



(12) 发明专利申请

(10) 申请公布号 CN 103202007 A

(43) 申请公布日 2013. 07. 10

(21) 申请号 201180053086. 9

(22) 申请日 2011. 09. 21

(30) 优先权数据

61/385, 020 2010. 09. 21 US

61/418, 509 2010. 12. 01 US

61/422, 574 2010. 12. 13 US

13/229, 580 2011. 09. 09 US

13/237, 827 2011. 09. 20 US

(74) 专利代理机构 北京安信方达知识产权代理有限公司 11262

代理人 苗源 王漪

(51) Int. Cl.

H04M 11/00 (2006. 01)

(85) PCT申请进入国家阶段日

2013. 05. 03

(86) PCT申请的申请数据

PCT/US2011/052662 2011. 09. 21

(87) PCT申请的公布数据

W02012/040398 EN 2012. 03. 29

(71) 申请人 海德沃特合作 I 有限公司

地址 美国加利福尼亚州

(72) 发明人 格雷戈里·G·罗利 詹姆斯·拉文

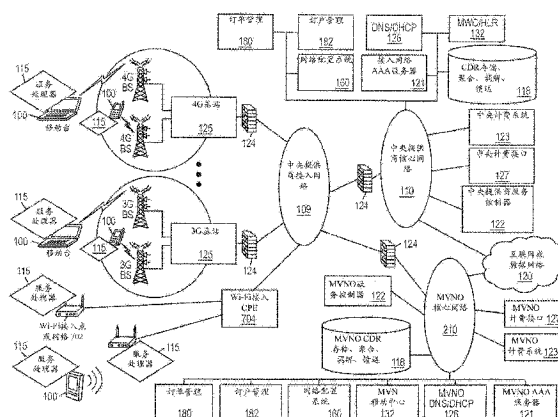
权利要求书2页 说明书62页 附图56页

(54) 发明名称

向具有装置上服务选择的装置代理发布的服务提供设置

(57) 摘要

在此披露了用于向终端用户装置上的装置代理发布服务提供设置并且用于在装置上选择服务的不同实施例。在一些实施例中，一种网络系统在无线接入网络上向终端用户装置发布服务提供设置，从该终端用户装置接收提供设置用户选择并且基于该提供设置用户选择来配置一个或多个网络功能。



1. 一种网络系统,包括:

存储器,该存储器被配置成存储一个服务提供设置,该服务提供设置包括有待传递到一个终端用户装置的一个或多个服务计划并且进一步包括可由一个终端用户装置用户行动的一个或多个服务计划选择选项;以及

一个或多个网元,该一个或多个网元被配置成:

从存储器中获得该服务提供设置,

在一个无线接入网络上向该终端用户装置发布该服务提供设置,

从该终端用户装置接收一个提供设置用户选择,并且

基于该提供设置用户选择配置一个或多个网络功能。

2. 如权利要求 1 所述的网络系统,其中该一个或多个网元中的至少一个包括一个服务控制器。

3. 如权利要求 1 所述的网络系统,其中该服务提供设置包括来自一个服务设计中心的信息,该服务设计中心包括被配置成接收多个服务提供设置设计参数的一个用户接口,该服务设计中心被配置成将这些服务提供设置设计参数提供到该网络系统,其格式为可以由该网络系统解释以协助将该服务提供设置传递到该终端用户装置。

4. 如权利要求 1 所述的网络系统,其中在一个无线接入网络上向该终端用户装置发布该服务提供设置包括:

将该服务提供设置配置成可以由该终端用户装置中的一个服务处理器解释的一种格式并且其中该可行的提供设置选择选项配置能够由该服务处理器在一个终端用户装置用户接口上显示,并且

将该格式化的服务提供设置推送到该服务处理器。

5. 如权利要求 1 所述的网络系统,其中在一个无线接入网络上向该终端用户装置发布该服务提供设置包括:

将该服务提供设置配置成可以由该终端用户装置中的一个服务处理器解释的一种格式并且其中该可行的提供设置选择选项配置能够由该服务处理器在一个终端用户装置用户接口上显示,并且

响应于来自该服务处理器的一个轮询而向该服务处理器提供该格式化的服务提供设置。

6. 如权利要求 1 所述的网络系统,其中该一个或多个网元中的至少一个被配置有一个应用程序接口(API),以协助在该无线接入网络上向该终端用户装置发布该服务提供设置,其中该 API 包括发布接口协议的一个统一的服务提供设置,该接口协议定义一个 API 通信协议和提供设置描述信息与可行的提供设置选择选项的一个配置,其方式为可以由实施该 API 统一接口协议的一个终端用户装置软件应用或 OS 功能解释并且处理而向该终端用户装置用户的一位用户呈现。

7. 如权利要求 6 所述的网络系统,其中该 API 为一个安全接口,该安全接口通过根据该 API 统一接口协议而提供一个装置凭证、一个用户凭证或一个应用凭证中的一个或多个来接入。

8. 如权利要求 1 所述的网络系统,其中该一个或多个网元中的至少一个被配置成基于在该提供设置用户选择中的信息来确定一个或多个网络配置指令。

9. 如权利要求 1 所述的网络系统,其中该一个或多个网元中的至少一个被配置有一个应用程序接口(API),以协助从该终端用户装置接收一个提供设置用户选择,其中该 API 包括接收接口协议的一个统一的服务提供设置,该接口协议指定定义一个终端用户装置软件应用或 OS 功能是如何配置描述用户选择的服务计划选择选项的信息的这些 API 通信协议。

10. 如权利要求 9 所述的网络系统,其中该 API 为一个安全接口,该安全接口通过根据该 API 统一接口协议而提供一个装置凭证、一个用户凭证或一个应用凭证中的一个或多个来接入。

11. 如权利要求 1 所述的网络系统,其中该一个或多个网元中的至少一个被配置成配置一个或多个网络数据路径网络接入控制元件。

12. 如权利要求 1 所述的网络系统,其中该一个或多个网元中的至少一个被配置成配置一个或多个网络服务记账或计费元件。

13. 如权利要求 1 所述的网络系统,其中该一个或多个网元中的至少一个被配置成配置一个或多个服务处理器代理策略强制执行设置。

14. 如权利要求 1 所述的网络系统,其中该一个或多个网元中的至少一个被配置成配置一个或多个策略强制执行元件或服务使用记账元件来促进一个临时服务租赁。

15. 一种终端用户装置,包括:

一个调制解调器,该调制解调器用于启用该终端用户装置以便通过一个接入网络接入一个网络数据服务;

一个用户接口;以及

一个服务处理器,该服务处理器被配置成:

从一个服务控制器中获得一个服务提供设置;

从该服务提供设置中提取信息,该提供设置包括服务计划提供描述信息和可行动的用户选择选项;

通过该用户接口呈现含有来自该服务提供设置的信息的一个通知消息;

通过该用户接口获得对该通知消息的一个用户响应;

生成一个包含以下信息的一个响应消息,该信息从呈由一个提供设置用户选择接收器预期的一种格式的这些可行动的用户选择选项之中指定一个用户选择项;并且

将该响应消息发送到该服务控制器。

16. 如权利要求 15 所述的终端用户装置,其中该服务提供设置处于由一个网络 API 定义确定以用于提供设置发布的一种格式。

17. 如权利要求 15 所述的终端用户装置,其中该服务处理器包括一个装置应用程序,该装置应用程序被配置成轮询一个网络 API 以便从该服务控制器获得该服务提供设置。

18. 如权利要求 15 所述的终端用户装置,其中该服务处理器包括一个装置应用程序,该装置应用程序被配置成通过接收来自一个网络 API 的一个推送来从该服务控制器获得该服务提供设置。

19. 如权利要求 15 所述的终端用户装置,其中由该提供设置用户选择接收器预期的该格式由一个网络 API 确定。

向具有装置上服务选择的装置代理发布的服务提供设置

发明背景

[0001] 随着大容量市场数字通信和内容分发的出现,许多接入网络如无线网络、电缆网络以及 DSL (数字用户线) 网络迫切要求用户容量,而例如 EVDO (演进数据优化)、HSPA (高速分组接入)、LTE (长期演进)、WiMax (全球微波互联接入)、以及 Wi-Fi (无线保真) 无线网络正越来越变得受到用户容量的约束。尽管无线网络容量将随着未来新的更高容量的无线射频接入技术(如 MIMO (多输入多输出)) 和被部署的更多的频谱而增长,这些容量增益可能会小于满足增长的数字联网要求的要求。

[0002] 类似地,尽管有线线路接入网络(如电缆和 DSL)可以具有每用户更高的平均容量,有线线路用户服务消费习惯正趋向非常高的带宽应用,这些带宽应用可以迅速消耗可用容量并且使总体网络服务体验降级。由于服务提供者成本的一些组成部分随着增长的带宽而增加,这个趋势还将对服务提供者的利润造成负面影响。

附图简要说明

[0003] 在以下详细说明和附图中披露了不同的实施例。

[0004] 图 1 展示了根据一些实施例的用于提供装置辅助 CDR 创建、聚合、调解以及计费的一个无线网络架构。

[0005] 图 2 展示了根据一些实施例的用于提供装置辅助 CDR 创建、聚合、调解以及计费的另一个无线网络架构。

[0006] 图 3 展示了根据一些实施例的用于提供装置辅助 CDR 创建、聚合、调解以及计费的另一个无线网络架构。

[0007] 图 4 展示了根据一些实施例的用于提供装置辅助 CDR 创建、聚合、调解以及计费的一个无线网络的配置。

[0008] 图 5 展示了根据一些实施例的用于提供装置辅助 CDR 的一个网络架构。

[0009] 图 6 展示了根据一些实施例的用于提供装置辅助 CDR 的另一个网络架构。

[0010] 图 7 展示了根据一些实施例的用于提供装置辅助 CDR 的另一个网络架构。

[0011] 图 8 展示了根据一些实施例的用于提供装置辅助 CDR 的另一个网络架构。

[0012] 图 9 为展示了根据一些实施例的一个基于装置的服务处理器和一个服务控制器的功能图。

[0013] 图 10 提供了汇总根据一些实施例的不同服务处理器功能元件的表。

[0014] 图 11 提供了根据一些实施例的汇总不同服务控制器功能元件的表。

[0015] 图 12 展示了根据一些实施例的一个装置堆栈,该装置堆栈从联网堆栈中的不同点处提供不同服务使用测量,以用于一个服务监控器代理、一个计费代理以及一个接入控制完整性代理从而来帮助验证服务使用度量和计费报告。

[0016] 图 13 展示一个与图 12 类似的实施例,其中根据一些实施例,服务处理器中的一些实施在调制解调器上,并且服务处理器中的一些实施在装置应用程序处理器上。

[0017] 图 14 展示了根据一些实施例的中间联网装置的不同实施例,这些中间联网装置包括用于可验证的服务使用测量、报告以及计费报告的目的的一个服务处理器。

[0018] 图 15 展示了根据一些实施例的用于提供装置辅助 CDR 创建、聚合、调解以及计费的包括一个代理服务器的一个无线网络架构。

[0019] 图 16 为展示了根据一些实施例的该服务处理器的服务控制装置链路和该服务控制器的服务控制服务链路的功能图。

[0020] 图 17 为展示了根据一些实施例的一个服务处理器通信帧和一个服务控制器通信帧的成帧结构的功能图。

[0021] 图 18A 至图 18E 提供了根据一些实施例的汇总不同服务处理器心跳功能和参数的表。

[0022] 图 19A 至图 19G 提供了根据一些实施例的汇总不同基于装置的服务策略实施验证技术的表。

[0023] 图 20A 至图 20C 提供了根据一些实施例的汇总用于保护该基于装置的服务策略免于受到危害的不同技术的表。

[0024] 图 21 展示了用 SGSN 通知开始或停止一个数据会话的一个过程的一个示例实施例。

[0025] 图 22 展示了用 GGSN 通知开始或停止一个数据会话的一个过程的一个示例实施例。

[0026] 图 23 展示了具有网络系统元件的一个示例实施例,这些网络系统元件可以被包括在一个服务控制器系统中,用于协助一个装置辅助服务(DAS)实施和这些元件之间的信息流。

[0027] 图 24 展示了一个服务控制器调和处理过程的一个示例实施例,该服务控制器调和处理过程可以用于使用来自终端用户装置的信息和来自第二源的信息来检测欺诈。

[0028] 图 25 展示了在以下情况下可能都为有利的一个示例实施例:令人希望的是,在网络中识别服务使用分类,用于为一位装置用户或服务赞助方提供机会来为由应用或网站分类的接入网络服务使用付费的目的。

详细说明

[0029] 本发明可以多种方式实施,包括如过程;仪器;系统;物质的组合;包含在计算机可读存储媒质上的计算机程序产品;和/或处理器,如被配置成执行存储在与该处理器相耦合的存储器上的和/或由其提供的指令的处理器。在本说明书中,这些实现方式或本发明可采取的任何其他形式可被称为技术。一般而言,所披露的过程的步骤的顺序在本发明的范围内是可改变的。除非另有说明,所描述的被配置成进行任务的组件如处理器或存储器可作为临时被配置成在给定的时间进行该任务的通用组件或被制作为进行该任务的特定的组件来实施。如在此使用的,术语“处理器”指被配置成处理数据(如计算机程序指令)的一个或多个装置、电路、和/或处理核心。

[0030] 以下与附图一起提供了本发明的一个或多个展示本发明的原理的实施例的详细说明。本发明是结合此类实施例进行描述的,但本发明并不限于任何实施例。本发明的范围不仅受权利要求的限制,并且本发明包括多种替代方案、改变以及等效物。随后的说明书中给出了许多具体的细节,从而提供对本发明的充分的理解。提供这些细节是为了示例的目的,并且可根据权利要求来实践本发明而不需要这些具体的细节的一些或所有。为了清晰的目的,未详细描述本技术领域已知的与本发明相关的技术材料,从而使得本发明不具

有不必要的晦涩。

[0031] 存在许多新类型的数字装置,其中变得令人希望的是,例如将这些装置连接至无线网络,包括无线广域网(WWAN,如 3G 和 4G)和 / 或无线局域(WLAN)网络。这些装置包括例如消费者电子装置、商业用户装置以及从灵活的广域数据连接和互联网中受益的机器对机器装置。示例装置包括上网本、笔记本、移动互联网装置、个人导航(例如 GPS 启用)装置、音乐和多媒体播放器、电子阅读器、工业遥测术、自动紧急响应和诊断、2 路家庭和工业电力计量和控制、自动售货机、停靠表以及许多其他装置。例如,高度有利的是,为这类装置提供服务使用和服务计费计划,这些计划对于每一种类型的装置和每一种类型的令人希望的用户体验而言是较为最优的。为了实现这一点,与目前存在的常规的基于网络的技术相比,需要更复杂的服务使用测量和服务使用计费系统。通过提供服务测量和计费上的更大的灵活性,可以创建更加有利和成本有效的服务计划来用于例如针对所有三个市场(例如消费者、商业和机器对机器)的以上援引的新的 WWAN 连接装置,这仍使得对于 WWAN 运营商的必要利润率成功地与这些不同服务业务一起维持。

[0032] 因此,在此所披露的不同实施例为现有运营商网络服务使用测量、服务使用记账以及服务使用计费系统和技术提供一个新的并且灵活的增添或替换。

[0033] 收费数据记录(CDR)为在此所使用的定义装置服务使用信息的一种格式化度量的术语,该格式化度量典型地由监视、监控和 / 或控制供装置的网络接入的一个或多个网络功能生成。CDR 典型地形成用于记录装置网络服务使用的基础,并且经常形成用于对这类使用进行计费的基础。在此提供不同实施例来用于装置辅助 CDR 创建、调解以及计费。当 CDR 由基于网络的功能或设备独占地生成时,存在对服务使用记录、聚合和 / 或计费的能力的限制。因此,通过用基于装置的服务使用度量来增添基于网络的服务使用度量,或者通过用基于装置的服务使用度量来替换基于网络的服务使用度量,可能的是创建具有优越或所更令人希望的能力 / 特征的一个 CDR 生成、聚合、调解和 / 或计费解决方案。虽然在理论上,可以在一个装置上被评估的服务使用度量中的许多度量也可以在网络数据路径中使用不同网络设备技术包括但不限于深度数据包检测(DPI)来评估,但是存在在装置处测量服务使用是所更令人希望或更实用的许多示例,或者在一些情况下,这是获得令人希望的度量的唯一方式。这类示例包括但不限于以下各项:

- 应用层服务使用度量(例如由应用或由应用、目的地和 / 或内容类型的组合归类的业务量使用);

- 使用度量,其不涉及用户业务量,但反而涉及网络开销业务量(例如,基本连接维持业务量、发信号业务量、网络注册 / AAA / 认证 / 监控业务量、服务软件更新业务量);

- 与服务相关联的使用,这些服务向另一个实体而不是终端用户收费(例如,基本网络连接服务提供业务量、与提供网络接入到服务销售信息或下载服务销售信息相关联的业务量、与广告赞助方服务相关联的业务量、与内容提供者赞助的服务相关联的业务量、911 服务业务量);

- 涉及加密业务量的使用度量(例如在加密联网协议上或安全端点之间通过的业务量);

- 跨越多个网络实施服务使用度量收集和 / 或服务使用计费,这些网络可能具有不同的或在一些情况下为不可兼容的、不可接入的(到记录的 CDR 系统)或不完全的服务使用测

量能力；

- 服务使用测量和 / 或服务使用计费能力,这些能力未被目前的网络网关、路由器、MWC/HLR、AAA、CDR 聚合、CDR 调解、计费和 / 或配置系统支持；

- 新服务使用度量和 / 或新服务使用计费能力,这些能力是令人希望的从而来以不需要较大改变或升级到现有网络网关、路由器、MWC/HLR、AAA、CDR 聚合、CDR 调解、计费和 / 或配置系统的方式实施；

- 新服务使用度量和 / 或新服务使用计费能力,这些能力是令人希望的从而来以允许快速定义和实施新服务度量和 / 或计费计划的方式实施；

- 新服务使用度量和 / 或新服务使用计费能力,这些能力是令人希望的从而来以一种方式实施,该方式能够以启用多个装置组定义的方式实施,在这些装置组定义中,每一个装置组得到用于服务使用收集、记账和 / 或计费的一个定制的程序控制的定义；

- 多装置计费；

- 多用户计费；

- 具有单用户和多用户的具有多装置和不具有多装置的中间装置计费；

- 从一个特定源下载内容到一个特定应用,其中该内容具有一种特定类型或甚至被识别为一个特殊内容 ID ;和 / 或

- 用于计费目的不同其他单事件交易。

为了这些和其他原因,令人希望的是提供一种利用装置辅助服务使用度量的系统 / 过程,该系统 / 过程提供对基于服务使用 CDR 系统能力和技术的现有网络的一个增强和 / 或对基于 CDR 系统能力和技术的网络的一个替换。

[0034] 在一些实施例中,利用装置辅助服务使用度量的如一种系统和 / 或过程的技术包括以下各项中的一项或多项:(1) 从与一个无线网络进行通信的一个装置中接收一个服务使用度量,(2) 验证或保护该服务使用度量的有效性,(3) 基于服务使用度量生成一个 CDR (例如装置辅助 CDR),(4) 聚合 CDR,并且 (5) 调解该 CDR 与网络 CDR。在一些实施例中,这些技术还包括提供一种设计和配置装置 / 网络设备来辨认这些 CDR。在一些实施例中,这些技术还包括配置从而辨认:装置属于一个装置辅助服务(DAS)装置组;并且相应的 CDR 应该被接受并且调解。在一些实施例中,装置辅助 CDR 还通过使用以下内容来生成:格式、网络通信协议、网络装置认证和 / 或配置以允许装置辅助 CDR 到网络 CDR 系统中、加密和 / 或如由网络所需的签名(例如来遵守网络生成的 CDR 要求或基于任何其他网络和 / 或服务提供者要求和 / 或标准)。

[0035] 在一些实施例中,调解规则包括多装置、多用户、单用户装置和 / 或可以是单用户或多用户的中间联网装置,如在此所描述。

[0036] 在一些实施例中,一个装置辅助 CDR 生成器收集基于装置的服务使用度量,这些基于装置的服务使用度量用作一个或多个(例如网络生成的)CDR 的基础或用作对一个或多个 CDR 的增强(例如作为一个增补或添加),该一个或多个 CDR 提供具有适当格式化的服务使用报告的一个或多个联网功能,当其从一个授权的源传输、被读取并且利用来帮助确定一个装置或一组装置的服务使用时,这个或这些网络功能接受这些报告。在一些实施例中,装置辅助 CDR 生成器与其共享 CDR 的网络功能典型地包括以下各项中的一项或多项:服务使用 / CDR 聚合和 / 或调解服务、网关、路由器、通信节点、移动无线中心(包括 HLR 的 MWC)、

数据库、AAA 系统、计费接口以及计费系统。例如,CDR 生成器中的 CDR 创建的过程典型地包括:或者使用一个或多个基于装置的服务使用度量或者一个或多个基于装置的服务使用度量与一个或多个基于网络的服务使用度量相组合;可能根据 CDR 创建、CDR 聚合和 / 或 CDR 调解规则集来处理一个或多个这类服务使用度量以得到一个最终装置使用度量,该最终装置使用度量例如随后用适当语法格式化、被成帧、可能被加密和 / 或签名并且封装到适于与网络功能共享的一个通信协议或数据包之中。在一些实施例中,CDR 生成器驻留在该装置之中。在一些实施例中,CDR 生成器驻留在接收装置辅助服务使用度量与可能的基于网络的使用度量的一个网络服务器功能中,并且随后创建一个 CDR (例如在服务控制器 122 中)。

[0037] 在一些实施例中,装置辅助 CDR 生成器可以驻留在服务处理器(例如服务处理器 115)中,例如在服务使用历史或计费服务器功能中。在一些实施例中,装置辅助 CDR 生成器可以驻留在装置本身中例如在服务处理器功能内,如计费代理或服务监控器代理。

[0038] 在不同的实施例中要考虑若干因素以便创建一个有用的、可靠的并且安全装置辅助 CDR 系统,包括例如但不限于:

- 用一个或多个使用交易码对每一个基于装置的服务使用度量的识别;
- 对这个或这些基于装置的使用度量的验证;
- 基于装置的使用度量到网络的安全通信;
- 基于装置的服务使用度量的高效(例如低带宽)通信;
- 基于装置的服务使用度量与一个或多个基于网络的服务使用度量的协调 / 比较 / 聚合;
- 将基于装置的使用度量格式化为一个 CDR,该 CDR 可以被正确地传递到处理服务使用信息的网络功能和 / 或设备;
- 引起用于 CDR 收集、聚合、调解和 / 或计费的基于网络的功能和 / 或设备来辨认、授权并且接受来自装置辅助 CDR 生成器的通信和 CDR、读取以及正确地实施用于 CDR 的正确的网络会话语境,这样使得 CDR 与该正确的装置 / 用户 / 会话正确地相关联;
- 实施 CDR 聚合规则,这些规则确定装置辅助 CDR 如何依照其被报告的通过网络 CDR 系统层级结构来收集并且聚合;
- 实施调解规则,这些规则确定不同的基于装置的服务使用交易码度量如何被组合并且与其他基于装置服务使用交易码调解来产生用于维护在网络中的交易码类别中的每一种的一致服务使用信息;
- 实施调解规则,这些规则确定装置辅助 CDR 如何被组合并且与基于网络的 CDR 调解来产生用于维护在网络中的交易码类别中的每一种的一致服务使用信息;
- 实施调解规则来调和基于网络的 CDR 使用度量与装置辅助 CDR 使用度量之间的变化量;
- 一个或多个装置组的分类,其中每一个组具有唯一地定义服务使用收集、记账和 / 或计费规则的能力;
- 收集在网络而不是家庭网络上生成的 CDR,这样使得可以在多个网络上测量、记账和 / 或计费服务使用;
- 多装置计费;
- 多用户计费;和 / 或

- 具有单用户和多用户的具有多装置和不具有多装置的中间装置计费。

[0039] 在一些实施例中,提供了装置辅助服务使用度量的相对准确性的验证。考虑到例如服务使用度量经常在从一个网络管理视角来看由公众或其他非安全人员轻松地在物理上接入的一个终端用户装置或一个装置上生成,在一些实施例中,在服务处理器 115 代理中的一个或多个中使用的装置代理受保护而免于非法侵入、电子欺骗和 / 或其他滥用。在此提供了不同技术来保护用于生成装置辅助服务使用度量的代理的完整性。

[0040] 在一些实施例中,服务使用度量由使用不同技术的基于网络的交叉检查来验证。例如,基于网络的交叉检查可以提供有价值的验证技术,因为例如即使例如用于保护装置代理的度量被击败或者如果没有采用装置保护度量,击败使用不同技术的良好设计的基于网络的交叉检查(如在此所描述的这些)通常也是不可能的或至少非常困难的。在一些实施例中,用于验证装置辅助服务使用度量的基于网络的交叉检查包括:比较基于网络的服务使用度量(例如由网络设备,如 BTS/BSC125、RAN 网关 410、传输网关 420、移动无线中心 / HLR132、AAA121、服务使用历史 / CDR 聚合、调解、馈送 118,或其他网络设备中的服务使用测量仪器生成的 CDR);将安全查询 / 响应命令顺序发送到涉及装置辅助 CDR 服务使用测量或 CDR 创建的一个或多个服务处理器 115 代理;将测试服务使用事件顺序发送到装置并且验证该装置正确地报告了服务使用;以及使用不同的其他技术,如在此相对于不同实施例所描述的这些。

[0041] 在一些实施例中,如果基于装置的服务使用度量被发现为错误或不准确,那么采取以下行动中的一个或多个:针对使用过量或缺乏策略装置而对用户计费;暂停装置;隔离装置;跨越装置;及 / 或向一个网络管理功能或个人报告装置。

[0042] 在一些实施例中,用于将装置辅助服务使用信息格式化为一个 CDR 的 CDR 语法和 / 或用于传输 CDR 的网络通信协议由工业标准(例如 3GPP TS32. 215 格式和 3GPP2TSG-X X. S0011 或 TIA-835 格式的不同变体)确定。在一些实施例中,对于一种给定的网络实现方式而言,网络设计师将指定对标准语法、格式和 / 或网络通信 / 传输协议的修改。在一些实施例中,对于一种给定的网络实现方式而言,网络设计师将指定与标准完全不同的语法、格式和 / 或网络通信 / 传输协议。

[0043] 在一些实施例中,在用于 CDR 的语法和格式化中,装置辅助服务使用典型地由一个交易码归类。例如,交易码可以与由用于生成 CDR 的网络设备使用的代码类似或相同,或者考虑到装置能够生成较丰富的服务使用度量集,交易码可以为由用于生成 CDR 的网络设备使用的代码的一个超集(例如在此提供了可以标识为交易码的使用活动的示例,当与纯粹地基于网络的 CDR 系统相比较时,这些交易码由装置辅助 CDR 系统更加轻松地支持)。

[0044] 在一些实施例中,装置发送用于一个使用活动标签的一个标识符,一个中间服务器确定如何聚合成 CDR 交易码并且要使用哪一个 CDR 交易码。

[0045] 在一些实施例中,装置服务处理器 115 由预先分配的装置活动交易码划分使用(例如可以存在主账户中的子交易、一个给定账户账单交易中的交易或一个账户账单交易中的子交易)。装置实施账户账单规则以发送用于每一个账户账单功能的不同使用报告。在一些实施例中,服务控制器 122 为装置编程来指示其如何划分这些账户账单服务使用活动,以便这些账户账单服务使用活动可以被映射到一个交易码中。

[0046] 在一些实施例中,装置报告较少划分的服务使用信息,并且服务控制器 122 将服

务使用活动映射到在一些情况下包括账户账单码的 CDR 交易码。

[0047] 在一些实施例中,发送到 118 或其他网络设备的 CDR 例如可以包括不同类型的交易码,这些不同类型的交易码包括但不限于一个原始装置使用 CDR、一个账户账单(例如一个子活动交易码)CDR、一个计费偏差 CDR 和 / 或一个计费信用 CDR。例如,确定这些不同类型的 CDR 交易码是如何由核心网络聚合并且调解的决定逻辑(也称为业务规则或 CDR 聚合和调解规则)和计费系统可以处于网络设备中(例如一个网元,如服务使用 118)、处于服务控制器 122 中和 / 或处于计费系统 123 中。

[0048] 在一些实施例中,装置辅助 CDR 生成器使用装置辅助服务使用度量来生成一个 CDR,该 CDR 包括服务使用信息、一个或多个服务使用交易码以及在一些实施例中的网络信息语境。在一些实施例中,服务使用信息、交易码和 / 或网络信息语境被格式化为与由常规联网设备使用的格式化兼容以生成 CDR 的通信成帧、语法、加密 / 签名、安全性和 / 或联网协议。例如,这允许用于 CDR 收集、记录、聚合、调解和 / 或转换的联网设备来计费记录以正确地接收、读取并且解释在基于装置服务使用测量的帮助下生成的 CDR。在一些实施例中,装置辅助服务度量被提供给称为一个服务控制器(例如服务控制器 122)的一个中间网络服务器。在一些实施例中,服务控制器使用用于一个无线网络的一个 CDR 馈送聚合器来为无线网络上的一个或多个装置收集装置生成的使用信息,并且以可以由无线网络使用的一个语法(例如收费数据记录(CDR))和一个通信协议(例如 3GPP 或 3GPP2 或其他通信协议或多个通信协议)来提供装置生成的使用信息,从而为无线网络上的一个或多个装置增添或替换网络生成的使用信息。

[0049] 在一些实施例中,调解规则包括多装置、多用户、单用户装置、可以为单用户或多用户的中间联网装置。例如,即使这些 CDR 源于都属于同一位用户的多个装置,装置辅助 CDR 也可以由装置辅助 CDR 生成器格式化,从而来包括针对一个用户账户的一个交易码。这是针对一个多用户装置辅助 CDR 计费解决方案的一个示例。在针对一个多用户装置辅助 CDR 计费解决方案的另一个示例中,来自多个装置和多个用户的装置辅助 CDR 可以都被记账到同一个账户(例如一个家庭计划或一个企业账户),但账户账单 CDR 交易记录可以通过计费系统来维护,以便提供子账户可见性,这样使得负责主账户的个人或实体可以获得关于哪些用户和 / 或装置在创建大部分服务使用计费的可见性。例如,这个类型的多用户、多装置辅助 CDR 计费解决方案也可以用来跟踪多种类型的服务使用和 / 或对多种类型的服务使用计费,这对于纯粹的基于网络的 CDR 系统而言记账和 / 或计费时不可能的或者至少是非常困难的。在一些实施例中,账户账单 CDR 交易记录可以用来提供被赞助的交易服务、对网络聊天记账、提供服务选择接口和用于多用户或多装置服务计划的其他服务。

[0050] 除了常规单用户装置(例如手机、智能机、上网本 / 笔记本、移动互联网装置、个人导航装置、音乐播放器、电子阅读器以及其他单用户装置),装置辅助服务使用测量和 CDR 也可用于其他类型的有网络能力的装置和 / 或联网装置,如中间联网装置(例如 3G/4G WWAN 到 WLAN 桥接器 / 路由器 / 网关、毫微微蜂窝区、DOCSIS 调制解调器、DSL 调制解调器、远程接入 / 备份路由器以及其他中间网络装置)。例如,在这类装置中,特别是就以一种安全方式来验证:装置辅助服务使用度量是相对准确的,和 / 或装置服务处理器 115 软件未受危害或未受非法侵入而言,许多新的服务提供者服务交付和计费模式可以使用在此所描述的技术来支持并且实施。例如,在一个 WiFi 到 WWAN 桥接器或路由器装置中,多个用户装置可以

用同一个中间联网装置支持,其方式为通过如在此所描述的发送装置辅助 CDR 而与中央提供者的 CDR 聚合和 / 或计费系统一致并且兼容,这些装置辅助 CDR 具有被引用到终端用户和 / 或特殊中间装置的一个服务使用和 / 或计费码。

[0051] 在一些实施例中,为中间联网装置生成的装置辅助 CDR 是与一个特殊终端用户相关联的,其中可以存在若干或许多终端用户使用用于联网接入的中间联网装置,并且在一些实施例中,每一个终端用户被要求进入一个唯一登陆到该中间联网装置。例如,以这种方式,使用 WiFi 连接至中间联网装置来使 WWAN 接入生成 CDR 的所有装置可以被记账到负责针对该装置的主账户的一个特殊终端用户,或者 CDR 可以具有来自同一个中间联网装置的针对多个终端用户的已验证的相对使用测量准确性的一种安全方式计费。在另一个示例中,一个终端用户可以具有允许接入到多个中间联网装置的一个账户,并且每一个中间联网装置可以为该用户生成具有交易码的一致的装置辅助 CDR,而不管终端用户登录哪一个中间联网装置。

[0052] 在一些实施例中,由中间联网装置提供的服务中的一些被记账到一个特定终端用户装置辅助 CDR 交易码,而其他账户账单服务被记账到其他交易码账户,如赞助伙伴交易服务账户、网络聊天账户、赞助广告商账户和 / 或服务签约账户。例如,以这种方式,提供了不同实施例,其中中间联网装置(例如一个 WWAN 到 WiFi 路由器 / 桥接器)可以出售给一个用户,但可以为其他用户服务并且用于为其他用户计费(例如,并且这可以涵盖在第一购买用户的服务条款中,可能来交换一个折扣),或这类中间联网装置可以处于希望接入的任何地方,而不考虑装置将受非法侵入以致可以免费获得装置。

[0053] 在一些实施例中,不同类型的服务使用交易在中间联网装置上被记账到一位或多位用户中的任何一位上,其中需要对这类服务计费的信息对中央提供者或 MVNO 网络设备而言是不可用的,正如例如具有常规单用户装置的情况。从在此所描述的不同实施例和技术来看,本领域的普通技术人员将认识到不仅对于 WWAN 到 WiFi 中间联网装置,而且对于毫微微蜂窝区、远程接入路由器、DOCSIS、DSL 以及其他中间 WWAN 到 WiFi 联网装置,类似模型是同样可适用的。

[0054] 图 1 展示了根据一些实施例的用于提供装置辅助 CDR 创建、聚合、调解以及计费的一个无线网络架构。如所示,图 1 包括例如由中央提供者运行的一个 4G/3G/2G 无线网络。如所示,不同无线装置 100 与基站 125 进行通信,从而与无线网络进行无线网络通信,并且其他装置 100 与 Wi-Fi 接入点(AP)或网络 702 进行通信,从而与和中央提供者接入网络 109 通信的 Wi-Fi 接入 CPE704 进行无线通信。在一些实施例中,无线装置 100 中的每一个包括一个服务处理器 115 (如所示),并且每一个服务处理器通过一个安全控制平面链路连接至一个服务控制器 122。在一些实施例中,基于网络的服务使用信息(例如,CDR)是从一个或多个网元中获得的。如所示,一个 MVNO 核心网络 210 还包括一个 CDR 存储、聚合、调解、馈送 118,一个 MVNO 计费接口 122,以及一个 MVNO 计费系统 123 (以及图 1 所示的其他网元)。

[0055] 如图 1 所示,CDR 存储、聚合、调解、馈送 118 (例如,服务使用 118,包括一个计费聚合数据存储和规则引擎)是一个功能型的描述符,在一些实施例中,用于描述处于联网设备组件中的一个或多个中的装置 / 网络等级服务使用信息收集、聚合、调解、及报告功能,这些联网设备组件附接到如图 1 所示的子网络中的一个或多个上(例如,中央提供者接入网络 109 和 / 或中央提供者核心网络 110),该一个或多个子网络与服务控制器 122 及一个中

央计费接口 127 进行通信。如图 1 所示,将服务使用 118 展示为与中央提供者核心网络 110 通信的一个功能。在一些实施例中,CDR 存储、聚合、调解、馈送 118 功能处于网络中的其他地方,或部分地处于其他地方或与其他网元整合 / 作为其他网元的一部分。在一些实施例中,CDR 存储、聚合、调解、馈送 118 功能性处于或部分处于 AAA 服务器 121 和 / 或移动无线中心 / 归属位置寄存器(HLR) 132 中(如所示,与 DNS/DHCP 服务器 126 进行通信)。在一些实施例中,服务使用 118 功能性处于或部分地处于基站、基站控制器和 / 或基站聚合器中,在图 1 中共同地被称为基站 125。在一些实施例中,CDR 存储、聚合、调解、馈送 118 功能性处于或部分地处于中央提供者接入网络 109 中的一个联网组件中、核心网络 110 中的一个联网组件中、中央计费系统 123 中、中央计费接口 127 中和 / 或其他网络组件或功能中。对基于网络和基于装置的服务使用信息收集、聚合、调解以及报告功能(例如 CDR 存储、聚合、调解、馈送 118)的可能位置的这个论述可以轻松地由本领域普通技术人员依照在此所描述并且依照在此所描述的其他图所示概括。还如图 1 所示,服务控制器 122 与中央计费接口 123 进行通信(有时也称为外部计费管理接口或计费通信接口)127,该中央计费接口与中央计费系统 123 进行通信。如所示,一个订单管理 180 及订户管理 182 也与中央提供者核心网络 110 进行通信,从而根据一些实施例,协助针对装置 100 的服务订单和订户管理。

[0056] 在一些实施例中,CDR 存储、聚合、调解、馈送 118 (和 / 或其他网元或网元的组合)提供了一个装置 / 网络等级服务使用信息收集、聚合、调解、及报告功能。在一些实施例中,CDR 存储、聚合、调解、馈送 118 (和 / 或其他网元或网元的组合)为在无线网络(例如,装置 100)上的一个或多个装置收集装置生成的使用信息;并且以无线网络可以使用的一个语法或一个通信协议来提供装置生成的使用信息,从而为无线网络上的一个或多个装置增添或替换网络生成的使用信息。在一些实施例中,该语法是一个收费数据记录(CDR),并且该通信协议选自以下各项中的一项或多项:3GPP、3GPP2 或其他通信协议。在一些实施例中,CDR 存储、聚合、调解、馈送 118 (和 / 或其他网元或网元的组合)包括一个服务使用数据存储(例如,计费聚合器)和用于聚合所收集的装置生成的使用信息的一个规则引擎。在一些实施例中,该语法是一个收费数据记录(CDR),并且该网络装置是一个 CDR 馈送聚合器,并且该 CDR 存储、聚合、调解、馈送 118 (和 / 或其他网元或网元的组合)也为无线网络上的一个或多个装置聚合 CDR;使用一个规则引擎(例如,按账户计费、交易计费和 / 或其他任何计费或用于服务使用信息收集、聚合、调解、及报告的其他规则)将一个规则集应用到所聚合的 CDR 上,并且将针对无线网络上的一个或多个装置的新的 CDR 集传递到一个计费接口或一个计费系统(例如,通过账户 / 服务提供具有计费偏差的 CDR)。在一些实施例中,CDR 存储、聚合、调解、馈送 118 (和 / 或其他网元或网元的组合)将针对无线网络上的一个或多个装置的新的 CDR 集传递到一个计费接口或一个计费系统。在一些实施例中,CDR 存储、聚合、调解、馈送 118 (和 / 或其他网元或网元的组合)与一个服务控制器进行通信,从而为无线网络上的一个或多个装置收集装置生成的使用信息。在一些实施例中,CDR 存储、聚合、调解、馈送 118 (和 / 或其他网元或网元的组合)与一个服务控制器进行通信,其中该服务控制器与一个计费接口或一个计费系统进行通信。在一些实施例中,CDR 存储、聚合、调解、馈送 118 (和 / 或其他网元或网元的组合)将装置生成的使用信息传递到一个计费接口或一个计费系统。在一些实施例中,CDR 存储、聚合、调解、馈送(和 / 或其他网元或网元的组合)与一个传输网关和 / 或无线接入网络(RAN)网关进行通信,从而为无线网络上的一个或多个装置收

集网络生成的使用信息。在一些实施例中,服务控制器 122 将装置辅助服务使用信息传递到 CDR 存储、聚合、调解、馈送 118 (和 / 或其他网元或网元的组合)。

[0057] 在一些实施例中,CDR 存储、聚合、调解、馈送 118 (和 / 或其他网元或网元的组合) 执行规则,从而通过账户聚合和调解功能执行一个账单。在一些实施例中,与 CDR 存储、聚合、调解、馈送 118 (和 / 或其他网元或网元的组合) 通信的服务控制器 122 执行一个规则引擎,从而聚合并且调解装置生成的使用信息。在一些实施例中,与 CDR 存储、聚合、调解、馈送 118 (和 / 或其他网元或网元的组合) 通信的一个规则引擎装置执行一个规则引擎,从而聚合并且调解装置生成的使用信息。

[0058] 在一些实施例中,规则引擎包括在(例如,整合于 / 作为其一部分)CDR 存储、聚合、调解、馈送 118 中。在一些实施例中,规则引擎及相关联的功能(如在此所描述)是一个单独的功能 / 装置。在一些实施例中,服务控制器 122 执行这些基于规则引擎的功能中的一些或所有(如在此所描述),并且与中央计费接口 127 进行通信。在一些实施例中,服务控制器 122 执行这些基于规则引擎的功能中的一些或所有(如在此所描述),并且与中央计费系统 123 进行通信。

[0059] 在一些实施例中,从网络设备向用于生成服务计费的计费系统 123 发送副本 CDR。在一些实施例中,过滤副本 CDR 从而仅发送那些用于由服务控制器和 / 或服务处理器(例如,所管理的装置)控制的装置的 CDR/ 记录。例如,本方法可提供与中央计费系统 123 所需的报告相比的同样等级的报告、较低等级的报告、和 / 或更高等级的报告。

[0060] 在一些实施例中,提供了一个账户账单计费偏差。例如,账户账单计费偏差信息可以通过提供聚合基于装置的服务使用数据馈送的一个 CDR 聚合器馈送而被通知到中央计费系统 123,从而为所管理的装置向中央计费接口 127 和 / 或中央计费系统 123 提供一个新的 CDR 集。在一些实施例中,使用类似的技术提供了交易计费。例如,可以向中央计费接口 127 和 / 或中央计费系统 123 提供交易计费日志信息。

[0061] 在一些实施例中,规则引擎(例如,由服务使用 118 或另一个网元执行的,如在此所描述)提供了一个账户账单计费偏差。例如,装置生成的使用信息(例如,收费数据记录(CDR)包括一个交易类型字段(例如,为相关联的服务使用信息指示一种类型的服务)。规则引擎可以基于与装置生成的使用信息相关联的被识别的服务而使用一条规则或一个规则集,从而确定一个账户账单计费偏差(例如,可以生成一个新的 CDR 以提供所确定的账户账单计费偏差)。在一些示例中,所确定的账户账单计费偏差可以提供为用户的服务使用账户的一个信用(例如,可以为用户的服务使用账户生成具有一个负偏差的一个新的 CDR,如用于网络聊天服务使用,或交易服务使用,或用于基于规则引擎执行的一条或多条规则的任何其他目的)。

[0062] 作为另一个示例,对于一个交易服务,可以对于该交易服务相关的使用为用户的服务使用账户生成具有一个负偏差的一个第一新 CDR,并且可以生成具有一个正服务使用值的一个第二新 CDR,从而对相同的服务使用为交易服务提供者收费(例如,亚马逊(Amazon)、易趣(eBay)、或另一个交易服务提供者)。在一些实施例中,服务控制器 122 生成这两个新的 CDR,并且服务使用 118 存储、聚合并且将这两个新的 CDR 传递到中央计费接口 127。在一些实施例中,服务控制器 122 生成这两个新的 CDR,并且服务使用 118 存储、聚合并且将这两个新的 CDR 传递到中央计费接口 127,其中中央计费接口 127 应用规则(例如,执

行规则引擎从而确定账户账单计费偏差)。

[0063] 在一些实施例中,服务控制器 122 将装置生成的 CDR 发送到规则引擎(例如服务使用 118),并且该规则引擎应用一个或多个规则,如在此所描述的这些和 / 或本领域普通技术人员将清楚的任何其他计费 / 服务使用相关的规则。在一些实施例中,服务控制器 122 生成类似于其他网元的 CDR,并且这些规则(例如账户账单)在中央计费接口 127 中执行。例如,对生成类似于其他网元的 CDR 的服务控制器 122 而言,在一些实施例中,服务控制器 122 被配置在无线网络上并且表现出大致上类似于如本领域普通技术人员将清楚的网络上的其他 CDR 生成器。

[0064] 在一些实施例中,服务控制器 122 被配置为一种新型的联网功能,该联网功能被网络中其他必需的元件(例如,服务使用历史 / CDR 聚合和调解服务器 118)辨认为一个对 CDR 有效的并且安全源。在网络仪器典型地仅从某些类型的联网设备辨认 CDR(例如 RAN 网关 410 或传输网关 420(如图 3 所示))的一些实施例中,服务控制器 122 可以向其他联网设备提供指示其是被批准的类型之一的设备的认证凭证(例如为了生成 / 提供 CDR 的目的)。在一些实施例中,服务控制器 122 和必需的 CDR 聚合以及调解设备之间的链路被保护安全、认证、加密和 / 或签名。

[0065] 在一些实施例中,CDR 存储、聚合、调解、馈送 118 舍弃从一个或多个网元接收的基于网络的服务使用信息(例如,基于网络的 CDR)。在这些实施例中,服务控制器 122 向 CDR 存储、聚合、调解、馈送 118 提供基于装置的服务使用信息(例如,基于装置的 CDR)(例如,CDR 存储、聚合、调解、馈送 118 可以仅提供一个或多个存储、聚合以及通信功能,并且将基于装置的服务使用信息提供到中央计费接口 127 或中央计费系统 123。

[0066] 在一些实施例中,基于装置的 CDR 和 / 或基于一个规则引擎执行而生成的新的 CDR(如在此所描述)仅为被管理的和 / 或基于装置组、服务计划或任何其他判据、归类和 / 或分组的装置而提供。

[0067] 图 2 展示了根据一些实施例的用于提供装置辅助 CDR 创建、聚合、调解以及计费的另一个无线网络架构。如图 2 所示,一些装置 100 与 DOCSIS 头端 125 进行通信,并且一些装置 100 与 DSLAM125 进行通信,从而与中央提供者接入网络 109 进行通信。

[0068] 图 3 展示了根据一些实施例的用于提供装置辅助 CDR 创建、聚合、调解以及计费的另一个无线网络架构。现参看图 3 所示的 4G/3G/2G 接入网络,4G/3G 和 3G/2G 基站 / 节点 125 经过一个无线接入网络 405 而与一个 4G/3G/2G 无线接入网络(RAN)网关 410 进行通信,从而经过一个接入传输网络 415 与一个 4G/3G/2G 传输网关 420 进行通信。中央提供者核心网络 110 与接入传输网络 415 进行网络通信(例如经过一个专门的 / 租赁的线路,并且如所述经过一个防火墙 124)。网络 120 经过一个防火墙 124 和这个或这些传输网关 420 而可用,如所示。同样,如所示,网络仪器配置系统 160、订单管理 180 以及订户管理 182 与中央提供者核心网络 110 进行通信。如所示,AAA 服务器 121、移动无线中心 / 归属位置寄存器(HLR) 132、DNS/DHCP126 以及 CDR 存储、聚合、调解、馈送 118 也与接入传输网络 415 通信。展示了中央计费系统 123 和中央计费接口 127 与中央提供者核心网络 110 通信。

[0069] 如所示,图 3 包括由例如一个中央提供者运行的一个 4G/3G/2G 无线网络。在一些实施例中,无线装置 100 中的每一个包括一个服务处理器 115(如所示),并且每一个服务处理器通过一个安全控制平面链路连接至一个服务控制器 122。在一些实施例中,基于网络

的服务使用信息(例如,网络生成的 CDR)是从一个或多个无线接入网络(RAN)网关 410 和 / 或一个或多个传输网关 420 中获得的。在一些实施例中,基于装置的服务使用信息(例如装置辅助 CDR)使用在此所描述的类似技术由服务处理器 115 和 / 或服务控制器 122 为一些或所有无线装置 100 而生成,并且在一些实施例中,这类基于装置的服务使用信息(例如装置辅助 CDR)被发送到 CDR 存储、聚合、调解、馈送 118 (例如,CDR 存储、聚合、调解、馈送 118 可以仅提供一个或多个存储、聚合以及通信功能),和 / 或发送到中央计费接口 127 或中央计费系统 123,如在此相对于不同实施例所类似地描述。

[0070] 图 4 展示了根据一些实施例用于提供装置辅助 CDR 创建、聚合、调解以及计费的一个无线网络的配置。如图 4 所示,所示地提供不同网络设备的配置,从而来将彼此辨认为一个 CDR 授权源(例如这可以手动地或以一种自动的方式完成)。例如,订单管理 180、订户管理、计费接口 127、计费系统 123、网络配置系统 160、服务控制器 122、接入网络 AAA 服务器 121、移动无线中心 132 以及 CDR 存储、聚合、调解馈送 118 针对这类配置而彼此通信,这可以使用不同技术来实施。在一些实施例中,配置不同网元来辨认装置辅助 CDR 由服务控制器 122 生成,这例如可以被提供给计费接口 127 和 / 或计费系统 123。在一些实施例中,网络生成的 CDR 由 RAN/ 接入网关 410、聚合 / 传输网关 425 和 / 或基站控制器 125 提供。在一些实施例中,其他网元生成 / 接收 / 存储装置辅助 CDR。

[0071] 在一些实施例中,提供了不同网络设备的配置来将一个给定的装置辨认为属于支持依赖和 / 或利用装置辅助 CDR 的一个服务使用和 / 或计费计划的一个装置组。

[0072] 在一些实施例中,为包括以下内容的生成 CDR 的每一个装置编程 CDR 格式、交易码以及 CDR 传输目的地:服务控制器 122 (例如,在一些实施例中,服务控制器 122 是用于 CDR 的中间物)和 / 或服务处理器 115 (例如,在一些实施例中,装置将 CDR 发送到网络 CDR 聚合或计费接口 127/ 计费系统 123,而没有中间服务器功能)。

[0073] 图 5 展示了根据一些实施例的用于提供装置辅助 CDR 的一个网络架构。如所示,网络生成的 CDR 从不同网元发送到 CDR 存储、聚合、调解、馈送 118 和服务控制器 122,如图 5 中具有箭头的虚线所示。在一些实施例中,网络生成的 CDR 用于验证装置辅助服务(DAS)使用和 / 或计费信息。在一些实施例中,将网络生成的 CDR 提供给服务控制器 122,并且该服务控制器 122 实施聚合和 / 或调解规则,从而检查并且在一些情况下聚合和 / 或调解网络生成的 / 基于网络的 CDR 与装置辅助的 / 基于装置的 CDR。

[0074] 在一些实施例中,装置辅助 CDR 从服务控制器 122 发送到 CDR 存储、聚合、调解、馈送 118 并且传递到计费系统 123,如图 5 中具有箭头的实线所示。在一些实施例中,CDR 存储、聚合、调解、馈送 118 使用 DAS 服务使用 CDR,来增添具有账户账单码的网络生成的 / 基于网络的 CDR (例如,如在此所类似地描述)。在一些实施例中,CDR 存储、聚合、调解、馈送 118 实施聚合和 / 或调解规则,来对一个新的账户账单交易码中的 DASCDR 使用量记账,并且从大块装置账户交易码中移除相同服务使用量。在一些实施例中,一个第一 DAS CDR 通过账户交易码而发送给新账单,并且一个第二 DAS CDR 被发送而用作对主装置使用账户交易码的一个校正(信用),并且 CDR 存储、聚合、调解、馈送 118 实施规则来执行这个调解。在一些实施例中,一个第一 DAS CDR 用于一个给定的账户账单交易码,并且一个第二 DAS CDR 用作主装置账户交易码,其中服务控制器 122 (或装置)已经实施了调解规则,这样使得 CDR 存储、聚合、调解、馈送 118 仅使这类 DAS CDR 在聚合其之后通过计费。

[0075] 图 6 展示了根据一些实施例的用于提供装置辅助 CDR 的另一个网络架构。图 6 也分别使用具有箭头的实线和虚线来展示装置辅助 CDR 和网络生成的 CDR 的通信。如所示, 在一些实施例中, CDR 存储、聚合、调解、馈送 118 为了不同的目的而将基于网络的 CDR 发送到服务控制器 122, 如以前在此所描述的这些。

[0076] 在一些实施例中, 服务控制器 122 发送 DAS CDR 来通过计费系统 123 而对不同使用进行计费。在一些实施例中, 计费系统 123 使用 DAS 服务使用 CDR 来为基于网络的 CDR 增添账户账单交易码。在一些实施例中, 计费系统 123 实施聚合和 / 或调解规则, 来对一个新的账户账单交易码中的 DAS CDR 使用量记账, 并且从大块装置账户交易码中移除相同服务使用量。在一些实施例中, 一个第一 DAS CDR 通过账户交易码而发送给新的账单, 并且一个第二 DAS CDR 被发送而用作对主装置使用账户交易码的一个校正(信用), 并且计费系统 123 实施规则来执行这个调解。在一些实施例中, 一个第一 DAS CDR 用于一个给定的账户账单交易码, 并且一个第二 DAS CDR 用作主装置账户交易码, 其中服务控制器 122 (或装置) 已经实施了调解规则, 这样使得计费系统 123 仅使这类 DAS CDR 在聚合其之后通过。

[0077] 图 7 展示了根据一些实施例的用于提供装置辅助 CDR 的另一个网络架构。图 7 也分别使用具有箭头的实线和虚线来展示装置辅助 CDR 和网络生成的 CDR 的通信。除如图 7 所示, 服务使用信息通过计费接口 127 而不是计费 CDR 聚合接口之外, 图 7 类似于图 6。例如, 装置使用明细的账户账单信息和偏差(信用) 信息可以被格式化为一个 CDR 或可以如由计费接口 127 需要的一个较高等级语法来格式化。

[0078] 图 8 展示了根据一些实施例的用于提供装置辅助 CDR 的另一个网络架构。图 8 也分别使用具有箭头的实线和虚线来展示装置辅助 CDR 和网络生成的 CDR 的通信。在一些实施例中, 如图 8 所示, 中央提供者无需修改现有 CDR 存储、聚合、调解、馈送 118, 因此以上相对于图 5 所论述的另外聚合和调解规则被实施为一个新网络功能中的一个新的规则层, 展示为处于计费系统与 CDR 存储、聚合、调解、馈送 118 之间的次级 DASCDR 聚合调解 118A。例如, 这个新的网络功能(例如次级 DAS CDR 聚合调解 118A) 可以驻留在网络中(如所示)或在服务处理器 115 中、在服务控制器 122 中或在网络中或在装置中的其他地方。

[0079] 图 9 为根据一些实施例的展示一个基于装置的服务处理器 115 和一个服务控制器 122 的功能图。例如, 这提供了基于特征较全面的装置的服务处理器实现方式和服务控制器实现方式。如所示, 这对应于其中服务控制器 122 连接至互联网 120 而不直接连接接入网络 1610 的一种联网配置。如所示, 以实线连接展示了一个数据平面(例如, 服务业务量平面) 通信路径, 而且以虚线连接展示了控制平面(例如, 服务控制平面) 通信路径。如将清楚的是, 在一个装置代理与另一个装置代理之间的功能性划分是基于例如设计选择项、联网环境、装置和 / 或服务 / 应用以及可用于各种不同的实现方式的各种不同的组合。例如, 能够以产品设计者认为合适的任何方式重新绘出功能线。如所示, 这包括用于装置代理的作为一个说明性的实现方式的某些划分和功能爆发区, 尽管潜在地更复杂的其他实施例可以包括用于装置代理功能性规范的不同的划分和功能爆发区例如以便管理开发规范和测试复杂性以及工作流程。另外, 在各种实施例中, 可以移动或重新排序运行、与数据路径交互作用或监控数据路径的代理的放置。例如, 以下相对于图 10 和图 11 来描述图 9 所示的功能元件。

[0080] 如图 9 所示, 服务处理器 115 包括一个服务控制装置链路 1691。例如, 由于涉及在

一个网络上的监视的基于装置的服务控制技术变得更复杂,具有在装置代理与网元之间的对服务策略进行通信、控制、监控或验证的一个高效而且灵活的控制平面通信链路变得越来越重要。在一些实施例中,服务控制装置链路 1691 为装置侧提供用于将服务代理传输到网元功能 / 从网元功能接收服务代理的一个系统。在一些实施例中,通过缓冲传输中的多个代理消息并将其成帧来增强该链路的业务量效率。在一些实施例中,通过控制传输频率或将传输频率链接到服务使用或业务量使用的速率来进一步改进业务量效率。在一些实施例中,使用一个或多个安全性或加密等级来使链路对于发现、窃听或受到危害而言是鲁棒的。在一些实施例中,服务控制装置链路 1691 还为代理心跳功能提供了通信链路和心跳计时。如下文所论述,在此公开的用于服务控制装置链路 1691 的各种实施例提供了用于用其他网元来传输并且接收服务策略实施、控制、监控和验证信息的一个高效的并且安全方案。

[0081] 如图 9 所示,服务控制器 122 包括一个服务控制服务器链路 1638。在一些实施例中,涉及在一个网络上(例如,在控制平面上)的监视的基于装置的服务控制技术是更复杂的,并且因为这样,具有在装置代理(例如,服务处理器 115 的)与网元(例如,服务控制器 122 的)之间的对服务策略进行通信、控制、监控、或验证的一个高效的并且灵活的控制平面通信链路变得越来越重要。例如,在服务控制器 122 的服务控制服务器链路 1638 与服务处理器 115 的服务控制装置链路 1691 之间的通信链路可以提供一个高效的并且灵活的控制平面通信链路、如图 9 所示的一个服务控制链路 1653,并且在一些实施例中,这个控制平面通信链路提供了一个安全(例如,加密的)通信链路,从而提供服务处理器 115 与服务控制器 122 之间的安全、双向的通信。在一些实施例中,服务控制服务器链路 1638 为网络侧提供了用于将服务代理传输到网元功能 / 从网元功能接收服务代理的一个系统。在一些实施例中,通过缓冲传输中的多个代理消息并将其成帧来增强该链路的业务量效率(例如,由此降低网络聊天)。在一些实施例中,通过控制传输频率和 / 或将传输频率链接到服务使用或业务量使用的速率来进一步改进业务量效率。在一些实施例中,使用一个或多个安全性和 / 或加密等级来使链路对于链路上的通信的潜在发现、窃听或受到危害而言是安全。在一些实施例中,服务控制服务器链路 1638 还为代理心跳功能提供通信链路和心跳计时。

[0082] 在一些实施例中,服务控制服务器链路 1638 为保护安全、签名、加密和 / 或以另外的方式在服务控制链路 1653 上发送此类通信之前保护通信而提供。例如,服务控制服务器链路 1638 可以为了传输而发送到传输层或直接发送到链路层。在另一个示例中,服务控制服务器链路 1638 进一步使具有传输层加密的通信安全,如 TCP TLS SSH 版本 1 或 2 或另一个安全传输层协议。作为另一个示例,服务控制服务器链路 1638 可以在链路层如使用 IPSEC、各种可能的 VPN 服务、其他形式的 IP 层加密和 / 或另一个链路层加密技术来加密。

[0083] 如图 9 所示,服务控制器 122 包括一个接入控制完整性服务器 1654。在一些实施例中,接入控制完整性服务器 1654 收集关于服务策略、服务使用、代理配置和 / 或代理行为的装置信息。例如,接入控制完整性服务器 1654 可交叉检查这个信息从而识别在服务策略实施和控制系统中的完整性破坏。在另一个示例中,接入控制完整性服务器 1654 可以在怀疑有一个服务策略违反或一个系统完整性破坏时发起行动。

[0084] 在一些实施例中,接入控制完整性服务器 1654 (和 / 或服务控制器 122 的另一其他代理)在接入控制完整性代理 1694 的报告和错误条件上作用。接入控制完整性代理 1654 的许多检查可以由服务器实现。例如,接入控制完整性代理 1654 检查包括以下各项中的一

项或多项；针对与策略一致的使用范围的服务使用度量（例如，来自网络和 / 或来自装置的使用度量）；代理的配置；代理的运行；和 / 或动态代理下载。

[0085] 在一些实施例中，假如策略旨在是正确的，则接入控制完整性服务器 1654（和 / 或服务控制器 122 的某一其他代理）通过将各种服务使用度量（例如，基于网络监控的信息，如通过使用 IPDR 或 CDR 和 / 或本地服务使用监控信息）与所期望的服务使用行为进行比较来验证装置服务策略实施。例如，假如策略旨在是正确的，则装置服务策略实施可以包括测量通过的总数据、在一段时间内通过的数据、IP 地址、每 IP 地址的数据和 / 或其他度量如位置、下载、接入的电子邮件、URL 以及将此类度量与所期望的服务使用行为相比较。

[0086] 在一些实施例中，接入控制完整性服务器 1654（和 / 或服务控制器 122 的某一其他代理）验证装置服务策略，并且可以指示服务度量与服务策略的一个失配的验证错误条件包括以下各项中的一项或多项：未授权的网络接入（例如，超过环境服务策略限制的接入）；未授权的网络速度（例如，超过服务策略限制的平均速度）；网络数据量不匹配策略限制（例如，在没有重新进入 / 修正服务策略的情况下，装置不停在限制处）；未授权的网络地址；未授权的服务使用（例如，VOIP、电子邮件和 / 或网页浏览）；未授权的应用使用（例如，电子邮件、VOIP、电子邮件和 / 或网络）；对于计划，服务使用速率太高，并且策略控制器不将其控制 / 节流到底；和 / 或服务度量与服务策略的任何其他失配。因此，在一些实施例中，接入控制完整性服务器 1654（和 / 或服务控制器 122 的某一其他代理）提供了一个策略 / 服务控制完整性服务，从而连续地（例如，周期性地和 / 或基于触发事件）验证装置的服务控制未受危害和 / 或未表现在策略外。

[0087] 如图 9 所示，服务控制器 122 包括一个服务历史服务器 1650。在一些实施例中，服务历史服务器 1650 从接入网络 AAA 服务器 1621 和服务监控代理 1696 收集并记录服务使用或服务活动报告。例如，尽管在某些实施例中，来自网元的服务使用历史可以是比来自装置的服务历史更不详细的，来自网络的服务历史可以为装置服务策略实施的验证提供一个有价值的源，因为例如，对于装置上的一个装置错误或危害事件而言，危害基于网络的设备和软件是十分困难的。例如，来自装置的服务历史报告可以包括不同服务跟踪信息，如以上所类似地描述。在一些实施例中，服务历史服务器 1650 根据请求来向其他服务器和 / 或一个或多个代理提供服务历史。在一些实施例中，服务历史服务器 1650 向装置服务历史 1618 提供服务使用历史。在一些实施例中，为了协助激活跟踪服务功能（以下描述）的目的，服务历史服务器 1650 维护装置已连接至其上的网络的历史。例如，这个网络活动汇总可以包括对所接入的网络、每次连接的活动 vs 时间和 / 或每次连接的业务量 vs 时间的汇总。作为另一个示例，可以进一步分析或报告这个活动汇总，从而为了计费共享调和的目的，估计与业务量活动相关联的服务计划的类型。

[0088] 如图 9 所示，服务控制器 122 包括一个策略管理服务器 1652。在一些实施例中，策略管理服务器 1652 经过服务控制链路 1653 将策略传输到服务处理器 115。在一些实施例中，策略管理服务器 1652 根据一个装置服务配置文件管理在装置上的策略设置（例如，如在此相对不同实施例所描述的不同策略设置）。在一些实施例中，策略管理服务器 1652 在策略实施代理（例如，策略实施代理 1690）上设置瞬时策略。例如，策略管理服务器 1652 可以下发策略设置、监控服务使用，并且必要时，修改策略设置。例如，在一位用户为网络而优选去管理其服务使用成本的情况下，或在需要任何自适应策略管理的情况下，策略管理服

服务器 1652 可以维护与装置进行的一个较高通信频率来收集业务量和 / 或服务度量并且下发新的策略设置。在这个示例中,周期性地和 / 或基于各种触发 / 事件 / 请求向策略管理服务器 1652 报告装置监控的服务度量和任何用户服务策略偏好的变化。在这个示例中,用户隐私设置通常要求与网络(例如,安全服务控制链路 1653)进行安全通信,如通过策略管理服务器 1652,从而保证在这类在网络上传输的配置请求 / 策略设置过程中,用户隐私的不同方面是被适当维护。例如,可以将信息划分到服务策略管理,并且不与用于 CRM 的其他数据库通信,从而维护用户隐私。

[0089] 在一些实施例中,策略管理服务器 1652 在装置上提供自适应策略管理。例如,策略管理服务器 1652 可以下发策略设置和目标,并依赖基于装置的策略管理(例如,服务处理器 115)来进行一些或所有的策略自适应。本方法可能需要较少的与装置的交互作用,由此为装置策略管理(例如,相对于以上描述的基于不同服务器 / 网络的策略管理方法,减少了网络聊天)的目的,降低在服务控制链路 1653 上的网络聊天。本方法还可以通过允许用户为了用户隐私偏好 / 设置来配置装置策略而提供鲁棒的用户隐私实施例,这样使得例如在没有用户的批准的情况下,敏感的信息(例如,地理位置数据、网站历史)不能与网络进行通信。在一些实施例中,策略管理服务器 1652 基于当日时间来调整服务策略。在一些实施例中,策略管理服务器 1652 接收、请求或以另外方式获得网络可用性的一个度量并且基于可用的网络容量来调整业务量成形策略和 / 或其他策略设置。

[0090] 如图 9 所示,服务控制器 122 包括一个网络业务量分析服务器 1656。在一些实施例中,网络业务量分析服务器 1656 为多个装置和 / 或多组装置收集 / 接收服务使用历史并且分析服务使用。在一些实施例中,网络业务量分析服务器 1656 以不同格式来呈现服务使用数据,从而识别网络服务质量和 / 或服务收益性的改进。在其他实施例中,网络业务量分析服务器 1656 为在可变设置下的网络在潜在的服务策略上估计服务质量和 / 或服务使用。在其他实施例中,网络业务量分析服务器 1656 通过引起问题的一个或多个装置为总网络服务质量或服务费用识别实际的或潜在的服务行为。

[0091] 如图 9 所示,服务控制器 122 包括一个 β 测试服务器 1658。在一些实施例中,该 β 测试服务器 1658 向一个或多个装置发布候选的服务计划策略设置。在一些实施例中, β 测试服务器 1658 为一个或多个候选的服务计划策略设置提供网络服务使用或用户反馈信息的汇总报告。在一些实施例中, β 测试服务器 1658 提供了一种针对不同的候选服务计划策略设置来比较 β 测试结果或为了进一步的策略设置优化而选择最优的候选者的机制。

[0092] 如图 9 所示,服务控制器 122 包括一个服务下载控制服务器 1660。在一些实施例中,该服务下载控制服务器 1660 提供了一个下载功能来安装和 / 或更新装置上的服务软件元件(例如,服务处理器 115 和 / 或服务处理器 115 的代理 / 组件),如在此所描述。

[0093] 如图 9 所示,服务控制器 122 包括一个计费事件服务器 1662。在一些实施例中,该计费事件服务器 1662 收集计费事件,向服务处理器 115 提供服务计划信息,向服务处理器 115 提供服务使用更新,用作装置和中央计费服务器 1619 之间的接口和 / 或为某些电子商务计费交易提供可信的第三方功能。

[0094] 如图 9 所示,接入网络 AAA 服务器 1621 与接入网络 1610 进行网络通信。在一些实施例中,接入网络 AAA 服务器 1621 提供必需的接入网络 AAA 服务(例如,对于装置接入层

的接入控制和授权功能)来允许装置到中央提供者接入网络和服务提供者网络上面。在一些实施例中,需要接入控制的另一个层来用于装置接入其他网络如互联网、一个企业网络和/或一个机器到机器网络。接入控制的这个附加层可以例如由服务处理器 115 在装置上实施。在一些实施例中,接入网络 AAA 服务器 1621 还提供了基于从服务控制器 122 接收的通信来为一个装置暂停服务并且为一个装置恢复服务的能力。在一些实施例中,接入网络 AAA 服务器 1621 在调用一个装置隔离条件时还提供为装置业务量引导路由选择到一个隔离网络或约束或限制网络接入的能力。在一些实施例中,接入网络 AAA 服务器 1621 还记录并且报告装置网络服务使用(例如,可以将装置网络服务使用报告到装置服务历史 1618)。

[0095] 如图 9 所示,装置服务历史 1618 与接入网络 1610 进行网络通信。在一些实施例中,装置服务历史 1618 在不同实施例中提供了用于不同目的服务使用数据记录。在一些实施例中,装置服务历史 1618 用于辅助验证服务策略实施。在一些实施例中,装置服务历史 1618 用于验证服务监控。在一些实施例中,装置服务历史 1618 用于验证计费记录和/或计费策略实施。在一些实施例中,装置服务历史 1618 用于同步和/或验证本地服务使用计数器。

[0096] 如图 9 所示,中央提供者计费服务器 1619 与接入网络 1610 进行网络通信。在一些实施例中,中央提供者计费服务器 1619 为中央提供者计费事件提供一个调解功能。例如,中央提供者计费服务器 1619 可以接受服务计划变化。在一些实施例中,中央提供者计费服务器 1619 提供在装置服务使用、服务计划限制和/或服务策略上的更新。在一些实施例中,中央提供者计费服务器 1619 收集计费事件,将账单用公式写出,为服务用户开账单,向服务控制器 122 和/或装置 100 提供某些计费事件数据和服务计划信息。

[0097] 如图 9 所示,在一些实施例中,调制解调器选择和控制 1811 选择接入网络连接并且与调制解调器防火墙 1655 进行通信,并且调制解调器驱动器 1831、1815、1814、1813、1812 为一个或多个调制解调器将数据业务量转换为调制解调器总线业务量,并且与调制解调器选择和控制 1811 进行通信。在一些实施例中,基于所选择的网络连接选择不同的配置文件(例如,针对 WWAN、WLAN、WPAN、以太网和/或 DSL 网络连接的不同的服务配置文件/策略),其在此也称为多模式配置文件设置。例如,服务配置文件设置可以基于 Wi-Fi 之后的真实接入网络(例如,家庭 DSL/ 电缆或工作网络)而不是它是 Wi-Fi (或其他任何网络,如 DSL/ 电缆、卫星、或 T-1) 的事实,其被视为与在咖啡店接入一个 Wi-Fi 网络不同。例如,在其中大量用户存在于 DSL 或 T-1 回程链路上的 Wi-Fi 热点状况中,服务控制器可处于一个服务提供者云或一个 MVNO 云中,服务控制可以由服务提供者提供的一个 VSP 能力提供,或者服务控制器可以由其自身使用服务控制器而不与接入网络服务提供者具有任何关联的热点服务提供者拥有。例如,服务处理器可以由服务控制器控制,从而根据 QoS 或用户共享规则(例如,与一些比其他用户具有更高的区别优先级(潜在地为了更高的服务支付)的用户)在热点划分可用带宽。作为另一个示例,可以为热点提供环境服务(如在此所类似地描述),以用于经过验证的服务处理器。

[0098] 在一些实施例中,服务处理器 115 和服务控制器 122 能够分配与多个服务计划相关联的多个服务配置文件,用户单独地或组合作为一个包而选择这些服务配置文件。例如,装置 100 由包括免费交易服务的环境服务开始,在免费交易服务中用户支付交易或事件而不是基本的服务(例如,新闻服务、电子阅读器、PND 服务、到期即付会话互联网),在这些交

易和事件中每个服务是由账户账单能力所支持的,从而正确地将任何受补贴的伙伴计费计算在内,以提供交易服务(例如,巴诺书店(Barnes and Noble)可支付电子阅读器服务并且向服务提供商提供收益股份,而用于从装置 100 购买的任何书籍或杂志交易)。在一些实施例中,账户账单服务还可以跟踪交易,并且在一些实施例中,为了收益分享的目的广告都使用在此披露的服务监控能力。在发起具有以上论述的免费环境服务的服务之后,用户随后可以选择一个后付月度互联网、电子邮件以及 SMS 服务。在这种情况下,服务控制器 122 在基于网络的计费的情况下将从计费系统 123(或在一些实施例中,在基于装置的计费的情况下,服务控制器 122 计费事件服务器 1622)获得用于新的互联网、电子邮件以及 SMS 服务的计费计划代码。在一些实施例中,这个代码是在一个数据库(例如,策略管理服务器 1652)中交叉引用的,从而与初始环境服务相组合来为新的服务找到适合的服务配置文件。随后应用新的超集服务配置文件,这样使得用户保持对环境服务的免费接入,并且计费伙伴继续补助那些服务,用户还获得到互联网服务的接入并且可以选择服务控制配置文件(例如,从在此所披露的实施例之一中)。超集配置文件是当把配置文件应用到相同的装置 100 服务处理器时提供两个或更多个服务配置文件的组合能力的配置文件。在一些实施例中,当一个以上的“可堆栈的”服务由用户选择或以另外方式应用到装置时,装置 100(服务处理器 115)可确定超集配置文件而不是服务控制器 122。在此描述的服务处理器 115 和服务控制器 122 实施例的灵活性考虑了有待单独地定义并应用的各种各样的服务配置文件,或者作为一个超集来达到所需的装置 100 服务特征。

[0099] 如图 9 所示,一个代理通信总线 1630 代表用于为不同服务处理器 115 代理和功能提供通信的一个功能描述。在一些实施例中,如图 9 中所示的功能图中所代表,总线的架构通常是多点到多点的,这样使得任何代理可以与任何其他代理、服务控制器或在一些情况中的装置的其他组件(如用户接口 1697 和 / 或调制解调器组件)进行通信。如以下所描述,该架构对于某些代理或通信交易而言还可以是点到点的,或为代理框架中的点到多点的,这样使得可以集中、或保护安全、或控制、或限制、或记录或报告所有的代理通信。在一些实施例中,代理通信总线被保护安全、签名、加密、隐藏、分区和 / 或以另外方式使其免受未授权的监控或使用。在一些实施例中,一个应用接口代理(未展示)用于字面地标记或实质上标记应用层业务量,这样使得这个或这些策略实施代理 1690 具有必需的信息来实施所选择的业务量成形解决方案。在一些实施例中,一个应用接口代理(未展示)与不同应用进行通信,包括一个 TCP 应用 1604、一个 IP 应用 1605 以及一个语音应用 1602。

[0100] 在一些实施例中,提供了用于提供一个活动映射从而将服务使用活动分类或归类的装置辅助服务(DAS)技术,以将不同的受监控的活动(例如,通过 URL、通过网络域、通过网站、通过网络业务量类型、通过应用或应用类型和 / 或任何其他的服务使用活动归类 / 分类)与关联的 IP 地址相关联。在一些实施例中,服务处理器 115 的一个策略控制代理(未展示)、服务监控器代理 1696 或另一个代理或功能(或其组合)提供了一个 DAS 活动映射。在一些实施例中,服务处理器的一个策略控制代理、服务监控器代理或另一个代理或功能(或其组合)提供了一个活动映射,从而将服务使用活动分类或归类,以将不同的受监控的活动(例如,通过统一资源定位符(URL)、通过网络域、通过网站、通过网络业务量类型、通过应用或应用类型和 / 或任何其他的服务使用活动分类 / 归类)与关联的 IP 地址相关联。在一些实施例中,服务处理器的一个策略控制代理、服务监控器代理或另一个代理或功能(或其组

合)使用不同技术来确定针对所监控的服务使用活动的相关联的 IP 地址从而来监听这个或这些 DNS 请求(例如,通过在装置 100 上执行此类监听技术,可以确定相关联的 IP 地址而无需可逆 DNS 查找的网络请求)。在一些实施例中,服务处理器的一个策略控制代理、服务监控器代理或另一个代理或功能(或其组合)记录并报告 IP 地址或包括 DNS 查找功能来报告 IP 地址或针对所监控的服务使用活动的 IP 地址和相关联的 URL。例如,服务处理器的一个策略控制代理、服务监控器代理或另一个代理或功能(或其组合)可以使用不同技术来确定针对所监控的服务使用活动的相关联的 IP 地址,从而执行 DNS 查找功能(例如,使用在所监控的装置 100 上的本地 DNS 高速缓存存储器)。在一些实施例中,这些技术中的一个或多个用于动态地建立及维护一个 DAS 活动映射,该 DAS 活动映射当可适用时将例如 URL 映射到 IP 地址、将应用映射到 IP 地址、将内容类型映射到 IP 地址和 / 或将任何其他可能的归类 / 分类映射到 IP 地址。在一些实施例中,DAS 活动映射用于不同的 DAS 业务量控制和 / 或节流技术,如在此相对于不同实施例所描述。在一些实施例中,DAS 活动映射用于向用户提供不同 UI 相关的信息和与服务使用相关的通知技术,如在此相对于不同实施例所描述。在一些实施例中,DAS 活动映射用于提供服务使用监控、未来服务使用预测 / 估计、服务使用计费(例如账户账单和 / 或其他服务使用 / 计费归类技术)、用于环境服务使用监控的 DAS 技术、用于生成微型 CDR(例如,也称为服务使用分区、服务使用记录分区、服务收费存储区、装置生成的 CDR,如在装置而不是一个网络组件生成使用记录、环境使用记录、专门的服务使用记录或生成的指示一个服务使用数据记录的其他条款从而为装置提供一个更精确的或更详细的服务使用分解的情况下)的 DAS 技术和 / 或如在此相对于不同实施例所描述的任何不同的其他 DAS 相关的技术。

[0101] 在一些实施例中,在此披露的服务处理器 115 的所有或部分的功能在软件中实施。在一些实施例中,服务处理器 115 的所有或部分的功能在硬件中实施。在一些实施例中,服务处理器 115 的所有或大体上所有功能性(如在此所论述的)在软件中实施并且存储,该软件可在装置 100 的不同组件上运行(例如,由其执行)。在一些实施例中,在所保护的或安全存储器中存储或实施某些部分或所有的服务处理器 115 是有利的,这样使得其他不希望的程序(和 / 或未授权的用户)在服务处理器 115 中难以接入功能或软件。在一些实施例中,服务处理器 115 至少部分地实施在和 / 或存储在安全非易失性存储器上(例如,非易失性存储器可以是安全非易失性存储器),该非易失性存储器在没有通过密钥和 / 或其他安全性机制的情况下是不可接入的。在一些实施例中,将服务处理器 115 软件的至少一部分加载到被保护的、非易失性存储器的能力还需要一个安全密钥和 / 或签名和 / 或需要加载到非易失性存储器中的服务处理器 115 软件组件也被安全地加密并且由一个权威机构正确地签名,该权威机构是为安全软件下载器功能所信任的,如在图 16 所示的服务下载器 1663。在一些实施例中,安全软件下载器还使用一个安全非易失性存储器。本领域普通技术人员还将会认识到所有的存储器可以是芯片上的、芯片外的、板上的和 / 或板外的。

[0102] 图 10 根据一些实施例提供了汇总不同服务处理器 115 功能元件的表。这些代理中的许多个类似于以上所描述,并且图 10 所示的表既不旨在是对这些代理的一个详尽的汇总,也不是对这些代理执行的或在此描述的所有功能的一个详尽的描述,相反地图 10 被提供为理解以下各项的一个汇总帮助:根据一些实施例的每一个代理的基本功能;和这些代理如何与彼此、与服务控制器服务元件和 / 或与在某些实施例中的其他网络功能交互作

用,从而来形成一个可靠的基于装置的服务投递解决方案和 / 或平台。

[0103] 图 11 提供了汇总根据一些实施例的不同服务控制器 122 功能元件的表。这些代理 / 元件中的许多个类似于以上所描述,并且图 11 所示的表既不旨在是对这些服务器元件的一个详尽的汇总,也不是对这些元件执行的或在此描述的所有功能的一个详尽的描述,相反地图 11 被提供为理解以下各项的一个汇总帮助:根据一些实施例的每一个元件的基本功能;和这些元件如何与彼此、与某些网元和 / 或与在某些实施例中的服务处理器代理交互作用,从而来形成一个可靠的基于装置的服务投递解决方案和 / 或平台。

[0104] 图 12 展示了根据一些实施例的一个装置堆栈,该装置堆栈从联网堆栈中的不同点提供不同服务使用测量,以用于一个服务监控器代理、一个计费代理以及一个接入控制完整性代理从而来帮助验证服务使用度量和计费报告。如图 12 所示,若干服务代理参与数据路径运行来达到不同数据路径改进,并且例如,若干其他服务代理可以为数据路径服务管理策略设置、为数据路径服务实施计费、为接入网络连接管理一个或多个调制解调器选择和设置、与用户和 / 或提供服务策略实施验证连接。另外,在一些实施例中,若干代理执行功能来辅助验证:旨在是合适的服务控制或监控策略被正确地实施,这些服务控制或监控策略被正确地遵守;服务处理器或一个或多个服务代理正在正确地运行,从而阻止在策略实施或控制中的非计划中的错误和 / 或阻止篡改服务策略或控制。如所示,标识为 I 至 VI 的服务测量点代表用于服务监控器代理 1696 和 / 或其他代理的不同服务测量点,以执行不同服务监控活动。在在此描述的不同实施例中,这些测量点中的每一个可以具有一个有用的目的。例如,在一个给定的设计中采用的业务量测量点中的每一个均可以由一个监控代理使用,以跟踪穿过通信堆栈的应用层业务量,从而协助策略实施功能,如策略实施代理 1690,或在一些实施例中的调制解调器防火墙代理 1655 或应用接口代理,在有时难于或不可能做业务量参数的一个完整决定的情况下,一旦在通信堆栈中的业务量较低,该调制解调器防火墙代理或应用接口代理则做关于业务量参数或类型的决定。在这些图中提供的对于测量点的特殊的位置旨在作为指导的示例,并且其他测量点可以用于不同的实施例,如鉴于在此所描述的实施例本领域普通技术人员将清楚。通常,在一些实施例中,在装置内的一个或多个测量点可以用于辅助服务控制验证和 / 或装置或服务故障排除。

[0105] 在一些实施例中,服务监控器代理和 / 或其他代理通过跟踪或追踪通过不同通信堆栈格式化、处理以及加密步骤的包流,并且向监控、控制、成形、节流或以另外方式观察、操纵或修改业务量的不同代理提供虚拟标签信息来实施虚拟的业务量标记。这个标记方法在此称为虚拟标记,因为不存在字面数据流、业务量流或附装到流或数据包的包标签,并且代替地,标记数据包的簿记通过跟踪或追踪通过堆栈的流或数据包完成。在一些实施例中,应用接口和 / 或其他代理识别一个业务量流,将其与一个服务使用活动相关联并且引起一个字面标签附装到与活动相关联的业务量或数据包上。这个标记方法在此称为字面标记。虚拟标记和字面标记方法二者都存在很多优点。例如,在一些实施例中优选的是,通过分配一个字面标签来降低跟踪或追踪通过堆栈处理的一个数据包所需的代理间通信,从而使得每一个流或数据包具有嵌入数据的其自身的活动关联。作为另一个示例,在一些实施例中优选的是,重新使用标准通信堆栈软件或组件的多个部分,从而通过插入与不同服务代理相关联的另外处理步骤并且监控多个点来增强标准堆栈的可验证的业务量控制或服务控制能力,而不是重写整个堆栈以正确地处理字面标记信息,并且在这类情况下,可能需要虚

拟标记方案。仍作为另一个示例,为一个数据包帧或流中的未使用的、未指定的或以另外方式可用的位字段提供一些标准通信堆栈,并且这些未使用的、未指定的或以另外方式可用的位字段可以用于字面地标记业务量,而无需重写所有标准通信堆栈软件,其中仅有被添加以增强标准堆栈的可验证的业务量控制或服务控制能力的堆栈的那些部分需要解码并且使用在可用的位字段中加密的字面标记信息。在字面标记的情况下,在一些实施例中,在将数据包或流传送到网络或传送到使用堆栈的应用之前移除这些标签。在一些实施例中,可以将实施虚拟或字面标记的方式发展成为一个通信标准规范,从而使得不同装置或服务产品开发者可以与服务控制器规范和其他装置或服务产品开发者的产品兼容的方式独立地开发通信堆栈和 / 或服务处理器硬件和 / 或服务软件。

[0106] 将认识到虽然在图 12 中展示的任何或所有测量点的实施 / 使用不需要具有一个有效的实施,如相对在此所描述的不同实施例而类似地展示,不同实施例可以从这些和 / 或类似的测量点中受益。还将认识到可以将准确的测量点移动到业务量处理堆栈中的不同位置,正如在此所描述的各实施例,在仍保持有效的运行时,可以具有影响移动到业务量处理堆栈中的不同点的策略实施的代理。在一些实施例中,一个或多个测量点被更深地提供在调制解调器堆栈中,其中例如如果将调制解调器设计为具有正确的软件和 / 或硬件安全性来保护调制解调器堆栈和一个或多个测量点的完整性,则更困难的是绕过并且可能更困难的是为了篡改的目的而接入。

[0107] 参见图 12,如所示从堆栈的底部到顶部描述了装置通信堆栈,该装置通信堆栈为在装置通信堆栈底部的装置的调制解调器中的每一个提供了一个通信层。示例测量点 VI 驻留在调制解调器驱动器层内或仅在其上。例如,调制解调器驱动器执行调制解调器总线通信、数据协议转换、调制解调器控制和配置,从而将联网堆栈业务量连接至调制解调器。如所示,测量点 VI 对于所有的调制解调器驱动器和调制解调器是共用的,并且对于某些实施例,区别从一个调制解调器穿过一个或多个其他调制解调器而发生的业务量或服务活动是有利的。在一些实施例中,测量点 VI 或另一个测量点处于一个或多个单独的调制解调器驱动器的上方、其内或下方。对于每一个调制解调器的对应调制解调器总线驻留在示例测量点 V 和 VI 之间。在下一个更高的层中,提供了用于基于多模式装置的通信的一个调制解调器选择和控制层。在一些实施例中,在这些网络中的一个是在可用的条件下,这个层由为一些或所有数据业务量选择最希望的网络调制解调器的一个网络决定策略控制,并且当最希望的网络不可用时,策略恢复到下一个最令人希望的网络,直到建立了一个连接。在一些实施例中,即使当这些数据业务量的一些或所有被路由选择到另一个网络时,某些网络业务量如验证、控制、冗余或安全业务量也被路由选择到这些网络中的一个。这个双重路由选择能力为多种增强的安全性、增强的可靠性或增强的可管理性装置、服务或应用提供。在下一个更高的层中,提供了一个调制解调器防火墙。例如,调制解调器防火墙提供传统的防火墙功能,但与传统的防火墙不同,为了依赖防火墙从而进行可验证的服务使用控制,如接入控制和阻止不想要的联网业务量或应用的安全性保护,将在此描述的不同服务验证技术和代理添加到防火墙功能,以验证与服务策略的兼容性并且阻止对服务控制的篡改。在一些实施例中,在堆栈上的很远处可能地与其他层相组合来实施调制解调器防火墙,如在其他图所示。在一些实施例中,提供了独立于其他处理层,如策略实施层、数据包转发层和 / 或服务应用层的专门的防火墙功能或层。在一些实施例中,在堆栈下的很远处实施调制解调器

防火墙,如在调制解调器驱动器内、在调制解调器驱动器下方、或在调制解调器自身中。示例测量点 IV 驻留在调制解调器防火墙层与一个 IP 排队和路由选择层之间。如所示,IP 排队和路由选择层与策略实施层分离,其中策略实施代理实施业务量控制和 / 或服务使用控制策略的一部分。如在此所描述,在一些实施例中,这些功能是分离的,这样使得一个标准网络堆栈功能可以用于 IP 排队和路由选择,并且实施策略实施代理功能必需的修改可以被提供在插入到标准堆栈中的一个新的层中。在一些实施例中,IP 排队和路由选择层与业务量或服务使用控制层相组合。例如,一个组合的路由选择和策略实施层实施例还可以与其他实施例一起使用,如图 12 所示。测量点 III 驻留在 IP 排队和路由选择层与一个策略实施代理层之间。测量点 II 驻留在策略实施代理层与传输层之间,包括 TCP、UDP、和如所示的其他 IP。会话层驻留在传输层的上方,其被示为套接字分配和会话管理(例如,基本 TCP 建立、TLS/SSL)层。网络服务 API (例如,HTTP、HTTPS、FTP (文件传送协议)、SMTP (简单邮件传送协议)、POP3、DNS) 驻留在会话层的上方。测量点 I 驻留在网络服务 API 层和应用层之间,示为图 12 中的装置通信堆栈中的应用服务接口代理。

[0108] 如图 12 所示,应用服务接口层在标准联网堆栈 API 的上方,并且在一些实施例中,其功能是监控,而在一些情况下是拦截并且处理在应用与标准联网堆栈 API 之间的业务量。在一些实施例中,在应用业务量流更困难或几乎不可能在堆栈中较低处识别之前,应用服务接口层识别应用业务量流。在一些实施例中,应用服务接口层以这种方式在虚拟和字面标记两种情况下辅助应用层标记。在上游业务量的情况下,应用层标记是直通的,因为业务量在应用层发起。在一些下游实施例中,其中业务量或服务活动分类依赖容易获得的业务量属性,如源地址或 URL、应用套接字地址、IP 目的地地址、当日时间或任何其他容易获得的参数,业务量类型可以被识别并且标记从而由防火墙代理或另一个代理(如其初始到达)处理。在其他实施例中,如在此所描述,在下游情况中,当需要其将业务量流受控制或被节流的方式进行分类的一个业务量参数,如与应用的一个方面的关联、内容类型、含有在 TLS、IPSEC 或其他安全格式中的某物或与业务量相关联的其他信息,在堆栈的较低等级上为不容易获得时,解决方案通常是更复杂的。因此,在一些实施例中,联网堆栈在其完全被表征、归类或与一个服务活动相关联之前识别业务量流,并且随后使业务量通过而到完成最终分类的应用接口层。在这类实施例中,应用接口层随后将业务量流 ID 与正确的分类相关联,这样使得在初始短业务量突发或时间段之后,策略实施代理可正确地控制业务量。在一些实施例中,还存在用于对业务量进行标记并且设置服务控制策略的一个策略,该策略不可以用标记的所有资源(包括应用层标记)完全地识别。

[0109] 如图 12 所示,一个也与代理通信总线 1630 通信的服务监控器代理与装置通信堆栈的不同层进行通信。例如,服务监控器代理在测量点 I 至 VI 的每一个上执行监控,接收包括应用信息、服务使用和其他服务相关的信息以及分配信息的信息。一个接入控制完整性代理经过代理通信总线 1630 与服务监控器代理进行通信,也如所示。

[0110] 图 13 展示类似于图 12 的一个实施例,其中根据一些实施例,服务处理器的一部分实施在调制解调器上,并且服务处理器的一部分实施在装置应用程序处理器上。在一些实施例中,服务处理器的一部分实施在调制解调器上(例如,在调制解调器模块硬件或调制解调器芯片集上),并且服务处理器的一部分实施在装置应用程序处理器子系统上。本领域普通技术人员将清楚的是图 13 中所描绘的实施例的变体是可能的,其中更多或更少的服务

处理器功能性移动到调制解调器子系统上或装置应用程序处理器子系统上。例如,与图 13 中所描绘的实施例类似的这类实施例可由包括调制解调器子系统上的一些或所有服务处理器网络通信堆栈处理和 / 或一些或所有其他服务代理功能的优点推动(例如,并且这类方法可以应用到一个或多个调制解调器)。例如,可以将服务处理器分布为含有于软件包的一个调制解调器芯片集硬件或调制解调器模块软件或软件包中的一个标准特征集,并且这类配置可以提供由装置 OEM 的更容易的采纳或开发、针对芯片集或调制解调器模块制造商的一个更高等级的区别、更高等级的性能或服务使用控制实施完整性或安全性、规范或互操作性标准化和 / 或其他益处。

[0111] 参见图 13,如所示从堆栈的底部到顶部描述了装置通信堆栈,该装置通信堆栈为在装置通信堆栈底部的调制解调器 MAC/PHY 层提供了一个通信层。测量点 IV 驻留在调制解调器 MAC/PHY 层的上方。调制解调器防火墙层驻留在测量点 IV 与 III 之间。在下一个较高的层中,提供了策略实施代理,其中该策略实施代理在调制解调器上(例如,在调制解调器硬件上)实施。测量点 II 驻留在策略实施代理与调制解调器驱动器层之间,测量点 II 随后在一个调制解调器总线层的下方展示。下一个较高的层被示为 IP 排队和路由选择层,在包括 TCP、UDP、及其他所示的 IP 的传输层之后。会话层驻留在传输层的上方,其被示为一个套接字分配和会话管理(例如,基本 TCP 建立、TLS/SSL)层。网络服务 API (例如,HTTP、HTTPS、FTP (文件传送协议)、SMTP (简单邮件传送协议)、POP3、DNS) 驻留在会话层的上方。测量点 I 驻留在网络服务 API 层与一个应用层之间,示为图 13 中的装置通信堆栈中的应用服务接口代理。

[0112] 图 14 展示了根据一些实施例的中间联网装置的不同实施例,这些中间联网装置包括用于可验证的服务使用测量、报告以及计费报告的目的的一个服务处理器。例如,图 14 (A) 至图 14 (E) 展示了不同的扩展调制解调器替代物,这些替代实施例通过具有一个到一个或多个装置 100 的连接(例如 LAN 连接)的一个中间调制解调器或联网装置组合而用于接入网络连接。

[0113] 在一些实施例中,装置 100 包括与到装置 100 的 Wi-Fi LAN 连接相组合的一个 3G 和 / 或 4G 网络接入连接。例如,中间装置或联网装置组合可以为仅将 Wi-Fi 数据转换到 WWAN 接入网络而没有实施如图 14 (A) 所示的服务处理器 115 的任何一部分的一个装置。在一些实施例中,一个中间装置或联网装置组合包括一种更为复杂的实现方式,该实现方式包括一个联网堆栈,并且在一些实施例中包括一个处理器,如例如在以下的情况下:如果中间联网装置或联网装置组合包括一个路由器功能,在这种情况下服务处理器 115 可以部分地或整体地在该中间调制解调器或联网装置组合上实施。该中间调制解调器或联网装置组合也可以是一个多用户装置,其中一位以上用户经过 Wi-Fi LAN 连接接入到 3G 或 4G 接入网络。在这样一类多用户网络的情况下,接入网络连接可以包括使用服务处理器 115 的多个实例化的若干受管理的服链路,每一个实例化例如全部地或部分地在装置 100 上实施,其中中间调制解调器或联网装置组合仅提供来自 Wi-Fi LAN 到 WWAN 接入网络的转换服务。

[0114] 现参看图 14 (B) 至图 14 (D),在一些实施例中,服务处理器 115 部分地或全部地在中间调制解调器或联网装置组合上实施。在服务处理器 115 部分地或全部地在中间调制解调器或联网装置组合上实施的情况下,服务处理器 115 可以为网络中的每一个装置或每

一位用户实施,这样使得存在多个受管理的服务提供者账户均通过同一中间调制解调器或联网装置组合接入。在一些实施例中,服务处理器 115 的功能在一个聚合账户上实施,该聚合账户包括用于连接至由中间调制解调器或联网装置组合提供服务的 Wi-Fi LAN 上的所有用户或装置的 WWAN 接入网络业务量。在一些实施例中,中央提供者也可以提供一个聚合的账户服务计划,如一个家庭计划、一个企业用户组计划和 / 或一个瞬时热点计划。在存在用于中间调制解调器或联网装置组合的一个账户的情况下,该中间调制解调器或联网装置组合可以实施一个服务本地划分到一个或多个装置 100 或用户,其中这些服务由该中间调制解调器或联网装置组合或装置 100 控制或管理,但是该管理不经受服务提供者控制并且辅助由服务处理器 115 执行的服务管理或服务策略实施。在一些实施例中,也可以支持另一个服务模型,其中存在与一个中间调制解调器或联网装置组合或一组中间调制解调器或联网装置组合相关联的一个聚合服务提供者计划,但其中每一个用户或装置仍具有其自身的服务计划,该计划是在该聚合计划下的一个子计划,这样使得每一个用户或装置具有拥有服务处理器 115 的一个唯一实例化的独立的服务策略实施,而不是具有服务处理器 115 的一个单个实例化的跨越组中的多个用户的聚合服务策略实施。

[0115] 如图 14 (B)所示,在一些实施例中,装置 100 包括一个 Wi-Fi 调制解调器、在中间调制解调器或联网装置组合 1510 上的与一个 3G 和 / 或 4G WWAN 调制解调器组合的一个 Wi-Fi 调制解调器,并且该中间调制解调器或联网装置组合经过 Wi-Fi 链路将 WWAN 接入网络业务量转发到装置 100 并且从装置转发 WWAN 接入网络业务量。例如,服务处理器 115 可以其整体在装置 100 上实施,并且服务提供者账户可以独占地与一个装置相关联。类似地,如图 14(C)所示,这样一类实现方式可以使用一个不同接入调制解调器和接入网络来提供,如取代到中间调制解调器或联网装置组合 1510 的 3G 和 / 或 4G 接入网络连接的一个 2G 和 / 或 3G WWAN、DSL 有线线路、电缆 DOCSIS 有线线路或光缆有线线路配置。此外,不同其他实施例类似地使用如图 14 (D) 所示的 DSL、USB、以太网、蓝牙或另外 LAN,或从装置 100 到中间调制解调器或联网装置组合 1510 的点对点连接,或如图 14 (E) 所示的一个毫微微蜂窝区调制解调器和 DSL/ 电缆 /T1/ 其他组合。

[0116] 图 15 展示了根据一些实施例的用于提供装置辅助 CDR 创建、聚合、调解以及计费的包括一个或多个代理服务器 270 的一个无线网络架构。如所示,图 2 包括与由例如一个中央提供者运行的一个 4G/3G/2G 无线网络通信的一个或多个代理服务器 270。例如,这个或这些代理服务器 270 可以用来实施和 / 或辅助提供在此所描述的不同技术,如服务使用测量和 / 或其他如在此所描述的技术。

[0117] 在一些实施例中,可能不能准确地将每个网络服务接入尝试或服务使用(例如或业务量接入)识别为属于一个给定的服务使用分区(例如,一个给定的环境服务使用、后台网络聊天使用、用户服务计划使用、紧急服务使用和 / 或其他类型的服务使用)。如在此所使用,术语“服务使用分区”、“服务使用记录分区”、“服务收费存储区”以及“微型 CDR”可互换使用。因此,令人希望的是为被允许并且未被确定地识别为属于一个已知服务收费存储区的业务量提供一个服务收费存储区。这允许技术对业务量采用一个“允许但验证”方法,该方法很可能与一个环境服务或一个用户服务或一个网络服务合法地相联系,该服务在与一个被允许的服务相关联时旨在被允许但未被确定地识别。

[0118] 作为一个示例,可能存在与一个环境服务相关联的一个网站接入,该网站接入不

具有一个引用标识符或允许服务处理器将其与正确的环境服务相关联的其他业务量参数。在这种情况下,假如接入控制策略是正确的,可以应用一个规则集来确定网站接入是否可能为一个合法的接入,并且是否可以允许该接入并且是否将该业务量使用记录在怀疑为相关联的环境服务收费存储区中,或者可以将该业务量使用记账到一个网络聊天服务使用存储区,或者可以将业务量使用记账到用户服务使用存储区,或者可以将业务量使用记录在一个“未被分类但被允许的”服务收费存储区中。在这类业务量被记账到该“未被分类但被允许的”服务使用收费存储区的一些实施例中,采用另外验证度量来确保未被分类但被允许的业务量的量不增加太大或变为用于服务使用错误的一个非法途径。例如,只要积累在该未分类的收费存储区中的服务使用费用的量保持在某些界限内,和/或被记账到该未分类的存储区的服务使用速率保持在某些界限内,用于允许未分类的业务量的接入控制策略规则就可以是相对地宽松的,但是如果该未分类的业务量变大或者未分类的业务量增长的速率变大,则操作何时允许未分类的业务量的规则可以是变紧的。

[0119] 作为另一个示例,一个浏览器应用可以接入已知为一个环境服务网站的一个网站,并且这个网站可能传回一系列的业务量流,其中的一些通过已知为网站部分的 URL 标识符来与该环境服务网站相关联,并且其他业务量可以借助于引用网站标签或报头而与环境服务网站相关联,并且一些业务量可以用近似于如环境业务量一样被识别的其他业务量的一个相对接近的时间返回到同一应用。在这个示例中,只要该未分类的业务量服务收费存储区在其尺寸上不超过一个给定的预置策略限制,和/或不比一个给定的预置策略速率增长地快,和/或在与接收其他环境服务收费存储区业务量时间不同的一个确定的预置策略时段内接收,则连续地允许该未分类的业务量。然而,如果该未分类的业务量量或增长率超过该预置策略限制,或者如果接收验证的环境服务业务量与接收该未分类的业务量的时间之间的该时段超过策略限制,则该未分类的业务量可能受阻或可能采取其他行动来进一步分析未分类的业务量。

[0120] 在一些实施例中,重要的是为一个装置上的不同服务使用分区提供一个服务使用收费规则的层级结构。作为一个示例,对于一个给定的服务计划,可以存在两个环境服务收费存储区、一个网络聊天(例如,或网络开销)服务收费存储区以及一个用户服务计划服务收费存储区,并且令人希望的是,保证没有环境服务或网络开销服务或未分类的服务被记账到用户服务计划,并且也令人希望的是,确保将所有已知环境服务业务量记账到适合的环境服务伙伴,并且令人希望的是,确保没有网络开销服务或未分类的服务被记账到环境服务伙伴。在这种状况下,可以如下提供一个服务收费存储区层级结构:确定一个业务量流(例如,或套接字)是否与网络开销相关联,并且如果是,则允许该业务量流并且对该服务存储区进行收费,随后确定一个业务量流(或套接字)是否与环境服务 #1 相关联,并且如果是,则允许该业务量流并且对该服务存储区进行收费,随后确定一个业务量流(或套接字)是否与环境服务 #2 相关联,并且如果是,则允许该业务量流并且对该服务存储区进行收费,随后确定一个业务量流(或套接字)是否与未分类的业务量相关联,并且如果是,则允许该业务量流并且对该服务存储区进行收费,随后如果该业务量不与以上服务收费存储区中的任何一个相关联,则允许该业务量流并且将其记账到该用户服务计划收费存储区。在另一个示例中,如果用户还没有选择来支付一个用户服务计划,则可以使用相同层级接入控制和服务收费策略,除将为如下的最后步骤之外:随后如果该业务量不与以上服务收费存

储区中的任何一个相关联,则阻塞该业务量。如在这些示例中所描绘的层级服务收费存储区识别可以是一个鲁棒的接入控制策略和 / 或服务收费策略系统的一个决定性方面。本领域普通技术人员现将清楚许多其他接入控制策略层级结构和服务收费存储区策略层级结构。

[0121] 在一些实施例中,该未分类的业务量根据服务收费规则来收费,这些规则依赖于该业务量的最可能的候选服务收费存储区。作为另一个示例,如果该未分类的业务量被投递到如其他已知环境业务量的同一应用,并且该已知环境服务业务量和该未分类的业务量的递送之间的时间差是小的,则可以根据指定这些条件的一个预置收费策略规则来将未分类的业务量记账到环境服务。本领域普通技术人员现将清楚其他实施例。例如,用于未分类的业务量的另一个收费规则可能执行将未分类的业务量按比例分配给所有其他服务收费存储区,其中该按比例分配基于用于每一个服务收费存储区的由装置使用的总业务量的百分比。作为另一个示例,可以根据包括于按比例分割的用于每一个服务的按比例的份额来将该未分类的业务量记账到用于装置的服务收费存储区(例如,所有环境服务加上网络开销服务)的一个子集。

[0122] 在一些实施例中,结构化用户服务计划协定,这样使得用户确认:其中接入连接至服务由一个实体而不是由用户赞助,支付和 / 或部分地补助的环境服务是有益于用户的,和 / 或用户确认:没有固有的权利来让环境服务免费,并且确认:服务使用记账系统不始终将供一个被赞助的或补助的环境服务(例如一些其他专门的服务)的使用正确地表征到正确的记账服务收费存储区中,并且因此,可能对这个业务量中的一些向用户服务计划账户收费和 / 或计费。具有了用户对这个形式的一个服务使用协定的确认,则可以将一些环境业务量记账到用户服务计划账户,包括例如被允许但未被分类的业务量、超过预置策略限制的过度的环境服务使用、在网络占线时期的过程中或对堵塞的网络资源的环境服务使用和 / 或其他判据 / 度量。在一些实施例中,可能通知用户其被收费了有时对用户而言是受补助的或免费的服务活动。如以上所论述,重要的是确保一个未分类的服务收费存储区不变为用于服务收费错误或非法侵入的一个非法途径。本领域普通技术人员现将清楚的是,可以用多种方式来验证未分类的服务使用费用,包括例如观察该未分类的服务收费存储区的尺寸而与装置上的其他服务使用费用(例如,总装置服务使用、环境服务使用、用户存储区服务使用和 / 或其他判据 / 度量)相比较、为该未分类的存储区设上限、和 / 或为该未分类的存储区的增长率设上限。

[0123] 在一些实施例中,重要的是不仅验证总装置服务使用量是正确的,而且验证服务使用正被报告在正确的服务收费存储区中。例如,如果服务处理器软件会受非法侵入,这样使得其正确地报告总服务使用,但在一个或多个环境服务存储区下报告用户服务计划业务量,则仅验证总服务使用量是正确的将不足以阻止装置获得可能被记账到环境服务伙伴的免费的用户服务。存在多种直接和间接的实施例来实现对服务收费存储区划分的这个验证。例如,在直接验证实施例中,采用服务使用的一个或多个替代度量来交叉检查服务收费存储区划分的准确性。在间接实施例中,采用以下两级验证中的一个:分析用于服务收费存储区的尺寸和增长率并且将其与一个预置组策略相比较,从而来检测和 / 或修改超过策略的服务收费存储区增长;和 / 或验证涉及服务收费存储区划分的服务处理器元件的正确的运行。

[0124] 涉及直接验证服务收费存储区使用和 / 或记账的不同实施例包括使用基于网络的服务使用度量, 如 CDR、IPDR、流数据记录 (例如, FDR—用于如打开的并且用来向装置或从装置传输数据的网络套接字连接的每一个服务流的服务使用的详细报告)、记账记录、中间记账记录或其他类似使用记录, 来验证装置是在服务策略内和 / 或基于装置的服务使用报告是准确的。在此描述这类网络生成的服务使用记录的使用来直接验证服务收费和 / 或正确的服务使用策略遵守。如在此所描述, 当网络地址目的地和 / 或源信息在这些记录中是可用时, 这可以用于一些实施例中来验证由装置服务处理器提供的服务收费存储区记账。在一些实施例中, 一些类型的服务使用记录中包括实时数据, 但不必包括帮助验证服务收费存储区记账所需的所有有用信息, 而其他类型服务使用记录提供更多明细 (例如, 用于目的地和源的 IP 地址), 但不总是实时到达。例如, 在一些实施例中, 每次打开并且随后关闭一个新服务流 (例如, 网络套接字连接), 则创建 FDR。在服务流关闭时, 指示源地址、目的地地址以及传输的数据量的一个 (例如, 可能是加时间戳的) 数据使用记录被创建并且发送到网络中的一个收费聚合功能。该收费聚合功能可以随后将这些 FDR 转发到用于验证或直接记账服务收费存储区记账的服务控制器。通过将 FDR 地址与已知环境服务业务量地址关联相比较, 可以验证一个或多个环境服务与其他服务之间的服务收费存储区, 如一个用户服务计划服务收费存储区服务收费存储区的划分。然而, 在一些情况下, 当一个装置服务流 (例如, 套接字) 保持打开一长段时间时, 可能要一长段时间来生成一个 FDR, 如例如在一个长文件下载、具有一个套接字保活的一个对等连接或具有一个套接字保活的一个代理服务器服务的情况下。在这类情况下, 可能不利的是, 具有大量待传送的数据而没有 FDR 来基于报告来确认装置服务处理器, 并且在一些情况下, 这可能为服务处理器服务报告非法侵入提供一个机会。这可以通过使用其他网络报告的服务使用信息而以各种方式补救来增添 FDR 信息。例如, 在一些实施例中, 开始和停止记账记录有时可以从一个网元中获得, 如一个服务网关或 AAA 服务器 (例如, 或取决于网络架构的其他网络设备元件)。尽管开始和停止记录不拥有 FDR、CDR、IPDR、中间记账记录或其他服务使用记录拥有的服务使用信息的明细, 但是这些开始和停止记录告知服务控制器一个装置连接至网络或者被停止连接。如果一个装置连接至网络并且不传输装置使用报告或心跳, 则向服务控制器报警: 可能有一个错误或非法侵入条件。作为两种或更多种类型的网络报告的服务使用信息可以用来创建装置服务使用上的一个更实时或接近实时的检查的另一个示例, 如果 FDR 和开始 / 停止记账记录两者是可用的, 则服务控制器可以将一个停止随后恢复服务命令发送到装置 (例如, 或可替代地, 将一个停止随后恢复服务命令发送到一个网络设备元件), 从而引起该装置在重启服务流之前终止所有打开的服务流, 并且一旦停止这些服务流, 则将完成并且传输 FDR 流记录来用于当下发停止服务命令时处于处理中但未被报告的任何服务流。这将引起在 FDR 流记录中报告任何长期打开的套接字文件传送, 因而堵塞了 FDR 服务使用记账验证方法中的潜在非法途径漏洞。

[0125] 作为展示多种类型的网络生成的服务使用记账记录如何用于彼此补充并且加强对服务收费存储区记账分区的验证的另一个示例, 中间数据记录可以与 FDR 一起使用。根据一些实施例, 中间数据记录是可用的, 其中这些中间数据记录在一个定期计划的基础上由一个网元 (例如网关、基站、HLR、AAA 和 / 或其他网元 / 功能) 生成。中间数据记录典型地为接近实时的记录, 这些记录在一个时间点时为装置报告聚合业务量使用, 但通常不包括

业务量地址信息或其他业务量明细。在其中中间记账记录和 FDR 两者均可用的实施例中，当中间记账记录正指示未在 FDR 流中报告的服务使用时，这证明一个装置具有打开的并且未终止的一个或多个长期套接字连接。在这种情况下，服务控制器可以验证：基于装置的使用报告正确地为由该中间记账记录报告的服务使用的总量记账，和 / 或服务控制器可以通过下发一个停止恢复服务命令来迫使做出针对打开的套接字的一个 FDR，如以上所类似地论述。

[0126] 如在此所描述，可以提供涉及对服务收费存储区记账的直接验证的其他实施例。一个示例为将环境服务业务量路由选择到一个代理服务器或路由器，该代理服务器或路由器被编程来支持允许环境服务的网络接入并且来为该环境服务使用记账。另外可以类似地为代理服务器或路由器编程而用于为装置服务计划的一部分的每一个环境服务，并且在一些实施例中，为另一个代理服务器或路由器编程来支持业务量控制并且为用户服务计划服务接入记账。通过为这些代理服务器或路由器中的每一个比较服务使用记账，可以直接验证装置生成的服务收费存储区记账。在一些实施例中，由代理服务器或路由器提供的使用记账直接用于服务使用记账。

[0127] 在一些实施例中，环境服务伙伴反馈用来验证服务收费存储区记账。例如，由环境服务伙伴使用来提供环境服务的网络服务器可以基于嵌入在 HTML 业务量中的报头信息来识别一个用户装置，并且随后在环境服务会话过程中为由装置使用的服务记账或者为用户完成的交易数量记账。如果记录了服务使用，则可以将其报告给服务控制器并且可以直接使用其来验证环境服务收费存储区记账。如果交易均被记录，则这可以被报告给服务控制器，并且可以将由装置使用的环境服务量与完成的交易数量相比较，来确定环境服务使用是否是合理的或者是否应该被节流或阻塞。本领域普通技术人员现将清楚的是，可以提供采用一种以上类型的网络生成的服务使用记录来验证服务使用记账和 / 或验证服务收费存储区记账的其他实施例。

[0128] 包括用于验证或控制服务收费存储区记账的间接方法的其他实施例包括监控环境服务使用的尺寸和 / 或增长率。在一些实施例中，当积累在环境服务收费存储区中的服务使用费用超过一个预置策略限制时，和 / 或当用于环境服务的服务使用的速率超过一个预置策略限制时，接入控制策略规则需要限制一个给定的环境服务接入。例如，一旦达到这些限制，环境服务可以被节流回一段时间，被阻塞一段时间，或者被记账到用户服务计划收费存储区。在一些实施例中，在这些行动发生之前，用户 UI 可以用来通知用户服务策略强制执行行动。在一些实施例中，对服务收费存储区记账的间接验证包括在此所描述的用于验证服务处理器代理软件的适当运行和 / 或保护服务处理器代理软件免受错误、操纵或非法侵入的不同技术。

[0129] 在一些实施例中，装置服务处理器将去往一个给定环境服务的业务量引导到被编程来支持该环境服务的一个代理服务器或路由器，并且用于该环境服务的任何业务量控制策略和 / 或接入控制策略在该代理服务器或路由器中实施。例如，在这类实施例中，可以为代理服务器或路由器编程来仅允许接入由装置服务计划授权的一个或多个环境服务，其中该代理服务器或路由器控制装置接入，这样使得不可用到达其他网络目的地。继续这个示例实施例，代理服务器或路由器可以为在一个环境服务收费存储区中的环境服务使用记账，如在其他地方所论述。在这类代理服务器或路由器环境服务控制实施例中，在其他地方

描述的如下相同业务量关联技术可以在代理服务器或路由器编程中实施：允许与一个环境服务网站或其他服务相关联的输入业务量被识别，被允许或阻塞，被潜在地节流，并且被记入一个服务收费存储区中。这类代理服务器或路由器实施例也可以实施用户服务计划服务收费存储区、用户服务计划业务量控制以及用户服务计划接入控制，如在此所论述。在一些实施例中，该代理服务器或路由器如在此所描述来分析业务量流的 HTML 业务量内容以执行这类关联、业务量控制和 / 或服务使用记账。类似地，在一些实施例中，一个代理服务器或路由器可以通过执行在此所描述的相同的浏览外 (surf-out) 业务量关联 (例如，HTML 分支引用关联和 / 或其他分支关联) 而提供在此所描述的“浏览外”能力。本领域普通技术人员现将清楚的是，可以用被适当编程的一个代理服务器或路由器来轻松地实施在此描述的用于一个服务处理器的自适应服务控制和服务使用收费功能中的许多个。

[0130] 在一些实施例中，用于一个或多个环境服务和 / 或用户服务计划服务的装置业务量到一个代理服务器或路由器的路由选择是由装置服务处理器使用在此所描述的装置服务处理器业务量控制实施例来实现的。在一些实施例中，用于一个或多个环境服务和 / 或用户服务计划服务的装置业务量到一个代理服务器或路由器的路由选择是由专用网络设备来实现的，如网关 (例如，SGSN、GGSN、PDSN 或 PDN)、归属代理、HLR 或基站，其中该网络设备由一个服务控制器配置 (例如，或具有为了这个目的类似功能的其他可互换网元)，从而来将该装置业务量引导到该代理服务器或路由器。在一些实施例中，环境服务业务量或用户服务计划由该代理服务器根据由服务控制器提供的一个服务计划策略集 (例如，或为了这个目的等价网络功能) 而控制。因此由代理服务器实施的该业务量控制服务策略可以基于以下各项的一个或多个来控制业务量：时段、网络地址、服务类型、内容类型、应用类型、QoS 级、当日时间、网络占线状态、带宽以及数据使用。

[0131] 在一些实施例中，一个代理服务器或路由器用来验证对一个给定的服务例如一个环境服务的记账。在一些实施例中，这由装置服务处理器将令人希望的服务流引导到被编程来处理这些令人希望的服务流的一个代理服务器或路由器而实现，其中该代理服务器或路由器被编程来仅允许接入到被用于令人希望的服务的接入控制策略允许的有效的网络目的地，并且该代理服务器或路由器还被编程来为用于令人希望的服务的业务量使用记账。在一些实施例中，代理服务使用记账随后可以用来验证由服务处理器报告的基于装置的服务使用记账。在一些实施例中，因此由代理服务器或路由器报告的记账可以直接用来为如环境服务使用或用户服务计划服务使用的服务使用记账。

[0132] 在一个代理服务器用于装置服务使用记账的一些实施例中，该代理服务器经过如在此所描述的心跳装置链路的一个安全通信链路来维护一个到装置服务通知 UI 的链路。例如，该代理服务器或路由器可以跟踪装置服务使用对比服务计划使用上限 / 限制，并且通过在服务控制器与装置之间的装置通信链路 (例如，心跳链路) 来通知用户装置 UI。在一些实施例中，代理服务器 / 路由器以各种方式与一个装置 UI 进行通信，如以下：通过一个装置链路 (例如，心跳链路) 的 UI 连接；通过连接至一个服务控制器 (例如，或为了这个目的具有类似功能的其他网元) 的一个装置链路；向装置呈现一个代理网页；为装置提供一个弹出页面；和 / 或在与代理服务器 / 路由器进行通信的装置上安装一个特别门户迷你浏览器。在一些实施例中，该到代理服务器 / 路由器的 UI 连接用作一个用户通知信道来传递使用通知信息、服务计划选择项或在此所描述的多个服务 UI 实施例中的任何一个。

[0133] 在一些实施例中,就用于实施服务业务量 / 接入控制和 / 或服务收费存储区记账的代理服务器 / 路由器技术而言,令人希望的是具有对装置上的服务处理器可用的相同信息,包括例如与业务量相关联的应用、网络占线状态、QoS 等级或关于在装置上可用的服务活动的其他信息。例如,这类信息可以用来帮助确定业务量控制规则和 / 或特殊服务信用是到期的(例如,环境服务信用)。在一些实施例中,在装置上可用的信息可以被传递到代理服务器 / 路由器并且以各种方式与业务量流或服务使用活动相关联。例如,辅助信息可以被传输到代理服务器 / 路由器,该代理服务器 / 路由器使一个业务量流或服务活动流与在装置上可用但在业务量流或服务活动流自身中不是随时可用的信息相关联。在一些实施例中,这类辅助信息可以在一个专用控制信道(例如,装置控制链路或心跳链路)上,或在一些实施例中可以为安全(例如 TLS/SSL 或一个安全通道)的一个标准的网络连接中通信。在一些实施例中,在装置上可用的该辅助信息可以经过数据中的嵌入信息(例如,在通信包中的报头和 / 或填充特别字段)而传递到代理服务器 / 路由器。在一些实施例中,在装置上可用的辅助信息可以通过将一个给定的安全链路或通道与该辅助信息相关联而传递到代理服务器 / 路由器。在一些实施例中,该辅助信息被收集在一个装置代理或装置 API 代理中,该装置代理或装置 API 代理监控业务量流,收集用于这些业务量流的辅助信息并且将与一个给定的流相关联的信息传输到一个代理服务器 / 路由器。本领域普通技术人员现将清楚的是,其他技术可以用来将装置上可用的辅助信息传递到一个代理服务器 / 路由器。

[0134] 例如,正如收费规则的层级结构对其中服务处理器正创建服务收费存储区记账的实施而言可能是重要的,在使用针对服务收费存储区记账的一个代理服务器或路由器的实现方式中,其也可能是重要的。因此,在此描述的用于创建一个服务使用收费规则层级结构的不同实施例可以被应用到代理服务器或代理路由器实施例中。本领域普通技术人员现将清楚的是,在此描述的用于被允许的但未被分类的存储区的服务收费存储区实施例和业务量控制与接入控制实施例同样地应用到该代理服务器 / 路由器实施例。例如,可以将预定义的服务策略规则编程到代理服务器 / 路由器中,以控制业务量流,和 / 或放置使用限制,或接入在一个环境服务或一个用户服务计划服务上的限制。本领域普通技术人员现将清楚的是,在此所描述的披露一个初始被允许的服务接入清单,临时允许另外服务活动直到其被确定为被允许或未被允许,扩大该被允许的服务活动清单,维护一个未被允许的服务活动清单并且扩大该未被允许的服务活动清单的实施例也同样地应用于代理服务器 / 路由器实施例。类似地,本领域普通技术人员现将清楚的是,可以采用这些代理 / 服务器路由器实施例来直接生成用来为服务使用提供另外明细和 / 或计费能力的服务收费存储区(或微型 CDR)使用报告。在装置服务处理器将业务量引导到一个代理服务器 / 路由器的一些实施例中,存在可以减小配置网络来检测并且迫使专门装置服务业务量到适合的代理服务器 / 路由器的需要的可用的有利的设计特征实施例。例如,这可以通过为由代理服务器 / 路由器支持的服务创建一个“使用信用”系统而完成。一方面总服务使用由装置服务处理器计数,或由另一个网络设备或这两者计数。另一方面用于未被记账到用户的环境服务或其他专门接入服务使用的信用随后提供以下服务:装置引导而通过支持特殊环境服务或其他专门接入服务的代理服务器 / 路由器目的地(例如,URL 或路由跳数)。如果装置将业务量正确地引导到代理服务器 / 路由器,则计数和 / 或接入规则由该代理服务器 / 路由器正确地实施。因此可以控制和 / 或记账服务。当服务被记账时,代理服务器 / 路由器将服务收费

存储区记账报告回服务控制器(例如,或负责服务收费存储区/微型CDR调解的其他网络设备)并且用户服务计划收费存储区账户可以为这些服务而被信贷。到达代理服务器/路由器编程的业务量由代理服务器/路由器的接入规则和/或业务量控制规则和/或QoS控制规则而控制,因此对关于用服务收费存储区支持的服务类型不存在疑问,这些服务收费存储区被报告到调解功能(例如,可以由服务控制器、使用调解、计费、AAA和/或HLR/归属代理执行调解功能)。因为代理服务器/路由器位于网络中并且可以被物理地保护安全并且保护而免受非法侵入,所以对以下存在高的可信度:旨在用于环境服务或一些其他专门服务的服务控制和/或收费规则被正确地实施,并且代理服务器/路由器连接用于旨在的服务并且不用于一些其他非计划中的非法侵入服务。如果装置以某种方式受非法侵入或以另外方式处于错误中,这样使得业务量未被引导通过适合的代理服务器/路由器,则代理服务器/路由器不将该业务量记入微型CDR/存储区中,并且没有专门的服务使用信用被发送到调解功能,因此不从装置用户服务计划服务使用总量中扣除使用信用。因此,当装置受非法侵入而避开代理服务器/路由器时,用户为服务付费。用户账户服务协定可以指定:如果用户篡改软件并且业务量被路由选择到服务器,则将不提供信用并且将对用户计划收费。

[0135] 在一些代理服务器/路由器实施例中,使用信用有时由检测哪一个装置正在执行接入的代理服务器/路由器记录。装置识别可以各种方式实现,包括由装置插入到业务量中的一个报头/标签、在指定用于该装置的网络中的一个路由、一个安全链路(例如,TLS/SSL、IP Sec或其他安全通道)、一个唯一装置IP地址或其他凭证(例如,其中代理服务器/路由器具有到一个有效IP地址查找功能的接入)、一个唯一代理服务器/路由器地址和/或用于装置的套接字。

[0136] 在一些实施例中,装置服务控制器业务量控制元件的协调可以使得定位、安装、配置并且运行代理服务器更为简单。代理服务器/路由器无需与接入网络呈“一列式”定位,因为确保业务量被路由选择到服务器/路由器否则不存在信用并且对使用账户收费是装置的责任。在一些实施例中,这使得其为不必要的或减小了在运营商网络中迫使做出装置业务量路由的需要。在一些实施例中,代理服务器/路由器可以定位在运营商网络中或在互联网上。如果代理服务器/路由器位于互联网上,则业务量可以在通过服务器/路由器来增强抵抗攻击的安全性之前,在一个防火墙中认证。

[0137] 在一些实施例中,代理服务器/路由器中的服务收费存储区记录软件可以直接编程到一个环境服务伙伴网络设备中,因此消除对特殊仪器的需要。环境服务伙伴的设备(例如,一个网络服务器、负载均衡器或路由器)可以辨认使用以上描述的技术中的一个的装置,聚合装置服务收费存储区记账,并且周期性地使用记账发送到服务控制器或其他网络服务使用调解功能。

[0138] 编程和/或配置在此描述的不同实施例中所披露的环境服务、用户计划服务和/或专门的服务可能是一个复杂的过程。在一些实施例中,一个简化的用户编程接口(在此也称为一个服务设计接口)用来编程用于这类服务令人希望的必要的策略设置。例如,提供一个服务设计接口,该服务设计接口组织和/或归类建立一个环境服务(例如,或其他服务)所需的不同的策略设置,这些策略设置包括以下各项中的一项或多项:在环境服务(例如,或其他服务)下被允许的服务活动的一个策略清单、接入控制策略、用于实施和/或适配一个网络目的地的被允许的清单的规则、用于实施和/或自适应一个网络目的地的受阻塞

的清单的规则、服务收费存储区策略、用户通知策略、服务控制和 / 或服务收费存储区验证策略、对验证错误待采取的行动。在一些实施例中,用于这些策略集中的一个或多个的所需信息被格式化为组织并且简化策略编程的一个 UI。在一些实施例中,该 UI 是部分图形的,从而帮助用户理解需要定义该信息和什么设置以便定义该服务。在一些实施例中,该 UI 与一个 XML 接口一起创建。在一些实施例中,该 UI 经过一个安全网络连接而提供。在一些实施例中,创建用于一个环境服务(例如,或另一个服务)的一个基本服务策略,其包括以上服务策略设置中的一个或多个,并且随后这个服务策略集变为可以在多个服务计划策略集定义中复制并且使用的一个清单或一个对象(例如,在一个图形 UI 中“拖动并且删掉”)。在一些实施例中,在这个服务设计接口创建的所得策略集随后被分发到网络中和 / 或装置上的必要策略控制元件,这些策略控制元件协调作用来实施用于一个给定装置组的服务策略集。例如,如果一个服务处理器与一个服务控制器一起使用,则服务设计接口可以将需要被编程在服务控制器和装置服务处理器上的服务策略设置子集加载到服务控制器中,并且服务控制器将这些服务控制器策略设置加载到控制这些策略的服务控制器组件中,并且将装置策略设置子集加载到属于该装置组的装置上。在一个代理服务器 / 路由器用来帮助控制并且记账服务的实施例中,在一些实施例中,服务设计接口将需要被编程在代理服务器 / 路由器上的服务策略设置子集加载到代理服务器 / 路由器中。在需要配置其他网元或为其他网元(例如,网关、基站、服务使用记录 / 聚合 / 馈送设备、AAA、归属代理 / HLR、调解系统和 / 或计费系统)或为其编程的一些实施例中,在一些实施例中,服务设计接口也将适合的装置组策略子集加载到设备元件中的每一个上。因此,如在此所描述的不同技术可以用来极大地简化以下复杂的任务:将一个服务策略集或服务计划转换成所有无数设备和 / 或装置设置;编程;和 / 或配置正确实施装置所需的命令。本领域普通技术人员现将清楚的是,这些技术中的若干可以类似地用于 VSP 服务设计接口。

[0139] 本领域普通技术人员将会认识到,可以为在此所描述的规则引擎提供不同其他规则。本领域普通技术人员还将会认识到,在此所描述的功能可以使用不同其他网络架构和网络实现方式(例如,使用不同其他联网协议和对应的网络设备和技术)来实施。

[0140] 在装置辅助服务(DSA)系统中,终端用户装置代理可以在策略实施或强制执行中辅助网络。例如,装置代理可以辅助网络在终端用户装置在一个接入网络上接入数据服务时保持记录来分配费用,强制执行用于装置的接入控制或服务限制策略,强制执行使用限制,或帮助通知用于关于与装置终端用户通信的网络接入服务的信息的策略。如果一个装置与一个装置代理一起配置,该装置代理被配置成在策略实施或强制执行中辅助网络,则可能存在装置上强制执行的一个网络策略的一个装置部分,并且可能存在由网络中的网元强制执行的一个接入网络服务策略的一个网络部分。在一些接入网络中,采用基于网络的系统来实施接入网络服务策略的网络部分,例如像,来管理允许一个装置在一个网络上的认证过程,或来确定一个或多个网络策略,该一个或多个网络策略应该由网元如接入控制策略、服务使用限制、服务使用记账或计费策略或服务使用通知策略强制执行。

[0141] 为达到一个总网络服务策略,接入网络服务策略的网络部分可以被配置成与接入网络服务策略的基于装置的部分一起工作,来达到一个总组合的网络服务策略。如果实施接入网络服务策略的装置部分所需的装置代理不存在于装置上或未被正确地配置,则总组合的网络服务策略可能处于错误中或不可能达到,从而潜在地导致一个不希望的网络服务

策略实施。在这类情况下,令人希望的是采用一个网络系统来检测这个条件并且修改由基于网络的元件强制执行的一个接入网络服务策略的网络部分,这样使得可以达到一个令人希望的网络服务策略强制执行。

[0142] 在一些实施例中,可以帮助在策略实施或强制执行中的网络的一个装置代理可以称为一个“装置策略实施代理”,在一些实施例中,其为服务处理器的一部分。

[0143] 适配一个接入网络服务策略的网络部分以便记账一个缺失的或未正确地配置的服务处理器何时是可能不利的示例包括但不限于:(i) 一个装置凭证已经被移动到不具有一个服务处理器的一个装置,(ii) 一个装置凭证已经被移动到具有一个服务处理器的一个装置,该服务处理器具有不同于原始地与该装置凭证相关联的服务处理器的一个配置,(iii) 一个装置服务处理器已经被篡改或具有一个不正确的配置。

[0144] 在一些实施例中,为了达到根据类别而不同的使用记账策略强制执行、接入控制策略强制执行、服务使用限制或通知策略强制执行的目的,服务处理器用来将服务使用辅助分类成子类别。在一些实施例中,分类可以用于一个或多个装置应用程序。在一些实施例中,分类可以用于一个或多个网络目的地。在一些实施例中,分类可以用于一个或多个网络类型。在一些实施例中,可以执行对服务使用的一个分类(在此称为一个赞助的服务或一个环境服务)来协助将全部地或部分地与被赞助的服务或环境服务相关联的接入网络费用分配到一个服务赞助方,该服务赞助方为一实体而不是装置用户。

[0145] 所需要的是检测终端用户装置上的一个服务处理器的存在与正确的配置或其缺乏的一个网络系统,其中该服务处理器(如果存在)在被配置有一个装置凭证的一个装置上强制执行一个接入网络服务策略的一个装置部分,并且如果该服务处理器存在并且被正确地配置,则其引起一个接入网络服务策略的一个第一网络部分在网络中强制执行,一个接入网络服务策略的该第一网络部分被配置成将副本策略强制执行提供到一个接入网络服务策略的一个装置部分来达到一个第一令人希望的总接入网络服务策略;并且如果服务处理器不存在并且未被正确地配置,则其引起一个接入网络服务策略的一个第二网络部分在网络中强制执行,该网络被配置成在没有一个装置副本策略的情况下运行来达到一个第二令人希望的总接入网络服务策略。

[0146] 在一些实施例中,一个网络系统用来检测不讲道德的用户何时尝试通过篡改一个服务处理器来获取免费数据服务,以便使用一个服务并且使服务使用记账分配到被赞助的一个第二服务。例如,如果一个装置将其数据使用的报告发送给网络,则一位用户可能尝试非法侵入装置,这样使得例如通过报告比装置实际使用更少的数据使用来报告含有比信息本身应该是的更有利于用户的信息。作为另一个示例,一个装置可能含有一个“被赞助的SIM”卡或允许装置使用一个固定数据量的另一个凭证,该数据量可能与以对用户的一个减小的费用或免费的一个特殊服务相关联。不讲道德的用户可能尝试找到途径来用被赞助的SIM卡增加其免费或补助的数据使用量。

[0147] 无线接入网络中的带宽限制正做出对服务提供者更不具吸引力的无限制的数据计划。同时,终端用户装置的用户想要对电气装置的数据使用具有更多的控制以控制费用。以高准确性来在比仅通过测量聚合数据使用更细的粒度等级上跟踪一个装置的数据使用的能力是满足这两个需要的一个重要的使能器新服务提供。例如,在一个服务接着服务或应用接着应用的基础上或在甚至更精细的等级上对一个装置的数据使用的准确跟踪将允

许服务提供者提供允许用户选择定制的特定应用或特定服务数据计划的一个卡服务计划。

[0148] 因此,需要安全措施来防止由改变装置凭证、一个服务处理器的不正确的配置或 DAS 系统中的欺诈导致的策略错误。特别地,需要允许网络检测欺诈性终端用户活动的工具。

[0149] 在此披露了响应于将一个装置凭证从一个装置移动到另一个装置、一个服务处理器的不正确配置、一个缺失的服务处理器或篡改装置辅助服务(DAS)系统中的一个服务处理器来防止、检测或采取行动的不同的实施例。

[0150] 在一些实施例中,网络中的服务控制器对服务处理器进行认证并且检查其正在以预期的方式(例如在预期的时间,包括预期的信息)用预期的真实性标记等来报告终端用户装置的使用。

[0151] 在一些实施例中,当终端用户装置报告使用时,服务控制器检查由服务处理器发送的报告是否与来自一个可信源如一个网元的报告相一致。

[0152] 在一些实施例中,当服务控制器检测到欺诈性或潜在欺诈性活动时,服务控制器通知一个网络管理员或网络资源,从而可以随后进一步评估状况和决定如何响应。在一些实施例中,增加订户的计费率。

[0153] 在一些实施例中,被配置成实施一个网络服务策略(例如,一个接入控制策略或业务量控制策略,一个装置软件或运行环境安全性策略、一个服务使用限制、一个服务记账或收费策略)的一个装置部分的一个装置客户端可以称为一个“装置策略实施客户端”,在一些实施例中,其可能为服务处理器的一部分。同样,在不失一般性的情况下,术语“服务控制器”可以用来指一个服务处理器认证和管理系统。服务处理器和服务控制器两者可以具有除在此所描述的这些功能之外的功能。

[0154] 在一些实施例中,一个装置被配置有负责用于实施或强制执行一个第一网络服务策略的一个装置部分的一个正确配置的服务处理器。在一些实施例中,该装置被配置成没有一个正确配置的服务处理器。在一些实施例中,一个服务控制器可以被配置成确定服务处理器是否存在于装置上,并且,如果是,其是否被正确地配置。

[0155] 在一些实施例中,如果服务控制器确定装置被配置有一个正确配置的服务处理器,则该服务控制器引起一个基于网络的接入网络服务策略强制执行系统实施或强制执行第一接入网络服务策略的一个第一基于网络的部分。在这种情况下,因为服务控制器已经验证一个正确配置的服务处理器存在于装置上,所以该服务控制器系统在装置正确地实施或强制执行该第一接入网络服务策略的装置部分的前提下运行。然而,如果服务控制器确定一个正确配置的服务处理器不存在于装置上,则该服务控制器引起一个基于网络的接入网络服务策略强制执行系统实施或强制执行第一接入网络服务策略的一个第二基于网络的部分。在这种情况下,该服务控制器系统在装置不正确地实施或强制执行一个接入网络服务策略的一个装置部分的前提下运行。

[0156] 在一些实施例中,一个终端用户装置被配置有:(1)连接至一个无线接入网络的一个无线调制解调器(连接至另一种类型的接入网络的另一个网络接入调制解调器);(2)一个或多个装置凭证源(例如,一个 SIM 卡、一个软 SIM、一个通用 SIM、一个 IMSI 源、一个无线调制解调器、一个电话号码源、一个 IMEI 源、一个 MEID 源、一个用户密码或 PIN、一个 MAC 地址源、一个 IP 地址源、一个安全装置标识符源、一个装置安全通信加密密钥源等),其存储

一个装置凭证并且将装置凭证提供给一个或多个网络服务策略强制执行元件(例如, AAA、HLR、PCRF、接入网络认证系统、准入系统或登录系统)以用于查找或获得准入无线接入网络(或其他接入网络)的目的;以及(3)一个服务处理器(例如,一个装置客户端),其被配置成实施或强制执行一个无线接入网络服务策略的一个基于装置的部分并且与一个基于网络的服务控制器进行通信以便提供服务处理器认证信息,该信息被配置成允许验证服务处理器存在于并且被正确地配置在装置上。

[0157] 在一些实施例中,一个基于网络的系统被配置有:(1)一个或多个基于网络的装置认证或准入元件(例如, AAA、HLR、PCRF、接入网络认证系统、准入系统、登陆系统等),其被配置成接收来自正尝试接收或正在接收接入网络服务的一个终端用户装置的一个装置凭证;(2)一个或多个服务策略强制执行元件(例如,一个网络网关、路由器、GGSN、SGSN、代理、收费元件、通知触发元件等),其被配置成实施与该装置凭证相关联的一个接入网络服务策略;(3)一个服务处理器认证和管理系统(例如,一个服务控制器),其被配置成接收服务处理器认证信息并且使用该信息来验证该服务处理器存在于并且被正确地配置在该装置上。在一些实施例中,服务处理器认证和管理系统进一步被配置成:(a)在服务处理器存在于并且被正确地配置在装置上的情况下,引起与装置凭证相关联的接入网络服务策略被执行为一个接入网络服务的一个第一网络部分;或(b)在服务处理器不存在于并且未被正确地配置的情况下,引起与装置凭证相关联的接入网络服务策略被执行为一个接入网络服务的一个第二网络部分。

[0158] 在不失一般性的情况下,在以下相关实施例中,术语“SIM卡”和“SIM”用来表示一个装置凭证源。如本领域普通技术人员将认识到其他装置凭证源(例如,一个软SIM、一个通用SIM、一个IMSI源、一个无线调制解调器、一个电话号码源、一个IMEI源、一个MEID源、一个MAC地址源、一个IP地址源、一个安全装置标识符源、一个装置安全通信加密密钥源等)可以在这些实施例的许多个中与SIM卡互换。例如,在一个SIM卡从一个装置移动到另一个装置的实施例中,另一种类型的装置凭证(例如,软SIM、通用SIM、一个IMSI源、一个无线调制解调器、一个电话号码源、一个IMEI源、一个MEID源、一个MAC地址源、一个IP地址源、一个安全装置标识符源、一个装置安全通信加密密钥源等)反而可以移动。作为另一个示例,当一位用户篡改与一个SIM相关联的一个服务处理器时,该用户可能篡改与另一种类型的装置凭证(例如,软SIM、通用SIM、一个IMSI源、一个无线调制解调器、一个电话号码源、一个IMEI源、一个MEID源、一个MAC地址源、一个IP地址源、一个安全装置标识符源、一个装置安全通信加密密钥源等)相关联的一个服务处理器。存在术语“SIM”可以交换装置凭证的另一个源的许多其他示例实施例,其中这些实施例太多而不能列出并且在此在教义的上文中对本领域的普通技术人员是明显的。

[0159] 在一些实施例中,该一个或多个装置凭证源包括一个SIM卡。在一些实施例中,服务控制器可以被配置成:辨认SIM与哪一个装置或服务处理器相关联;使用该SIM与装置关联来查找一个无线接入网络服务策略的一个令人希望的装置部分;并且将策略传递到该适合的装置服务处理器。在一些实施例中,一个无线接入网络策略的这两个不同的装置部分根据包括一个或多个SIM凭证和/或一个或多个服务处理器凭证的一个装置组或用户组服务策略定义而确定,并且这些策略定义被键入管理服务控制器和/或装置服务处理器策略的一个虚拟的服务提供者工作站。

[0160] 在一些实施例中,服务控制器被配置成辨认 SIM 卡何时从具有一个第一服务处理器的一个第一装置移动到具有一个第二服务处理器的一个第二装置。在一些这类实施例中,服务控制器可以被配置成:辨认 SIM 与哪一个装置或服务处理器相关联;使用该 SIM 与装置关联来查找一个无线接入网络服务策略的一个令人希望的网络部分;并且引起一个无线接入网络服务策略的该网络部分在一个或多个网络服务策略强制执行元件中实施或强制执行。在一些实施例中,一个无线接入网络策略的这两个不同的网络部分根据包括一个或多个 SIM 凭证和 / 或一个或多个服务处理器凭证的一个装置组或用户组服务策略定义而确定,并且这些策略定义被键入管理服务控制器和 / 或网络服务策略强制执行元件策略的一个虚拟的服务提供者工作站。

[0161] 在一些实施例中,该一个或多个装置凭证源包括一个 SIM 卡。在一些实施例中,服务控制器被配置成检测一个装置用户何时将 SIM 卡从被配置有一个正确配置的服务处理器的一个第一装置移动到未被配置有一个正确配置的服务处理器的一个第二装置。在一些实施例中,服务控制器可以被配置成:确定该第一装置被配置有一个正确配置的服务处理器;并且将一个无线接入网络服务策略的一个装置部分传递到该适合的装置服务处理器。在一些实施例中,一个无线接入网络策略的装置部分根据包括一个 SIM 凭证和 / 或一个服务处理器凭证的一个装置组或用户组服务策略定义而确定,并且这些策略定义被键入管理服务控制器和 / 或装置服务处理器策略的一个虚拟的服务提供者工作站。在一些实施例中,服务控制器可以被配置成:确定该第一装置被配置有一个正确配置的服务处理器;并且引起一个无线接入网络服务策略的一个第一网络部分在一个或多个网络服务策略强制执行元件中实施或强制执行。在一些实施例中,服务控制器可以被配置成:确定该第二装置未被配置有一个正确配置的服务处理器;并且引起一个无线接入网络服务策略的一个第二网络部分在一个或多个网络服务策略强制执行元件中实施或强制执行。在一些实施例中,一个无线接入网络策略的装置部分根据包括一个 SIM 凭证的一个装置组或用户组服务策略定义而确定,并且这些策略定义被键入管理服务控制器和 / 或网络服务策略强制执行元件策略的一个虚拟的服务提供者工作站。

[0162] 在这些实施例中的一些中,一个无线接入网络服务策略的第一网络部分与一个无线接入网络服务策略的第二网络部分之间的差异可以包括网络接入特权上的一个差异、可允许的网络目的地上的一个差异、用于“大块”接入的服务使用记账或计费上的一个差异、用于接入分类的服务使用记账或计费上的一个差异、用于“大块”接入的服务使用记账率或计费率上的一个差异、用于接入分类的服务使用记账率或计费率上的一个差异、被赞助的(环境)服务记账或计费上的一个差异、服务速度或质量上的一个差异、装置或用户接入哪一个网络上的一个差异、提供给终端用户的服务使用通知上的一个差异、漫游服务策略或许可或记账 / 计费率上的一个差异、对装置或用户接入能力的一个隔离、(例如,禁用或以另外方式修改)装置运行的一个或多个特征之间的差异或暂停装置接入网络。

[0163] 在一些实施例中,一个 SIM 和一个服务处理器与服务使用的一个分类和接入网络服务策略强制执行的一个对应装置部分相关联。服务控制器随后负责正确地认证与 SIM 相关联的服务处理器的正确的配置,以便确定应该被强制执行的网络接入服务策略的适合的网络部分。

[0164] 在一些实施例中,一个 SIM 和一个服务处理器与一个或多个特定应用服务相关

联,其中该装置网络接入服务具有特定于一个装置软件或固件应用的策略元件。一个特定软件或固件应用服务可以包括但不限于:具有与一个用户应用程序相关联的特定策略元件的一个服务;一个操作系统程序、程序库或功能;一个后台应用服务,如一个应用更新、内容高速缓存、软件更新或其他后台应用服务。

[0165] 在一些实施例中,一个 SIM 和一个服务处理器与一个或多个网络目的地特定服务相关联,其中该装置网络接入服务具有特定于一个网络目的地或资源的策略元件。一个网络目的地或资源可以包括但不限于一个服务器、网关、目的地地址、域名、网站或 URL。

[0166] 在一些实施例中,一个 SIM 和一个服务处理器与一个装置应用程序、网络目的地或资源;一种类型的网络;一个漫游情况(例如,家庭或漫游网络);一个时间段;一个网络拥塞等级;一个网络服务质量(QoS)等级;以及一个后台或前台通信的任意组合相关联。

[0167] 在一些实施例中,一个 SIM 和一个服务处理器与一个或多个被赞助的服务相关联(在此也称为环境服务),其中用于一个或多个服务使用分类的一部分或所有服务使用记账被记账、收费或记账到一个服务赞助者而不是为用户服务计划付费的装置用户或团体。被赞助的服务的部分可以为所有装置接入或装置接入的一部分或一类。在一些实施例中,对服务被赞助的部分的分类(例如,对应该被分配到服务赞助方的接入网络的装置使用部分的识别)用一个服务处理器在装置上实现。在一些实施例中,对服务被赞助的部分的分类使用 DPI 元件、网关元件、服务器元件、代理元件、网站元件或网络服务元件而在网络中实现。在一些实施例中,对服务被赞助的部分的分类用由装置上的一个服务处理器(例如,将服务的一个分类经过一个重引导、重路由或通道[例如安全 SSL、VPN、APN 或其他通道协议]引入一个给定的网元)和一个或多个网元(例如, DPI 元件、网关元件、服务器元件、代理元件、网站元件或网络服务元件)的一个组合实施的一个分类策略来实现。在一些实施例中,被赞助的服务部分包括用于一个装置应用程序或一组装置应用程序的服务。在一些实施例中,被赞助的服务部分包括用于一个网络目的地或资源、一个服务器或网站或一组网络目的地、服务器或网站的服务。在一些实施例中,被赞助的服务部分包括在特定类型网络上的服务。在一些实施例中,被赞助的服务部分包括在一个家庭网络或一个漫游网络上的服务。在一些实施例中,被赞助的服务部分包括在一个时间段过程中的服务。在一些实施例中,被赞助的服务部分包括用于一定范围的网络拥塞的服务。在一些实施例中,被赞助的服务部分包括用于一定范围的网络 QoS 的服务。在一些实施例中,被赞助的服务部分包括用于一个网络后台或前台数据通信的服务。在一些实施例中,被赞助的服务部分包括装置应用程序、网络目的地或资源、一种类型的网络、一个漫游情况(例如,家庭或漫游网络)、一个时间段、一个网络拥塞等级、一个网络 QoS 等级以及一个后台或前台通信的任意组合。

[0168] 在一些实施例中,安装或存在一个 SIM (或用户凭证或装置凭证的其他源,如以前所解释)而与配置有提供接入网络策略强制执行的一个装置服务处理器配置的一个装置相关联。在这类实施例中,一个或多个网元可以实施或强制执行接入网络策略强制执行的一个基于网络的部分,并且装置服务处理器可以被配置成实施或强制执行接入网络策略强制执行的一个基于装置的部分。在一些实施例中,一个或多个 SIM 凭证可以至少部分地用来识别接入网络策略的该基于网络的部分。在一些实施例中,一个或多个 SIM 凭证可以至少部分地用来识别接入网络策略的该基于装置的部分。

[0169] 在包括一个 SIM 模块策略关联的一些实施例中,策略强制执行包括以下各项中的

一项或多项：接入策略强制执行；服务使用限制；接入记账策略强制执行；以及接入服务用户通知策略强制执行。在一些实施例中，接入控制策略强制执行包括以下各项中的一项或多项：允许；限制；阻塞；推迟；延迟或用于“大块”接入（例如未分类的接入）的业务量成形装置网络接入；或一种或多种特定分类的接入网络服务活动。在一些实施例中，接入记账策略强制执行包括以下各项中的一项或多项：对适量的“大块”（例如，“未分类的”）接入网络服务使用进行统计；或对用于一种或多种特定分类的接入网络服务活动的适量接入网络服务使用进行统计。在一些实施例中，接入服务通知策略强制执行包括以下各项中的一项或多项：当一个预先定义的服务使用条件为“大块”（例如“未分类的”）接入网络服务使用而发生时，通知一位终端用户；或当一个预先定义的服务使用条件为一种或多种特定分类的接入网络服务活动而发生时，通知一位终端用户。特定分类的接入网络服务活动的示例包括通过一个应用或 OS 功能的接入、到一个或多个网络目的地或网络资源（如一个网站、域名、IP 地址或其他地址标识符、URL、套接字元组、网络服务器、网络路由或 APN、网络网关或代理、网络内容源或子网络）的接入。特定分类的接入网络服务活动的另外示例包括到具有不同 QoS 服务等级的网络服务的装置接入。在一些实施例中，与特定分类的接入网络服务相关的一部分策略用一个基于装置的服务处理器实施或强制执行，并且接入网络服务策略的其他部分在一个或多个基于网络的元件中强制执行。

[0170] 在一个或多个网元实施或强制执行接入网络策略强制执行的一个基于网络的部分，并且一个装置服务处理器被配置成实施或强制执行接入网络策略强制执行的一个基于装置的部分的一些实施例中，一个或多个装置 SIM 凭证至少部分地被识别或使用以确定由网络强制执行的策略。在这类实施例中，可以依赖装置服务处理器来实施或强制执行未在网络中实施或强制执行的接入网络服务策略的某些方面。

[0171] 在一些实施例中，接入网络服务策略的一个第一部分至少部分地由一个或多个 SIM 凭证确定并且由一个或多个网元实施，并且接入网络服务策略的一个第二部分旨在由一个基于装置的服务处理器实施，但是 SIM 安装在未被配置有一个能够实施接入网络服务策略的第二部分的服务处理器的一个装置中。在一些这类实施例中，一个网元识别 SIM 是否安装在一个装置中，该装置被配置有一个能够实施旨在在该装置上实施的接入网络服务策略的第二部分的服务处理器。在一些实施例中，该识别由实施以下装置配置检测和网络策略选择功能中的一个或多个的一个网络系统实现：(1) 识别其凭证至少部分地用来识别接入网络策略的一个基于网络的部分的一个 SIM 何时安装在被配置成包括一个能够实施或强制执行接入网络服务策略的一个基于装置的部分的服务处理器的一个装置中，并且将一个第一基于网络的服务策略配置到实施或强制执行接入网络服务策略的一个或多个基于网络的策略强制执行元件中；(2) 识别其凭证至少部分地用来识别接入网络策略的该基于网络的部分的一个 SIM 何时安装在被配置成包括一个能够实施或强制执行接入网络服务策略的一个基于装置的部分的服务处理器的一个装置中，并且在实施或强制执行接入网络服务策略的一个或多个基于网络的策略强制执行元件中实施一个第二基于网络的服务策略。

[0172] 在一些实施例中，当确定其凭证至少部分地用来识别接入网络策略的该基于网络的部分的一个 SIM 安装在被配置成包括一个能够实施或强制执行接入网络服务策略的一个基于装置的部分的服务处理器的一个装置中时，一个基于网络的服务策略配置系统将一

个第一基于网络的服务策略配置到一个或多个网元中(例如,将策略编程或发送到一个或多个网元)并且还将一个基于装置的服务策略配置到一个装置服务处理器中。在一些实施例中,当确定其凭证至少部分地用来识别接入网络策略的该基于网络的部分的一个 SIM 安装在未被配置成包括一个能够实施或强制执行接入网络服务策略的一个基于装置的部分的服务处理器的一个装置中时,一个基于网络的服务策略配置系统将一个第二基于网络的服务策略配置到一个或多个网元中,并且不存在用于一个基于装置的服务处理器的策略配置。

[0173] 这类实施例例如在一个基于装置的服务处理器能够实施或强制执行一个网络接入服务策略时是有利的,该网络接入服务策略具有不在网络中以另外的方式实施或强制执行的精细粒度分类方面。例如,在一些实施例中,一个 SIM 安装在包括一个基于装置的服务处理器的一个第一装置配置中,该基于装置的服务处理器能够对与一个或多个装置软件应用相关联的接入网络服务使用进行分类并且为该分类强制执行用于接入控制、服务限制、接入记账或接入服务通知的一个策略。在这种情况下,可以将一个第一基于网络的接入网络服务策略集配置到实施或强制执行接入网络服务策略的网元中。如果同一 SIM 安装到不包括令人希望的服务处理器能力的一个第二装置配置中,则可以将一个第二基于网络的接入网络服务策略集配置到实施或强制执行接入网络服务策略的网元中。在这类实施例中,第一装置配置可以包括确定用于一个或多个应用的网络接入允许的在服务处理器中的一个可信接入控制或服务限制策略,并且第一网络服务策略被配置成协助这个基于装置的应用接入控制或服务限制。相反地,不具有服务处理器的第二装置配置不具有可信接入控制或服务限制策略,并且因此该第二网络服务策略可能以方式为只有当与该 SIM(或第二装置或 SIM 用户)相关联的服务计划或服务账户包括对“大块”接入、“未分类的”接入或由网络并且不由装置分类的接入的许可时允许接入来配置。

[0174] 在一些实施例中,第二网络服务策略被配置成根据在没有一个装置辅助的分类组件的辅助下仅存在于网络中的能力而修改网络接入服务的分类。

[0175] 在一些实施例中,第二网络服务策略包括不同于第一网络服务策略的接入服务记账或收费率的一个第二接入服务记账或收费率。例如,在 SIM 安装在包括一个服务处理器能力(例如,装置能够执行服务分类、记账、控制或通知功能)的一个装置配置中的情况下,对终端用户的服务记账或服务收费方法不同于在 SIM 安装在不包括服务处理器能力的一个装置配置的情况下,对终端用户的服务记账或服务收费方法。例如,如果 SIM 安装在包括一个服务处理器能力的一个装置配置中,则一个给定的应用(例如,社交联网应用、电子邮件应用、搜索应用、语音应用、新闻应用等)可能具有定义一个第一收费度量(例如,对一个应用、网站、内容类型、服务类型 QoS 级的基于时间的使用;或者例如,对于一个应用、网站、内容类型、服务类型 QoS 级等的基于兆字节的使用)的一个第一记账或收费策略和/或当装置配置包括一个服务处理器能力时具有第一收费率(例如,每分钟 X 美元,或例如每兆字节 Y 美元等),然而当 SIM 未安装在包括一个服务处理器能力的一个装置配置中时,所有的业务量均以相同方式(例如,基于时间或基于兆字节)定费率,潜在地具有一个较高价格。在一些实施例中,当 SIM 未安装在包括一个服务处理器能力的一个装置配置中时,变更装置网络接入许可,或可以隔离或阻塞装置的通信。

[0176] 在一些实施例中,当一个 SIM 安装在具有一个第一装置配置的一个装置中时,该

服务处理器被配置成基于网络拥塞等级、当日时间、QoS 等级或后台 / 前台接入(例如,后台内容高速缓存或装置 / 用户分析的后台上传、后台软件或 OS 更新、后台应用 / 服务器通信等)来区别地处理一种或多种分类的接入网络服务活动,但是可替代地,同一 SIM 可以安装在不具有这类服务处理器能力(例如,具有一个第二装置配置的一个装置)的一个装置中。在这样一类实施例中,接入控制或服务限制策略的基于网络的部分、记账或收费策略的基于网络的部分或用户通知策略的基于网络的部分中的一个或多个可以取决于该 SIM 是安装在具有第一装置配置还是具有第二装置配置的一个装置中而变化。例如,如果 SIM 由与第一装置配置相关联的网络辨认,则一个较低记账费率或服务使用价格可以应用到如下业务量:(i) 分配到后台状态的;(ii) 基于网络拥塞等级而受控制的;(iii) 基于当日时间而受控制的;(iv) 基于一个较低 QoS 分类允许而受控制的等,然而如果该 SIM 由与第二装置配置相关联的网络辨认,则可以应用一个单个的、潜在较高的记账费率或服务使用价格。在一些实施例中,如果 SIM 由与第二装置配置相关联的网络辨认,则可以变更装置网络接入许可,或可以隔离或阻塞装置的通信。

[0177] 在一些实施例中,当一个 SIM 由待安装在包括一个服务处理器服务使用收费能力的一个装置配置中的一个网元确定时,一个或多个网元被配置成将装置接入定为零费率(即,该一个或多个网元不会将由一个或多个网元记录的服务使用记账应用到用户的账单),并且用户服务记账或收费移交给接收来自服务处理器的服务使用记账或计费信息的一个服务控制器。

[0178] 在一些实施例中,当一个 SIM 由待安装在包括为一种或多种服务活动分类而将业务量路由、重引导或以另外方式引入到一个或多个代理网关 / 服务器的一个服务处理器能力的一个装置配置中的一个网元确定时,一个或多个网元被配置成将装置接入定为零费率(即,该一个或多个网元不会将由一个或多个网元记录的服务使用记账应用到用户的账单),并且用户服务记账或收费移交给被配置成为装置服务使用记账或收费的一个或多个代理网关 / 服务器。

[0179] 在一些实施例中,当一个 SIM 由待安装在包括为一种或多种服务活动分类而将业务量路由、重引导或以另外方式引入到一个或多个代理网关 / 服务器的一个服务处理器能力的一个装置配置中的一个网元确定时,一个或多个代理网关 / 服务器为一种或多种分类的服务使用执行另外业务量接入控制或服务限制策略实施或强制执行。

[0180] 在一些实施例中,当一个 SIM 由待安装在包括一个服务处理器能力的一个装置配置中的一个网元确定,该服务处理器能力为一种或多种服务活动分类而将业务量路由、重引导或以另外方式引入到一个或多个代理网关 / 服务器时,该一个或多个代理网关 / 服务器为了服务使用记账、接入控制、服务限制或用户通知的目的而执行另外服务使用分类。

[0181] 在一些实施例中,当一个 SIM 由待安装在不包括为一种或多种服务活动分类而将业务量路由、重引导或以另外方式引入到一个或多个代理网关 / 服务器的一个服务处理器能力的一个装置配置中的一个网元确定时,网元而不是代理网关 / 服务器潜在地以与当一个 SIM 由待安装在包括为一种或多种服务活动分类而将业务量路由、重引导或以另外方式引入的一个服务处理器能力的一个装置配置中的一个网元确定时不同的费率来为服务使用记账。

[0182] 在装置配置包括为一种或多种服务活动分类而将业务量路由选择、重引导或以另

外方式引入到一个或多个代理网关 / 服务器的一个服务处理器能力的一些实施例中, 装置路由选择、重引导或引入通过为一种或多种服务使用分类而将装置业务量路由选择、重引导或引入到与代理网关 / 服务器相关联的一个特定网络目的地或资源而实现。在一些实施例中, 路由选择、重引导或引入使用通过网络的一个安全通道来实现。在一些实施例中, 路由选择、重引导或引入用 VPN 或 APN 通道来实现。

[0183] 在一些实施例中, 一个基于网络的服务收费策略系统与一个用户服务协定确认系统一起使用, 其中该用户协定确认系统提供如下确认: 用户已同意接入服务使用条款在一个 SIM 被检测出与包括一个服务处理器能力的一个装置配置相关联时, 规定接入服务使用记账或收费的一个第一费率, 并且在一个 SIM 被检测出与不包括一个服务处理器能力的一个装置配置相关联时, 规定接入服务使用记账或收费的一个第二费率。在一些实施例中, 如果一位用户移除或篡改包括一个服务处理器能力的一个装置配置, 或者如果一位用户将一个 SIM 安装到未被配置有一个服务处理器能力的一个装置中, 则改变了用户服务使用计费条件。在一些实施例中, 取决于装置配置 (例如, 具有或不具有一个服务处理器能力), 以针对“大块”服务使用的一个不同费率对用户计费, 或以针对一种或多种分类的服务使用的一个不同费率对用户计费。

[0184] 在一些实施例中, 一个基于网络的服务收费策略系统与一个用户服务协定确认系统一起使用, 其中该用户协定确认系统提供如下确认: 用户已同意接入服务使用条款在一个 SIM 被检测出与包括一个服务处理器能力的一个装置配置相关联时, 规定一个第一接入服务特权集, 并且在一个 SIM 被检测出与不包括一个服务处理器能力的一个装置配置相关联时, 规定一个第二接入服务特权集。在一些实施例中, 如果一位用户移除或篡改包括一个服务处理器能力的一个装置配置, 或者如果一位用户将一个 SIM 安装到未被配置有一服务处理器能力的一个装置中, 则修改了用户服务使用许可。在一些实施例中, 这个修改可以包括变更被允许的网络目的地、变更被允许的网络服务、变更被允许的网络资源、隔离接入或阻塞接入。

[0185] 在一些实施例中, 一个装置处理器与一个 SIM 组合存在引起服务控制器向用户提供有利的网络接入服务。示例包括但不限于在此所论述的被赞助的服务、用户付费的基于应用的服务 (例如, 其中对于一个或多个装置应用程序的接入以与总互联网接入相比潜在较低的费用包括于一个服务允许中的用户付费服务)、用户付费目的地服务 (例如, 其中对于一个或多个网络目的地或资源的接入以与总互联网接入相比潜在较低的费用包括于一个服务允许中的用户付费服务)、漫游服务 (例如当装置连接至一个漫游网络时, 例如通过告知用户其正在漫游并且询问其是否想要继续或中断漫游服务使用, 更新漫游服务使用指示或费用指示、漫游服务费率指示, 允许一位用户来决定在漫游时其想要哪一种装置服务使用分类等来帮助用户的服务); 或服务使用通知服务 (例如为用户提供对已引发多少服务使用或服务的更新, 告知用户什么计划是可用的, 基于用户正尝试的一个活动或一组活动来告知用户一个服务计划签约何时可能为有利于用户的, 或为用户提供可以在一个装置用户接口 (UI) 中选择或购买的服务计划签约选择项集等)。在一些实施例中, 这些用户服务通过装置上的服务处理器的能力与一个接入服务提供者网络上的一个服务控制器或其他网元的一个特定配置而成为可能。

[0186] 在一些实施例中, 如果从装置上移除用于一个第一网络服务提供者的 SIM 并且安

装用于一个第二网络或服务提供者的另一个 SIM, 则用户可能不能接入相同的服务。在一些实施例中, 装置上的服务处理器检测 SIM 已被改变, 并且通过一个装置用户接口 (UI) 通知来告知用户如果用户改变 SIMS 或服务提供者网络, 则该用户将丢失某些服务。在一些实施例中, 将被丢失的服务被列出在一个 UI 通知中。在一些实施例中, UI 通知陈述如果用户想要重新获得接入到某些服务, 则用户可以重新安装原始的 SIM。

[0187] 在一些实施例中, 一个或多个网元确定一个终端用户装置是否具有一个有效服务处理器。在一些实施例中, 网络中的一个服务控制器认证该服务处理器。

[0188] 在一些实施例中, 服务控制器执行对服务处理器的认证来确保其存在并且被正确地配置成实施一个接入网络服务策略的一个装置部分。图 16 和图 17 展示了用于一个装置服务处理器到服务控制器通信链路的系统图, 该链路可用帮助安全通信和服务处理器认证以及验证功能。

[0189] 图 16 为根据一些实施例的展示服务处理器 115 的服务控制装置链路 1691 和服务控制器 122 的服务控制服务链路 1638 的功能图。具体地, 如图 16 所示, 根据一些实施例, 服务处理器 115 的服务控制装置链路 1691 和服务控制器 122 的服务控制服务链路 1638 在服务控制链路 1653 上提供服务处理器 115 与服务控制器 122 之间的安全控制平面通信。不同实施例包括服务控制链路路上的两个或三个加密层, 其中一个实施例或层在加密功能 (2408, 2428) 和解码功能 (2412, 2422) 上实施, 并且另一个实施例或层在传输服务堆栈 (2410, 2420) 上实施。加密的一个任选第三实施例或层在传输服务堆栈的下方, 例如用 IPSEC 或另一个 IP 层加密、VPN 或隧道技术方案来实施。例如, 不同已知安全加密技术可以在加密功能 (2408, 2428) 中用公共 / 私用或完全私用的密钥和 / 或签名来实施, 这样使得可以达到用于服务处理器控制平面业务量的非常强的安全性等级, 即使基本传输范围 (2410, 2420) 用标准的安全或开放的网络联网协议, 如 TLS 或 TCP 来实施。例如, 对装置而言为本地的服务处理器代理通信可以经由服务控制装置链路 1691 连接被传导到服务控制器元件或从服务控制器元件传导到代理通信总线 1630。服务控制装置链路 1691 与代理通信总线 1630 的组合 (在一些实施例中其也被安全地加密或签名) 提供服务处理器与服务控制器服务器元件和服务控制器与服务控制器代理之间的一个无缝的、高度安全异步控制平面连接, 该连接在广泛的接入网络上工作, 如具有在接入网络上、另一个私用网络或在互联网上将 IP 或 TCP 业务量连接至另一个 TCP 或 IP 端点的能力的任何接入网络。如在此所描述, 在一些实施例中, 代理通信总线 1630 也提供一个第四等级加密或签名通信, 来在装置上形成一个安全封闭的系统以用于代理到代理通信, 从而例如使得软件或应用以任何除服务控制装置链路 1691 之外的方式接入装置上的服务处理器代理中的一个或多个是非常困难或实际上不可能的。以这种方式, 在一些实施例中, 代理通信总线 1630 和服务处理器代理当必要时可以仅由彼此接入, 或者由代理通信策略或由具有在服务控制装置链路 1691 上通信的适当安全性凭证的服务控制器或其他授权网络功能许可。此外, 在一些实施例中, 两个或更多个代理的子集之间或一个或多个代理与一个或多个服务控制器服务元件之间的通信用唯一密钥或签名加密, 其方式为提供一个提供私用点对点、点对多点或多点对多点的安全通信线路的第四等级安全性。

[0190] 在一些实施例中, 所有服务控制装置链路 1691 通信均被变换到一个连续控制平面连接中, 其中频率基于服务使用速率、连接之间的一个最小设置期和 / 或用于建立通信

频率的其他方法。在一些实施例中,这个心跳功能提供了一个连续的验证链路,服务控制器通过该链路验证服务处理器和 / 或装置正在正确地运行,同时正确的服务策略被实施。鉴于在此所描述的以下心跳功能实施例,本领域普通技术人员将清楚的是,用于实施不同心跳实施例的不同方法是可能的,并且显然存在许多方式来达到启用一个可依赖的有时为连续的控制链路和为了以一个可验证的方式辅助服务使用控制的目的验证功能的必要特征。如所示,在服务处理器 115 之内,服务控制装置链路 1691 包括与代理通信总线 1630 通信的心跳发送计数器 2402。例如,心跳发送计数器 2402 可以在服务处理器 115 通信(例如,基于一个心跳机构的周期性通信)应该被发送到服务控制器 122 时为触发提供一个计数,并且也与代理通信总线 1630 进行通信的心跳缓冲器 2404 根据基于不同心跳的实施例而缓冲用于下一个服务处理器 115 的任何这类信息,如在此所类似地描述。心跳缓冲器 2404 与用于使任何服务处理器 115 通信成帧并且加密的成帧元件 2406 和加密元件 2408 进行通信,这些服务处理器通信由传输服务堆栈 2410 在服务控制链路 1653 上传输到服务控制器 122。类似地,如所示在服务控制器 122 之内,服务控制服务器链路 1638 包括与服务控制器网络 2440 进行通信的心跳发送计数器 2434 和也与服务控制器网络 2440 进行通信的心跳缓冲器 2432,该心跳缓冲器根据基于心跳的不同实施例而缓冲用于下一个服务控制器 122 的任何这类信息,如在此所类似地描述。心跳缓冲器 2432 与用于使任何这类服务控制器 122 通信成帧并且加密的成帧元件 2430 和加密元件 2428 进行通信,这些服务控制器通信由传输服务堆栈 2420 在服务控制链路 1653 上传输到服务控制器 115。

[0191] 也如所示,在图 16 的服务处理器 115 之内,服务控制装置链路 1691 包括:解码元件 2412,其用于对任何接收的服务控制器 122 通信进行解码(例如对加密的通信进行解密);拆开元件 2414,其用于拆开接收的服务控制器 122 通信(例如,汇编分组的通信);以及代理路由 2416,其用于将接收的服务控制器 122 通信(例如,命令、指令、关于心跳的信息或状态报告、关于策略的信息或配置设置和 / 或更新、挑战 / 响应查询、代理刷新和 / 或新软件安装)路由选择到服务处理器 115 的适合代理。类似地,如所示,在服务控制器 122 之内,服务控制服务器链路 1638 还包括:解码元件 2422,其用于对任何接收的服务处理器 115 通信进行解码(例如对加密的通信进行解密);拆开元件 2424,其用于拆开接收的服务处理器 115 通信(例如,汇编分组的通信);以及代理路由 2426,其用于将接收的服务处理器 115 通信(例如,响应指令和 / 或命令、关于心跳的信息或状态报告、关于策略的信息或配置设置和 / 或更新、挑战 / 响应查询、代理状态信息、网络服务 / 费用使用和 / 或任何其他关于报告的信息)路由选择到服务控制器 122 的适合代理。因此,如在此相对于不同实施例所描述,服务控制器 122 与服务处理器 115 之间的不同安全通信可以使用如图 16 所示的实施例来执行,并且本领域普通技术人员还将认识到各种其他实施例可以用来类似地提供服务控制器 122 与服务处理器 115 之间的不同安全通信(例如,使用不同软件和 / 或硬件架构来提供安全通信,如使用用于提供这类安全通信的另外和 / 或较少元件 / 功能或其他设计选择项)。

[0192] 在一些实施例中,提供服务处理器与服务控制器之间的一个高效并且有效的通信成帧结构,并且以下实施例(例如,如相对于图 17 所示并且描述)传授这样一类结构:其将不同的服务处理器代理控制平面通信和不同的服务控制器元件控制平面连接压缩成不消耗过多带宽的一个格式来启用装置与服务控制器之间的一个连续的控制平面连接。在一些实施例中,提供服务处理器与服务控制器之间的一个高效并且有效的通信成帧结构来在成

帧并且传输之前如以基于服务使用速率的一个心跳频率缓冲这类通信消息长达某段时间。在一些实施例中,提供服务处理器与服务控制器之间的一个高效并且有效的通信成帧结构来允许轻松地压缩、加密、解码、拆开该帧并且允许分发消息。鉴于在此所描述的不同实施例,本领域普通技术人员将清楚的是,许多成帧结构将为了组织代理通信或将其成帧和将这样一类系统元件与装置服务控制器功能、服务处理器功能、服务控制验证功能相组合的唯一性和重要性的旨在的目的和 / 或其他目的而工作。

[0193] 图 17 为根据一些实施例展示服务处理器通信帧 2502 和服务控制器通信帧 2522 的一个成帧结构的功能图。具体地,根据一些实施例,服务处理器 115 的服务控制装置链路 1691 和服务控制器 122 的服务控制服务链路 1638 (例如,如图 16 所示)在服务处理器 115 与服务控制器 122 之间的服务控制链路 1653 上,使用如图 17 所示的呈服务处理器通信帧 2502 和服务控制器通信帧 2522 的格式的通信帧来提供安全控制平面通信。如所示,服务处理器通信帧 2502 包括服务处理器成帧顺序号 2504、时间戳 2506、代理第一个功能 ID2508、代理第一个功能消息长度 2510、代理第一个功能消息 2512 以及(假定一个以上消息在这个帧中传输)代理第 N 个功能 ID2514、代理第 N 个功能消息长度 2516 以及代理第 N 个功能消息 2518。因此,服务处理器通信帧 2502 可以包括如图 17 所示的一个或多个消息,这会取决于联网帧长度要求和 / 或其他设计选择项。类似地,如所示,服务控制器通信帧 2522 包括服务控制器成帧顺序号 2524、时间戳 2526、代理第一个功能 ID2528、代理第一个功能消息长度 2530、代理第一个功能消息 2532 以及(假定一个以上消息在这个帧中传输)代理第 N 个功能 ID2534、代理第 N 个功能消息长度 2536 以及代理第 N 个功能消息 2538。因此,服务控制器通信帧 2522 可以包括如图 17 所示的一个或多个消息,这会取决于联网帧长度要求和 / 或其他设计选择项。

[0194] 图 18A 至图 18E、图 19A 至图 19G 以及图 20A 至图 20C 呈现了多个实施例,这些实施例可以单独地或组合地由一个服务控制器使用,来认证服务处理器以确保其存在并且被正确地配置成实施一个接入网络服务策略的一个装置部分。图 18A 至图 18E 根据一些实施例提供了汇总不同服务处理器心跳功能和参数(例如,由不同代理、组件和 / 或在软件和 / 或硬件中实施的功能实施)的表。以上以类似的方式描述了这些心跳功能和参数中的许多个,并且图 18A 至图 18E 所示的这些表不旨在为对这些心跳功能和参数的一个详尽的汇总,相反地被提供为对根据在此所描述的一些基于心跳的实施例的这些功能和参数理解的帮助。

[0195] 图 19A 至图 19G 提供了根据一些实施例的汇总不同基于装置的服务策略实施验证技术的表。以上以类似的方式描述了这些基于装置的服务策略实施验证技术中的许多个,并且图 19A 至图 19G 所示的这些表不旨在为对这些基于装置的服务策略实施验证技术的一个详尽的汇总,相反地被提供为对根据在此所描述的一些基于装置的服务策略实施例的这些技术理解的帮助。

[0196] 图 20A 至图 20C 提供了根据一些实施例的汇总用于保护基于装置的服务策略免于受到危害的不同技术的表。以上以类似的方式描述了这些用于保护基于装置的服务策略免于受到危害的技术中的许多个,并且图 20A 至图 20C 所示的这些表不旨在为对这些用于保护基于装置的服务策略免于受到危害的技术的一个详尽的汇总,相反地被提供为对根据在此所描述的一些基于装置的服务策略实施例的这些技术理解的帮助。

[0197] 图 21 展示用 SGSN 通知来开始或停止一个数据会话的一个过程的一个示例实施例。终端用户装置 100 尝试通过将 GPRS 连接消息发送到 SGSN2230 而开始一个数据会话。SGSN2230 通知服务控制器 122 终端用户装置 100 已开始一个数据会话。服务控制器 122 等待一段预先确定的时间,例如一分钟以接收来自服务处理器 115 的一个登陆或认证请求。在一些实施例中,服务控制器 122 设置一个登陆计时器。如果服务控制器 122 在计时器期满之前接收到该登陆或认证请求,则其尝试认证服务处理器 115。

[0198] 当服务控制器 122 尝试认证服务处理器 115 时,可能发生一个或多个认证错误。例如,服务处理器 115 可能具有无效凭证。作为另一个示例,服务处理器 115 可能发送无效应用或核心签名。作为另一个示例,服务处理器 115 可能报告终端用户装置“根”检测错误。作为另一个示例,服务处理器 115 可能使用一个已由一个不同的终端用户装置使用的标识符来联系服务控制器 122。

[0199] 如果服务控制器 122 未在预先确定的时间内接收到来自服务处理器 115 的请求,或者如果服务控制器 122 由于某一原因不能认证服务处理器 115,则服务控制器 122 假定 (1) 终端用户装置 100 不含有一个服务处理器,并且因此不能参与装置辅助服务,或者 (2) 尽管终端用户装置 100 具有一个服务处理器,但是服务处理器 115 已被禁用。服务控制器 122 将一个通知(“无有效 SP”消息)发送到数据评级元件 2220 来指示:终端用户装置 100 不具有提供数据调解元件 2210 所必需的信息以生成例如“微型 CDR”的详细数据使用报告的能力。在一些实施例中,服务控制器 122 将一个触发发送到网络来指示:应该对终端用户装置 100 以“标准”大块费率来对使用进行收费。在一些实施例中,服务控制器 122 在发送到服务调解元件 2210 的 CDR 中指定一个“标准”大块费率收费码。在一些实施例中,数据评级元件 2220 在基于运营商的记录的基础上确定由终端用户装置 100 的数据使用。

[0200] 如果服务控制器 122 在预先确定的时间内接收到来自服务处理器 115 的登陆或认证请求并且成功地认证了服务处理器 115,则服务控制器 122 将一个通知(“装置 OK”消息)发送到数据评级元件 2220 来指示终端用户 100 具有一个服务处理器并且能够支持装置辅助服务。在一些实施例中,当服务控制器 122 确定终端用户装置 100 具有一个有效服务处理器时,数据评级元件 2220 期望接收到来自数据调解元件 2210 的“微型 CDR”报告。在一些实施例中,数据评级元件 2220 在基于比平常的 CDR 含有更高粒度的信息的微型 CDR 来确定使用。例如,鉴于一个平常的 CDR 可能仅报告一个终端用户装置使用了 100 兆字节(MB)数据,一个微型 CDR 集可能报告终端用户装置使用了 15MB 电子邮件、35MB 社交联网以及 50MB 流式视频。

[0201] 在一些实施例中,数据调解元件 2210 将基于运营商的使用报告(例如,CDR)发送到服务控制器 122。服务控制器 122 为终端用户装置 100 在使用数据库 2200 中查询基于装置的使用报告(例如,微型 CDR)。服务控制器 122 从基于运营商的使用报告中确定终端用户装置 100 的数据使用。服务控制器 122 从基于装置的使用报告中确定终端用户装置 100 的数据使用。服务控制器 122 将从基于运营商的使用报告中确定的使用与从基于装置的使用报告中确定的使用相比较。如果服务控制器 122 确定这两个使用度量不相匹配(例如,不相同或不在彼此阈值内),则服务控制器 122 将一个通知(例如,一个欺诈报警)发送到数据评级元件 2220 来指示终端用户装置处于一个欺诈的状态,并且数据评级元件 2220 应该在基于运营商的使用报告的基础上为终端用户装置 100 计费使用。服务控制器 122 将基于运营

商的使用报告和基于装置的使用报告发送到数据调解元件 2210。

[0202] 当 SGSN2230 接收到“GPRS 分离”消息时,SGSN2230 将用于终端用户装置 100 的数据会话被关闭的一个通知发送到服务控制器 122。

[0203] 图 22 展示了用 GGSN 通知开始或停止一个数据会话的一个过程的一个示例实施例。该过程类似于参看图 21 所描述,除如何开始并且结束数据会话之外。终端用户装置 100 通过将数据业务量发送到 GGSN2240 而开始一个数据会话。GGSN2240 辨认一个新的数据会话的开始并且通知服务控制器 122 终端用户装置 100 已开始一个数据会话。当 GGSN2240 确定该数据会话已关闭时,其将用于终端用户装置 100 的数据会话被关闭的一个通知发送到服务控制器 122。

[0204] 如以上所论述,在一些实施例中,一个装置服务处理器可以提供信息来辅助针对装置应用程序、网络目的地或资源、一种类型的网络、一个漫游情况(例如,家庭或漫游网络)、一个时间段、一个网络拥塞等级、一个网络 QoS 等级以及一个后台或前台通信的任意组合的服务使用分类。在一些实施例中,当一个装置服务处理器为涉及装置应用程序、网络目的地或资源、一种类型的网络、漫游情况(例如,家庭或漫游网络)、一个时间段、一个网络拥塞等级、一个网络 QoS 等级以及一个后台或前台通信的一种分类服务使用提供服务使用时,服务处理器 115 生成称为“微型 CDR”的一个服务使用报告,该报告随后传递到一个网元(例如,一个服务控制器)。与不提供这样一类使用记账故障的一个“大块”CDR 相比,该微型 CDR 以更精细的明细提供一个服务使用记账分解(例如,包括关于一个装置应用程序、网络目的地或资源、一种类型的网络、漫游情况(例如,家庭或漫游网络)、一个时间段、一个网络拥塞等级、一个网络 QoS 等级以及一个后台或前台通信)。

[0205] 在一些实施例,一个装置被配置成接收接入网络服务并且进一步被配置成包括一个服务处理器能力来为一个或多个服务活动分类记账并且将该记账发送到一个服务控制器。在一些实施例中,服务控制器被配置成将作为一个服务使用信用的至少一部分服务处理器服务记账传递到一个服务使用调和系统。应注意,在此一个服务使用调和系统在不同的实施例中也称为一个服务使用调解系统或类似涉及调解的术语。在一些实施例中,该服务使用调和系统被配置成从一个用户服务记账或使用账单中移除一个信用。在一些实施例中,从一个用户服务记账或使用账单中移除的该服务使用信用被分配到赞助方服务记账或账单。

[0206] 在一些实施例中,有利的是针对一个可信源来调和从一个服务处理器中接收的这些微型 CDR 服务使用记账报告。在一些实施例中,这通过一个系统来实现,该系统为用一个可信源调和或由其证实的一个或多个微型 CDR 使用报告提供使用信用。在一些实施例中,如果提供了这类信用,则根据与微型 CDR 分类相关联的服务使用记账规则来从用户“大块”使用中移除对应使用并且将其重新分配给用户。在一些实施例中,可以设计这些微型 CDR 记账规则,来将微型 CDR 服务使用报告记账记入一个付费用户服务分类中(例如,一个基于装置应用程序的服务记账、一个基于网络目的地或资源的服务记账、一个漫游服务使用记账等)。在一些实施例中,可以设计这些微型 CDR 记账规则,来将微型 CDR 服务使用报告记账记入一个被赞助的服务分类中(例如,一个基于被赞助的装置应用程序的服务记账、一个基于网络目的地或资源的服务记账、一个服务使用的被赞助的背景分类、一个服务使用的被赞助的内容源分类、一个被赞助的购物服务等)。

[0207] 在一些实施例中,用来证实微型 CDR 服务使用分类报告的可信源为一个 FDR (流数据记录) 源,该 FDR 源报告指示网络源或目的地(例如,域名、URL、IP 地址等)和可能地一个或多个端口和协议的一个详细分类等级。在一些实施例中,FDR 源为一个网元。在一些实施例中,FDR 源为一个装置代理。在一些实施例中,生成 FDR 报告的代理处于装置上的一个安全执行环境中。在一些实施例中,生成 FDR 报告的代理处于装置上的一个安全硬件环境中。在一些实施例中,生成 FDR 报告的代理与服务控制器一起使用一个安全传输协议,该服务控制器以一种方式排序并且签名和 / 或加密,其中如果 FDR 报告的顺序或 FDR 报告的内容被篡改,则可以由服务控制器检测一个 FDR 完整性违反。在一些实施例中,从该服务控制器到生成 FDR 报告的代理的通信以一种方式排序并且签名和 / 或加密,其中如果 FDR 报告的顺序或 FDR 报告的内容被篡改,则可以由生成 FDR 报告的代理检测一个 FDR 完整性违反。在一些实施例中,当生成 FDR 报告的代理报告一个 FDR 完整性违反时,生成 FDR 报告的代理引起装置接入对一个或多个接入网络而隔离或受阻塞。在一些实施例中,其他装置通信链路而不是接入网络链路也可以受隔离或受阻塞,包括有线装置接入端口(例如,以太网、USB、火线等)、蓝牙、WiFi 以及近场通信中的一个或多个。

[0208] 在一些实施例中,用来证实微型 CDR 服务使用分类报告的可信源为一个基于网络的元件,如处理与微型 CDR 相关联的服务分类的一个服务器、网关、代理或路由器。在一些实施例中,基于网络的元件将与微型 CDR 相关联的服务使用分类,测量服务使用并且将一个服务使用分类报告提供回一个服务控制器,这样使得可以针对微型 CDR 报告而对其进行调和。

[0209] 在一些实施例中,一个装置被配置成接收接入网络服务并且进一步被配置成包括一个服务处理器能力来为一个或多个服务活动分类将业务量路由选择、重引导或以另外方式引入到一个或多个代理网关 / 服务器。在一些这类的实施例中,一个服务使用调和系统被配置成从该一个或多个代理网关 / 服务器接收装置服务使用信息(例如,一个信用量),并且该服务使用信息用于从由服务使用调和系统分配或记账到一个用户账单的服务使用中移除一个量(例如,一个信用量)。在一些实施例中,装置路由选择通过为一个或多个服务使用分类将装置业务量路由选择、重引导或引入到与该网关 / 服务器相关联的一个特定的网络目的地或资源而实现。在一些实施例中,路由选择、重引导或引入使用通过网络的一个安全通道而实现。在一些实施例中,路由选择、重引导或引入使用 SSL、VPN 或 APN 通道来实现。

[0210] 在一些实施例中,一个装置服务处理器根据一个服务分类策略来将服务使用分类并且将与该分类策略相关联的业务量路由选择、重引导或引入到为该服务使用记账生成微型 CDR 的一个网元(例如,处理与微型 CDR 相关联的服务分类的一个服务器、网关或路由器)。以这种方式,装置可以将用于装置应用程序或 OS 功能的服务使用与一个特定网络目的地相关联,进而进一步处理业务量并且生成被发送到服务控制器以用于调和(例如,调解)的适合微型 CDR,如以上所描述。服务处理器可以通过将业务量重引导到与适合网元相关联的网络目的地、将业务量路由选择到与适合网元相关联的网络目的地或将业务量通过隧道传输或安全地通过隧道传输(例如,SSL、VPN、APN)到与适合的网元相关联的网络目的地来引入根据分类策略分类的业务量。

[0211] 在一些实施例中,用来证实微型 CDR 服务使用分类报告的可信源为提供服务的

服务器或网站,并且该证实以良好的客户反馈的形式提供,该客户反馈与可以用来确定将信用提供给哪一个装置或用户的一个用户凭证、一个服务处理器凭证或一个装置凭证相关联。例如,如果一个网站与为一个微型 CDR 定义的服务使用分类相关联,并且该网站由具有一个给定装置凭证或用户凭证的装置来访问,并且该网站服务器跟踪访问数量、交易数量、生成的业务量、传递的数据量或与网站的装置交互作用的另一个度量,则对这个与网站的装置交互作用的汇总可以被传递到服务控制器,并且该服务控制器可以为微型 CDR 提供信用。

[0212] 在一些实施例中,限制由于服务处理器不正确的配置或篡改一个服务处理器的不正确的服务使用记账的可能性的另一个手段可以通过在允许一个给定的微型 CDR 服务使用分类类别的一个给定的时段期间为服务量设上限而实现(例如,通过限制在一个给定的时段中的用于一个或多个服务使用分类,包括一个装置应用程序、网络目的地或资源、一种类型的网络、一个漫游情况(例如,家庭或漫游网络)、一个时间段、一个网络拥塞等级、一个网络 QoS 等级以及一个后台或前台通信的服务使用量)。在一些实施例中,在允许一个给定的微型 CDR 服务使用分类类别的一个给定的时段期间为服务量设上限而作为为基于服务使用的一个特定分类的一个用户付费服务限制服务使用费用的一种方法是有利的。在一些实施例中,在允许一个给定的微型 CDR 服务使用分类类别的一个给定的时段期间为服务量设上限而作为为基于服务使用的一个特定分类的一个被赞助的服务限制服务使用费用的一种方法是有利的。在一些实施例中,篡改一个或多个微型 CDR 服务使用分类分类的服务使用报告的可能性通过组合使用开始/停止记账、CDR 反馈、FDR 反馈等中的一个或多个对服务使用调和与在允许微型 CDR 服务使用分类类别中的一个或多个的使用上设置限制而限制。

[0213] 在一些实施例中,篡改一个或多个微型 CDR 服务使用分类类别的服务使用报告的可能性通过针对用于从一个可信源中接收的大块 CDR 报告的总服务量而比较用于所有组合的微型 CDR 服务使用分类的总服务使用而限制。

[0214] 在使用关联分类(也指自适应环境服务使用分类)的一些实施例中,不能直接识别为属于一个给定的微型 CDR 服务使用分类的某一环境使用基于以下各项中的一项或多项被分配到微型 CDR 服务使用分类:(i) 与在属于微型 CDR 分类时识别的一个或多个已知服务使用流的时间邻近度,(ii) 自属于微型 CDR 分类的一个或多个已知服务使用流被识别之后发生的最大服务使用量(例如,字节计数),或(iii) 未识别的服务使用与作为属于微型 CDR 分类的一个或多个已知服务使用流的同一应用相关联的事实。

[0215] 在一些这类关联分类(自适应环境服务分类)的实施例中,服务使用欺诈暴露可以通过在可以“未被记账”的服务使用量上设置限制而限制,这样使得如果大部分使用可以被分类为属于一个微型 CDR 服务使用分类类别,则允许未被记账的服务使用在同一微型 CDR 记账中被记账。以这种方式,如果欺诈性服务使用活动导致分类为属于微型 CDR 使用分类类别为未知的一个大百分比的服务使用,则可以声明一个微型 CDR 记账完整性违反。可替代地,超过限制的不能被调和(记账)的服务使用可以一个商定的合同费率记账(例如,记账到用户)。在一些实施例中,商定的费率与用于用户付费的大块服务费率同样高或比其更高(例如高于基于被赞助的并且专门的应用或服务网站的服务计费的费率)。在一些实施例中,由服务控制器将以较高费率对用户计费的通知发送到用户。在一些实施例中,用户签约一份

服务协定,其中用户同意在服务处理器受到危害或微型 CDR 记账受到危害的情况下以较高费率对用户计费。

[0216] 在一些实施例中,微型 CDR 报告包括由服务处理器识别为已知属于微型 CDR 服务使用类别的服务使用量。在一些实施例中,可以在用于已知属于微型 CDR 分类的服务使用的微型 CDR 报告中提供一个流标识符(例如,域名、URL、IP 地址、端口或与 [发起或终止] 业务量相关联的装置应用程序)。在一些实施例中,服务控制器对这些“已知良好”的微型 CDR 流标识符取样或扫描来确保这些流事实上属于该微型 CDR 服务使用分类,并且如果这些流不属于,则可以声明一个微型 CDR 记账完整性违反。在一些实施例中,可以在用于不能被分类为属于微型 CDR 分类的服务使用的微型 CDR 报告中提供一个流标识符(例如,域名、URL、IP 地址、端口或与 [发起或终止] 业务量相关联的装置应用程序)。在一些实施例中,服务控制器对这些“未知的”微型 CDR 流标识符取样或扫描来确定服务目的地模式是否指示与微型 CDR 分类策略不一致的欺诈性服务使用,并且如果是,则可以声明一个微型 CDR 记账完整性违反。

[0217] 在一些实施例中,期望安装在被配置有一个正确配置的服务处理器的一个装置中的 SIM 在一个接入网络服务使用策略的网络部分中被分配有一个相对小的服务使用上限,这样使得该装置可以连接至网络并且允许用服务控制器来认证服务处理器。通过在用服务控制器认证服务处理器之前限制允许的服务使用的初始量,不可能在确保一个正确配置的服务处理器存在于装置上之前得到大量服务。在一些实施例中,一旦装置服务处理器被认证,则可以向接入网络服务策略的网络部分中的使用限制添加一个增量。在一些实施例中,当装置服务处理器生成的 CDR、FDR 或微型 CDR 由服务控制器接收时,可以向接入网络服务策略的网络部分添加另外使用限制增量。在一些实施例中,任何时候,如果来自装置的 CDR、FDR 或微型 CDR 被篡改或停止,则服务控制器停止增加在接入网络服务策略的网络部分中的使用限制,并且拒绝装置接入。可替代地,在一些实施例中,与用于由服务控制器提供的微型 CDR 信用(例如,基于用户付费的应用服务、基于用户付费的网站服务、用户付费的内容服务、基于被赞助应用的服务、基于被赞助网站的服务或基于被赞助内容的服务)的一个或多个微型 CDR 计费率相比较,接入网络服务策略的网络部分要求一个较高计费率的应用,而不是当服务处理器被移除或受篡改时停止服务。在一些实施例中,如果服务处理器中止将微型 CDR 发送到服务控制器,则用户中止信贷微型 CDR 服务使用,并且所有使用均以可能高于微型 CDR 服务费率的大块费率计费。

[0218] 在一些实施例中,向用户提供或出售一个 SIM,其中该 SIM 与被赞助的服务相关联,这些被赞助的服务是基于配置在网络策略强制执行元件和服务控制器中的网络接入服务策略的。在这类实施例中,问题由以下引起:SIM 可能安装在不具有一个正确配置的服务处理器的装置中,从而导致一位用户可能用被赞助的 SIM 接收非计划中的免费服务。以上描述的实施例可以通过限制在接入网络服务策略的初始网络部分中被允许的初始服务使用量,在用服务控制器认证服务处理器之前,用来限制允许 SIM 接收的接入量。然而,如果多个被赞助的 SIM 是随时可用的并且是廉价或免费的,则一位用户可能潜在地调换若干 SIM 到装置中,并且当服务控制器未能认证服务处理器时移除每一个 SIM。在一些实施例中,在被赞助的 SIM 首次获取服务使用并且未能为该装置认证服务处理器时,服务控制器辨认 SIM 和一个第二装置凭证(例如,一个 IMEI、一个调制解调器凭证或一个装置凭证)。一

旦服务处理器未能用服务控制器认证,则服务控制器重设置接入网络服务策略的网络部分以在下一一次 SIM 尝试用与原始 SIM 相关联的装置凭证认证时拒绝服务。

[0219] 在一些实施例中,在没有装置上的一个服务处理器的情况下,良好的客户反馈可以直接用作一个微型 CDR 信用源。例如,在一些实施例中,一个网站与为一个微型 CDR 定义的服务使用分类相关联,并且由具有一个给定装置凭证或用户凭证的装置访问的该网站或服务器跟踪访问数量、交易数量、生成的业务量、传递的数据量或与该网站或服务器的装置交互作用的另一个度量中的一个或多个,创建与网站或服务器的这个装置交互作用的一个汇总报告,并且随后将该汇总报告传递到一个服务控制器。该服务控制器可以随后通过应用一个用户服务使用信用评级规则来从用户账户中扣除服务使用的一个大块部分并且将服务使用的一个分类添加到该用户账户而调和对与该网站或服务器的装置交互作用的良好客户反馈汇总报告,为了计费目的,该用户账户由用于给定的微型 CDR 分类的一个评级规则来定费率。可替代地,服务控制器可以从用户账户中扣除一部分良好的客户微型 CDR 服务使用记账或计费并且将其添加到一个赞助方实体账户,如提供网站或服务器服务的实体。以这种方式,对用户付费分类和被赞助分类二者而言,一个微型 CDR 服务使用收费系统可以为具有专门的服务使用分类费率的分类服务使用在一个网络中实施,而无需一个装置上服务处理器。

[0220] 图 23 展示具有网络系统元件的一个示例实施例,这些网络系统元件可以被包括在一个服务控制器系统中,来协助一个装置辅助服务(DAS)实施和这些元件之间的信息流。图 23 展示了信息流以协助装置生成的数据使用记录和与一个终端用户装置相关联的网络生成的(例如,无线网络运营商生成的)数据使用记录的调和。此外,图 23 为了发布一个提供设置的目的而展示了从一个运营商到一个终端用户装置的信息流。终端用户装置的一位用户可以随后在该提供设置上选择或作用。

[0221] 运营商生成的收费数据记录(CDR)或实时报告记录(RTR)(或其他实时或近实时使用记录格式,例如像,FDR、批处理使用记录、连续使用记录事件馈送或 SMS 格式化使用记录消息)从运营商设备 2650(其可以为例如一个实时报告系统、一个网络网关、一个网络使用收费系统元件、一个 AAA、一个 HLR、一个计费元件等)流动到负载均衡器 2652 从而到 RTR 过滤元件 2654。

[0222] 在一些实施例中,负载均衡器 2652 选择在服务控制器信息处理系统中可用的许多 CDR/RTR 处理线程中的一个。在一些实施例中,该处理线程是在网关或服务器 CPU 上运行的一个异步软件或固件程序。在一些实施例中,处理线程为存在于网关或服务器 CPU 或虚拟机的一个资源池中的一个虚拟机处理线程,该资源池可以包括地理上分离或冗余的资源池。如图 23 所示,每一个处理线程包括以下功能步骤:CDR/RTR 过滤 2654、JMS 队列 2656、CDR/RTR 处理器 2658 以及到 CDR/RTR 数据库 2660 的接口。在一些实施例中,处理线程为异步的,因为这些处理线程在负载均衡器 2652 将一个或多个 CDR/RTR 数据传送引导到线程时发起并且在处理过的 CDR/RTR 信息已经被处理并且存放在 CDR/RTR 数据库 2660 中时终止。应注意,图 23 仅展示了潜在地许多可用 CDR/RTR 处理线程中的一个。

[0223] CDR/RTR 过滤元件 2654 选择与包括一个装置客户端的装置相关联的记录,该装置客户端与服务控制器进行通信(例如,该装置客户端可以为一个服务处理器,该服务处理器被配置成提供服务使用通知更新、用 UI 选项显示和用户选择行动的装置上服务计划购买

或激活、装置辅助接入控制策略强制执行、装置辅助服务使用收费策略强制执行、装置辅助服务通知消息等)。在一些实施例中,支持 DAS 的装置由如在此所描述的传递到服务控制器的装置凭证或用户凭证识别,其中该装置凭证或用户凭证是由服务控制器管理的一个装置组或用户组的成员。

[0224] 在一些实施例中,因为实时处理要求,服务器处理线程可扩展性以及可维护性要求或服务器处理线程地理冗余度要求,所以服务器 CDR/RTR 过滤元件 2654 可以有利地用来快速地接收并且确认一个 CDR/RTR 记录来提供异步功能性。在一些实施例中,过滤了消除 JMS 队列 2656 和 / 或 CDR/RTR 数据库 2660 上的不必要负载。CDR/RTR 过滤元件 2654 放置来自已知被配置有一个装置客户端(例如,被配置成提供服务使用通知更新、用 UI 选项显示和用户选择行动的装置上服务计划购买或激活、装置辅助接入控制策略强制执行、装置辅助服务使用收费策略强制执行、装置辅助服务通知消息等的一个服务处理器)的终端用户装置的记录,该装置客户端通过 Java 消息传送服务(JMS)队列 2656 与服务控制器进行通信。在一些实施例中,CDR/RTR 过滤元件 2654 为可能具有服务处理器形式的装置过滤出装置记录,但服务处理器尚未用服务控制器正确地认证。在一些实施例中,已知被配置有与服务控制器进行通信的一个装置客户端的装置客户端通过在一个装置组或用户组管理数据库中(例如,在 SDC 数据库 2692 或订户管理系统 182 (例如,图 1 至图 3 所示))查询与 CDR 或 RTR 相关联的一个装置凭证或用户凭证来确定。

[0225] JMS 队列 2656 缓冲在 CDR/RTR 过滤 2654 之后剩余的 CDR/RTR 信息并且将一个或多个 CDR/RTR 分配到 CDR/RTR 处理器 2658 中的一个服务使用处理线程。在一些实施例中,JMS 队列 2656 是一个持久性队列。在一些实施例中,JMS 队列 2656 是应用之间的一个主要消息传送系统。

[0226] CDR/RTR 处理器 2658 检索来自 JMS 队列 2656 的记录,变换这些记录并且将其存储在 CDR/RTR 数据库 2660 中。在一些实施例中,CDR/RTR 处理器 2658 为一个应用或一个处理线程。在一些实施例中,在一个交易中,CDR/RTR 处理器 2658 从 JMS 队列 2656 中拉取一个 CDR/RTR 记录,变换该记录并且将经变换的记录存储在 CDR/RTR 数据库 2660 中以便在系统故障的情况下提供容错。在一些实施例中,CDR/RTR 处理器 2658 格式化 CDR/RTR 信息,以提供一个共用服务使用信息格式,来协助服务使用处理、报告、分析、比较、调解以及在服务控制器系统内执行的调和运行中的一项或多项。在一些实施例中,CDR/RTR 处理器 2658 观察 CDR/RTR 时间戳并且时间同步、时间对齐或时间聚合多个 CDR/RTR 报告,这样使得具有一个共用时间基准的更一致的使用度量可以在服务控制器系统内达到,以用于服务使用处理、报告、分析、比较、调解以及调和目的中的一个或多个。

[0227] 在一些实施例中,能够进行 DAS 报告的终端用户装置(例如,被配置有与服务控制器如在此所描述的一个服务处理器进行通信的装置客户端的装置)周期性或偶尔连接至使用报告网关 2672 来报告装置数据使用。在一些实施例中,DAS 报告信息包括但不限于以下各项中的一项或多项:用户服务计划购买或激活选择选择项、装置用户服务策略配置优选选择项选择(例如,针对应用、网站、网络类型或家庭 / 漫游策略的用户生成的服务策略分配)、DSA 服务使用报告、DSA 装置策略状态报告、DAS 软件环境完整性报告以及在图 18 至图 20 中的这些表中所列出的其他报告。

[0228] 在一些实施例中,DAS 装置使用报告和分析从运营商装置网络 2668 (例如,被配置

有与服务控制器进行通信的服务处理器的装置)流动到负载平衡器 2670 从而到使用报告网关 2672。在一些实施例中,负载平衡器 2670 选择在服务控制器信息处理系统中可用的许多使用报告处理线程中的一个。在一些实施例中,该使用报告处理线程是在网关或服务器 CPU 上运行的一个异步软件或固件程序。在一些实施例中,使用报告处理线程为存在于网关或服务器 CPU 或虚拟机的一个资源池中的一个虚拟机处理线程,该资源池可以包括地理上分离或冗余的资源池。如图 23 所示,每一个使用报告处理线程均由以下功能步骤组成:使用报告网关 2672、JMS 队列 2674、报告处理器 2676 以及到使用报告数据库 2678 的接口。在一些实施例中,使用报告处理线程为异步的,因为这些处理线程在负载平衡器 2670 将一个或多个使用报告数据传送引导到一个线程时发起并且在处理过的使用报告信息已被处理并且存放在使用报告数据库 2678 中时终止。应注意,图 23 仅展示了潜在地许多可用使用报告处理线程中的一个。

[0229] 使用报告网关 2672 接收来自被配置有一个装置客户端(例如,被配置成提供服务使用通知更新、用 UI 选项显示和用户选择行动的装置上服务计划购买或激活、装置辅助接入控制策略强制执行、装置辅助服务使用收费策略强制执行、装置辅助服务通知消息等的一个服务处理器)的装置的报告,该装置客户端与服务控制器进行通信并且将这些报告放置在 JMS 队列 2674 上。在一些实施例中,使用报告网关 2672 仅接收来自用服务控制器系统认证的装置服务处理器的装置报告。在一些实施例中,使用报告网关 2672 仅接收来自装置服务处理器的装置报告,这些装置服务处理器被配置有为由服务控制器管理的一个装置组或用户组的构件的装置凭证或用户凭证。在一些实施例中,使用报告网关 2672 排斥来自不具有已认证的服务处理器的终端用户装置的报告。在一些实施例中,使用报告网关 2672 为一个应用或一个处理线程。在一些实施例中,使用报告网关 2672 快速地接收并且确认终端用户装置报告。在一些实施例中,用户报告网关 2672 提供有利于支持实时处理要求的异步功能性。

[0230] 在一些实施例中,在报告被放到 JMS 队列 2674 上之前认证终端用户装置。在一些实施例中,JMS 队列 2674 是一个持久性队列。在一些实施例中,JMS 队列 2674 是应用之间的一个主要消息传送系统。

[0231] 报告处理器 2676 检索来自 JMS 队列 2674 的报告,变换这些报告并且将这些经变换的报告存储在使用报告数据库 2678 中。在一些实施例中,报告处理器 2676 是一个 EAI。在一些实施例中,在一个单个交易中,报告处理器 2676 从 JMS 队列 2674 中检索报告,变换这些报告并且将经变换的报告存储在用户报告数据库 2678 中以便在系统故障的情况下提供容错。在一些实施例中,报告处理器 2676 格式化装置使用报告信息,以提供一个共用服务使用信息格式,来协助服务使用处理、报告、分析、比较、调解以及在服务控制器系统内的调和目的内部处理和比较中的一项或多项。在一些实施例中,报告处理器 2676 观察装置使用报告时间戳并且时间同步、时间对齐或时间聚合多个装置使用报告,这样使得具有一个共用时间基准的更一致的使用度量可以在服务控制器系统内达到,以用于服务使用处理、报告、分析、比较、调解以及调和目的中的一个或多个。

[0232] 在一些实施例中,CDR/RTR 过滤 2654、CDR/RTR 处理器 2658、报告处理器 2676 以及使用报告网关 2672 共享一个主机。

[0233] 在一些实施例中,微型 CDR 生成器 2680 从 CDR/RTR 数据库 2660 中检索记录并且

从使用报告数据库 2678 中检索报告。在一些实施例中,微型 CDR 生成器 2680 为一个微型 CDR 服务使用分类确定一个服务使用量,将一个使用记账标识符分配给为与一个装置凭证或用户凭证相关联的装置而将该使用识别为记入一位装置用户账户的微型 CDR 报告,并且将这个服务使用量报告给运营商网络 2666 (在图 23 的示例实施例中,通过 JMS 队列 2662 和 FTP 或发布器 2664)。在一些实施例中,微型 CDR 生成器 2680 为一个微型 CDR 服务使用分类确定一个服务使用量,将一个使用记账标识符分配给将该使用识别为记入一位服务赞助方账户的微型 CDR 报告,并且将这个服务使用量报告给运营商网络 2666。在一些实施例中,用于被赞助的服务使用报告的该微型 CDR 还包括用于装置凭证或用户凭证的一个标识符。在一些实施例中,在微型 CDR 中被记账的服务使用量从一个装置或用户大块服务使用记账中调解或调和开。在一些实施例中,微型 CDR 生成器 2680 将微型 CDR 发送到 JMS 队列 2662。在一些实施例中,FTP 或发布器 2664 从 JMS 队列 2662 中检索微型 CDR 并且将这些微型 CDR 推送到运营商 2666。

[0234] 在一些实施例中,欺诈分析器 2682 从 CDR/RTR 数据库 2660 中检索记录。在一些实施例中,欺诈分析器 2682 从使用报告数据库 2678 中检索报告。在一些实施例中,欺诈分析器 2682 从微型 CDR 生成器 2680 中检索微型 CDR。在一些实施例中,欺诈分析器 2682 使用由 CDR/RTR 数据库 2660、使用报告数据库 2678 以及微型 CDR 生成器 2680 组成的记录和报告信息源中的一个或多个来执行一个欺诈分析。在一些实施例中,欺诈分析器 2682 比较与来自 CDR/RTR 数据库 2660、使用报告数据库 2678 以及微型 CDR 生成器 2680 中的一个或多个的一个特定装置或用户凭证相关联的使用记录,从而确定服务使用是否在预先定义的服务使用策略行为限制之外。在一些实施例中,欺诈分析器 2682 比较与来自 CDR/RTR 数据库 2660、使用报告数据库 2678 以及微型 CDR 生成器 2680 中的一个或多个的一个特定装置或用户凭证相关联的服务使用信息,从而确定是否达到或超过一个预先定义的服务使用限制。在一些实施例中,欺诈分析器 2682 比较与来自 CDR/RTR 数据库 2660、使用报告数据库 2678 以及微型 CDR 生成器 2680 中的一个或多个的一个特定装置或用户凭证相关联的服务使用信息,从而确定该特定装置或用户是否展示与一个装置或用户总体的服务使用行为相比较在预先定义的统计限制之外的一个服务使用行为。在一些实施例中,欺诈分析器 2682 将其对欺诈分析的结果存储在数据仓库 2694 之中。在一些实施例中,欺诈分析器 2682 将欺诈报警发送到运营商网络 2666。

[0235] 在一些实施例中,一个服务设计中心用来创建服务提供(例如,服务计划提供以购买或激活一个大块服务计划、一个特定应用服务计划、一个特定应用组服务计划、一个网站服务计划、一个网站组服务计划等)。在一些实施例中,这些服务提供被发布到 DAS 启用装置。为了将一个提供发布到运营商装置网络 2668 中的一个或多个装置,运营商 2696 将信息键入服务设计中心 2690 中。服务设计中心 (SDC) 2690 将提供设置存储在 SDC 数据库 2692 中。该提供设置随后流动到装置消息队列 2688。在一些实施例中,装置消息队列 2688 是一个支持数据库的持久性队列。在一些实施例中,当具有一个已认证的服务处理器的终端用户装置连接到提供设置网关 2686 时,提供设置网关 2686 将该提供设置推送到终端用户装置。在一些实施例中,提供设置网关在下次使用报告中将该提供设置推送到终端用户装置。在一些实施例中,该新供应是购买或激活一个服务计划的提供,并且该提供通知被配置有允许装置用户来选择一个选项以购买或激活装置 UI 中的服务提供的提供接受特征。

[0236] 在一些实施例中,一个服务提供清单对一个装置组或用户组可用,其中该服务提供清单在一个服务设计中心用户接口中创建,被存储在 SDC 数据库 2692 中并且向属于装置组或用户组的装置发布。

[0237] 在一些实施例中,一个提供设置在服务设计中心(SDC) 2690 中定义。在一些实施例中,这个提供设置包括多个服务计划,这些服务计划可以被传递到装置服务处理器,以用于通过装置 UI 为服务计划选择、购买或激活而向装置终端用户显示。在一些实施例中,该提供设置 UI 显示被配置成允许用户在提供设置内实时或近实时地购买或激活一个服务计划。在一些实施例中,从服务控制器中检索提供设置信息并且由一个装置服务处理器处理该提供设置信息以供 UI 显示。在一些实施例中,服务处理器提供设置信息处理和 UI 显示被配置成允许用户在提供设置内实时或近实时地购买或激活一个服务计划。在一些实施例中,对供购买或激活的一个服务计划的用户的用户的选择经过由一个服务处理器配置的一个提供设置 UI 显示而传递到用户,并且该服务处理器经过一个到通知和提供设置网关 2686 的通信接口而与一个服务控制器进行通信,从而来实时或近实时地购买或激活服务计划。在一些实施例中,该通知和提供设置网关 2686 将服务计划的用户选择传递到提供用户选择接收器 2710,从而随后引起对应于用户的服务计划选择的服务计划策略强制执行设置通过将用户的服务计划选择传递到网络配置系统 160(或订户管理 182、订单管理 180、移动无线中心 132、计费 123 等)而实施,进而与运营商网络 2712 进行通信以引起适当服务计划策略强制执行设置被编程在负责服务计划策略强制执行的不同网元中。以这种方式,在一些实施例中,可以在负责基于网络的策略强制执行的不同网元(例如,聚合 / 传输网关 420[例如, PDN 或 GGSN]、移动无线中心 132[例如, HLR]、AAA 服务器 121、RAN/ 接入网关 410[例如, SGSN、PDSN]、BSC125)中配置为装置实施新的服务计划所需的网络服务策略强制执行。在一些实施例中,可以在负责基于网络的策略强制执行的不同网元的服务处理器装置代理中配置为装置实施新的服务计划的网络服务策略强制执行。在一些实施例中,当完成服务计划策略配置时,服务控制器与装置服务处理器进行如下通信:已购买或激活该新服务计划。在一些实施例中,服务处理器将已购买或激活新服务计划的消息从服务控制器传递到装置 UI。

[0238] 在一些实施例中,服务处理器提供设置信息处理和 UI 显示被配置成允许用户在提供设置内实时或近实时地购买或激活一个服务计划。在一些实施例中,对供购买或激活的一个服务计划的用户的用户的选择通过由一个服务处理器配置的一个提供设置 UI 显示来接收,并且该服务处理器与一个服务控制器进行通信以允许用户来实时或近实时地购买或激活服务计划,并且这些服务计划策略设置由该服务控制器传递到服务处理器,这样使得可以配置为装置实施新服务计划的服务处理器策略强制执行代理。

[0239] 在一些实施例中,提供负责基于网络的策略强制执行的不同网元的配置(这样使得装置可以接收适当服务计划允许和策略)可能花费大量时间例如数分钟或甚至更长,这可能产生不实时或不近实时的一个不良的用户体验。在这类情况下,服务控制器可以通过配置负责基于网络的策略强制执行的不同网元的一个子集来创建一个临时服务租赁,以允许在所有负责基于网络的策略强制执行的所需网元之前安放在位的一个临时服务计划,并且可能地可以配置提供服务使用记账或计费。例如,临时租赁可以配置所需的业务量路径或数据路径处理元件中的一些或所有,以允许对应于用户已选择的服务计划中的可允许的服务使用分类的装置服务使用分类,但不将该使用记入正确的服务使用记账或计费系统配

置中,直到完成了记账或计费元件的配置。作为另一个示例,在完成记账或计费元件的配置之前的临时服务租赁期过程中,服务控制器可以跟踪在临时服务租赁期过程中引发的服务使用,并且在完成记账或计费元件的配置之后,将在临时租赁期过程中引发的服务使用传送到适合的服务使用记录数据库,这样使得在临时服务租赁期引发的使用被正确地记账或计费。在另一个示例实施例中,在临时服务租赁过程中,服务控制器引起一个临时服务配置在负责网络接入控制的不同网元中生效,其中该临时服务配置提供允许服务计划允许所需的必要数据路径配置的所有或一个子集,这些服务计划允许对应于用于用户已选择的服务计划的接入控制策略,并且在临时服务租赁期过程中引发的服务使用被记入一个临时记账中而不是最终记账,一旦新的用户选择的服务计划的配置完全生效,该最终记账将生效。在一些实施例中,临时记账为被配置成在临时租赁期过程中跟踪装置使用的一个捕捉存储区账户。在一些实施例中,临时记账具有不同于在完全配置了新的用户选择的服务计划之后将生效的服务使用费率(例如,一个零费率的记账)的一个服务使用费率。在一些实施例中,跟踪在临时租赁期过程中的服务使用并且在完全配置了新的用户选择的服务计划之后,接着将其传送到适合的服务记账。

[0240] 在一些实施例中,直接在一个装置 UI 上激活一个新的服务计划的一些延迟可以与为用户的信用凭证或服务账户凭证执行一个信用检查或用户服务身份检查有关。在这类情况下,类似于以上所披露的这些实施例的实施例可以用来提供可能具有最后传送到最终使用记账的临时服务记账的一个临时服务租赁。如果在临时服务租赁期过程中,用户的信用或用户服务身份不足以提供用户已选择的服务计划的一个指示被返回到服务控制器,则可以通知该用户这个问题(可能带有如何解决这个问题的指令),并且可以取消该临时服务租赁,因而如果已批准了信用检查并且发生最终服务计划提供,则禁用可能已经提供给装置的该网络接入许可。在这类实施例中,在取消该临时租赁之前可以在临时租赁期过程中跟踪使用,并且可以将这个服务使用记入一个账户中,该账户用于由于未通过的信用检查或未通过的用户服务身份检查的跟踪使用丢失目的。在一些实施例中,在由于一个未通过的信用检查或未通过的用户服务身份检查而最后被取消的一个临时租赁过程中引发的使用可以被记账回另一个用户记账或计费,并且在一些实施例中,这是根据一个用户服务协议定的。

[0241] 如本领域普通技术人员现将认识的是,在网络可以完全配置由一个装置 UI 上的装置用户选择的一个新的服务计划的时间之前,此处不胜枚举许多另外相关实施例来协助快速地启用相同于或类似于网络接入许可的装置网络接入许可,在完全配置新的用户选择的服务计划之后,该装置将最后被允许,这样使得装置用户可以享有从用户为一个装置上购买或激活选择一个服务计划的时间至完全配置网络来实施该新的服务计划的时间的一个相对短的时间延迟。

[0242] 在一些实施例中,服务处理器被配置成向装置终端用户显示一个或多个服务计划提供,并且通过用户正用装置在做什么或装置处于何处(例如,终端用户装置尝试接入网络;装置上的一个应用尝试接入网络;使用或尝试使用一个给定的应用或应用集;装置进入一个漫游状态等)来确定这个显示发生的时间。在一些实施例中,服务处理器通过检测用户正用装置做什么或由用户引起的装置条件(例如,装置正在漫游等)而确定向装置用户显示一个或多个服务提供的时间。

[0243] 在一些实施例中,一个服务设计中心用来创建装置用户通知消息(例如,一个服务提供消息、一个服务使用通知消息、指示使用的大块服务量的一个消息、指示使用的微型 CDR 服务分类量的一个通知、指示已达到的大块使用限制的一个通知、指示已达到的微型 CDR 使用分类使用限制的一个通知等)。在一些实施例中,这些通知消息向一个装置服务处理器(或属于一个装置组或一个用户组的一组装置服务处理器)发布,并且该服务处理器确定何时存在用于显示一个特定通知消息的触发条件。在一些实施例中,一个服务使用通知触发条件(例如,装置使用的一个状态,如大块服务使用或企图使用、应用使用或企图使用、网站使用或企图使用、家庭/漫游使用或企图使用、微蜂窝式/WiFi 使用或企图使用等的一个状态)与每一个消息相关联。在一些实施例中,一个装置上的服务处理器确定何时满足该触发条件并且显示与该触发条件相关联的一个预先存储的通知消息。在一些实施例中,一个网元确定何时满足该触发条件并且经过装置消息队列 2688 而使用通知和提供设置网关 2686 来将通知消息传输到装置以用于由装置服务处理器显示。在一些实施例中,一个装置服务通知消息包括来自 CDR/RTR 数据库 2660 的一个服务使用更新,该服务使用更新经过装置消息队列 2688 而发送通过通知和提供设置网关 2686。在一些实施例中,一个装置服务通知消息包括来自微型 CDR 生成器 2680 的一个服务使用更新,该服务使用更新经过装置消息队列 2688 而发送通过通知和提供设置网关 2686。在一些实施例中,来自 CDR/RTR 数据库 2660 或微型 CDR 生成器 2680 中的一个或多个的服务使用更新在循环基础上经过装置消息队列 2688 而发送通过通知和提供设置网关 2686。在一些实施例中,该循环基础是基于达到的一个预先确定的使用量的(例如,一个预先确定的字节计数、预先定义的时间计数或一个预先定义的限制的预先定义的百分比等)。在一些实施例中,该循环基础是基于一个使用通知更新频率或时间间隔的。

[0244] 图 24 展示了一个服务控制器调和处理过程的一个示例实施例,该服务控制器调和处理过程可以用于使用来自终端用户装置的信息和来自一个第二源的信息来检测欺诈(如以下所解释)。服务处理器 115(未示出)或终端用户装置 100(未示出)上的应用生成使用度量 2300。基于使用度量 2300,终端用户装置 100 将第一使用记录发送到服务控制器 122,或者服务控制器 122 从终端用户装置 100 请求第一使用记录。服务控制器 122 在装置使用记录预处理 2310 中处理这些第一使用记录。在一些实施例中,装置使用记录预处理 2310 修改第一使用记录的格式来协助服务使用处理、报告、分析、比较、调解以及在服务控制器系统内执行的调和运行中的一项或多项。在一些实施例中,装置使用记录预处理 2310 观察第一使用记录和时间戳并且时间同步、时间对齐或时间聚合多个第一使用记录,这样使得具有一个共用时间基准的更一致的使用度量可以在服务控制器系统内达到,以用于服务使用处理、报告、分析、比较、调解以及调和目的中的一个或多个。服务控制器 122 将这些第一使用记录存储在装置使用记录 2320 中。

[0245] 第二源(未示出)生成或提供第二服务使用度量 2370。在一些实施例中,第二源为一个网元,如一个调解元件、一个网关、一个实时报告元件、一个收费元件、一个计费元件或类似元件。在一些实施例中,该第二源是一个数据库。在一些实施例中,该第二源为一个漫游伙伴网元。在一些实施例中,第二源为生成安全装置数据记录的终端用户装置 100 上的一个元件。在一些实施例中,第二源为一个伙伴网络目的地,该伙伴网络目的地提供关于该目的地的客户使用或与该目的地的交易的信息。在一些实施例中,第二源为终端用户装置

100 上的一个应用。

[0246] 基于第二服务使用度量,第二源将第二使用记录(以下描述)发送到服务控制器 122,或者服务控制器 122 获得来自该第二源的第二使用记录。服务控制器 122 在记录规范化、时间调和以及预先预处理 2360 中处理这些第二使用记录。在一些实施例中,记录规范化、时间调和以及预先预处理 2360 修改第二使用记录的格式来协助服务使用处理、报告、分析、比较、调解以及在服务控制器系统内执行的调和运行中的一项或多项。在一些实施例中,记录规范化、时间调和以及预先预处理 2360 观察第二使用记录和时间戳并且时间同步、时间对齐或时间聚合多个第二使用记录,这样使得具有一个共用时间基准的更一致的使用度量可以在服务控制器系统内达到,以用于服务使用处理、报告、分析、比较、调解以及调和目的中的一个或多个。服务控制器 122 将这些第二使用记录存储在第二源使用记录 2350 中。

[0247] 服务控制器 122 应用调和与验证处理算法 2340 以将装置使用记录 2320 中的记录与第二源使用记录 2350 中的记录调和,并且来证实装置使用记录 2320 中的记录。服务控制器 122 基于调和与验证处理算法 2340 的结果来将信息存储到数据仓库 2330 中。

[0248] 在一些实施例中,调和与验证处理算法 2340 从一个大块服务使用记账中调和出详细的服务使用分类(例如,微型 CDR)并且将其调和到服务使用记账的一个微型 CDR 分类上。在一些实施例中,调和与验证处理算法 2340 通过在传递到运营商网络调解或计费系统的微型 CDR 使用记录中提供一个详细的微型 CDR 收费码标识符而实现对一个详细的服务使用分类的收费。在一些实施例中,调和与验证处理算法 2340 通过从被记账到大块服务使用的服务使用量中调解出(或减去)被报告在微型 CDR 中的服务使用量而实现对一个详细的服务使用分类的收费。在一些实施例中,调和与验证处理算法 2340 将收费数据记录(例如,CDR、微型 CDR 等)发送到运营商数据调解 2380。

[0249] 在一些实施例中,调和与验证处理算法 2340 使用来自第二源使用记录 2350 和装置使用记录 2320 中的一者或两者的信息来执行一个欺诈分析。在一些实施例中,调和与验证处理算法 2340 比较与来自第二源使用记录 2350 和装置使用记录 2320 中的一者或两者的一个特定装置或用户凭证相关联的使用记录,从而确定服务使用是否在预先定义的服务使用策略行为限制之外。在一些实施例中,调和与验证处理算法 2340 比较与来自第二源使用记录 2350 和装置使用记录 2320 中的一者或两者的一个特定装置或用户凭证相关联的服务使用信息,从而确定是否达到或超过一个预先定义的服务使用限制。在一些实施例中,调和与验证处理算法 2340 比较与来自第二源使用记录 2350 和装置使用记录 2320 中的一者或两者的一个特定装置或用户凭证相关联的服务使用信息,从而确定该特定装置或用户是否展示了与一个装置或用户总体的服务使用行为相比较在预先定义的统计限制之外的一个服务使用行为。在一些实施例中,调和与验证处理算法 2340 将其对欺诈分析的结果存储在数据仓库 2330 之中。在一些实施例中,调和与验证处理算法 2340 将欺诈报警发送到运营商 CRM 系统 2390(例如,一个运营商欺诈处理系统、运营商人员、一个装置用户、一个系统管理员等)。

[0250] 在一些实施例中,这些第二使用记录包括来自多个其他度量或报告的信息。在一些实施例中,第二使用记录是基于来自终端用户装置 100 的信息、度量或报告的。在一些实施例中,第二使用记录是基于来自其他终端用户装置的信息、度量或报告的。在一些实施例

中,第二使用记录基于来自一个或多个网元(例如,一个基站、RAN、核心或使用装置辅助手段等)的信息、度量或报告来确定。

[0251] 在一些实施例中,第二使用记录包括由终端用户装置 100 对大块(例如,聚合或未分类的)数据使用的一个度量。例如,在一些实施例中,第二使用记录包括由网络、由一个应用服务提供者或由一个服务器生成的特定于终端用户装置 100 的一个大块使用报告。在一些实施例中,第二使用记录是基于由终端用户装置 100 发送的一个或多个以前报告中的信息的。

[0252] 在一些实施例中,第二使用记录包括与接入网络状态相关联的信息。在一些实施例中,第二使用记录从网络状态标记信息中确定。在一些实施例中,第二使用记录包括可以指示网络占线状态和网络类型的来自一个装置数据记录(DDR)的信息。在一些实施例中,第二使用记录从标记 DDR 网络状态的信息中确定。

[0253] 在一些实施例中,第二使用记录包括来自流数据记录的信息。在一些实施例中,流数据记录(FDR)报告指示由网络源或目的地(例如,域名、URL、IP 地址等)和可能地一个或多个端口和协议分解的服务使用的一个详细的服务使用分类等级。在一些实施例中,该FDR 报告指示由装置用户应用或 OS 应用分解的使用的一个详细的服务使用分类等级。在一些实施例中,FDR 报告指示由当日时间、网络拥塞状态或服务 QoS 等级分解的服务使用的一个详细的服务使用分类等级。在一些实施例中,FDR 报告由网络类型(例如,2G、3G、4G、WiFi 等)分解的一个详细的服务使用等级。在一些实施例中,FDR 报告由家庭或漫游网络分解的一个详细的服务使用等级。

[0254] 在一些实施例中,FDR 来源于能够分类业务量的一个网元(例如,一个深度数据包检测 [DPI] 网关、一个代理服务器、专用于一个给定服务分类的一个网关或服务器、在此在其他地方所描述的一个良好客户反馈源)。在一些实施例中,第二使用记录从一个装置服务监控器获得。在一些实施例中,第二使用记录从一个可信装置服务监控器获得。在一些实施例中,该可信装置服务监控器处于不能由一位用户或用户安装的应用软件接入的装置上的一个安全执行环境中。

[0255] 在一些实施例中,第二使用记录允许服务控制器 122 来确定终端用户装置 100 的接入行为(假定网络状态)是否指示终端用户装置 100 正实施正确的策略控制。在一些实施例中,服务控制器 122 确认服务处理器 115 在其数据使用报告中正报告正确的网络状态。在一些实施例中,一个网元基于一组装置来确定正确的网络状态。该信息被报告给服务控制器 122 或另一个适合的网络功能。服务控制器 122 (或另一个适合的网络功能)基于连接至该子网络部分的终端用户装置总体而表征子网络的多个部分(例如,基站、基站扇区、地理区域、无线接入网络(RAN)等)。网元也可以从网络设备中收集网络占线状态度量,如从基站或通过 RAN 取样,从而来确定第二度量。

[0256] 在一些实施例中,第二使用记录提供关于由终端用户装置 100 的聚合数据使用量上的一个上限的信息。服务控制器 122 验证如在第一使用记录中所报告的终端用户装置 100 的总数据使用不超过该上限。如果第一使用记录为由终端用户装置 100 使用的单独服务提供数据使用量,则服务控制器 122 验证针对该单独服务的使用量的总和不超过该上限。

[0257] 在一些实施例中,网络将 FDR 分类为已知服务组件,确定针对每一个服务组件的

被分类使用信用,确保服务组件使用不超过特定限制(或匹配对该组件的终端用户装置报告),并且检查组件的总和是否匹配大块度量。

[0258] 存在可以由服务控制器 122 使用在此所披露的实施例中的一个或多个,如图 24 中所示的该示例实施例检测的若干潜在地欺诈性环境。在一些实施例中,如果服务控制器 122 从一个网元接收基于运营商的使用报告并且从服务处理器 115 接收 UDR,则服务控制器生成一个欺诈报警,但含有于报告中的使用计数在一个特定容差内不相一致。为了在这些环境下生成一个欺诈报警,在一些实施例中,服务控制器 122 对仍可能在终端用户装置 100 上的未发送的使用报告记账。

[0259] 图 25 展示了在以下情况下可能都为有利的一个示例实施例:令人希望的是,在网络中识别服务使用分类,而用于为一位装置用户或服务赞助方提供机会来为由应用或网站分类的接入网络服务使用付费的目的。图 25 也展示了多个示例性元件,在一些实施例中,这些元件基于微型 CDR 服务使用类别的一个网络分类而提供微型 CDR 的生成。图 25 也展示了为了计费的目的而将网络生成的微型 CDR 传输到运营商网络 2666 的一个示例性手段。在一些实施例中,在网络中生成的微型 CDR 用来实施用户付费应用计划、网络计划或内容类型计划。在一些实施例中,在网络中生成的微型 CDR 用来实施被赞助的应用计划、网站计划或内容类型计划。

[0260] 图 25 所示的示例性系统在与图 23 所示的示例性系统相同的原则上运行。为微型 CDR 生成的详细使用报告从运营商网络 2698 中的一个 FDR 源获得(例如,该源可以为一个 DPI 网关、代理服务器、专用服务服务器、良好的客户反馈等)。来自 FDR 源的 FDR 由负载均衡器 2700 递送到详细使用报告网关 2702。在一些实施例中,详细使用报告网关 2702 观察 FDR 时间戳并且时间同步、时间对齐或时间聚合多个 FDR 报告,这样使得具有一个共用时间基准的更一致的使用度量可以在服务控制器系统内达到,以用于服务使用处理、报告、分析、比较、调解以及调和目的中的一个或多个。已处理的 FDR 由详细使用报告网关 2702 递送到 JMS 队列 2704,进而将其递送到详细的报告处理器 2706。图 25 中的另外功能类似于在图 23 的上下文中所描述的这些功能。如将由本领域普通技术人员所了解,图 25 的示例性实施例为用户付费的应用和网站服务或被赞助的应用或网站服务提供微型 CDR 服务使用记账的优点。

[0261] 在一些实施例中,FDR(流数据记录)报告指示由网络源或目的地(例如,域名、URL、IP 地址等)和可能地一个或多个端口和协议分解的服务使用的一个详细的服务使用分类等级。在一些实施例中,这些 FDR 报告指示由装置用户应用或 OS 应用分解的使用的一个详细的服务使用分类等级。在一些实施例中,FDR 报告指示由当日时间、网络拥塞状态或服务 QoS 等级分解的服务使用的一个详细的服务使用分类等级。在一些实施例中,FDR 报告由网络类型(例如,2G、3G、4G、WiFi 等)分解的一个详细的服务使用等级。在一些实施例中,FDR 报告由家庭或漫游网络分解的一个详细的服务使用等级。

[0262] 在一些实施例中,FDR 来源于能够分类业务量的一个网元(例如,该源为一个深度数据包检测 [DPI] 网关、一个代理服务器、专用于一个给定服务分类的一个网关或服务器等)。在一些实施例中,FDR 从一个装置服务监控器获得。在一些实施例中,FDR 从一个可信装置服务监控器获得。在一些实施例中,该可信装置服务监控器处于不能由一位用户或用户安装的应用软件接入的装置上的一个安全执行环境中。

[0263] 在一些实施例中,FDR 不仅报告由一个装置尝试并且允许的服务使用,而且报告由一个装置尝试并且不允许的服务使用。在一些实施例中,报告加以尝试但未被允许的服务使用的一个 FDR 可以包括在此所描述的不同分类能力。以这种方式,一个 FDR 不仅可以为一个应用、网站、网络类型等检测大块服务使用或被分类的服务使用,而且也可以为针对一个应用、网站、网络类型等的大块服务或被分类的服务检测何时一位用户尝试得到接入服务。

[0264] 在一些实施例中,从网络使用监控源派生的微型 CDR 使用记账被反馈到一个装置服务处理器中的一个用户服务使用通知功能,以便为用户付费的应用和网站服务或被赞助的应用或网站服务提供一个服务使用分类分解。这个路径在图 25 中由从微型 CDR 生成器 2680 至装置消息队列 2688 的虚线连接和一个微型 CDR 服务使用分类更新经过通知和提供设置网关 2686 到装置服务处理器的随后处理和传输指示。

[0265] 在一些实施例中,服务处理器被配置成向装置终端用户显示一个或多个服务计划提供,并且通过用户用装置正在做什么(例如,用户尝试接入网络;装置上的一个应用尝试接入网络;使用或尝试使用一个给定的应用或应用集;装置进入一个漫游状态等)来确定这个显示发生的时间。在一些实施例中,服务控制器通过检测用户正用装置做什么而确定向装置用户显示一个或多个服务提供的时间。在一些实施例中,服务控制器通过观察 FDR 或微型 CDR 中的接入模式或尝试的接入模式来检测用户正用装置做什么。在一些实施例中,服务控制器从被拒绝的装置中观察报告一个接入服务尝试的 FDR,并且这触发了服务处理器来发起提供一个服务提供的一个装置通知消息,并且该服务提供通知经过通知和提供设置网关 2686 传输。在一些实施例中,服务控制器从针对一个服务使用分类的装置如一个应用或网站中观察报告一个接入服务尝试的 FDR,并且这触发了服务处理器来发起提供针对一个应用服务或一个网络服务的一个服务提供的一个装置通知消息,并且该服务提供通知经过通知和提供设置网关 2686 传输。

[0266] 在一些实施例中,可以一种 API 形式来将用于通知和提供设置网关 2686 的接口协议暴露给装置 OEM 或应用开发者。在一些实施例中,用于通知和提供设置网关 2686 的 API 为装置应用程序软件或 OS 软件开发者提供一个统一手段来写入可以利用一个统一接口的不同应用软件,以用于从一个服务控制器请求对装置可用的一个服务提供清单,并且向装置用户接口显示该清单。在一些实施例中,使用一个服务设计中心用户接口创建对一个装置组或用户组可用的一个服务提供清单;将该服务提供清单存储在一个 SDC 数据库中;并且将其发布给用于通知和提供设置网关 2686 的 API。在一些实施例中,用于网络接入许可或业务量控制、服务使用限制、服务使用收费或记账或服务使用通知中的一个或多个的服务计划强制执行策略也被配置在服务设计中心 2690 中。在一些实施例中,用于通知和提供设置网关 2686 的 API 为装置应用程序软件或 OS 软件开发者提供一个统一手段来写入可以利用一个统一接口的不同应用软件以用于为一个装置 UI 上的服务购买或激活提供用户服务计划选择项;收集用户选择项;并且将该用户选择项传输到随后为该装置激活新服务的一个服务控制器。在一些实施例中,与一个 XML 接口一起创建用于通知和提供设置网关 2686 的 API 的可用服务计划清单或服务计划购买或激活用户选择组件。在一些实施例中,经过一个安全网络连接来提供用于通知和提供设置网关 2686 的 API 的可用服务计划清单或服务计划购买或激活用户选择组件。

[0267] 在一些实施例中,可以一种 API 形式来将用于通知和提供设置网关 2686 的接口协

议暴露给被赞助的装置提供商或被赞助的应用提供商。在一些实施例中,用于通知和提供设置网关 2686 的 API 为被赞助的服务提供商提供一个统一手段来开发可以利用一个统一接口的装置应用程序软件或 OS 软件,以用于从一个服务控制器为该装置请求一个被赞助的服务计划的一个服务控制器激活。在一些实施例中,通过 API 提供并且激活的被赞助的服务计划是用于赞助所有装置接入的。在一些实施例中,通过 API 提供并且激活的被赞助的服务计划是用于赞助一个应用或一组应用的。在一些实施例中,通过 API 提供并且激活的被赞助的服务计划是用于赞助一个网站或一组网站的。在一些实施例中,用于通知和提供设置网关 2686 的 API 为被赞助的装置应用程序软件或 OS 软件开发者提供一个统一手段来写入可以利用一个统一接口的不同应用软件,以用于为装置、一个应用或一个网站激活一个被赞助的服务计划。

[0268] 在一些实施例中,可以一种 API 形式来将用于通知和提供设置网关 2686 的接口协议暴露给装置 OEM 或应用开发者,该 API 为装置应用程序软件或 OS 软件提供一个统一的接口来从一个服务控制器请求服务使用信息更新。在一些实施例中,服务使用信息更新由服务控制器以大块服务使用的形式提供。在一些实施例中,服务使用信息更新由服务控制器以服务使用分类或微型 CDR 服务使用更新的形式提供。在一些实施例中,一个装置用户软件应用或 OS 功能被配置成利用一个统一接口,以用于从一个服务控制器中获得服务使用更新,并且向一个装置用户接口显示这些服务使用更新。在一些实施例中,向装置 UI 显示的服务使用更新呈以下形式:一个量规、仪表、条形码、使用量、剩余量、使用百分数或剩余百分数。在一些实施例中,一个装置用户软件应用或 OS 功能被配置成利用一个统一接口,以用于从一个服务控制器中获得针对一个服务使用分类(例如,一个应用分类或网站分类,或另一个分类)的服务使用更新,并且向一个装置用户接口显示这些服务使用更新。在一些实施例中,使用一个服务设计中心用户接口创建待由用于通知和提供设置网关 2686 的 API 提供给属于一个装置组或用户组的装置的一组一个或多个服务使用通知;将该组服务使用通知存储在一个 SDC 数据库 2692 中;并且将其发布给用于通知和提供设置网关 2686 的 API。在一些实施例中,服务计划通知策略(例如,触发一个给定的服务使用通知和该通知的信息内容的条件)也被配置在服务设计中心 2692 中。在一些实施例中,与一个 XML 接口一起创建用于通知和提供设置网关 2686 的 API 的服务使用通知接口组件。在一些实施例中,经过一个安全网络连接来提供用于通知和提供设置网关 2686 的 API 的服务使用通知接口组件。

[0269] 在一些实施例中,用于通知和提供设置网关 2686 的 API 包括一个安全接口,该接口可以仅通过提供对应于网络上的一个已知装置或用户账户的装置凭证(例如,一个 SIM 卡凭证、一个 IMSI、一个电话号码、一个 MDID、一个签名的 API 通信、一个加密的 API 通信或与 API 的另一种形式的安全装置代理通信)而接入。在一些实施例中,用于通知和提供设置网关 2686 的 API 包括一个安全接口,该接口可以仅通过提供对应于网络上的一个已知装置或用户账户的用户凭证(例如,一个用户 PIN、密码、安全问题答案、生物测定凭证或通常对装置用户或受该装置用户信任的一个实体可用的其他安全用户凭证)而接入。在一些实施例中,用于通知和提供设置网关 2686 的 API 包括一个安全接口,该接口可以仅通过提供对应于被允许接入用于通知和提供设置网关 2686 的 API 的一个已知应用的一个应用凭证(例如,应用凭证、签名、散列信息、已签名的通信、已加密的通信、已加密的消息或安全地

识别一个应用或 OS 功能的其他应用凭证) 而接入。在一些实施例中, 一个装置软件应用或 OS 功能必须根据一个正确的预先定义的 API 格式而提供一个安全装置凭证、安全应用凭证或安全用户凭证, 以从用于通知和提供设置网关 2686 的 API 获得服务使用通知信息。在一些实施例中, 一个装置软件应用或 OS 功能必须根据一个正确的预先定义的 API 格式而提供一个安全装置凭证、安全应用凭证或安全用户凭证, 以从用于通知和提供设置网关 2686 的 API 获得服务提供设置信息。在一些实施例中, 一个装置软件应用或 OS 功能必须根据一个正确的预先定义的 API 格式而提供一个安全装置凭证、安全应用凭证或安全用户凭证, 以将用户服务计划选择信息传递到用于通知和提供设置网关 2686 的 API。在一些实施例中, 一个装置软件应用或 OS 功能必须将一个安全装置凭证、安全应用凭证或安全用户凭证提供给用于通知和提供设置网关 2686 的 API, 以便接收一个被赞助的服务。在一些实施例中, 用于通知和提供设置网关 2686 的 API 包括一个安全 XML 接口。在一些实施例中, 用于通知和提供设置网关 2686 的 API 包括一个安全网络连接。

[0270] 尽管为了理解清晰的目的, 已相当详细地描述了前述的实施例, 本发明没有限制在所提供的细节中。存在实施本发明的许多可替代的方式。公开的实施例是示意性的而不是限制性的。

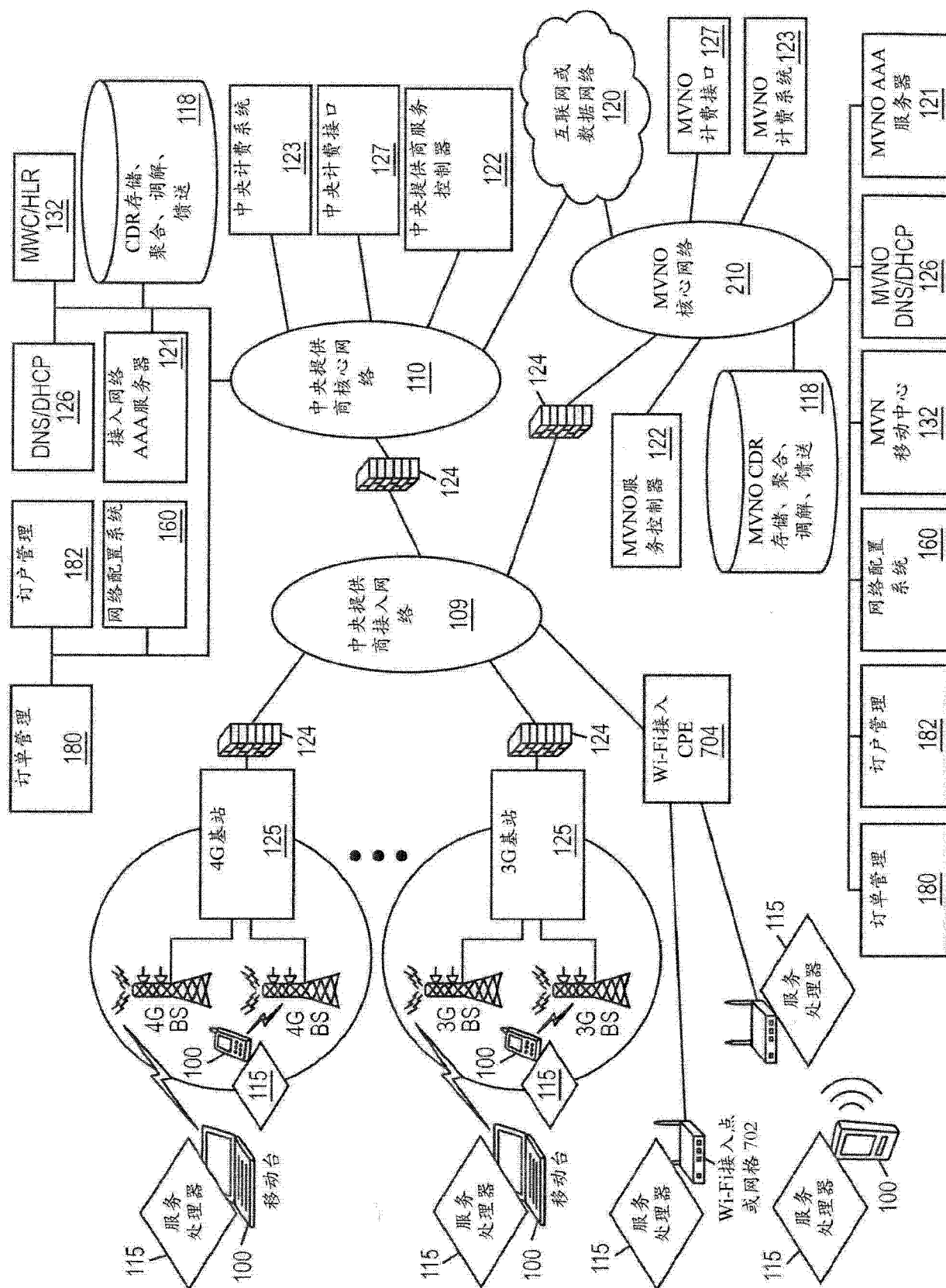


图 1

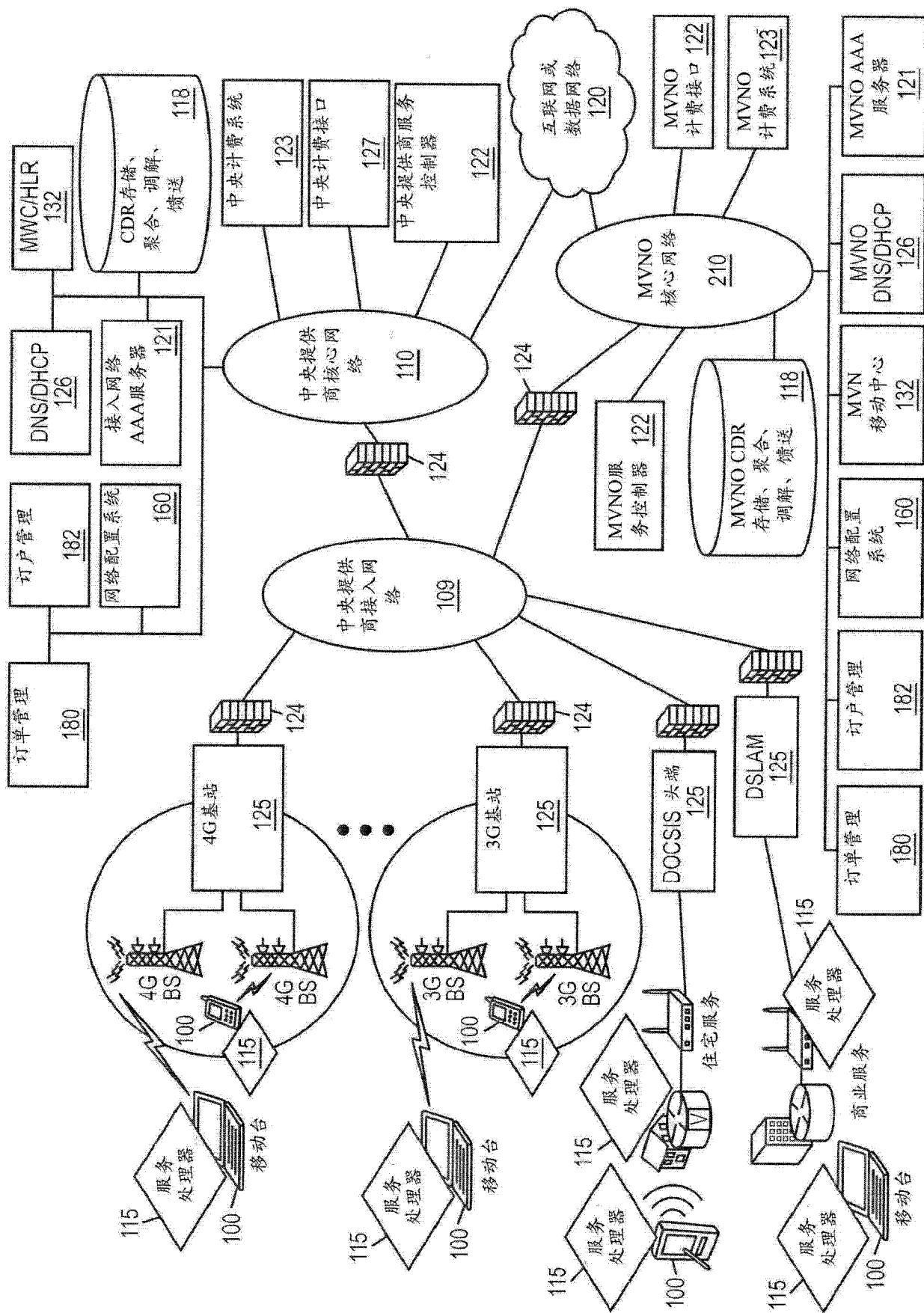


图 2

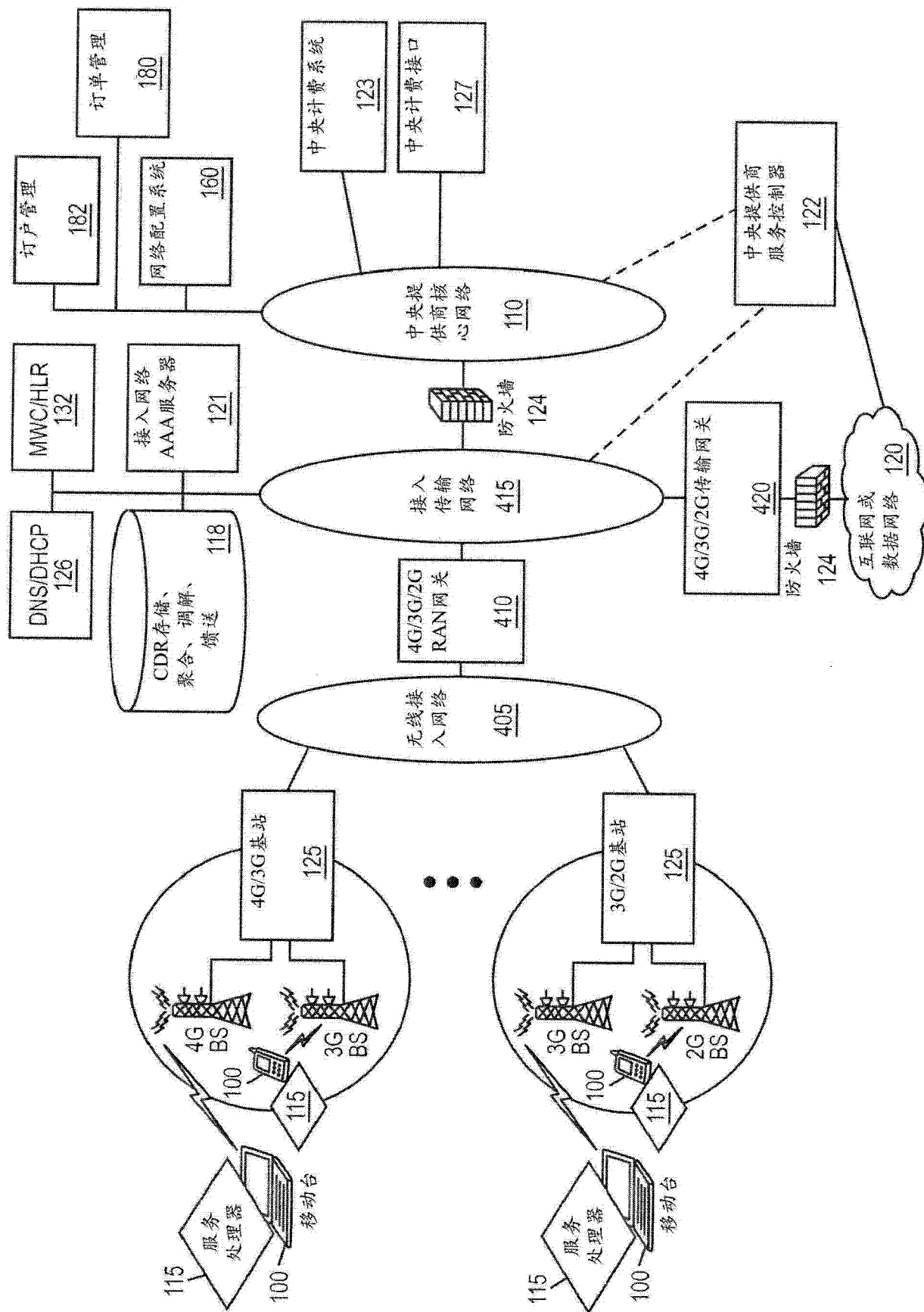


图 3

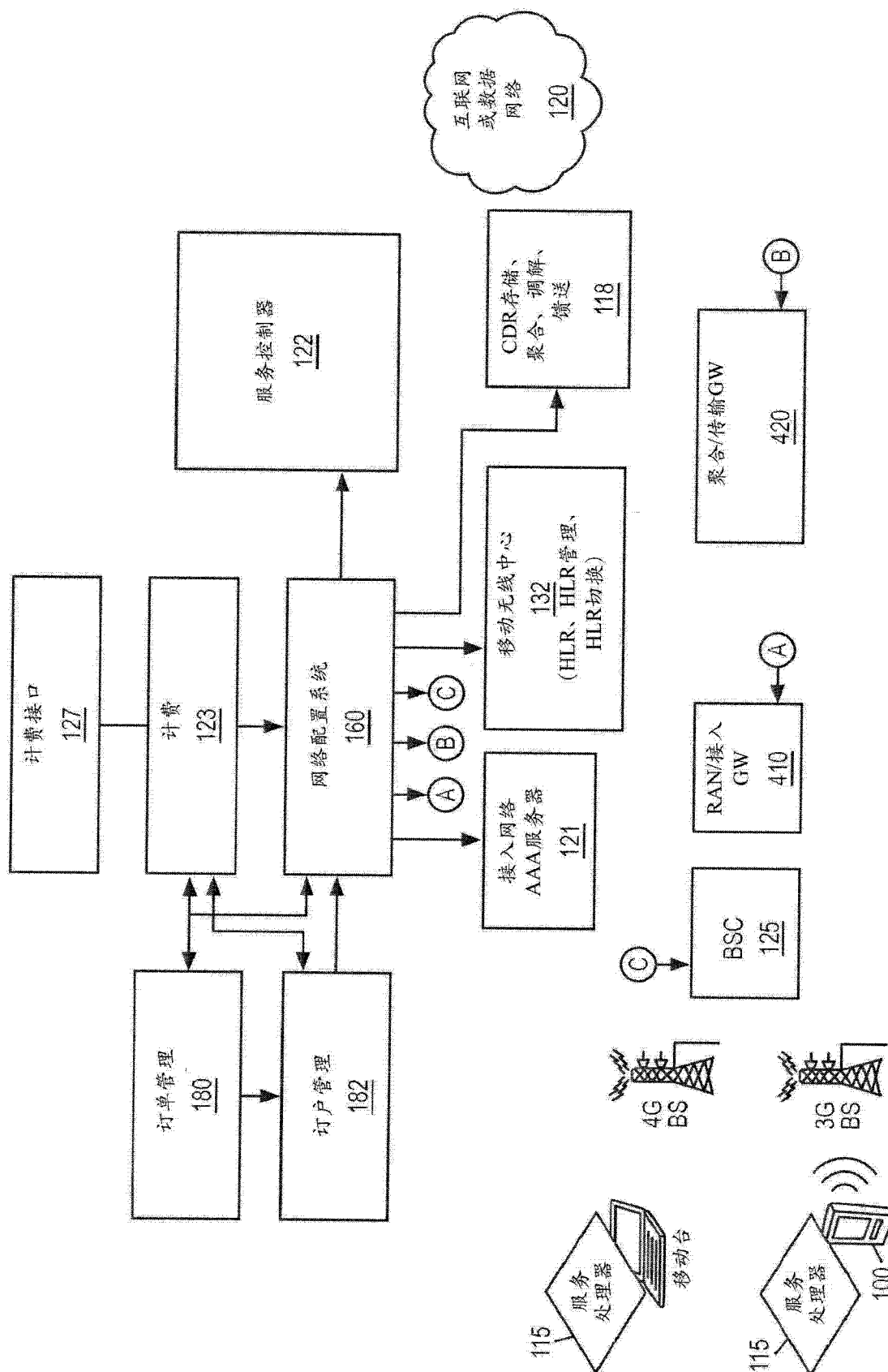


图 4

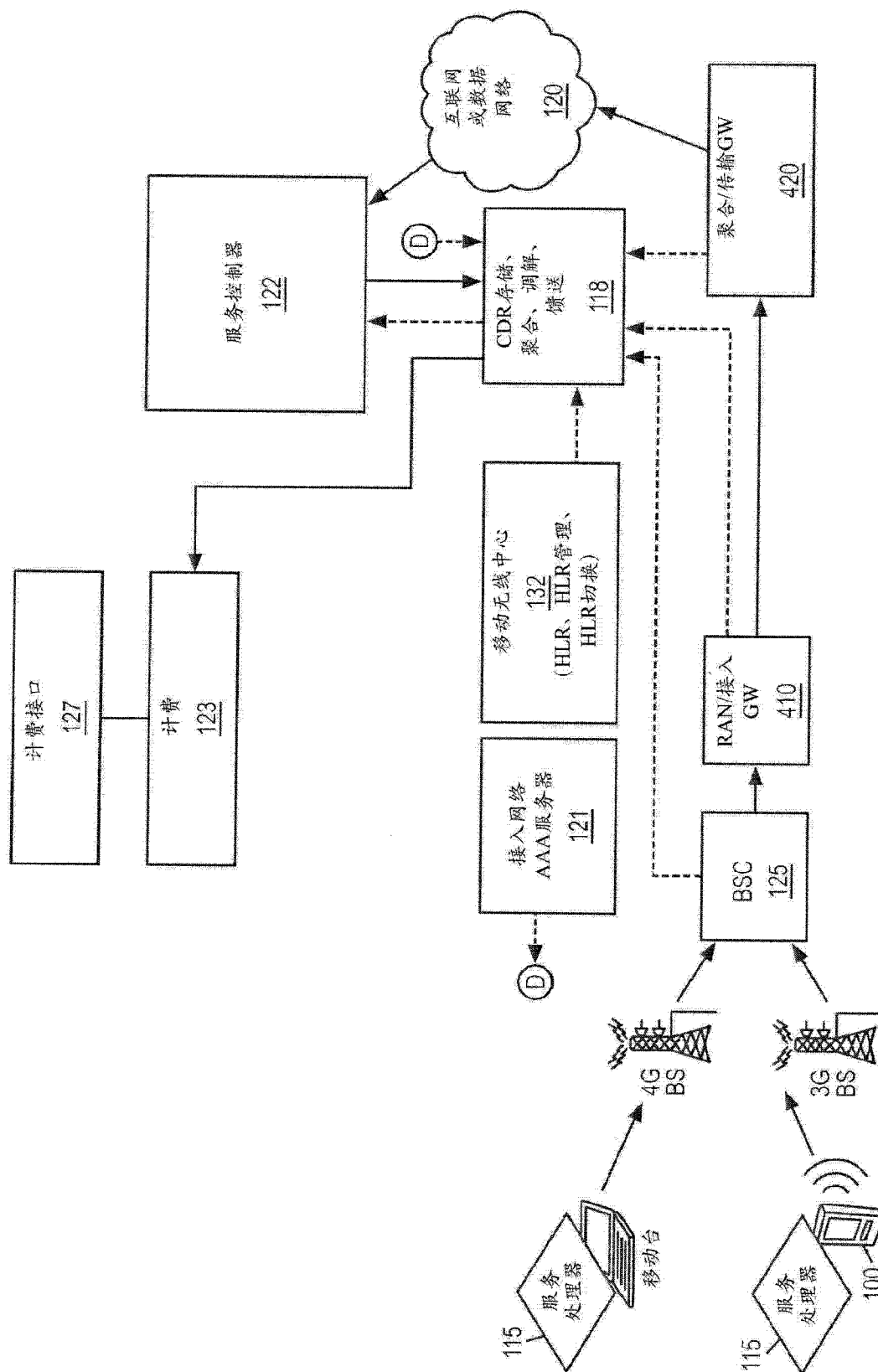


图 5

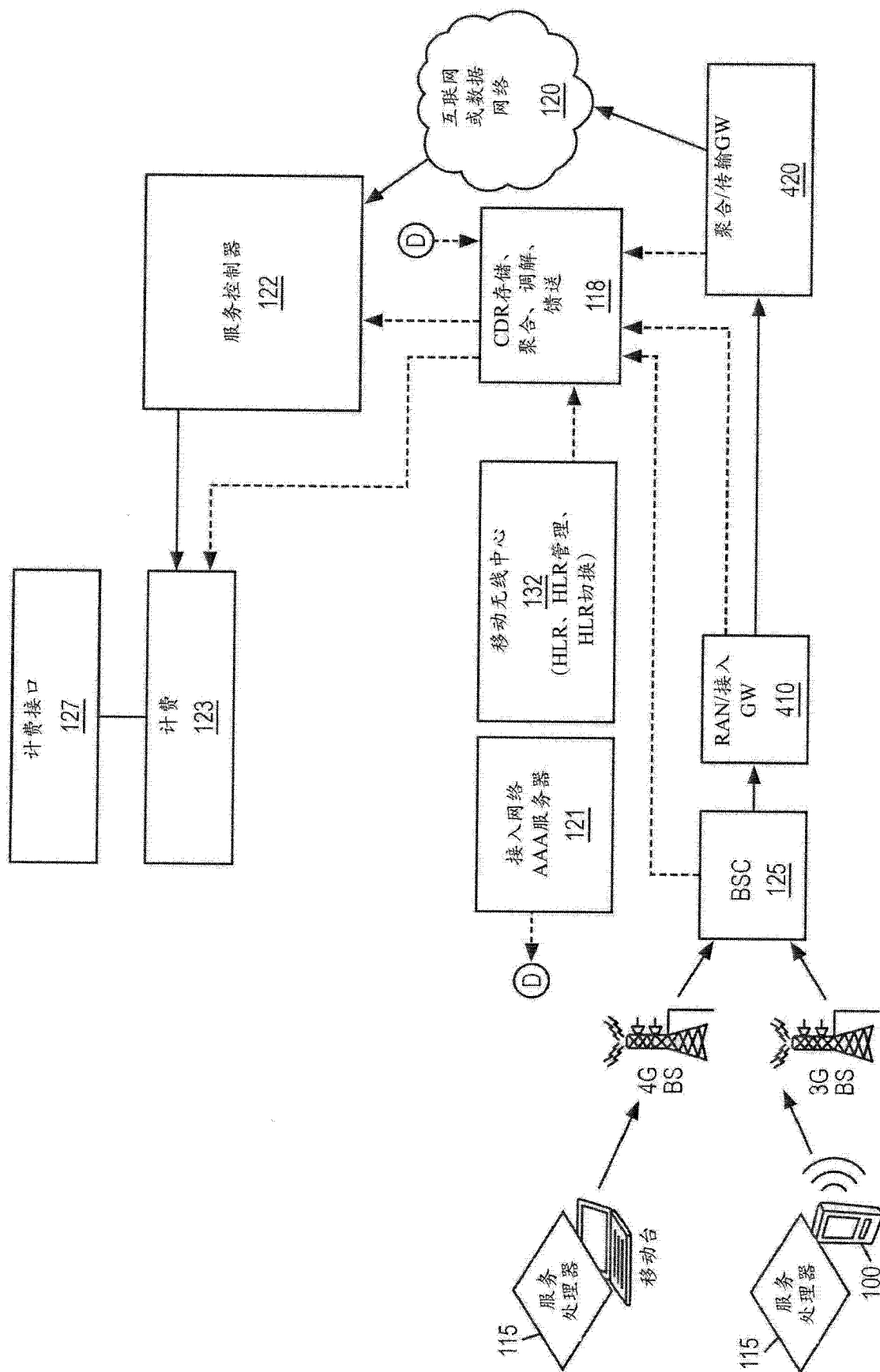


图 6

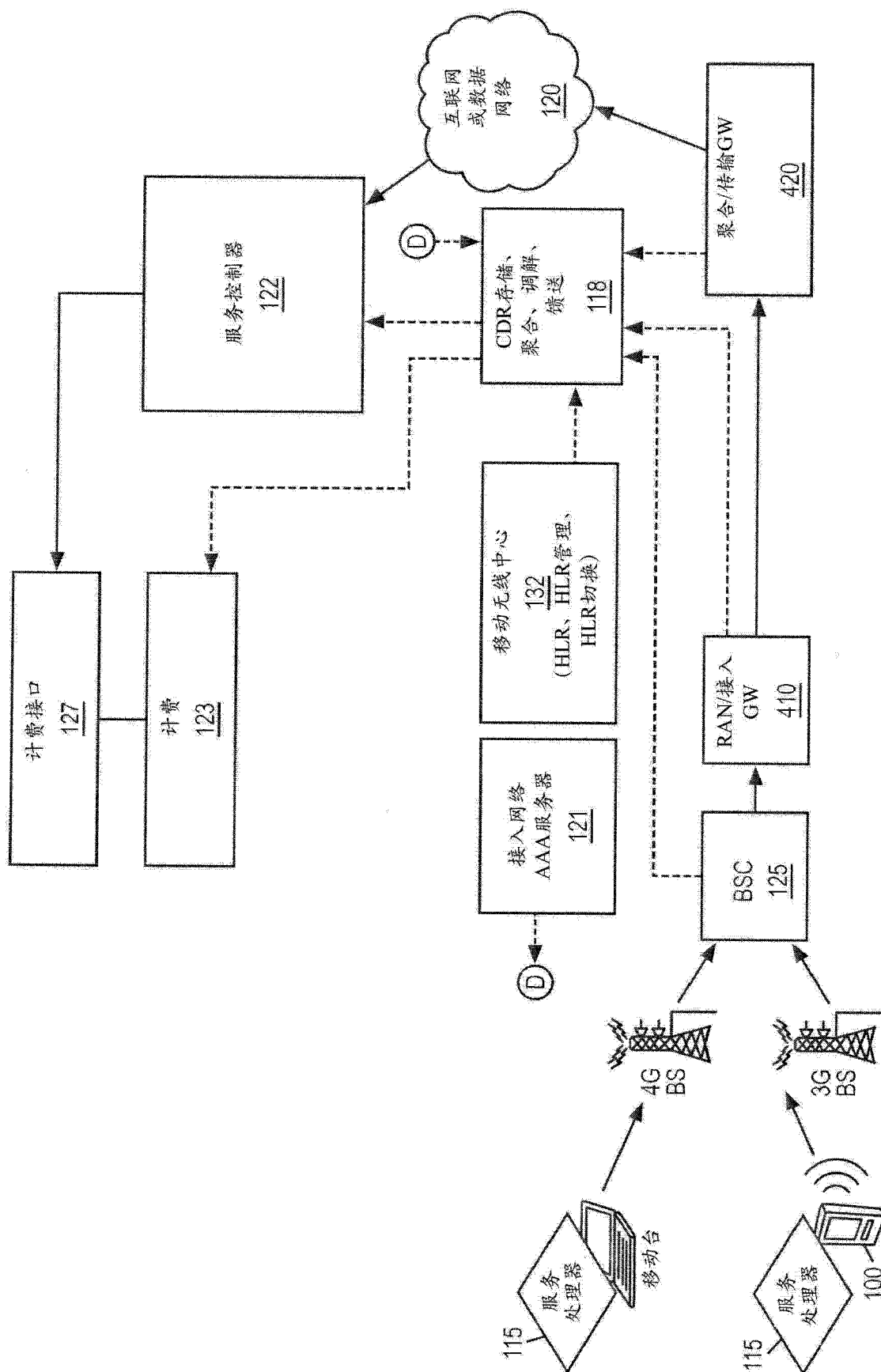


图 7

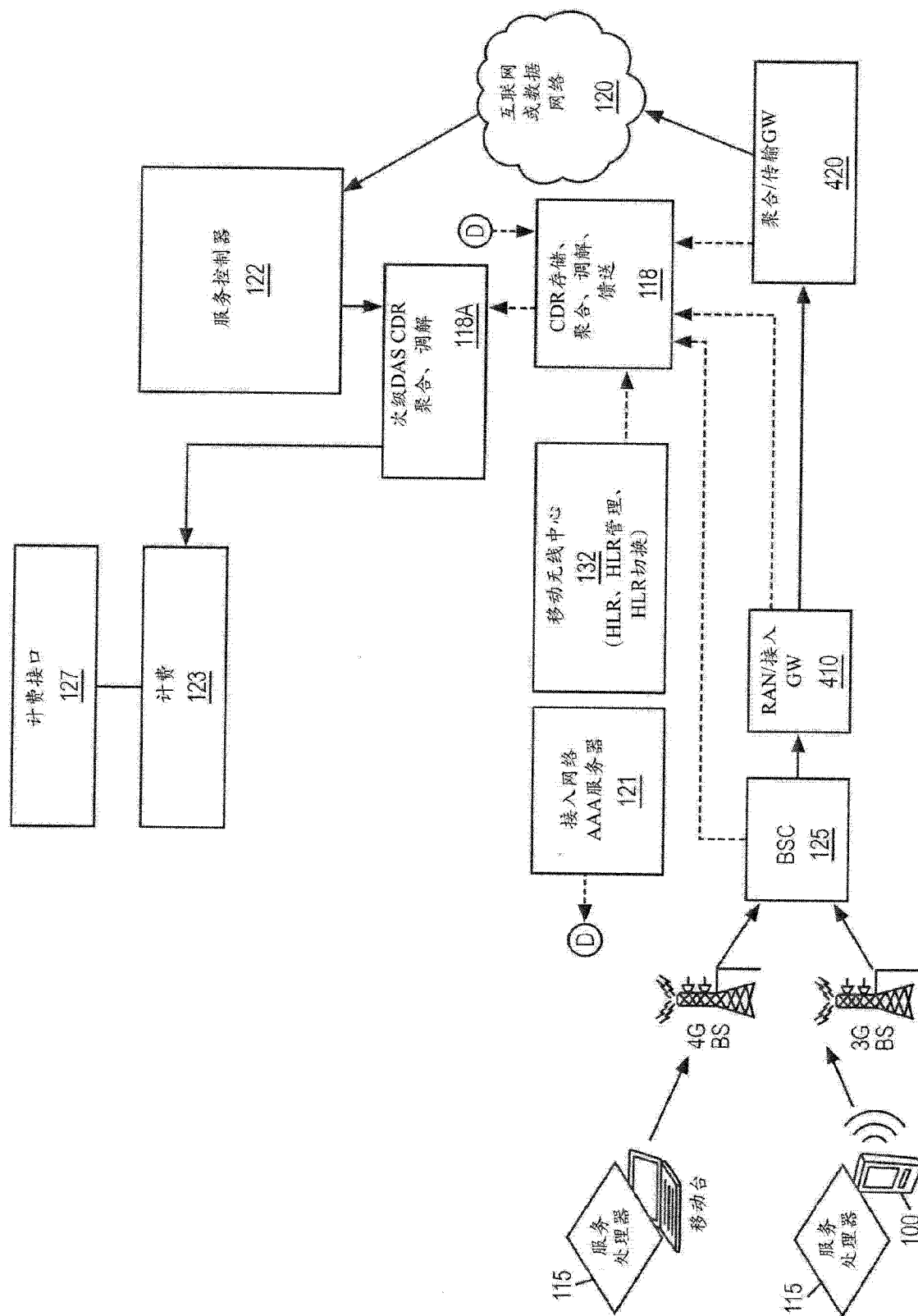


图 8

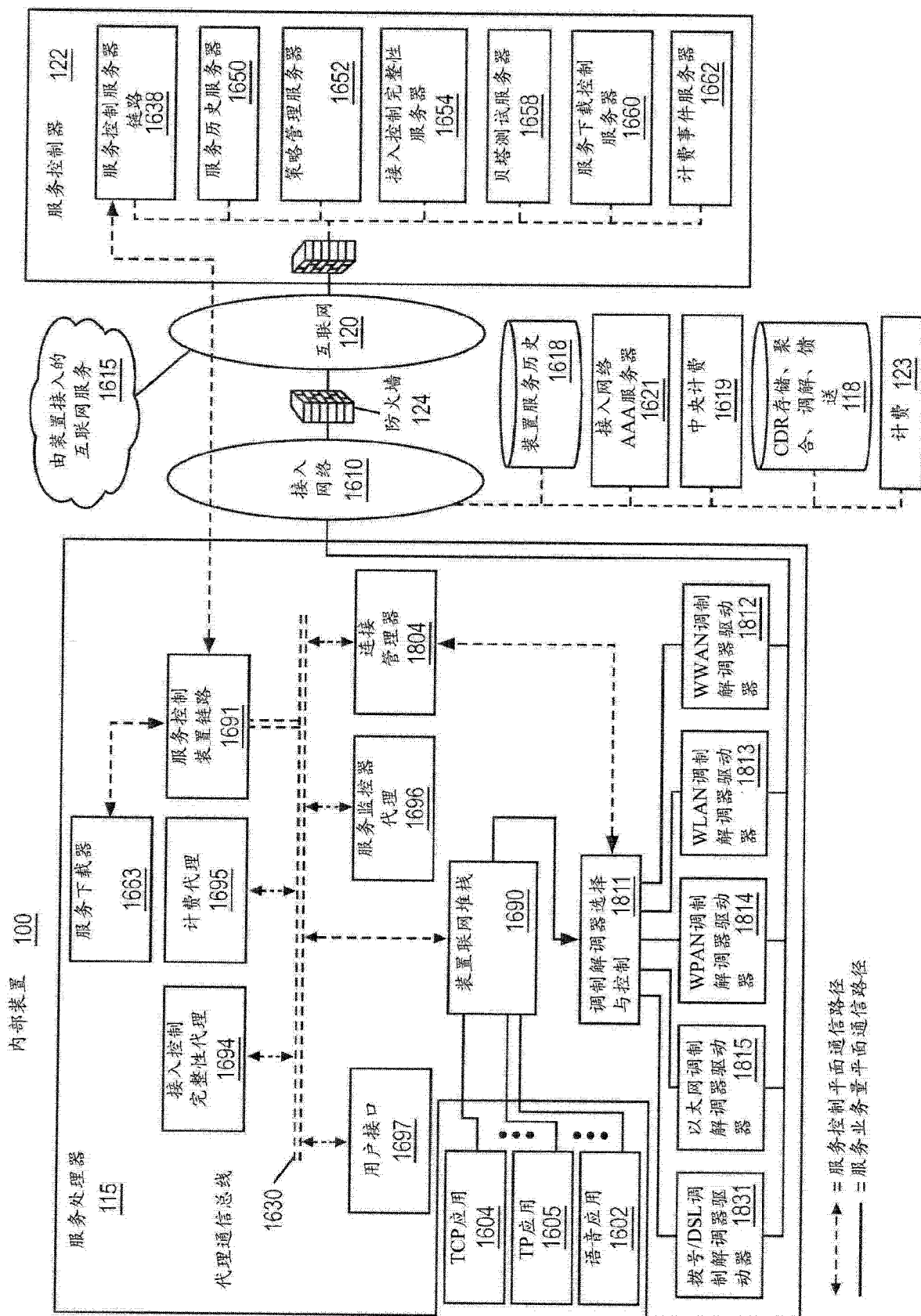


图 9

服务处理器115实施例	实施例功能的部分汇总
服务控制装置链路 1691	在一些实施例中，用于将服务处理器415连接至服务控制器的装置侧控制平面链路也充当用于代理心跳功能的链路。
接入控制完整性代理 1694	收集关于服务策略、服务使用、代理配置和代理行为的装置信息。交叉检查这个信息来识别服务策略实施和控制系统中的完整性破坏。当怀疑有一个服务策略违反或一个系统完整性破坏时，启动行动。在一些实施例中，验证其他代理的配置或执行挑战响应顺序测试。在一些实施例中，监控软件加载活动、受保护的存储器接入或与服务器代理器代理的通信来检测服务器软件或配置的未授权的变化。
服务监控器代理 1696	记录并且报告装置服务使用。在一些实施例中，通过联网堆栈策略实施辅助传递业务量流的应用标记。在一些实施例中，维护历史并且提供除由服务器控制器控制的网络外装置已连接至的网络的报告或汇总报告。在一些实施例中，这个网络活动汇总可以包括对所接入的网络、每次连接的活动vs时间、每次连接的业务量vs时间的一个汇总。
计费代理 1695	检测并且报告计费事件。在一些实施例中，与用户接口代理497交互作用来为用户提供服务计划选项，接收服务计划选择，提供关于服务使用等级的通知，提供关于服务使用控制策略的选项，接收对于服务使用策略的选项，提供交易选项或接收交易选项。在一些实施例中，与交易服务器134交互作用来用中央计费进行电子商务交易。
用户接口 1697	将服务接口提供给用户
服务下载器 1663	提供一个下载功能来安装或更新装置上的服务软件元件。
连接管理器 1804	为连接至一个接入网络的一个或多个调制解调器驱动器或调制解调器提供一个控制和监视功能。
调制解调器选择和控制在 1811	选择接入网络连接
调制解调器驱动器 1831,1815,1814,1813,1812	将数据业务量转换成用于一个或多个调制解调器的调制解调器总线业务量。
调制解调器 2141,2125,2124,2123,2122	将装置连接至一个或多个网络。

图 10

服务处理器122实施例	实施例功能的部分汇总	
服务控制服务器链路 1638	用于连接服务控制器122与服务处理器115的网络侧控制平面链路。在一些实施例中，也充当用于代理心跳的链路。	
接入控制完整性服务器 1654	收集关于服务策略、服务使用、代理配置和代理行为的装置信息。交叉检查这个信息来识别服务策略实施和控制系统中的完整性破坏。当怀疑有一个服务策略违反或一个系统完整性破坏时，启动行动。	
服务历史服务器 1650	收集并且记录用于接入网络AAA服务器1621和服务监控代理1696的装置使用报告。在一些实施例中，维护除由服务控制器控制的网络之外的装置已连接到的网络的历史。在一些实施例中，这个网络活动汇总可以包括对所接入的网络、每次连接的活动对比时间、每次连接的业务量对比时间的一个汇总。在一些实施例中，这个活动汇总进一步被分析或报告来估计与业务活动相关联的服务计划的类型以为了账单共享和的目的。	
中央提供商计费系统 123	为中央提供商计费事件提供调解功能。接收服务计划变化。在一些实施例中，提供装置服务使用、服务计划限制或服务策略上的更新。	
计费事件服务器 1662	在一些实施例中，收集计费事件，将服务计划信息提供给服务处理器115，将服务使用更新提供给服务处理器115，充当装置与中央提供商计费系统123之间的接口，或为某些电子商务计费交易提供可信的第三方功能。	
服务下载控制服务器 1660	提供一个下载功能来安装或更新装置上的服务软件元件。	

图 11

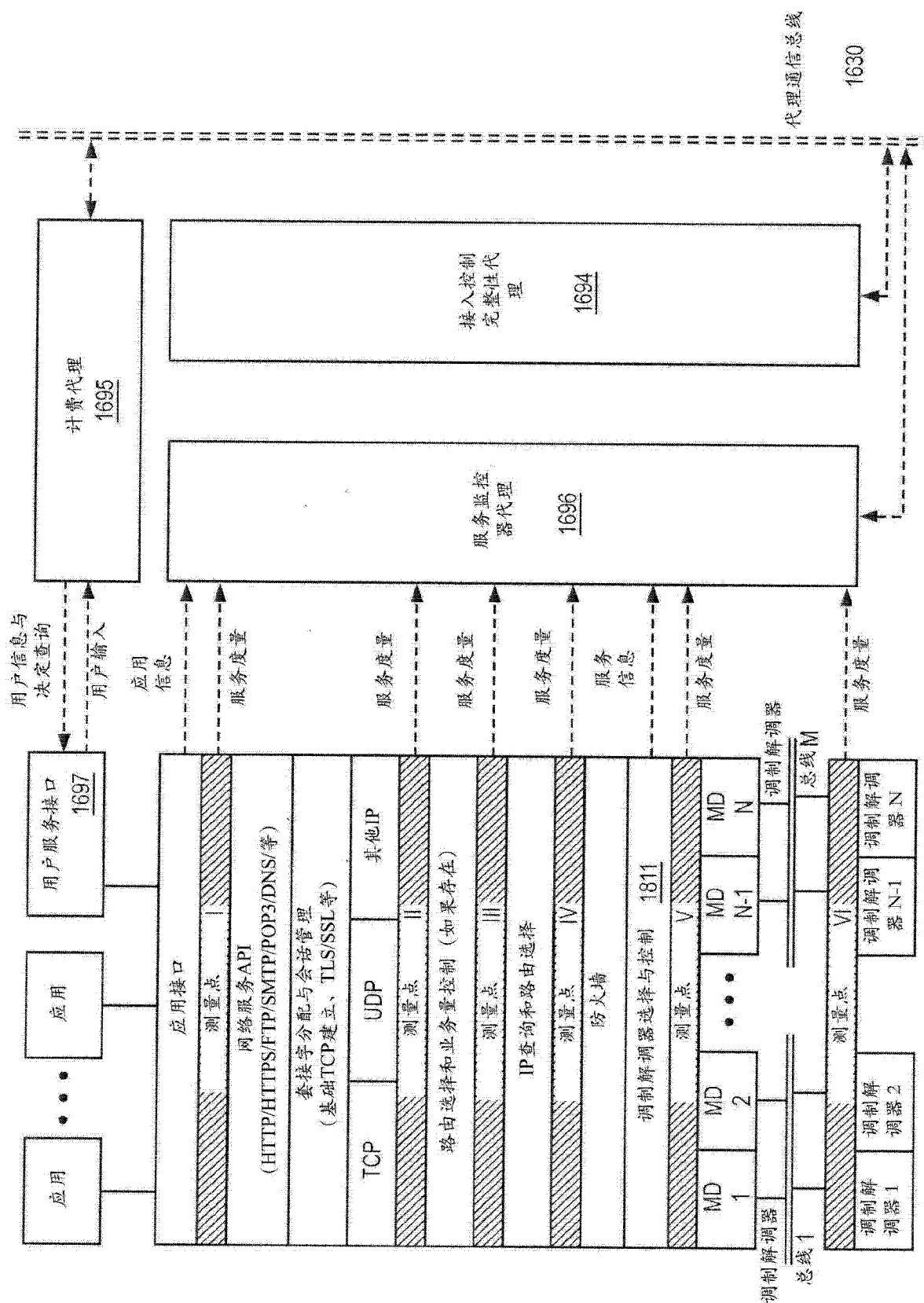


图 12

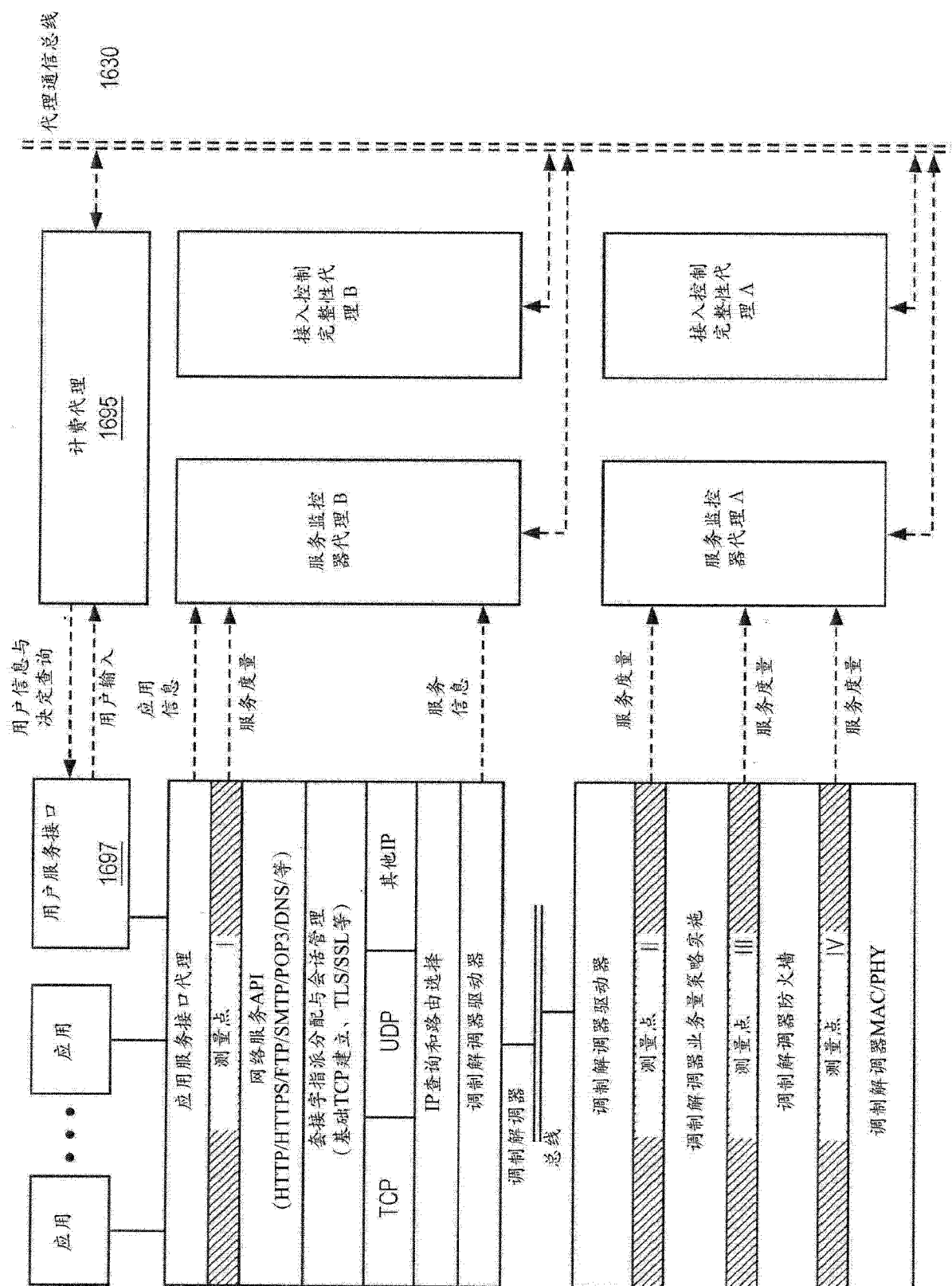


图 13

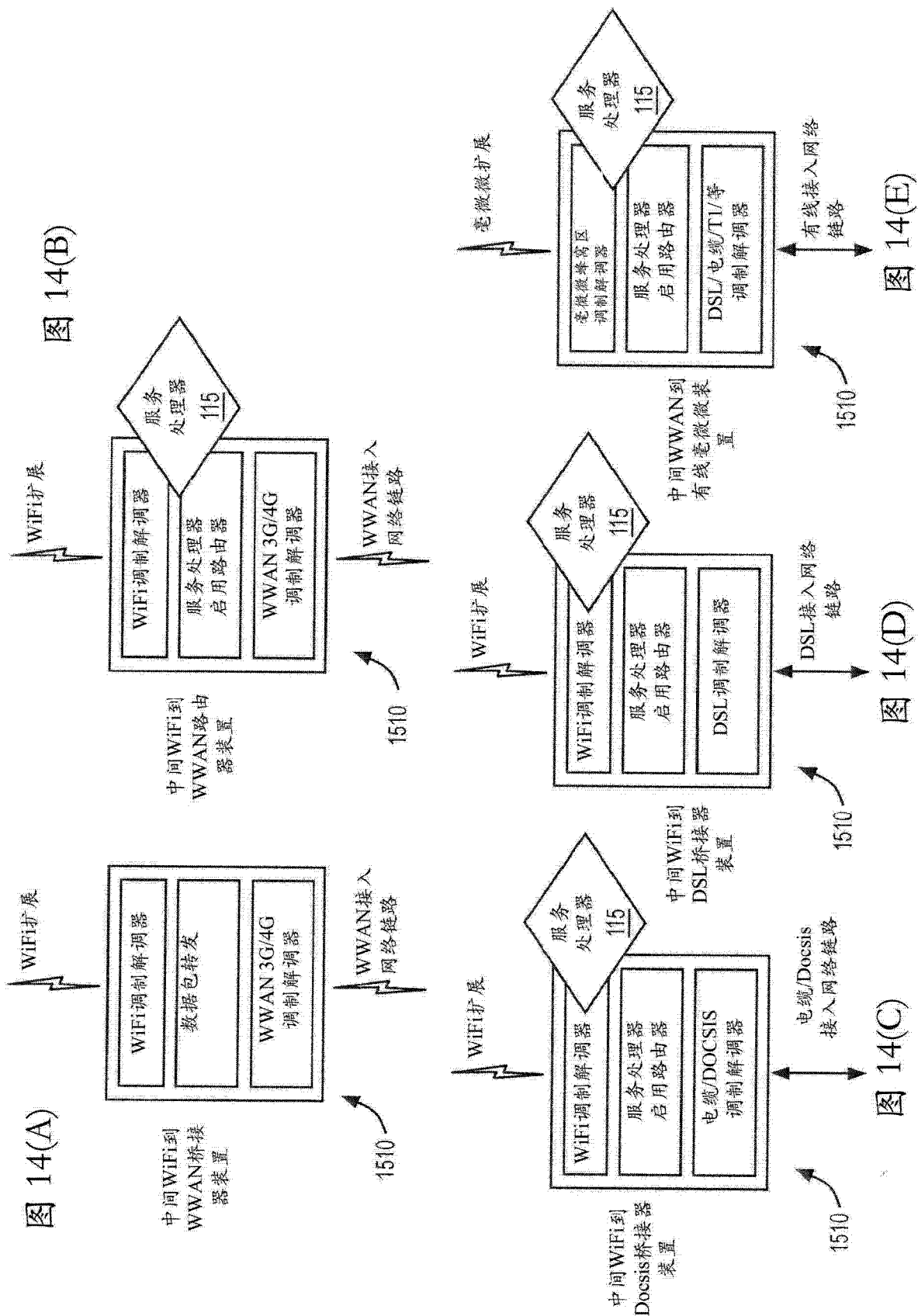


图 14

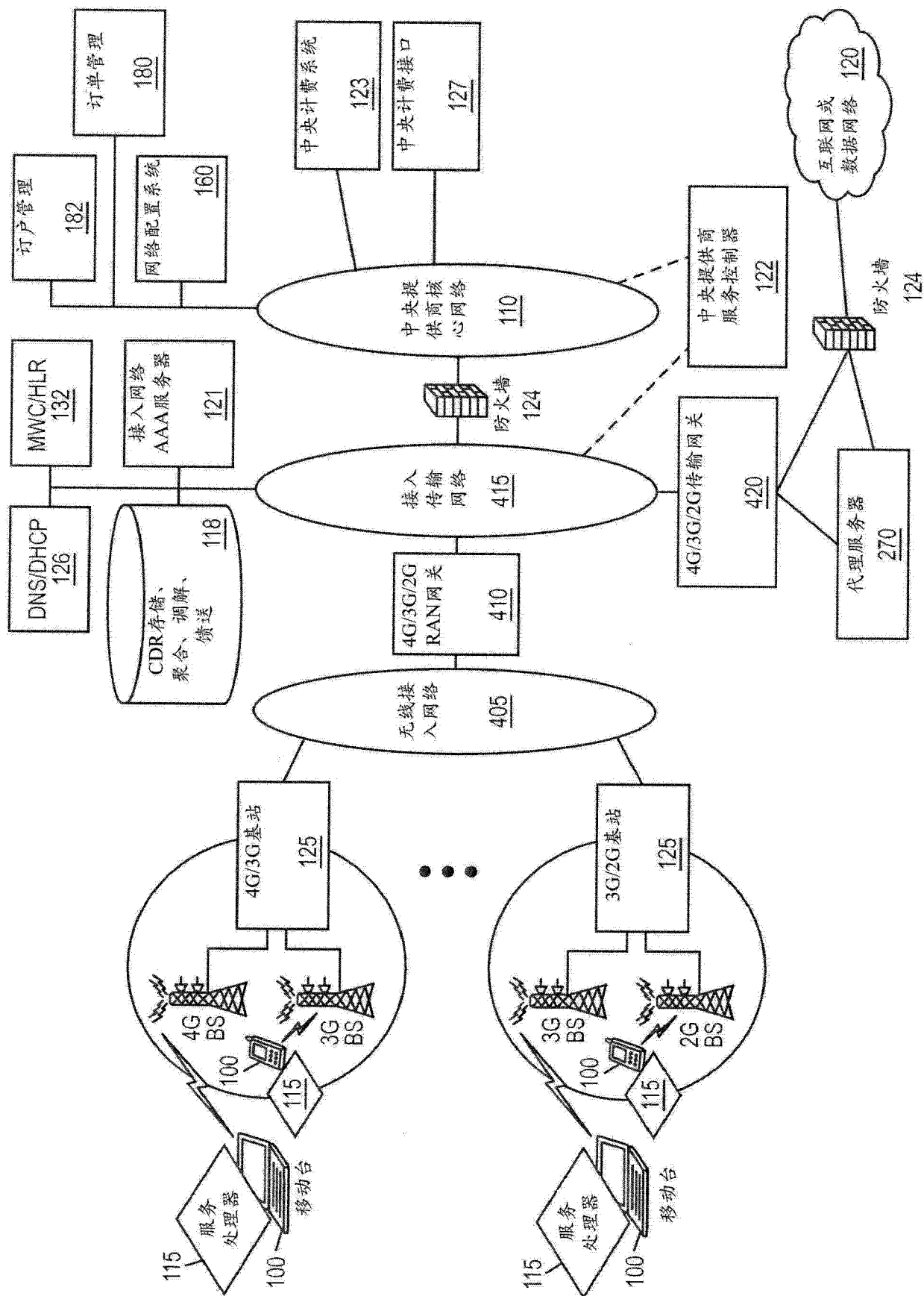


图 15

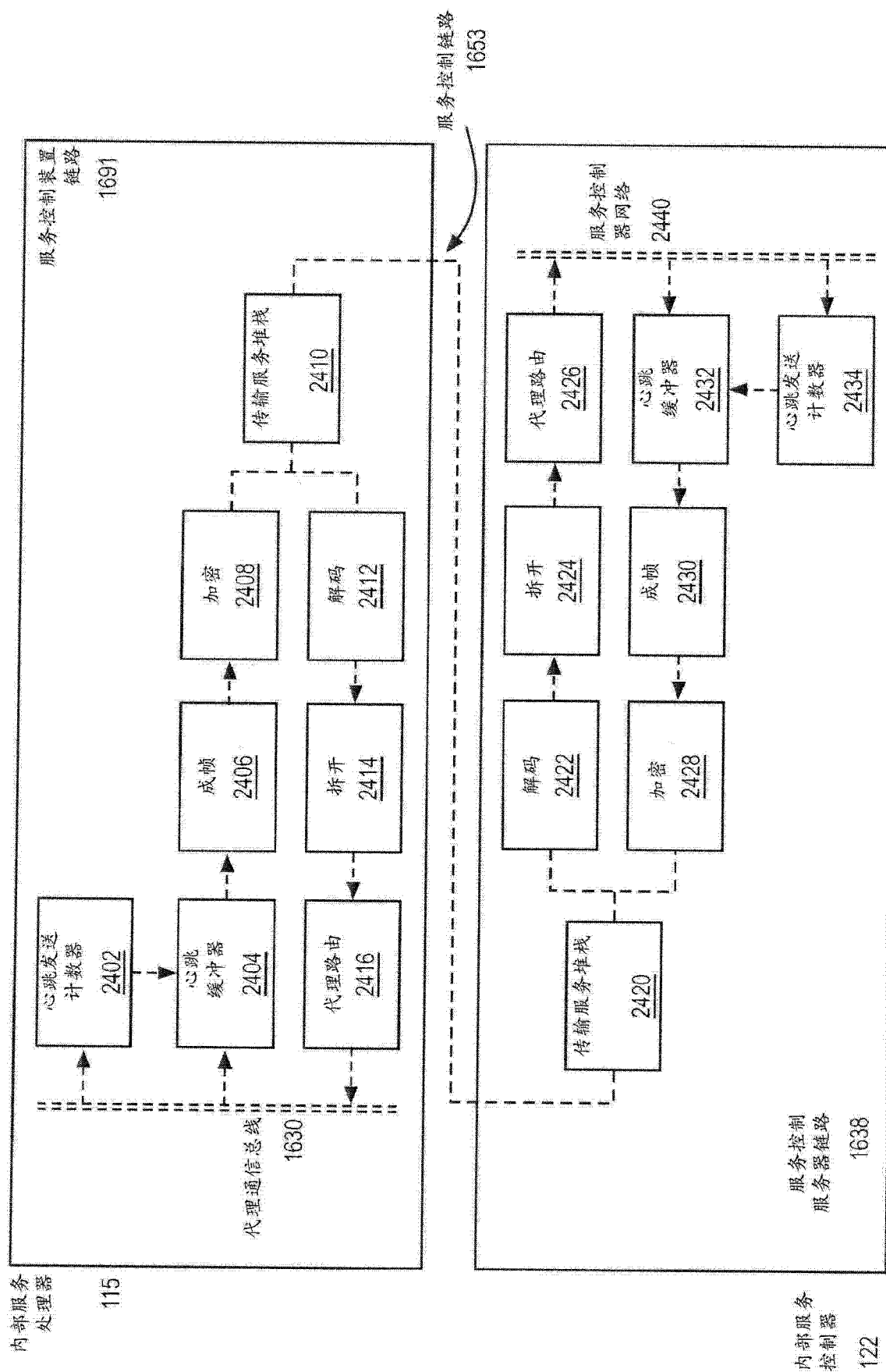


图 16

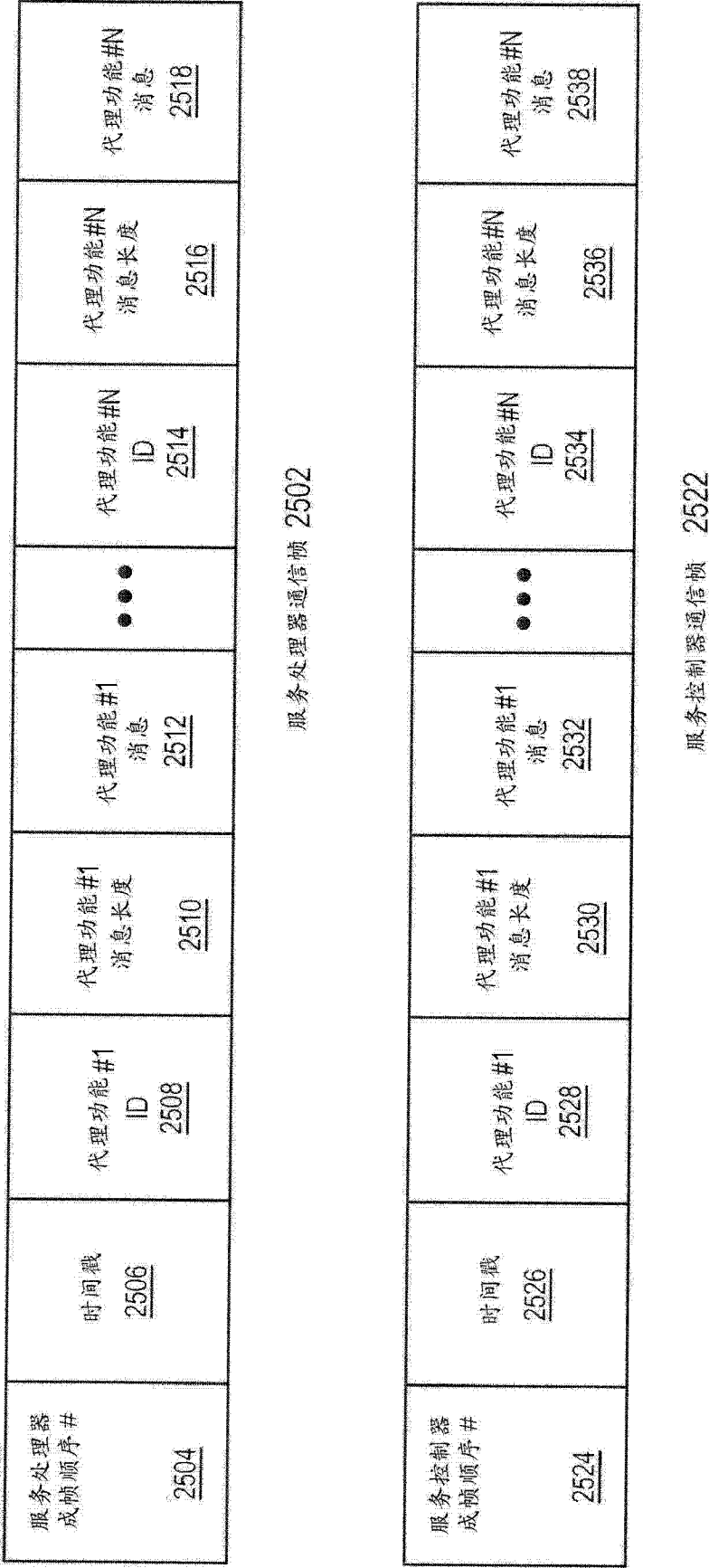


图 17

示例性服务处理器心跳参数实施示例	描述	频率
接入控制完整性报告	含有接入控制完整性代理的最新结果 服务处理器系统统检查并且报告任何错误事件。	如果不存在错误, 则不必在每次心跳时报告。可以仅在错误时报告, 设置一个最小频率或响应服务控制器轮询。
服务监控器报告	报告服务监控器代理管理的已过滤的汇总。汇总减少控制业务量并且过滤出未授权的私人信息。	每次心跳。一些实施例将这链接至数据路径中的数据使用量来保持低开销。在从服务控制器轮询时立即报告。
计费事件报告	自最后心跳之后报告任何计费活动。计费事件可以包括服务使用事件、交易事件、账户账单记录、账户账单偏差报告或引起一个计费事件报告的任何其他事件。	在计费事件时发送。在来自服务控制器的轮询时立即报告。
服务处理器设置报告	报告用于所有服务处理器代理的服务策略设置。	不必每次心跳时发送。一些实施例将这链接至数据使用量来减少开销。可以每N次心跳时报告。在来自服务控制器的轮询时立即报告。
客户资源管理报告	报告服务监控器代理度量的已过滤的汇总或其他装置或用户活动, 如服务优先项、广告行为以及位置的已过滤的汇总。汇总减少控制业务量并且过滤出未授权的私人信息。	不必每次心跳时发送。一些实施例将这链接至数据使用量来减少开销。可以每N次心跳时报告。在来自服务控制器的轮询时立即报告。
响应服务处理器代理查询	将代理响应发送到来自服务控制器的挑战-响应查询。	在来自服务控制器的轮询时立即报告。

图 18A(1)

示例性服务处理器心跳参数实施例	描述	频率
位置跟踪服务更新	报告位置跟踪信息的已过滤的汇总。汇总减少控制业务量并且过滤出未授权的私人信息。	不必每次心跳时发送。一些实施例需要一个基于最少时间的传输频率。
基于装置使用的传输频率	通过缓冲并且保存来自代理和服务器的跳通信而降低开销，直到在网络中已传输或接收一定数据量或已消耗一定服务量。当参数被正确地选择时，这可以引起网络控制平面业务量开销占数据路径业务量的一个小百分比或引起控制平面业务量费用占服务使用费用的一个小百分比。	取决于设置的范围。例如，如果典型地需要传递5个代理消息，并且每一个消息均小于100字节，并且服务控制器心跳成帧加上网络开销将引起一个小于1000字节的数据包大小，并且该心跳数据包在已在数据路径上传递10,000,000字节时传输，随后由于每一个方向上的一个心跳数据包引起的开销损耗小于0.02%。
恒定频率传输	因为装置可以长时期处于离线，其中服务控制处理器需要验证装置控制完整性，在一些实施例中，以一个最小速率来传输心跳数据包而不管数据业务量活动可以是有利的。这通过设置按定期调度来发送已排入队列的心跳数据包的一个计时器而实现。	取决于设置和应用的范围
服务控制器轮询传输	在一些实施例中，服务控制器可以作为一个心跳传输轮询服务处理器，此时服务处理器将使所有已排入队列的心跳消息成帧并且将其传输。	取决于应用的范围。在一些实施例中，这用作一个按需功能，而在其他实施例中，其用作在服务控制器中设置心跳传输计时功能的一种方式。
服务处理器轮询传输	在一些实施例中，服务处理器为一个心跳传输而轮询服务控制器，此时服务控制器将使所有已排入队列的心跳消息成帧并且将其传输。	取决于应用的范围。在一些实施例中，这用作一个按需功能，而在其他实施例中，其用作在服务处理器中设置心跳传输计时功能的一种方式。

图 18A(2)

示例性服务处理器心跳参数实施例		描述	代理报告不同代理自诊断规程的结果以确保：代理被正确地配置，从而正确地运行，正确地实施服务控制策略；或未被篡改，[提供多个示例，这些示例为典型软件安全自诊断报告的扩展]。	频率	在一些实施例中，在每一次心跳传输过程中做出一个报告。在其他实施例中，该报告由来自服务控制器的一个请求生成。在其他实施例中，该报告通过由装置确定的计时时而生。在一些实施例中，该报告在存在一个被识别出的某一类验证错误时而生。
代理自检查报告			一个或多个代理为这些代理中的一个或多个扫描存储或执行环境，以便识别对服务实施或代理完整性的潜在威胁，并且做出一个报告。在一个示例实施例中，完成一个扫描来确定未授权的软件或硬件是否正在一个安全代理环境中执行。在另一个实施例中，完成一个扫描来确定该软件已加载到装置运行环境、存储器或存储空间的一部分中，并且针对一个已知威胁清单来引用该软件清单。在一个示例实施例中，扫描接入一个或多个代理的实体的清单来确定是否已发生到一个代理的未授权的接入。在另一个实施例中，执行一个扫描来确定是否已发生到安全执行环境、存储器或存储空间的未授权的接入。在另一个示例实施例中，记录并且分析用于装置的网络接入模式，以便确定是否存在已知与对服务或代理控制完整性的一个威胁相关的一个接入模式。在另一个示例实施例中，记录并且分析内部装置软件、存储器或外围接入模式，以便确定是否存在已知与对服务或代理控制完整性的一个威胁相关的一个接入模式。		在一些实施例中，在每一个心跳传输过程中做出一个报告。在其他实施例中，该报告由来自服务控制器的一个请求生成。在其他实施例中，该报告通过由装置确定的计时时而生。在一些实施例中，该报告在存在一个被识别出的某一类验证错误时而生。
环境报告					

图 18B(1)

示例性服务处理器心跳参数实施例	用户通知响应报告	描述 计费代理、UI代理或另一个代理记录用户通知事件和事件对通知事件的响应。在一些实施例中，这些事件可以交叉引用到通知策略，该通知策略应该在装置和装置服务使用上生效以确保遵守正确的通知顺序。在其他实施例中，用户通知项、计费事件并且用来记载对通知或服务费用控制决定。在一些实施例中，可以要求用户提供一个密码、生物测定签名、硬件密钥或其他机制来积极地识别用户拥有装置，或来验证服务正确地运行或正被正确地实施。在一些实施例中，可以要求用户来确认一个服务过量通知和其他机制来验证服务过量确认应答。	频率 在一些实施例中，在每一个心跳传输过程中做出一个报告。在其他实施例中，该报告由来自服务控制器的一个请求生成。在其他实施例中，该报告通过由装置确定的计时时生成。例如，在针对用户的一个用户通知顺序行动时生成。在一些实施例中，该报告在存在一个被识别出的某一类验证错误时生成。
------------------------	-----------------	--	--

图 18B (2)

示例性服务处理器心跳参数实施例	描述	频率
用户报警响应报告	计费代理、UI代理或另一个代理记录用户报警事件和对报警事件的用户响应。在一些实施例中，用户响应用来确定用户是否积极地控制装置。在一些实施例中，该响应用来确认一个计费过量或其他服务费用事件。在一些实施例中，可以要求用户提供积极密码、生物测定签名、硬件密钥或其他机制来积极地识别用户拥有装置或来验证服务正确地运行或正被正确地实施。	在一些实施例中，在每一个心跳传输过程中做出一个报告。在其他实施例中，该报告由来自服务控制器的一个请求生成。在其他实施例中，该报告通过由装置确定的计时时生成。例如，在针对用户的一个报警顺序活动时生成。在一些实施例中，该报告存在一个被识别出的某一类验证错误时生成。
代理通信日志报告	报告建立或尝试建立与代理的通信的实体。在一个实施例中，报告实体与代理通信或尝试与代理通信的一个清单和次数。在另一个实施例中，当未授权的实体尝试建立与一个代理的通信时，报告一个错误标志。	在一些实施例中，在每一个心跳传输过程中做出一个报告。在其他实施例中，该报告由来自服务控制器的一个请求生成。在其他实施例中，该报告通过由装置确定的计时时生成。在一些实施例中，该报告存在一个被识别出的某一类验证错误时生成。

图 18C(1)

示例性服务处理器心跳参数实施例	描述	频率
服务使用同步数据	IPDR 或其他数据用来使装置服务使用计数器同步。在一些实施例中，数据被加时间戳，这样使得在一个时间点的服务使用可以在本地装置使用计数器与基于网络的使用计数器之间调和，并且随后自该时间点后，本地装置使用计数器可以用来估计目前的实时使用计数器。在一些实施例中，来自装置的服务使用数据由网络使用作为用于装置的账单功能使用或计费数据基础。在其他实施例中，账户账单功能被包括在服务使用同步数据中，这样使得可以将服务使用计费到不同账户中，而不是一个单个主用户账户中。	服务使用同步是与一些实施例中的每一次心跳相连续的。在其他实施例中，服务使用同步是基于来自将 IPDR 信息发送到装置的服务控制器或其他网络功能的一个推送的。在其他实施例中，该装置请求一个同步数据传输。
服务费使用同步数据	来自一个基于网络的功能的一个服务费使用计数器和对本地装置的一个服务费使用估计的信息。类似于服务使用计数器，在一些实施例中，服务费使用信息可以在装置与基于网络的功能之间调和，并且随后服务费使用的本地度量可以用来估计目前的实时服务费使用。在一些实施例中，本地服务费使用通过获取记录的计费事件并且查找一个或多个计费事件的网络功能中可用的查找数据库的一个服务使用来确定。在一些实施例中，服务费使用估计完全在网络中完成，并且该结果被推送到装置 UI。在其他实施例中，服务费使用估计在本地使用估计和查找表的一个本地使用上在装置中完成。	服务费使用同步在一些实施例中是与每一次心跳相连续的。在其他实施例中，服务费使用同步是基于来自将 IPDR 信息发送到装置的服务控制器或其他网络功能的一个推送的。在其他实施例中，该装置请求一个同步数据传输。

图 18C(2)

[illegible]

图 18D(1)

示例性服务处理器心跳参数实施例	描述	频率
系统消息和响应	在一些实施例中，心跳功能可以用作向终端用户显示由网络功能或服务器生成的一个系统消息或屏幕的一个安全控制信道，并且可能将用户输入报告给UI消息或屏幕。示例包括……等。	系统消息由服务控制器生成并且在一些实施例中根据需要进行传输。在其他实施例中，一些系统消息响应于用户输入或请求而生成。在其他实施例中，系统消息在一个定期时间表上或根据一定服务使用量而生成。
UI屏幕消息和响应	在一些实施例中，心跳功能可以用作向终端用户显示由一个网络功能或服务生成的用户接口消息或屏幕的一个安全控制信道，并且可能将用户输入报告给UI消息或屏幕。示例包括服务使用UI、服务选项UI、更新UI、交易UI、销售UI、计费UI、用户识别确认UI、用户服务报警UI、用户潜在服务篡改相应请求UI等。	UI屏幕消息由服务控制器生成并且在一些实施例中根据需要进行传输。在其他实施例中，一些用户UI消息响应于用户输入或请求而生成。在其他实施例中，UI消息在一个定期时间表上或根据一定服务使用量而生成。
本地代理登记历史	记录并且报告向一个本地代理完整验证功能做出的代理登记或自报告。	在一些实施例中，在每一个心跳传输过程中做出一个报告。在其他实施例中，该报告由来自服务控制器的一个请求而生成。在其他实施例中，该报告通过由装置确定的计时而生成。在一些实施例中，该报告在存在一个被识别出的某一类验证错误时生成。

图 18D(2)

示例性服务处理器心跳参数数实施例	描述	频率
软件安装报告	记录并且报告已在装置上发生的软件安装的一个或多个方面。	在一些实施例中，在每一个心跳传输过程中做出一个报告。在其他实施例中，该报告由来自服务控制器的一个请求生成。在另一些实施例中，该报告通过装置确定的计时时生成。在另一些实施例中，该报告在存一个被识别出的某一类验证错误时生成。在一些实施例中，该报告在安装新的SW时生成。
测试计费事件	在一些实施例中，服务控制器或其他网络功能可以发送或引起一个测试计费事件，其中该装置触发一个本地计费顺序，以用于验证计费顺序被正确地记录、进行并且报告的目的。计费顺序可以与一个服务使用事件或顺序、一个交易事件或顺序或应当引起一个计费事件的任何其他事件或顺序相关。	在一些实施例中，测试计费事件计时由服务控制器或其他网络功能确定。在其他实施例中，其由装置或按一个定期调度生成。
测试服务事件	在一些实施例中，服务控制器或其他网络功能可以发送或引起一个服务使用事件，其中该装置触发一个本地服务使用事件或顺序，以用于验证服务使用事件或顺序被正确地记录并且报告的目的。	在一些实施例中，测试服务使用事件计时由服务控制器或其他网络功能确定。在其他实施例中，其由装置或按一个定期调度生成。

图 18E

服务策略实施验证技术实施例	示例性错误触发条件实施例	示例性错误响应实施例
验证网络中的服务使用度量与所期望的服务行为为相一致	网络服务使用度量与所期望的服务使用相冲突。示例：业务量使用在限制之外、地址接入在限制之外、未遵循业务量成形成规则。	在一些实施例中，错误严重性和/或错误持续性和/或其他错误的存在性用来确定适合的响应或行动。在一些实施例中，重置服务策略并观看错误是否持续。在一些实施例中，执行代理设置检查来验证代理服务使用控制策略设置是正确的。在一些实施例中，运行动态代理加载，在一些情况下对新代理码的差异加密、排序或模糊处理来刷新一个或多个代理。在一些实施例中，将一个用户参与警告发送到UI来通知用户，确认装置是由用户拥有的，或使用用户参与警告或错误的过程中，或来辅助验证基于装置的服务控制。在一些实施例中，装置标识号被放置在一个错误清单上以用于进一步错误处理。在一些实施例中，装置被放置在一个SPAN过程中、或一个类似的业务量或服务检验过程、或另一个服务使用监视状态上来紧密地监控服务行为并且确定其是否与一个正确的服务使用策略相一致。在一些实施例中，报告计费事件或服务使用事件。在一些实施例中，装置被放置在隔离网络路由选择状态上，其中可能发送一个用户消息来通知用户，其中可能发送一个用户消息来通知用户，装置被放置在隔离网络路由选择状态上，其中可能发送一个用户消息来通知用户。在一些实施例中，将一个错误消息发送到网络中的一个人机界面以用于进一步错误分析。

图 19A(1)

服务策略实施验证技术实施例	示例性错误触发条件实施例	示例性错误响应实施例
验证在装置处的服务使用度量与所期望的服务行为为相一致	装置服务使用度量与所期望的服务使用相冲突。示例：业务量使用太高、地址接入在限制之外、接入的电子邮件与策略对立。	与以上相同。
验证网络中的服务使用度量与在装置处的服务使用度量相一致	装置服务使用度量与网络服务使用度量极大地不同	与以上相同。
验证在装置中的一个点处的服务使用度量与在装置中的一个第二点处的服务使用度量相一致	在装置堆栈中的一个点处的服务使用度量与在另一个点处的服务使用度量不一致指示错误或潜在的寄生使用	与以上相同。在一些实施例中，装置上的服务度量上的差异可以用来评估服务使用策略实施问题的性质。

图 19A(2)

服务策略实施验证技术实施例	示例性错误触发条件实施例	示例性错误响应实施例
验证生效的服务策略是如预期的一样	服务策略设置查询产生不同于预期的设置	在一些实施例中，重置服务策略并且查看错误是否持续。如果这没有清除错误，或如果这不是所采用的错误校正方法，则执行以下行动中的一项或多项：在一些实施例中，执行代理查询/响应来确定代理完整性。在一些实施例中，运行动态代理加载，在一些情况下对新代理码的差异加密、排序或模糊处理来刷新一个或多个代理。在一些实施例中，将一个用户查询或报警发送到UI来通知用户，确认装置是由用户拥有的，或使用用户参与确定源或错误的过程中，或来辅助验证基于装置的服务控制。在一些实施例中，装置标识号被放置在一个错误清单上以用于进一步错误处理。在一些实施例中，装置被放置在一个SPAN过程上、或一个类似的业务量或服务检验过程、或另一个服务使用监视状态上来紧密地监控服务行为并且确定其是否与正确的服务使用策略相一致。在一些实施例中，执行一个计费事件测试或一个服务使用测试来确定装置是否正确地报告计费事件或服务使用事件。在一些实施例中，装置被放置在隔离网络路由选择状态上，其中可能发送一个用户消息来通知用户。在一些实施例中，可能在向用户发送可以包括对过程的指令以用于校正错误并且恢复服务的一个消息之后，暂停装置服务。在一些实施例中，作为对发送到装置的一个消息的替代物或删除发送到装置的消息之外，这些用户消息通过一个替代的消息传送系统，如电子邮件或文本消息传送而发送。在一些实施例中，将一个错误消息发送到网络中的一个界面以用于进一步错误分析。

图 19A(3)

服务策略实施验证技术实施例	示例性错误触发条件实施例	示例性错误响应实施例
验证服务处理器代理的存在	代理不响应代理通信或查询--响应	在一些实施例中，运行动态代理加载，在一些情况下用对新代理码的差异加密、排序或模糊处理来刷新一个或多个代理。如果这没有清除错误，或如果这不是所采用的错误校正方法，则执行以下行动中的一项或多项：在一些实施例中，将一个用户查询或报警发送到UI来通知用户，确认装置是由用户拥有的，或使用用户参与确定源或错误的过程中，或未辅助验证基于装置的服务控制。在一些实施例中，装置标识号被放置在一个错误澄清单上以用于进一步错误处理。在一些实施例中，装置被放置在一个SPAN过程上、或一个类似的业务量或服务检验过程、或另一个服务使用监视状态上来紧密地监控服务行为并且确定其是否与旨在是正确的服务使用策略相一致。在一些实施例中，执行一个计费事件测试或一个服务使用事件测试来验证装置是否正确地被放置在隔离网络路由选择状态上，其中可能发送一个用户消息来通知用户。在一些实施例中，可能在向用户发送一个消息之后，对过程指令以用于校正错误并且恢复服务的一个消息之后，暂停装置服务。在一些实施例中，作为对发送到装置的一个消息的一个替代物或除发送到装置的消息之外，这些消息通过一个替代的消息传递系统，如电子邮件或文本消息传递而发送。在一些实施例中，将一个错误消息发送到网络中的一个个人界面以用于进一步错误分析。

图 19B(1)

服务策略实施验证技术实施例	示例性错误触发条件实施例	示例性错误响应实施例
验证服务处理器代理的配置	代理配置带计或配置自检查失败。	在一些实施例中，运行动态代理加载，在一些情况下用对新代理码的差异化加密、排序或模糊处理来刷新一个或多个代理。如果这没有清除错误，或如果这不是所采用的错误校正方法，则执行以下行动中的一项或多项：在一些实施例中，错误严重性和/或错误持续性和其他错误的存在性用来确定适合的响应或行动。在一些实施例中，重置服务策略并且观看错误是否持续。在一些实施例中，执行代理设置检查来验证代理服务使用控制策略设置是正确的。在一些实施例中，将一个用户查询或报告发送到UI来通知用户，确认装置是由于用户拥有的，或使用用户参与确定源或错误的过程中，或来辅助验证基于装置的服务控制。在一些实施例中，装置标识号被放置在一个错误清单上以用于进一步错误处理。在一些实施例中，装置被放置在一个SPAN过程上、或一个类似的业务量或服务检验过程、或另一个正确的服务使用策略上、或一个类似地监控服务行为并且确定其是否与旨在正确的服务使用策略一致。在一些实施例中，执行一个计费事件或服务使用事件。在一些实施例中，装置被放置在隔离网络路由选择状态上，其中可能发送一个用户消息来通知用户。在一些实施例中，可能在向用户发送可以包括对过程的指令以用于校正错误并且恢复服务的一个消息之后，暂停装置服务。在一些实施例中，作为对发送到装置的一个消息的替代物或除发送到装置的消息之外，这些用户消息通过一个替代的消息传递系统，如电子邮件或文本消息传递而发送。在一些实施例中，将一个错误消息发送到网络中的一个个人机界面以用于进一步错误分析。

图 19B(2)

服务策略实施验证技术实施例	示例性错误触发条件实施例	示例性错误响应实施例
验证计费事件被报告或被正确地报告	计费代理查询揭示已报告的所记录的计费事件。	在一些实施例中，执行一个计费事件测试来确定计费事件报告顺序是否正在正确地运行。在一些实施例中，运行动态代理加载，在一些情况下用对新代理码的差异加密、排序或模糊处理来刷新一个或多个代理。如果这没有清除错误，或如果这些不是所采用的错误校正方法，则执行以下行动中的一项或多项：在一些实施例中，错误严重性和/或错误持续性和/或其他错误的存在性用来确定适合的响应或行动。在一些实施例中，重置服务策略并且观看错误是否持续。在一些实施例中，执行代理设置检查来验证代理服务使用控制策略设置是正确的。在一些实施例中，执行代理查询/响应来确定代理完整性。在一些实施例中，将一个用户参与或报警发送到UI来通知用户，确认装置是由用户拥有的，或使一个用户参与确定或错误的过程中，或未辅助验证基于装置的服务控制。在一些实施例中，装置标识号被放置在一个错误清单上以用于进一步错误处理。在一些实施例中，装置被放置在一个SPAN过程上、或一个类似的业务量或服务检验过程、或另一个服务使用监视状态上来紧紧地监控服务行为并且确定其是否与旨在是正确或服务使用策略相一致。在一些实施例中，执行一个服务使用测试来确定装置是否正在报告服务使用事件。在一个用户消息中，装置被放置在隔离网络路由选择状态上，其中可能发送一个用户消息来通知用户。在一些实施例中，一个消息之后，暂停装置服务。在过程的一些实施例中，作为对发送过一个消息的替代物或除发送到装置的消息之外，这些用户消息通过一个替代的消息传递系统，如电子邮件或文本消息传递而发送。在一些实施例中，将一个错误消息发送到网络中的个人界面以用于进一步错误分析。

图 19B(3)

服务政策实施验证技术实施例	示例性错误触发条件实施例	示例性错误响应实施例
验证网络报告的服务使用度量与报告的装置计费数据相一致。	计费代理没有为服务使用、交易、账户账单或其他计费事件功能正确地报告计费事件。	在一些实施例中，执行一个服务使用测试来确定服务使用报告顺序是否正在正确地运行。在一些实施例中，运行动态代理加载，在一些情况下用对新代理码的差异加密、排序或模糊处理的错误刷新一个或多个代理。如果这没有清除错误，或如果这些不是所采用的错误校正方法，则执行以下行动中的一项或多项：在一些实施例中，错误严重性和/或错误持续性和其他错误的存在性用来确定适合的响应或行动。在一些实施例中，重置服务策略并且观看错误是否持续。在一些实施例中，执行代理/查询响应来处理服务使用控制策略设置是正确的。在一些实施例中，将代理/查询响应来通知用户，确认装置是由用户拥有的，或使一个用户查询或报告发送到UI来通中，或来辅助验证基于装置的服务控制。在一些实施例中，装置标识号被放置在一个错误清单上以用于进一步错误处理。在一些实施例中，装置被放置在一个SPAN过程上、或一个类似的业务量或服务检验过程、或另一个服务使用监视状态上来紧密地监控服务行为并且确定其是否与旨在是正确选择使用策略相一致。在一些实施例中，装置被放置在隔离网络路由由选个在向用户发送可以包括对过程的指令以用于校正错误并且恢复服务的一个消息之后，暂停装置服务。在一些实施例中，作为对发送到装置的一个消息的替代物或删除发送到装置的消息之外，这些消息通过一个替代的消息传送系统，如电子邮件或文本消息传送而发送。在一些实施例中，将一个错误消息发送到网络中的一个人机界面以用于进一步错误分析。

图 19C(1)

服务策略实施验证技术实施例	示例性错误触发条件实施例	示例性错误响应实施例
验证装置报告的服务使用度量与所报告的装置计费数据相一致。	计费代理报告与服务使用报告不相一致。	在一些实施例中，执行一个计费事件测试来确定计费报告顺序是否正在正确地运行。在一些实施例中，运行动态代理加载，在一些情况下用对新代理码的差异加密、排序或模糊处理来刷新一个或多个代理。在一些实施例中，执行一个服务使用测试来确定服务使用报告顺序是否正在正确地运行。在一些实施例中，运行动态代理加载，在一些情况下用对新代理码的差异加密、排序或模糊处理来刷新一个或多个代理。如果这没有清除错误，或如果这些不是所采用的错误校正方法，则执行以下行动中的一项或多项：在一些实施例中，错误严重性和/或错误持续性策略并且观看错误的存在性用来确定适合的响应或行动。在一些实施例中，重置服务使用控制策略设置是正确的。在一些实施例中，执行代理设置检查来验证代理服务完整性。在一些实施例中，将一个用户查询或报警发送到UI来通知用户，确认装置是由用户拥有的，或使用户参与确定源或错误的过程中，或来辅助验证基于装置的服务控制。在一些实施例中，装置标识号被放置在一个错误清单上以用于进一步的错误处理。在一些实施例中，装置被放置在一个SPAN过程上、或一个类似的业务量或服务检验过程、或另一个服务使用策略状态上来紧密地监控服务行为并且确定其是否与旨在是正确的服务使用策略相一致。在一些实施例中，装置被放置在隔离网络路由选择状态上，其中可能发送一个用户消息来通知用户。在一些实施例中，可能在向用户发送可以包括对过程的指令以用于校正错误并且恢复服务的一个消息之后，暂停装置服务。在一些实施例中，作为对发送到装置的一个消息的替代物或删除发送到装置的消息之外，这些用户消息通过一个替代的消息传送系统，如电子邮件或文本消息传送而发送。在一些实施例中，将一个错误消息发送到网络中的一个用户界面以用于进一步错误分析。

图 19C(2)

服务策略实施验证技术实施例	示例性错误触发条件实施例	示例性错误响应实施例
通过装置发送测试计费事件并且验证其被报告。	测试计费事件也未由该装置正确地报告。	在一些实施例中，运行动态代理加载，在一些情况下用对新代理码的差异加密、排序或模糊处理来刷新一个或多个代理。如果这没有清除错误，或如果这些不是所采用的错误校正方法，则执行以下行动中的一项或多项：在一些实施例中，错误严重性和/或错误持续性和/或其他错误的存在用来确定适合的响应或行动。在一些实施例中，重置服务策略并且观看错误是否持续。在一些实施例中，执行代理设置检查来验证代理服务使用控制策略设置是正确的。在一些实施例中，执行代理/查询响应来确定代理完整性。在一些实施例中，将一个用户查询或报警发送到UI来通知用户，确认装置是由用户拥有的，或使用用户参与确定源或错误的过程中，或来辅助验证基于装置的服务控制。在一些实施例中，装置标识号被放置在一个错误清单上以用于进一步错误处理。在一些实施例中，装置被放置在一个SPAN过程上、或一个类似的业务量或服务检验过程、或另一个服务使用监视状态上来紧紧地监控服务行为并且确定其是否与旨在是正确的服务使用策略相一致。在一些实施例中，执行一个服务使用测试来确定装置是否正报告服务使用事件。在一些实施例中，装置被放置在隔离网络路由选择状态上，其中可能发送一个用户消息来通知用户。在一些实施例中，可能在向用户发送可以包括对过程的指令以用于校正错误并且恢复服务的一个消息之后，暂停装置服务。在一些实施例中，作为对发送到一个消息的替代物或除发送到装置的消息之外，这些用户消息通过一个替代的消息传送系统，如电子邮件或文本消息传送而发送。在一些实施例中，将一个错误消息发送到网络中的一个用户界面以用于进一步错误分析。

图 19D(1)

服务策略实施验证技术实施例	示例性错误触发条件实施例	示例性错误响应实施例
验证装置报告从交易服务器报告的计费事件。	交易服务器接收不对应于来自装置的计费事件。	在一些实施例中，执行检查来确定服务交易服务器接收是否有效的。在一些实施例中，运行动态代理加载，在一个或多个代理。如果这没有清除错误，或如果这些不是所采用的错误校正方法，则执行以下行动中的一个或多个：在一些实施例中，错误严重性和/或错误持续性和其他错误的存在用来确定适合的响应或行动。在一些实施例中，重置服务策略并查看错误是否持续。在一些实施例中，执行代理设置检查/查询响应来确定代理完整性。在一些实施例中，将一个用户参与确定源或错误的过程中，或来辅助验证基于装置的服务控制。在一些实施例中，装置标识号被放置在一个错误清单上以用于进一步错误处理。在一些实施例中，装置被放置在一个SPAN过程上、或一个类似的业务量或服务检验过程、或另一个服务使用使用策略一致。在一些实施例中，装置且确定其是否与旨在正确的服务状态上，其中可能发送一个用户消息来通知用户。在一些实施例中，可能在向用户发送可以包括对过程的指令以用于校正错误或恢复服务的一个消息之后，暂停装置服务。在一些实施例中，作为对发送到一个替代的消息传递系统，如电子邮件或文本消息而发送。在一些实施例中，将一个错误消息发送到网络中的一个个人界面以用于进一步错误分析。

图 19D(2)

服务策略实施验证技术实施例	示例性错误触发条件实施例	示例性错误响应实施例
验证激活跟踪系统存在、配置或运行	激活跟踪服务不存在、不提供计划的网络活动报告、或展示错误的报告。	在一些实施例中，该响应旨在将装置ID放置在怀疑具有激活跟踪功能的一个装置清单上，这些实施例中，安装来自一个本地存储的装置副本或者一个网络下载的激活跟踪服务代理软件的一个新副本。在存在授权来管理装置软件和服务跟踪的一些方面的一些实施例中，对装置服务完整性运行进一步检查，如代理查询响应。在存在授权来管理一个装置接入服务连接的一些实施例中，将错误消息发送到装置UI，暂停装置或将装置放置隔离路由上。在一些实施例中，将错误消息发送到人机界面以用于故障处理。
验证装置信誉或服务计划信誉	在记录上没有服务计划或装置未经授权	在一些实施例中，如果装置仍未用一个服务计划激活，则为UI提供激活顺序。在一些实施例中，如果装置未针对由服务控制器控制的网络上的服务而被授权，则向UI发送指导用户如何进行错误消息。在一些实施例中，为旨在针对该装置的环境服务配置服务处理软件。在一些实施例中，下载适于该装置的适合的服务代理器软件。

图 19D(3)

服务策略实施验证技术实施例	验证服务处理器代理的适当运行	策略实施代理、防火墙代理上的输入到输出事件。检查计费事件的报告来验证系统。用服务控制器的跳报告正确的代理完整性自检查、交叉检查以及响应顺序。	示例性错误触发条件实施例	示例性错误响应实施例
在一些实施例中，错误严重性和/或错误持续性性和/或其他错误的存在用来确定适合的响应或行动。在一些实施例中，重置服务策略并查看错误是否持续。在一些实施例中，执行代理设置检查来验证代理服务使用控制策略设置是正确的。在一些实施例中，运行动态代理加载，在一些情况下用对新代理码的差异化或加密、排序或模糊处理来刷新一个或多个代理。在一些实施例中，将一个用户查询或报告发送到UI来通知用户，确认装置是由用户拥有的，或使用户参与确定源或错误的过程，或来帮助验证基于装置的服务控制。在一些实施例中，装置标识号被放置在一个错误清单上以用于进一步错误处理。在一些实施例中，装置被放置在一个SPAN过程上、或一个类似的业务量为并且确定其是否与服务使用策略，略相一致。在一些实施例中，报告计费事件测试使用策略来确定装置被放置在隔离网络路由选择状态上，其中可能发送一个用户消息来通知用户。在一些实施例中，可能在向用户发送一个用户对过程的指令以用于校正错误并且恢复服务的一个消息之后，暂停装置发送到装置的一些实施例，作为对发送到一个替代的消息传送系统，如电子邮件或文本消息传送而发送。在一些实施例中，将一个错误消息发送到网络中的一个个人机界面以用于进一步故障处理。				

图 19E(1)

服务策略实施验证技术实施例	示例性错误触发条件实施例	示例性错误响应实施例
服务处理器心跳响应报告	心跳报告中的一个或多个指示运行、配置或篡改和错误防止系统中的一个错误。心跳功能未正确地起作用，但装置仍指示网络上的服务使用。	在一些实施例中，错误严重性和/或错误持续性和/或其他错误的存在用来确定适合的响应或行动。在一些实施例中，重置服务策略并且观看错误是否持续。在一些实施例中，执行代理设置检查来验证代理服务使用控制策略设置是正确的。在一些实施例中，执行代理查询/响应来确定对新代理码的差异化加密、排序或模糊处理来刷新一个或多个代理。在一些实施例中，将一个用户查询或报警发送到UI来通知用户，确认装置是由用户拥有的，或使用用户参与确定源或错误的过程中，或来辅助验证基于装置的服务控制。在一些实施例中，装置标识号被放在一个错误清单上以用于进一步错误处理。在一些实施例中，装置被放在一个SPAN过程上、或一个类似的业务量或服务检验过程、或另一个服务使用监视状态上来紧密地监控服务行为并且确定其是否与是正的服务使用策略一致。在一些实施例中，执行一个计费事件测试或一个服务使用测试来确定装置是否正确地报告计费事件或服务使用事件。在一些实施例中，装置被放置在隔离网络路由选择状态上，其中可能发送一个用户消息来通知用户。在一些实施例中，可能在向用户发送可以包括对过程的指令以用于校正错误并且恢复服务的一个消息之后，暂停装置服务。在一些实施例中，作为对发送到装置的一个消息的替代物或除发送到装置的消息之外，这些用户消息通过一个替代的消息传送系统，如电子邮件或文本消息传送而发送。在一些实施例中，将一个错误消息发送到网络中的一个界面而用于进一步错误分析。

图 19E(2)

服务策略实施验证技术实施例	示例性错误触发条件实施例	示例性错误响应实施例
测试服务事件	服务使用报告系统未正确地报告测试服务使用事件	在一些实施例中，运行动态代理加载，在一个或多个代理的情况下用对新代理码的差异加密、排序或模糊处理来刷新一个代理。如果这没有清除错误，或如果这不是所采用的错误校正方法，则执行以下行动中的一项或多项：在一些实施例中，重置服务策略并且观看错误是否持续。在一些实施例中，执行代理设置检查来验证代理服务使用控制策略设置是正确的。在一些实施例中，执行代理查询/响应来确认代理完整性。在一些实施例中，将一个用户查询或报警发送到UI来通知用户，或确认装置是由用户拥有的，或使用用户参与确定或错误的过程中，或来辅助验证基于装置的服务控制。在一些实施例中，装置标识号被放置在一个错误清单上以用于进一步错误处理。在一些实施例中，装置被放置在一个SPAN过程上、或一个类似的业务量或服务检验过程、或另一个服务使用监视状态上来紧密地监控服务行为并且确定其是否与旨在是正确的服务使用策略相一致。在一些实施例中，执行一个计费测试来确定装置是否正报告计费事件。在一些实施例中，装置被放置在隔离网络路由选择状态上，其中可能发送一个用户消息来通知用户。在一些实施例中，可能在向用户发送可以包括对过程的指令以用于校正错误并且恢复服务的一个消息之后，暂停装置服务。在一些实施例中，作为对发送到装置的一个消息的替代物或发送到装置的消 息之外，这些消息通过一个替代的消息传递系统，如电子邮件或文本消息传递而发送。在一些实施例中，将一个错误消息发送到网络中的一个个人界面以用于进一步错误分析。

图 19E(3)

服务策略实施验证技术实施例	示例性错误触发条件实施例	示例性错误响应实施例
加载一个最近版本的服务处理软件并且执行完整性报告	在加载新近的接入控制完整代理之后，代理发现其他代理中的一个或多个损坏。	运行动态代理加载，在一些情况下用对新代理码的差异加密、排序或模糊处理来刷新其他代理并且观看问题是否持续。如果这没有清除错误，或如果这不是所采用的错误校正方法，则执行以下行动中的一项或多项：在一些实施例中，重置服务策略并且观看错误是否持续。在一些实施例中，执行代理验证来验证代理服务使用控制策略设置是正确的。在一些实施例中，将一个用户查询或报警发送到UI来通知用户，确认装置是由用户拥有的，或使用户参与确定源或错误的过程中，或来帮助验证基于装置的服务控制。在一些实施例中，装置标识号被放置在一个错误清单上以用于进一步错误处理。在一些实施例中，装置被放置在一个SPAN过程上，或一个类似的业务量或服务检验过程、或另一个服务使用监视状态上来紧密地监控服务行为并且确定其是否与一个计费事件或服务使用测试一致。在一些实施例中，执行一个计费事件或服务使用测试来确定装置是否正确地报告计费事件或服务使用事件。在一些实施例中，装置被放置在隔离网络路由选择状态上，其中可能发送一个用户消息来通知用户。在一些实施例中，可能在向用户发送时包括对过程的指令以用于校正错误并且恢复服务的一个消息之后，暂停装置服务。在一些实施例中，作为对发送到装置的一个消息的替代物或删除发送到装置的消息之外，这些用户消息通过一个替代的消息传送系统，如电子邮件或文本消息传送而发送。在一些实施例中，将一个错误消息发送到网络中的一个界面以用于进一步错误分析。

图 19F(1)

服务策略实施验证技术实施例	示例性错误触发条件实施例	示例性错误响应实施例
用代理自诊断检查来验证服务处 理器配置	在运行一个自检之后，代理中的一个或多个指示一个错误。	运行动态代理加载，在一些情况下用对新代理码的差异加密、排序或模糊处理来刷新其他代理并且观看问题是否持续。如果这没有清除错误，或如果这不是所采用的错误校正方法，则执行以下行动中的一项或多项：在一些实施例中，重置服务策略并且观看错误是否持续。在一些实施例中，执行代理设置检查来验证代理服务使用控制策略设置是正确的。在一些实施例中，将一个用户查询或报警发送到UI来通知用户，或来辅助验证基于装置的服务控制。在一些实施例中，装置标识号被放置在一个错误清单上以用于进一步错误处理。在一些实施例中，装置被放置在一个SPAN过程上、或一个类似的业务量或服务检验过程、或另一个服务使用监视状态上来紧密地监控服务行为并且确定其是否与旨在是正确的服务使用策略相一致。在一些实施例中，执行一个计费事件或服务使用事件。在一些实施例中，装置被放置在隔离网络路由选择状态上，其中可能发送一个用户消息来通知用户。在一些实施例中，可能在向用户发送可以包括对过程的指令以用于校正错误并且恢复服务的一个消息之后，暂停装置服务。在一些实施例中，作为对发送到装置的一个消息的替代物或除发送到装置的消息之外，这些用户消息通过一个替代的消息传送系统，如电子邮件或文本消息传送而发送。在一些实施例中，将一个错误消息发送到网络中的一个人机界面以用于进一步错误分析。

图 19F(2)

服务策略实施验证技术实施例	示例性错误触发条件实施例	示例性错误响应实施例
验证装置仅在授权之后使用服务	装置接入网络并且没有用接入控制策略完整性服务来登记，并且服务度量指示装置在网络上。	在一些实施例中，重置服务策略并且观看错误是否持续。在一些实施例中，执行代理检查来验证代理策略使用控制策略设置是正 确的。在一些实施例中，执行代理查询/响应来确定代理完整性。在 一些实施例中，运行动态刷新一个或多个代理。在一些实施例中 差异加密、排序或模糊处理来刷新一个或多个代理。在实施例 中，将一个用户查询或报警发送到UI来通知用户，确认装置是由用 户拥有的，或使用用户参与确定源或错误的过程中，或来辅助验证基 于装置的服务控制。在一些实施例中，装置标识号被放置在一个错 误清单上以用于进一步错误处理。在一些实施例中，装置被放置在一 个SPAN过程上、或一个类似的业务量或服务检验过程、或另一 个服务使用监视状态上来紧密地监控服务行为并且确定其是否与旨 在是正确的服务使用策略相一致。在一些实施例中，执行一个计费 事件测试或一个服务使用测试来确定装置是否正确地报告计费事 件或服务使用事件。在一些实施例中，装置被放置在隔离网络路由 选择状态上，其中可能发送一个用户消息来通知用户。在一些实施 例中，可能在向用户发送可以包括对过程的指令以用于校正错误并 且恢复服务的一个消息之后，暂停装置服务。在一些实施例中，作 为对发送到装置的一个消息的替代物或除发送到装置的消息之外， 这些用户消息通过一个替代的消息传送系统，如电子邮件或文本消 息传送而发送。在一些实施例中，将一个错误消息发送到网络中的 一个人机界面以用于进一步错误分析。

图 19F(3)

服务策略实施验证技术实施例	示例性错误触发条件实施例	示例性错误响应实施例
验证用户信誉	用户未用正确的响应来响应UI查询，如请求ID、密码或生物测定输入。这个过程可以为处理一个受怀疑错误的部分。	在一些实施例中，装置标识号被放置在一个错误清单上以用于进一步错误处理。在一些实施例中，装置被放置在一个SPAN过程上、或一个类似的业务量或服务检验过程、或另一个服务使用监视状态上来紧密地监控服务行为并且确定其是否与旨在是正确的服务使用策略相一致。在一些实施例中，装置被放置在隔离网络路由选择状态上，其中可能发送一个用户消息来通知用户。在一些实施例中，可能向用户发送一个消息以包括对过程的指令以用于校正错误并且恢复服务的一个消息之后，暂停装置服务。在一些实施例中，作为对发送到装置的一个消息的替代物或除发送到装置的消息之外，这些用户消息通过一个替代的消息传送系统，如电子邮件或文本消息传送到发送。在一些实施例中，将一个错误消息发送到网络中的一个界面以用于进一步错误分析。在一些实施例中，可以要求用户来确认一个服务过量通知和/或也提供一个密码、生物测定签名、硬件密钥或其他机制来验证服务过量确认应答。

图 19G(1)

服务策略实施验证技术实施例	示例性错误触发条件实施例	示例性错误响应实施例
代理通信日志	检测到与一个或多个代理的未授权的通信	在一些实施例中，执行代理查询/响应来确定代理完整性。在一些实施例中，运行动态代理加载，在一些情况下用对新代理码的差异加密、排序或模糊处理来刷新一个或多个代理。在一些实施例中，将一个用户查询或报警发送到UI来通知用户，确认装置是由用户拥有的，或使用用户参与确定或错误的过程中，或来辅助验证基于装置的服务控制。在一些实施例中，装置标识被放置在一个错误清单上以用于进一步错误处理。在一些实施例中，装置被放置在一个SPAN过程上、或一个类似的业务量或服务检验过程、或另一个服务使用监视状态上来紧密地监控服务行为并且确定其是否与旨在正确的服务路由选择状态上，其中可能发送一个用户消息来通知用户。在一些实施例中，可能在向用户发送一个消息之后，暂停装置服务。在一些实施例中，作为对发送用户消息的一个消息的替代物或除发送到装置的消息之外，这些用户消息通过一个替代的消息传送系统，如电子邮件或文本消息而发送。在一些实施例中，将一个错误消息发送到网络中的一个界面以用于进一步错误分析。

图 19G(2)

服务策略实施篡改或错误保护技术	示例性错误触发条件	示例性错误响应
检测或阻塞对服务处理器的运行潜在有害的装置联网活动。	在适合指示有害软件可能存在于装置上的已知模式的服务监控器报告中观察网络活动。	启动或安装并且启动根除软件。阻塞来自怀疑实体的业务量。在一些实施例中，如果软件不能被根除或阻塞，则将消息发送到UI并且暂停装置，将其放置在SPAN上，放置在监视清单上，放置在另外行动清单上或者放置在隔离网络上。在一些实施例中，将错误消息发送到人机界面用于进行故障处理。
检测或阻塞未授权的服务处理器软件加载。	接入控制完整性代理发现一个已知恶意清单上的软件。	与以上相同。
检测或阻塞对受保护的服务处理器软件或硬件存储器的未授权接入。	检测到未授权的接入，存储器内容损坏或无响应。	如果可能，识别已接入服务处理器的实体，并且根除。在一些实施例中，用动态代理加载，在一些情况下用对新代理码的差异加密、排序或模糊处理而修复任何受危害的代理。在一些实施例中，将消息发送到UI并且暂停装置，将其放置在SPAN上，放置在监视清单上，放置在另外行动清单上或者放置在隔离网络上。在一些实施例中，将错误消息发送到人机界面用于进行故障处理。

图 20A(1)

服务策略实施篡改或错误保护技术	示例性错误触发条件	示例性错误响应
检测或阻塞与服务处理器软件或硬件的未授权通信。	检测到未授权通信。	如果可能，识别已接入服务处理器的实体，并且根除。在一些实施例中，用动态代理加载，在一些情况下用对新代理码的差异加密、排序或模糊处理来修复任何受危害的代理。在一些实施例中，将消息发送到UI并且暂停装置，将其放置在SPAN上，放置在监视清单上，放置在另外行动清单上或者放置在隔离网络上。在一些实施例中，将错误消息发送到人机界面以用于进行故障处理。
具有签名的SW的安全负载器安装到受保护的存储器之中	检测到未授权的接入，存储器内容损坏或无响应。	如果可能，识别已接入服务处理器的实体，并且根除。在一些实施例中，用动态代理加载，在一些情况下用对新代理码的差异加密、排序或模糊处理而修复任何受危害的代理。在一些实施例中，将消息发送到UI并且暂停装置，将其放置在SPAN上，放置在监视清单上，放置在另外行动清单上或者放置在隔离网络上。在一些实施例中，将错误消息发送到人机界面以用于进行故障处理。
服务处理器代理之间的安全加密的通信。	安全通信链路错误或检测到未授权的接入。	如果可能，识别已接入服务处理器的实体，并且根除。在一些实施例中，用动态代理加载，在一些情况下用对新代理码的差异加密、排序或模糊处理而修复任何受危害的代理。在一些实施例中，运行动态代理加载，在一些情况下用对新代理码的差异加密、排序或模糊处理来刷新具有处于错误中的通信链路或整个服务处理器的代理。在一些实施例中，将消息发送到UI并且暂停装置，将其放置在SPAN上，放置在监视清单上，放置在另外行动清单上或者放置在隔离网络上。在一些实施例中，将错误消息发送到人机界面以用于进行故障处理。

图 20A(2)

服务策略实施篡改或错误保护技术	示例性错误触发条件	示例性错误响应
服务处理器与服务控制器之间的安全加密的通信。	服务处理器通信丢失。	将错误消息发送到装置UI (如果可能)，暂停装置，将其放置在SPAN上，放置在监视清单上，放置在另外行动清单上，或者将装置放置在隔离路由上。在一些实施例中，将错误消息发送到人机界面用于进行故障处理。
在安全存储器内的服务处理器软件件的执行。	检测到未授权的接入，存储器内容损坏或无响应。	如果可能，识别已接入服务处理器的实体，并且根据除。在一些实施例中，用动态代理加载，在一些情况下用对新代理码的差异化加密、排序或模糊处理而修复任何受危害的代理。在一些实施例中，将消息发送到UI并且暂停装置，将其放置在SPAN上，放置在监视清单上，放置在另外行动清单上，或者将装置在隔离网络上。在一些实施例中，将错误消息发送到人机界面用于进行故障处理。

图 20A(3)

服务策略实施篡改或错误保护技术	示例性错误触发指标条件	示例性错误响应
在安全存储设备中的服务处理软件 的存储	安全存储设备违反或储存在非安全存储设备中的服务处理	如果可能, 识别已接入服务处理器的实体, 并且根除。在一些实施例中, 用动态代理加载, 在一些情况下用对新代理的差异化加密、排序或模糊处理而修复任何受危害的代理。在一些实施例中, 将消息发送到UI并且暂停装置, 将其放置在SPAN上, 放置在监视网络上, 放置在另外行动清单上, 或者放置在隔离网络上。在一些实施例中, 将错误消息发送到人机界面用于进行故障处理。
检测或移除被认为是服务处理 器运行有害的软件。	检测到未授权软件。	启动或安装并且启动根除软件。阻塞来自怀疑实体的业务量。在一些实施例中, 如果软件不能够被根除或阻塞, 则将消息发送到UI并且暂停装置, 将其放置在SPAN上, 放置在监视网络上, 放置在另外行动清单上, 或者放置在隔离网络上。在一些实施例中, 将错误消息发送到人机界面用于进行故障处理。
记录并且报告软件加载签名、软件 活动签名或网络活动签名以用于威胁 顺序的稍后识别。	检测到未授权软件或恶意网络活动。	与以上相同。
将关键的服务处理软件实施为通过 运行自我审计和重新安装过程, 如将 审计功能放置在不可接入的存储设备或 OS功能或基本输入输出系统中而抵抗 消息损坏的一个自刷新程序。	重新安装功能报警: 需要重新安装。连续重新安装或未能重新安装报警增加了报警的严重性。	如果可能, 识别已接入服务处理器的实体, 并且根除。在一些实施例中, 将报文消息发送到UI并且暂停装置, 将其放置在SPAN上, 放置在监视网络上, 放置在另外行动清单上, 或者放置在隔离网络上。在一些实施例中, 将错误报文消息发送到人机界面用于进行故障处理。

图 20B(1)

服务政策策略实施篡改或错误保护技术	示例性错误触发指标条件	示例性错误响应
加密的代理码	代码检查、代理查询--响应、代理自检或其他代理配置检查发现代码加密中的错误	在一些实施例中，用动态代理加载，在一些情况下对新代理码的差异加密、排序或模糊处理而修复任何受危害的代理。在一些实施例中，将消息发送到UI并且暂停装置，放置在SPAN上，放置在监视清单上，放置在另外行清单上或者放置在隔离网络上。在一些实施例中，将错误消息发送到人机界面用于进行故障处理。如果可能，识别可能已接入服务处理器的实体并且根除。
被模糊处理的代理码	代码检查、代理查询--响应、代理自检或其他代理配置检查发现代码模糊处理中的错误	与以上相同。
唯一代理标识号和签名	发现代理具有不正确的ID或未签名	与以上相同。
安全代理通信总线	代理通信总线监控发现未授权的通信，或发现到一个或多个代理的其他未授权的接入。	与以上相同。
代理等级消息加密	代理被发现在没有代理通信加密所需等级的情况下进行通信	与以上相同。

图 20B(2)

服务策略实施篡改或错误保护技术	示例性错误触发指标条件	示例性错误响应
服务控制链路消息等级加密	在服务控制链路上发现未授权的通信业务量	在一些实施例中，用动态代理加载，在一些情况下用对新代理码的差异加密、排序或模糊处理而修复任何受危害的代理。在一些实施例中，将消息发送到UI并且暂停装置，放置在SPAN上，放置在监视清单上，放置在另外行动清单上或者放置在隔离网络上。在一些实施例中，将错误消息发送到人机界面用于进行故障处理。如果可能，识别可能已接入服务处理器的实体，并且根除。
服务控制链路传输层加密	在服务控制链路上发现未授权的通信业务量	与以上相同。
代理通信接入许可	用一个或多个代理发现未授权的通信	与以上相同。
代理通信日志	用一个或多个代理发现未授权的通信	与以上相同。
用于下载的加密的代理码	代理下载被发现具有不正确的或没有加密或签名	与以上相同。
安全下载器存储器	未授权的接入或存储在安全下载器存储器中被发现	与以上相同。

图 20C

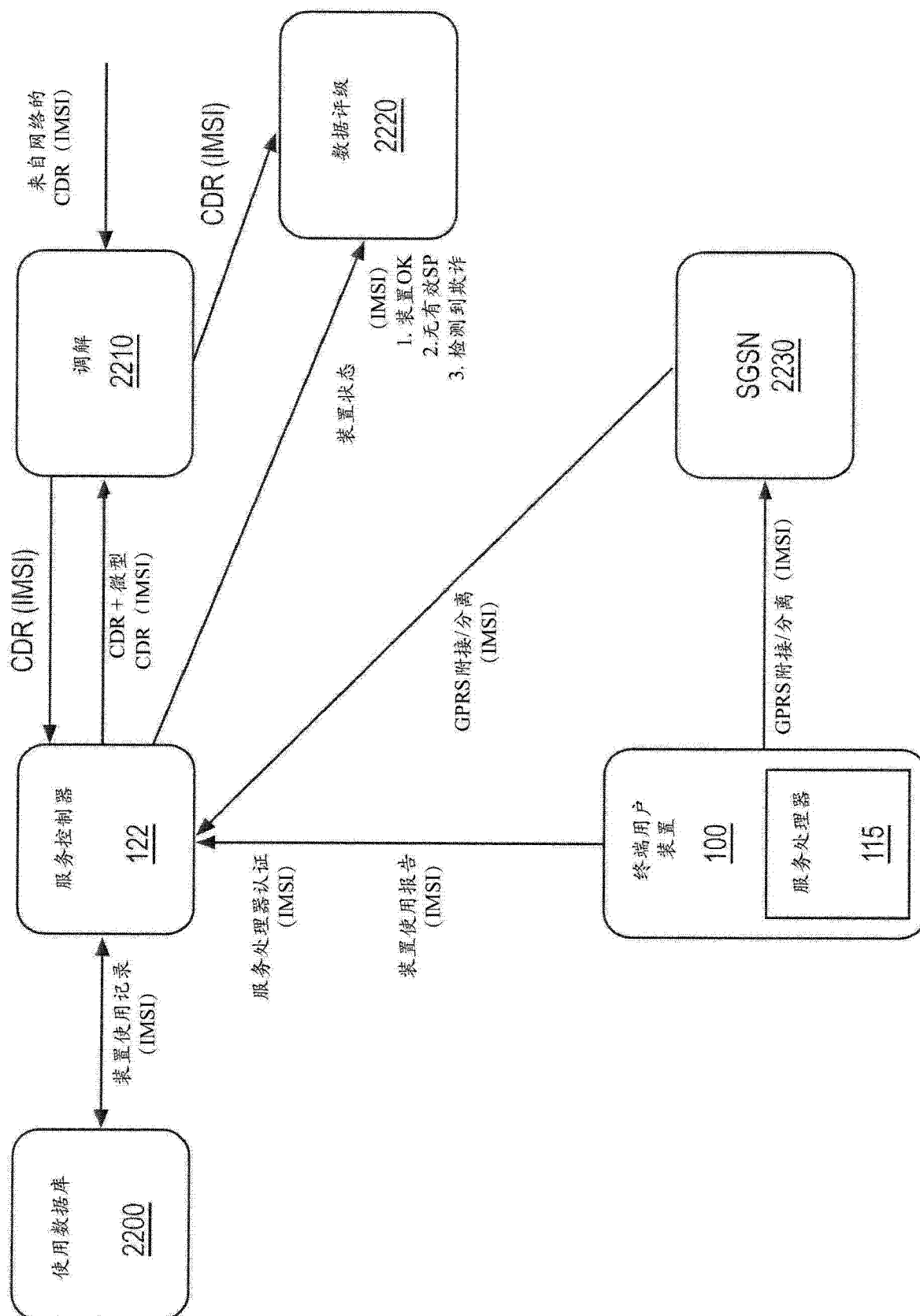


图 21

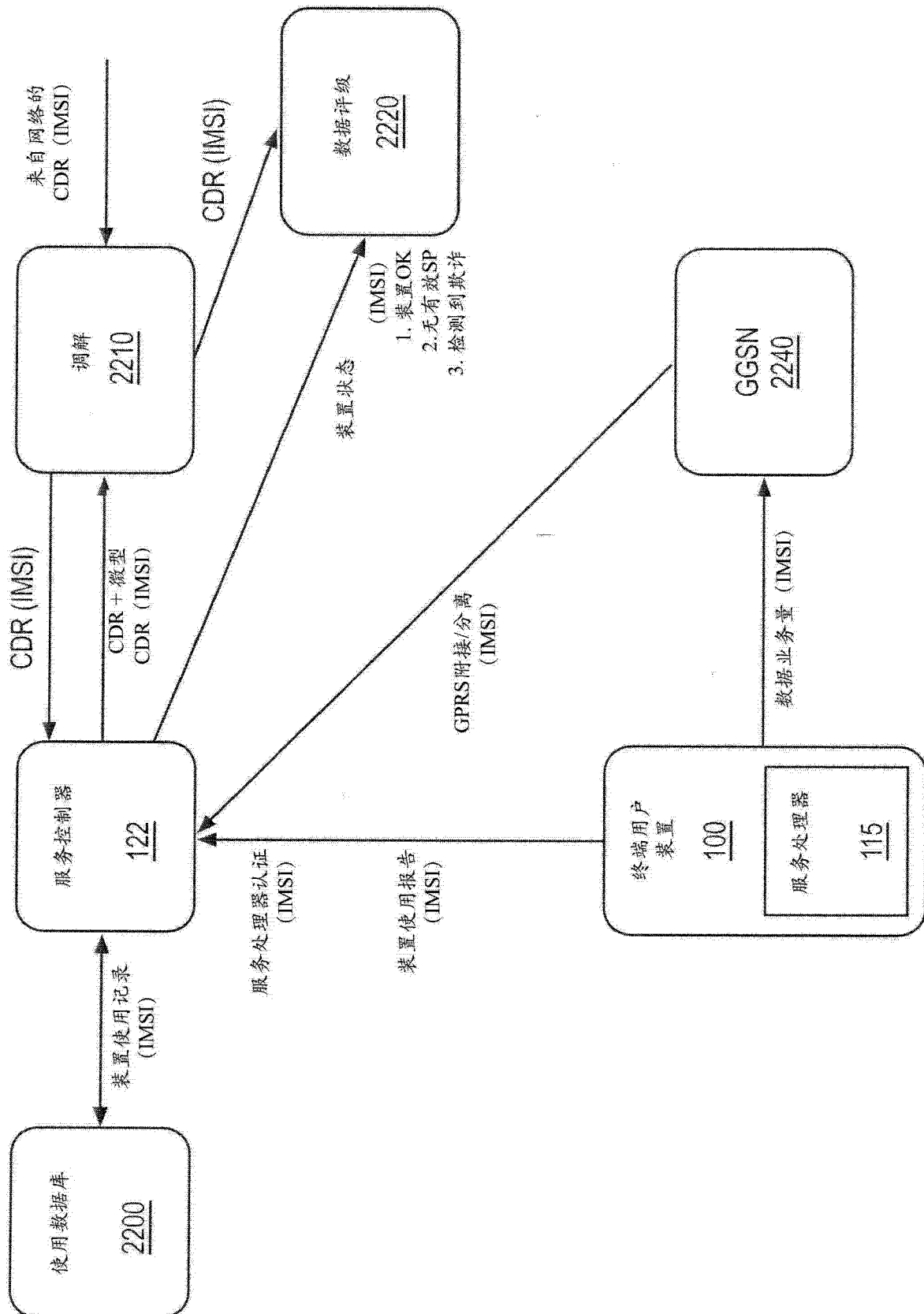


图 22

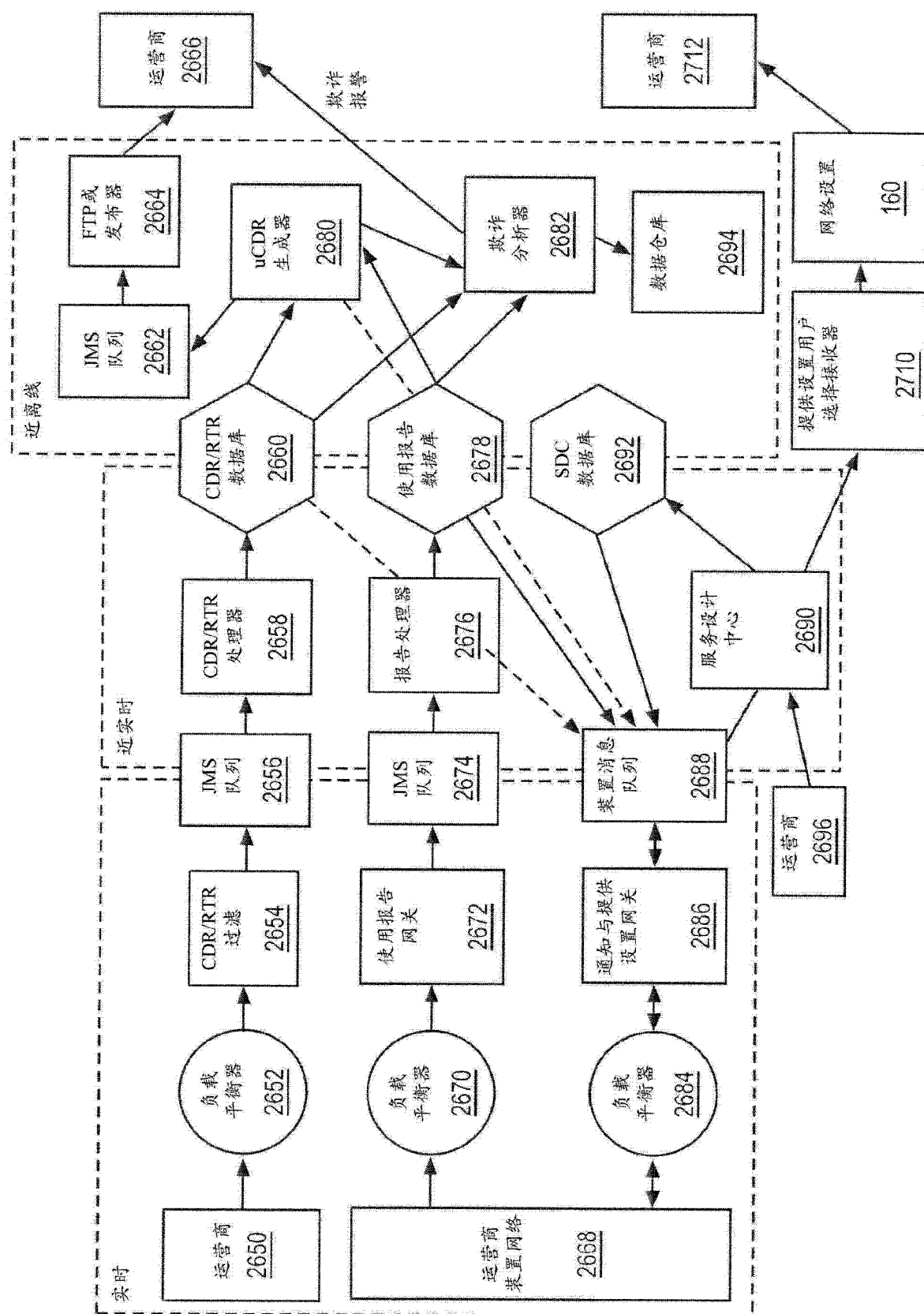


图 23

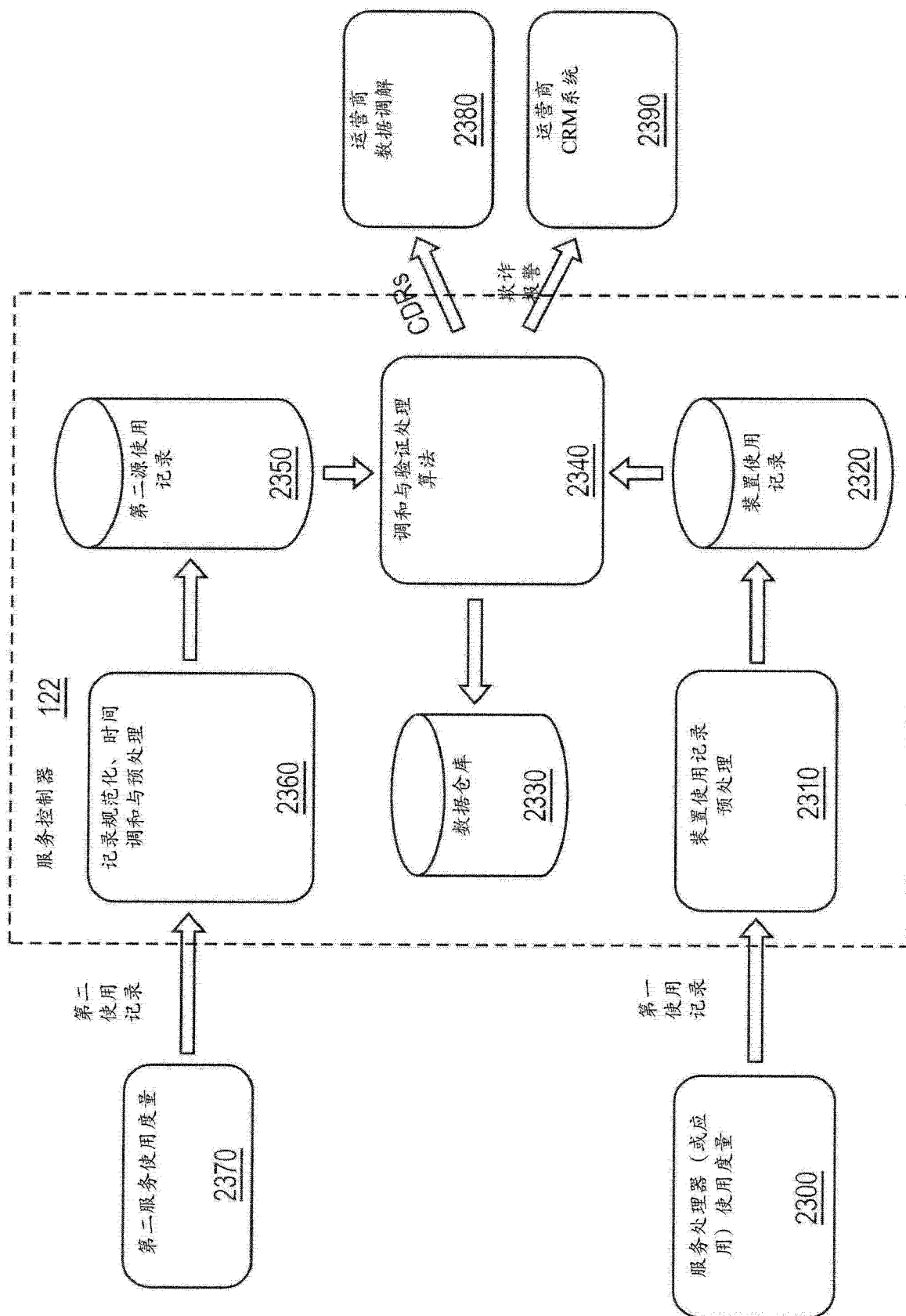


图 24

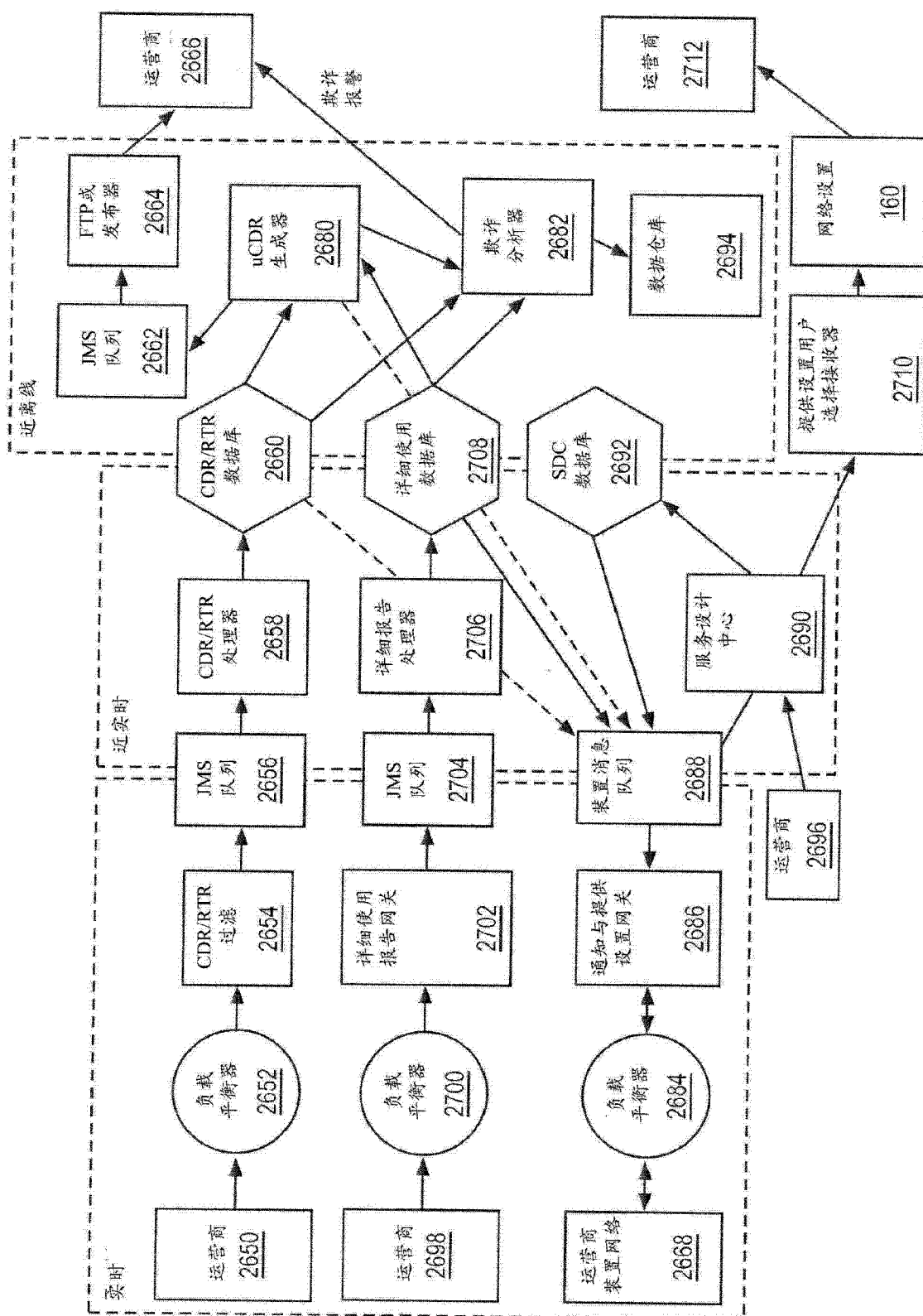


图 25