RALEP032C1)

As the below named inventor, I hereby declare that:

This declaration is directed to:

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

filed on _____.

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

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

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

WARNING:

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

LEGAL NAME OF INVENTOR

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

Signature: _____

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

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

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

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

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

Title of Invention	Device-Assisted Services for Protecting Network Capacity (RALEP032C1)

As the below named inventor, I hereby declare that:

This declaration is directed to:

- [x] The attached application, or
- [ ] United States application or PCT international application number _____ filed on _____.

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

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

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

WARNING:

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

LEGAL NAME OF INVENTOR

Inventor: James Lavine Date (Optional): 11/11/13

Signature: _____

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

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

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

Privacy Act Statement

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

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

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

Document code: WFEE

United States Patent and Trademark Office
Sales Receipt for Accounting Date: 12/17/2013

ASAHLE ADJ #00000002 Mailroom Dt: 11/15/2013
Seq No: 7668 Sales Acctg Dt: 11/18/2013 505876 14082040
06 FC : 1504 300.00 CR