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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 April 2012 (12.04.2012)

PCT

(10) International Publication Number
WO 2012/047275 A1

(51) International Patent Classification:
G06F 17/00 (2006.01)

(21) International Application Number:
PCT/US2011/001683

(22) International Filing Date:
28 September 2011 (28.09.2011)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/387,243 28 September 2010 (28.09.2010) US
61/422,565 13 December 2010 (13.12.2010) US

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

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **RALEIGH, Gregory, G.** [US/US]; 131 Fox Hollow Road, Woodside, CA 94062 (US). **RAISSINIA, Alireza** [US/US]; 15147 Elm Park, Monte Sereno, CA 95030 (US). **GREEN, Jeffrey** [US/US]; 1381 Arleen Avenue, Sunnyvale, CA 94087 (US).

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

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

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

Published:

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

(54) **Title**: ENTERPRISE ACCESS CONTROL AND ACCOUNTING ALLOCATION FOR ACCESS NETWORKS

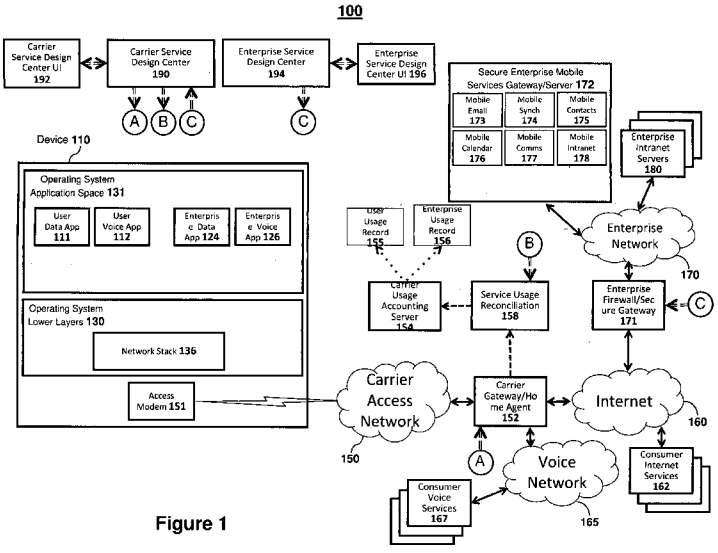

Figure 1

(57) **Abstract**: Enterprise and consumer billing allocation for wireless communication device service usage activities is provided. In some embodiments, enterprise and consumer billing allocation for wireless communication device service usage activities includes monitoring a service usage activity of a wireless communication device, and determining an enterprise and consumer billing allocation for the monitored service usage activity. In some embodiments, enterprise and consumer billing allocation for wireless communication device service usage activities includes monitoring a service usage activity of a wireless communication device, and reporting the monitored service usage activity to a network element, in which the network element determines an enterprise and consumer billing allocation for the monitored service usage activity.

WO 2012/047275 A1

ENTERPRISE ACCESS CONTROL AND ACCOUNTING ALLOCATION FOR ACCESS NETWORKS

BACKGROUND

[0001] With the advent of mass market digital communications and content distribution, many access networks such as wireless networks, cable networks and DSL (Digital Subscriber Line) networks are pressed for user capacity, with, for example, EVDO (Evolution-Data Optimized), HSPA (High Speed Packet Access), LTE (Long Term Evolution), WiMax (Worldwide Interoperability for Microwave Access), and Wi-Fi (Wireless Fidelity) wireless networks increasingly becoming user capacity constrained. Although wireless network capacity will increase with new higher capacity wireless radio access technologies, such as MIMO (Multiple-Input Multiple-Output), and with more frequency spectrum being deployed in the future, these capacity gains are likely to be less than what is required to meet growing digital networking demand.

[0002] Similarly, although wire line access networks, such as cable and DSL, can have higher average capacity per user, wire line user service consumption habits are trending toward very high bandwidth applications that can quickly consume the available capacity and degrade overall network service experience. Because some components of service provider costs go up with increasing bandwidth, this trend will also negatively impact service provider profits.

BRIEF DESCRIPTION OF THE DRAWINGS

[0003] Various embodiments of the invention are disclosed in the following detailed description and the accompanying drawings.

[0004] **Figure 1** illustrates a functional diagram of a network architecture for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments.

[0005] **Figure 2** illustrates a functional diagram of another network architecture for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments.

[0006] **Figure 3** illustrates a functional diagram of another network architecture for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments.

[0007] **Figure 4** illustrates a functional diagram of another network architecture for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments.

[0008] **Figure 5** illustrates a functional diagram of another network architecture for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments.

[0009] **Figure 6** illustrates a functional diagram of another network architecture for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments.

[0010] **Figure 7** illustrates a functional diagram of another network architecture for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments.

[0011] **Figure 8** illustrates a functional diagram of another network architecture for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments.

[0012] **Figure 9** illustrates a functional diagram of another network architecture for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments.

[0013] **Figure 10** illustrates a functional diagram of another network architecture for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments.

[0014] **Figure 11** illustrates a functional diagram of another network architecture for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments.

[0015] **Figure 12** illustrates a functional diagram of another network architecture for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments.

[0016] **Figure 13** illustrates a functional diagram of a secure device application architecture for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments.

[0017] **Figure 14** illustrates a functional diagram of another secure device virtual machine architecture for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments.

[0018] **Figure 15** illustrates a functional diagram of another secure device hardware execution partition architecture for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments.

[0019] **Figure 16** illustrates a functional diagram of another secure device service processor architecture for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments.

[0020] **Figure 17** illustrates a functional diagram of another network architecture for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments.

[0021] **Figure 18** illustrates a functional diagram of another network architecture for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments.

[0022] **Figure 19** illustrates a functional diagram of another network architecture for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments.

[0023] **Figure 20** illustrates a functional diagram of another network architecture for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments.

[0024] **Figure 21** illustrates a functional diagram of another network architecture for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments.

[0025] **Figure 22** illustrates a functional diagram of another network architecture for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments.

[0026] **Figure 23** illustrates a functional diagram of a secure device application architecture with device based service usage monitoring for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments.

[0027] **Figure 24** illustrates a functional diagram of a secure device virtual machine architecture with device based service usage monitoring for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments.

[0028] **Figure 25** illustrates a functional diagram of a secure device hardware execution partition architecture with device based service usage monitoring for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments.

[0029] **Figure 26** illustrates a functional diagram of a secure device service processor architecture with device based service usage monitoring for providing enterprise and consumer

billing allocation for wireless communication device service usage activities in accordance with some embodiments.

[0030] **Figure 27** illustrates a flow diagram for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments.

[0031] **Figure 28** illustrates another flow diagram for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments.

[0032] **Figure 29** illustrates another flow diagram for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments.

[0033] **Figure 30** illustrates another flow diagram for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments.

DETAILED DESCRIPTION

[0034] The invention can be implemented in numerous ways, including as a process; an apparatus; a system; a composition of matter; a computer program product embodied on a computer readable storage medium; and/or a processor, such as a processor configured to execute instructions stored on and/or provided by a memory coupled to the processor. In this specification, these implementations, or any other form that the invention may take, may be referred to as techniques. In general, the order of the steps of disclosed processes may be altered within the scope of the invention. Unless stated otherwise, a component such as a processor or a memory described as being configured to perform a task may be implemented as a general component that is temporarily configured to perform the task at a given time or a specific component that is manufactured to perform the task. As used herein, the term 'processor' refers to one or more devices, circuits, and/or processing cores configured to process data, such as computer program instructions.

[0035] A detailed description of one or more embodiments of the invention is provided below along with accompanying figures that illustrate the principles of the invention. The invention is described in connection with such embodiments, but the invention is not limited to any embodiment. The scope of the invention is limited only by the claims and the invention encompasses numerous alternatives, modifications and equivalents. Numerous specific details are set forth in the following description in order to provide a thorough understanding of the invention. These details are provided for the purpose of example and the invention may be practiced according to the claims without some or all of these specific details. For the purpose of clarity, technical material that is known in the technical fields related to the invention has not been described in detail so that the invention is not unnecessarily obscured.

[0036] Some enterprises only allow certain specialized wireless devices to be used for connection to their enterprise network. Such devices typically contain secure data storage and enterprise program execution environments to protect enterprise information and network access. This approach is generally directed towards maintaining enterprise data integrity and enterprise network security. However, this approach does not address the various problems associated with allocating service usage or billing between consumer or non-enterprise service usage activities and enterprise service usage activities.

[0037] Accordingly, there is a need to provide for an enterprise and consumer billing allocation for wireless communication device service usage activities. There is also a need to address various issues with enterprise policies that can vary from employee to employee. For example, roaming policies can be configured differently for a global sales person than for a finance administrator who does not travel as much on enterprise business. Furthermore, some enterprises may not elect to pay for employee wireless communication device purchase or all employee wireless communication service usage needs or desires. As a result, some enterprises would benefit from techniques that allowed such enterprises to piggy back on consumer device or service purchases while maintaining an enterprise and consumer billing allocation for wireless communication device service usage activities.

[0038] Also, some consumers prefer to select their own wireless communication device that may not be an enterprise approved wireless communication device or a specialized enterprise device specified by enterprise IT managers. For example, certain enterprises may only offer certain Blackberry smart phone devices, and certain employees may prefer Apple iPhone and/or various Android based smart phone devices. Another trend suggests that a growing number of enterprise employees desire to use a single wireless communication device for their enterprise mobile communication, enterprise information access, and enterprise network access as well as for, for example, their personal mobile communication, access, and application needs (e.g., consumer/personal, that is, non-enterprise, use of cellular calls, text messaging, web browsing, social networking, games, and various other service usage activities). Such dual persona devices, where a first persona is oriented to enterprise access and/or application needs and a second persona is oriented to personal access and/or application needs, are enabled by the disclosure herein.

[0039] As a result, enterprise network managers generally need a way to safely allow consumers to perform consumer mobile access services that the enterprise can specify that will not be paid for by the enterprise. Various network architectures and techniques are described herein that allow an enterprise to determine how much service usage (e.g., how much of a corresponding service bill) should be allocated to device user services or consumer services and how much should be allocated to enterprise services in which the enterprise sponsors the enterprise access. Various design approaches and techniques are described herein for allocating enterprise and consumer billing in a secure manner that works with both specialized enterprise wireless communication devices as well as other wireless communication devices.

For example, crediting a user bill with sponsored enterprise service usage is provided using various techniques described herein. As another example, providing enterprise employee reimbursement for enterprise services used on the employee wireless communication device or allowing an enterprise to deduct employee consumer service usage from their paycheck is provided using various techniques described herein. As yet another example, allowing a consumer to select from an instant activation platform on a wireless communication device that comes pre-loaded with various enterprise services is provided using various techniques described herein. As yet a further example, providing for a capability to install or download an enterprise application that provides secure enterprise mobile services access and allocating enterprise and consumer billing for consumer wireless communication devices is provided using various techniques described herein.

[0040] Various techniques for monitoring service usage and providing for secured and verifiable device assisted services (DAS), including DAS based service usage monitoring, are disclosed in co-pending U.S. Patent Application No. 12/380,758 (Attorney Docket No. RALEP003), entitled VERIFIABLE DEVICE ASSISTED SERVICE USAGE MONITORING WITH REPORTING, SYNCHRONIZATION, AND NOTIFICATION, filed on March 2, 2009, published as U.S. Pub. App. No. 20100191612, co-pending U.S. Patent Application No. 12/695,019 (Attorney Docket No. RALEP022), entitled DEVICE ASSISTED CDR CREATION, AGGREGATION, MEDIATION and BILLING, filed on January 27, 2010, published as U.S. Pub. App. No. 20100197266, co-pending U.S. Patent Application No. 12/695,020 (Attorney Docket No. RALEP024), entitled ADAPTIVE AMBIENT SERVICES, filed on January 27, 2010, published as U.S. Pub. App. No. 20100198698, co-pending U.S. Patent Application No. 12/694,445 (Attorney Docket No. RALEP025), entitled SECURITY TECHNIQUES FOR DEVICE ASSISTED SERVICES, filed on January 27, 2010, published as U.S. Pub. App. No. 20100199325, co-pending U.S. Patent Application No. 12/694,451 (Attorney Docket No. RALEP026), entitled DEVICE GROUP PARITIONS AND SETTLEMENT PLATFORM, filed on January 27, 2010, published as U.S. Pub. App. No. 20100197267, which are incorporated herein by reference for all purposes.

[0041] In some embodiments, allocating enterprise and consumer billing for service usage activities on a wireless communication device is provided for service usage activities that an enterprise configures as approved and/or sponsored for enterprise billing (e.g., such service usage activities are paid for at least in part by the enterprise) and consumer applications and

service usage activities that the device user chooses to use from the wireless communication device and that the enterprise does not sponsor. Various embodiments are disclosed herein describing a wide range of devices that users and enterprises may desire to use for such dual-purpose application scenarios. In some embodiments, devices for such applications can include a less specialized and secure device program execution environment as further described herein.

[0042] Accordingly, enterprise and consumer billing allocation for wireless communication device service usage activities is provided. In some embodiments, enterprise and consumer billing allocation for wireless communication device service usage activities includes monitoring a service usage activity of a wireless communication device (e.g., the monitoring can be performed in the wireless communication device and/or the monitoring of enterprise application service usage can be performed using a secure application server in the enterprise network), and determining an enterprise and consumer billing allocation for the monitored service usage activity. In some embodiments the allocation is determined by classifying the service usage activities as associated with a consumer service usage activity (e.g., in a consumer service usage activity list) or associated with an enterprise service usage activity (e.g., in an enterprise service usage activity list; or, as another example, if the monitored service usage activity is not included in the enterprise service usage activity list, then it can be automatically classified as a consumer service usage activity by default).

[0043] In some embodiments, enterprise and consumer billing allocation for wireless communication device service usage activities includes providing a service design center (SDC) for configuring an enterprise and consumer billing allocation of monitored service usage activities for a plurality of wireless communication devices associated with an enterprise account, and implementing the configured enterprise and consumer billing allocation for monitored service usage activities for the plurality of wireless communication devices associated with the enterprise account.

[0044] In some embodiments, enterprise and consumer billing allocation for wireless communication device service usage activities includes monitoring service usage of a wireless communication device, and determining whether a user is acting as a consumer (e.g., personal service usage activities on the wireless communication device) or a professional (e.g., enterprise service usage activities on the wireless communication device, that is, the user is

working on the wireless communication device in his or her capacity as an employee for an enterprise, in which the wireless communication device is associated with an enterprise account for the enterprise) based on the monitored service usage activity (e.g., based on place, time of day, application or service activity, and/or other criteria or factors). In some embodiments, enterprise and consumer billing allocation for wireless communication device service usage activities differentially charges and/or allocates billing between the enterprise and the consumer based on a classification of the monitored service usage activity as allocated to the enterprise or to the consumer for billing/charging purposes. Such embodiments enable a dual persona device user experience.

[0045] In some embodiments, enterprise and consumer billing allocation for wireless communication device service usage activities includes monitoring a service usage activity of a wireless communication device, and reporting the monitored service usage activity to a network element (e.g., a service controller, a service usage reconciliation function, another service control or billing/charging function in the network, or another network element), in which the network element determines an enterprise and consumer billing allocation for the monitored service usage activity. In some embodiments, the network element (e.g., a service controller, a service usage reconciliation function, another service control or billing/charging function in the network, or another network element) determines an enterprise and consumer billing allocation for the monitored service usage activity. In some embodiments, a service usage reconciliation function determines how much service usage is due to enterprise service usage activities and how much is due to consumer service usage activities. In some embodiments, after determining the allocation between consumer and enterprise service usage activities, the service usage reconciliation function provides the information to a service usage accounting function (e.g., a carrier billing server or an enterprise service usage accounting server), which in turn delivers a consumer usage report or bill and/or an enterprise usage report or bill. In some embodiments, the service usage reconciliation function determines the amount of enterprise service usage and creates a service usage credit record so that a device user's account can be credited or a device user can be compensated or reimbursed for enterprise service usage costs. In some embodiments, a service usage monitor is configured to monitor service usage activities of a device. In some embodiments, the service usage monitor is configured to classify the monitored service usage activities as enterprise service usage activities. In some embodiments, the service usage monitor is configured to classify the monitored service usage activities as consumer service usage activities. In some embodiments,

the service usage monitor is configured to monitor a first group of service usage activities for service usage allocation to a device user (e.g., using a list of service usage activities associated with a consumer service usage), and a second group of service usage activities for service usage allocation to an enterprise (e.g., using a list of service usage activities associated with an enterprise service usage). In some embodiments, service usage activities (e.g., service activities, such as applications, network, and/or voice based activities that use wireless network service usage resources) are classified using various techniques described herein, such as based on application (e.g., application credential), device (e.g., device credential), time of day, network destination, network traffic protocol and/or port, and various other criteria/factors. In some embodiments, the service usage monitor is implemented in the network (e.g., on one or more network elements in the carrier network and/or enterprise network, as described herein). In some embodiments, the service usage monitor is implemented in the device (e.g., using various techniques described herein, including verifiable and/or secured device-based implementations). In some embodiments, the service usage monitor is implemented using both network-based and device-based techniques, as described herein with respect to various embodiments.

[0046] In some embodiments, a set of service activities that will be sponsored by an enterprise (e.g., a specified or configured list of enterprise sponsored service activities) is managed by an enterprise service design center. In some embodiments, a list of service activities and the associated service policies for each service activity are compiled to form an enterprise sponsored service activity policy set. For example, enterprise email, enterprise calendar, and enterprise contacts can be configured as sponsored service activities. In some embodiments, the sponsored enterprise services list includes a list of network destinations that are associated with the services (e.g., an enterprise mail server address and/or an enterprise internal corporate network). For example, the enterprise email can be a sponsored service that is associated with an enterprise sponsored email service policy, which can limit destinations for corporate email, sizes of emails and/or email attachments, and/or other email related usage criteria or factors (e.g., a service usage charging policy).

[0047] In some embodiments, the monitored service usage is reported to the reconciliation function by a carrier network service usage monitoring element (e.g., a home agent (HA), access network gateway, or other network element, such as a deep packet inspection (DPI) function). In some embodiments, the monitored service usage is reported to the reconciliation

function by an enterprise network service usage monitoring element (e.g., a carrier network gateway or a mobile services gateway/server or other element in the enterprise network that can measure service usage and associate it with a given device credential or application credential). In some embodiments, the monitored service usage is reported to the reconciliation function by an element in the mobile device (e.g., a service usage monitor in a secure enterprise mobile services application or a Service Processor function, which can be securely implemented and/or verified using various techniques described herein).

[0048] In some embodiments, a service design center for implementing enterprise and consumer billing allocation for wireless communication device service usage activities is provided. For example, an enterprise manager can use the service design center to select one or more services that the enterprise agrees to pay for/is responsible for paying for and to select one or more other services that the employees of the enterprise must agree to pay for/are responsible for paying for (e.g., if the employee elects to use/have such services that are not charged to the enterprise, or included as enterprise services that are charged to or paid for by the enterprise).

[0049] In some embodiments, a service design center that facilitates configuration of sponsored enterprise services for implementing enterprise and consumer billing allocation for wireless communication device service usage activities is provided. In some embodiments, a service design center for implementing enterprise and consumer billing allocation for wireless communication device service usage activities includes providing a service design center for a carrier network and another service design center for an enterprise network (e.g., in some cases, these service design centers can be combined).

[0050] In some embodiments, an enterprise sponsored service activity policy set is created by an enterprise network administrator through an enterprise service design center user interface (UI). In some embodiments, the enterprise sponsored service activity policy set includes a list of network destination addresses that corresponds to the desired sponsored service activity list, along with an access policy or service usage charging policy for the service activities. In some embodiments, all service activities in the enterprise sponsored service activity policy set receive the same access policies or charging policies. In some embodiments, a first subset of one or more of the service activities in the enterprise sponsored service activity policy set receive access policies or charging policies that are different than

that of a second subset of service activities. For example, a sponsored enterprise email service can be in the first subset, and sponsored mobile voice services can be in the second subset, as certain employees (e.g., traveling sales personnel and/or executives) can be granted international and/or roaming mobile voice services, and other employees can be granted more limited sponsored mobile voice services.

[0051] In some embodiments, the enterprise network administrator uses the enterprise service design center to create an enterprise sponsored service device group list that includes device credentials or device application credentials that the carrier network and/or the enterprise network can use to identify a device or an application on a device as belonging to the group of devices for which the enterprise desires to sponsor enterprise service activities. In some embodiments, a sponsored service activity policy set is created by an enterprise network administrator through an enterprise service design center UI, and an enterprise sponsored service device group list is created by an enterprise network administrator through an enterprise service design center UI, and the two lists are stored in the enterprise service design center in which they are associated with one another for the purpose of provisioning the carrier network, the enterprise network, and/or the devices to provide the desired enterprise sponsored services policy set to the enterprise sponsored services device group, as described herein with respect to various embodiments.

[0052] In some embodiments, the association between an enterprise sponsored services device group and an enterprise sponsored service policy set is used by a service design center to create a provisioning table, in which the provisioning table is a list of the provisioning programming required for the various carrier network elements, enterprise network elements, and/or device elements to implement the desired sponsored service activity policy set for the enterprise sponsored services device group.

[0053] For example, an enterprise can use the service design center to configure certain destinations/services as enterprise services or potentially enterprise services based on various factors (e.g., corporate sites, corporate email/email servers, corporate web pages/intranet, and can, for example, agree to pay for a certain level of general web browsing by usage/time of day and/or other factors, corporate contacts/calendars, corporate videoconferencing; and certain applications, such as web conferencing applications or other applications; certain telephone service usages, etc.). As another example, the service design center can present a configuration

interface that allows users to select from one or more service plans that include various consumer and enterprise allocations and/or to select an enterprise only service plan.

[0054] In some embodiments, the service design center specifies one or more service plans the device user can select from and these service plan selection options are configured into a configuration interface on a device software application that allows users to select from one or more service plans that includes various consumer and enterprise allocations and/or to select an enterprise only service plan. In some embodiments, the configuration interface is made available directly on the device via a device client that provides a service plan selection user interface that displays one or more service plan options configured in the service design center or the enterprise service design center. In some embodiments, the configuration interface is presented directly on a device user interface (UI) when the user attempts to use an access service usage activity that requires a service plan to be activated or purchased. In some embodiments, the configuration interface presented via the device UI accepts a user response, transmits it to a carrier network element responsible for provisioning a new user service plan that in turn activates the service plan chosen by the user, possibly after confirming service payment credit for the user or enterprise entity. In some embodiments, the carrier network element responsible for provisioning a new user service plan is a carrier usage accounting server. In some embodiments, the carrier network element responsible for provisioning a new user service plan is a consumer internet services element. In some embodiments, the carrier network element responsible for provisioning a new user service plan is a carrier gateway or home agent. In some embodiments the carrier network element responsible for provisioning a new user service plan is a billing system or service plan provisioning system. In some embodiments, the configuration interface is made available to the user in the form of a web site that provides a service plan selection user interface that displays one or more service plan options configured in the service design center or the enterprise service design center.

[0055] In some embodiments, the initial configuration of the end-user device includes one or more enterprise access service plans that allow the user to access certain applications or network destinations associated with enterprise access services, and the user can choose from one or more additional consumer oriented service plans offered directly on the device UI by a device software application in communication with a carrier network element responsible for provisioning a new user service plan that in turn activates the service plan chosen by the user, possibly after confirming service payment credit for the user or enterprise entity. In some

embodiments, these access service plan options are configured with a service design center. In some embodiments, these access service plan options are configured with an enterprise service design center.

[0056] In some embodiments, enterprise data locally stored on the wireless communication device is secured and access to an enterprise network from the wireless communication device is secured so that only authorized devices or applications can access the network. In some embodiments, security for enterprise data and network access is accomplished by connecting the wireless communication device to the enterprise network via a secure mobile services application on the wireless communication device that connects via a secure channel to a secure mobile services gateway server in the enterprise network. In some embodiments, the SDC is programmed to provision the network and/or device apparatus to detect service usage communication with the mobile services gateway server and record that as a usage charge for network services. In some embodiments, such service usage communication with the mobile services gateway server is credited to the user's carrier account or used as a reimbursement to the user bill.

[0057] In some embodiments, determining the enterprise and consumer billing allocation for wireless communication device service usage activities is performed using a classifier implemented on the wireless communication device that classifies the monitored service usage activity (e.g., service usage can also be measured by the classifier and/or another function implemented on the wireless communication device, which can similarly be implemented in a secure execution area or in a secure memory), in which the classifier is executed in a secure execution area or a secure memory of the wireless communication device. In some embodiments, the security of the classifier is verified, periodically or at other times, using various techniques, such as by comparing a local service usage measure with a network based service usage measure and/or comparing a secured local service usage measure with another local service usage measure. In some embodiments, a secured application protects one or more enterprise applications (e.g., email, calendar, contacts, intranet access, and/or other enterprise specified applications, such as applications configured as approved or authorized enterprise applications for a particular enterprise by an enterprise manager using a service design center) from unauthorized use or tampering.

[0058] In some embodiments, the secure mobile services application also provides for usage monitoring of the enterprise service usage of the device. In some embodiments, the secure mobile services application also provides for service access control for the enterprise services of the device so that enterprise network access policies can be locally enforced on the device.

[0059] In some embodiments, security for enterprise data and network access is provided by connecting to the enterprise network via a secure mobile services application executed securely (e.g., in a virtual machine or in a hardware secured execution partition) on the wireless communications device that connects via a secure channel to a secure mobile services gateway server in the enterprise network. In some embodiments, security for enterprise data and network access is provided by connecting to the enterprise network via a secure mobile services application executed on a wireless communications device that includes a service processor, as described herein, that connects via a secure channel to a secure mobile services gateway server in the enterprise network. In some embodiments, the SDC is programmed to provision the network and/or wireless communications device apparatus to detect service usage communication with the mobile services gateway server, and record that as a usage charge for network services. In some embodiments, such service usage communication with the mobile services gateway server is credited to the user's carrier account or used as a reimbursement to the user bill.

[0060] In some embodiments, the service processor also provides for service usage monitoring of the enterprise service usage of the device, as described herein with respect to various embodiments. In some embodiments, the service processor also provides for service access control for the enterprise services of the device so that enterprise network access policies can be enforced on the device, as described herein with respect to various embodiments.

[0061] In some embodiments, enterprise and consumer billing allocation for wireless communication device service usage activities includes associating the wireless communication device and/or an authorized user of the wireless communication device (e.g., using device/user credentials) with an enterprise account (and, in some embodiments, a consumer account), associating an application with a service, and associating the service with the enterprise account (e.g., a service for the wireless communication device that the enterprise agreed to pay for). In some embodiments, enterprise and consumer billing allocation for

wireless communication device service usage activities further includes using application-based monitoring and/or control using, for example, device assisted services.

[0062] In some embodiments, enterprise and consumer billing allocation for wireless communication device service usage activities includes crediting an associated consumer account for service usage allocated to an enterprise account. In some embodiments, enterprise and consumer billing allocation for wireless communication device service usage activities includes billing the enterprise for service usage allocated to the enterprise account. In some embodiments, enterprise and consumer billing allocation for wireless communication device service usage activities includes reporting to the enterprise (and, in some embodiments, the consumer) service usage allocated to the enterprise account, and the enterprise can, for example, provide an expense reimbursement to the consumer (e.g., employee, partner, associate, or contractor of the enterprise).

[0063] In some embodiments, enterprise and consumer billing allocation for wireless communication device service usage activities includes associating the wireless communication device with an enterprise account and a consumer account, associating an application with a service, and associating the service with the consumer account (e.g., a service for the wireless communication device that the consumer, such as an employee of the enterprise, agreed to personally pay for). In some embodiments, enterprise and consumer billing allocation for wireless communication device service usage activities further includes using application-based monitoring and/or control using, for example, device assisted services.

[0064] In some embodiments, enterprise and consumer billing allocation for wireless communication device service usage activities includes crediting an associated enterprise account for service usage allocated to a consumer account. In some embodiments, enterprise and consumer billing allocation for wireless communication device service usage activities includes billing the consumer for service usage allocated to the consumer account. In some embodiments, enterprise and consumer billing allocation for wireless communication device service usage activities includes reporting to the enterprise (and, in some embodiments, the consumer) service usage allocated to the consumer account, and the enterprise can, for example, deduct the cost for such service usage as an expense from the consumer's periodic/next paycheck.

In some embodiments, enterprise and consumer billing allocation for wireless communication device service usage activities does not require a network element or a device element to control services. For example, a user with a device associated with a bulk service usage plan can be automatically credited for sponsored enterprise service usage. If the bulk service usage plan has a service plan cap associated with the user's consumer service plan, then the service usage classified as sponsored enterprise service usage can be deducted from the total service usage such that the sponsored enterprise service usage does not count towards the user's capped consumer service plan usage. As another example, an enterprise account associated with the wireless communication device and/or user can allow the user to exceed a monthly or other service plan cap for sponsored enterprise service usage (e.g., based on various criteria and/or other factors, such as a more restrictive enterprise service policy to avoid potential misuse of sponsored enterprise services for personal use).

[0065] In some embodiments, enterprise and consumer billing allocation for wireless communication device service usage activities is provided using network-based and/or device-based techniques as described herein with respect to various embodiments. For example, using various techniques described herein, an enterprise manager can control the services for wireless communication devices for the enterprise, including access to such services and/or charging for such services (e.g., services used by employees in which some are charged to the enterprise on behalf of the employee and some are charged to the employee as a consumer of such services) and user notification messages. For example, the enterprise manager or another network element/function can cap and/or control service usage for consumer services and/or enterprise services.

[0066] In some embodiments, a service usage reconciliation function is provided. In some embodiments, the service usage reconciliation function implements the rules for a billing split for the enterprise and consumer billing allocation for wireless communication device service usage activities, as described herein with respect to various embodiments. In some embodiments, the service usage reconciliation function also facilitates fraud detection, as described herein with respect to various embodiments.

Carrier Managed Billing Allocation With Service Usage Monitoring In Carrier Network

[0067] **Figure 1** illustrates a functional diagram of a network architecture 100 for providing enterprise and consumer billing allocation for wireless communication device service usage

activities in accordance with some embodiments. In some embodiments, a wireless communication device 110 includes a memory, an application processor (e.g., or more than one application processor or general processor), and a wireless modem, shown as an access modem 151. As shown, the wireless communication device 110 includes an operating system application space 131 for executing applications and communicating wirelessly using operating system lower layers 130, network stack 136, and the access modem 151. As used herein, application space refers to a portion of memory and a portion of a processor operating system execution environment for executing application programs. As also shown, the wireless communications device 110 includes operating system lower layers 130. As used herein, operating system lower layers refers to one or more OS layers that typically implement networking functions (e.g., network stack 136). In some embodiments, operating system lower layers 130 is where certain application data and communications security functions are implemented as described herein. In some embodiments, operating system lower layers 130 is where certain service usage monitoring and reporting functions are implemented as described herein. In some embodiments, operating system application space 131 executes various user applications, including one or more of user data application 111 and user voice application 112, and various enterprise applications, including enterprise data application 124 and enterprise voice application 126. In some embodiments, the execution environment for user applications and enterprise applications is the same (e.g., as shown in Figures 1 through 7). For example, a consumer Internet browser can execute in the operating system application space 131 for providing Internet web site browsing or web based email service via network stack 136 and wireless access modem 151 (e.g., a wireless modem), and an enterprise email program can also execute in the operating system application space 131 to communicate with an enterprise email server also via network stack 136 and wireless access modem 151. In some embodiments, the execution environment for user applications and enterprise applications are not the same (e.g., as shown in Figures 8 through 12).

[0068] In some embodiments, device 110 accesses various network-based voice services, such as consumer voice services 167 and/or enterprise sponsored/paid-for consumer voice services usage, via voice network 165. As shown, voice network 165 is in communication with carrier access network 150 via carrier gateway/home agent (HA) 152. In some embodiments, device 110 accesses various Internet based services, such as consumer Internet services 162 and/or enterprise sponsored/paid-for consumer Internet services usage, via Internet 160.

[0069] As also shown in Figure 1, device 110 is in wireless communication (e.g., 2G/3G/4G access) with carrier access network 150. The carrier provides a carrier usage accounting server 154 (e.g., a carrier billing server) in communication with carrier access network 150. Carrier network access 150 is shown in communication with both Internet 160 and enterprise network 170 via Internet 160. Enterprise network 170 is shown in communication with Internet 160 as via enterprise firewall and secure access gateway 171 for protecting enterprise network 170 from unauthorized access. In some embodiments, to access enterprise network 170 through enterprise firewall and secure access gateway 171, device 110 includes a secure data application or a virtual private network application/function to facilitate secure authorization with enterprise firewall and secure access gateway 171 and to also protect the communication (e.g., encrypt such data communications). As also shown, behind enterprise firewall and secure access gateway 171, enterprise network 170 provides communication with secure enterprise mobile services gateway/server 172 in communication with enterprise network 170. As shown, secure enterprise mobile services gateway server 172 includes various enterprise applications/functions, including as shown, mobile email 173, mobile synchronization 174, mobile contacts 175, mobile calendar 176, mobile communications 177, and mobile intranet 178. In some embodiments, secure enterprise mobile services gateway server 172 provides mobile device mobile access to various enterprise network intranet services via enterprise intranet servers 180. In some embodiments, the enterprise mobile services include email, contacts, calendar, enterprise communications, mobile device synchronization services, intranet internal web sites, internal enterprise applications, enterprise file systems, and/or other enterprise networking services. In some embodiments, secure enterprise mobile services gateway server 172 provides optimized mobile application formatting of the enterprise information or synchronization services to synchronize the enterprise database for the above services in an efficient and/or timely manner.

[0070] In some embodiments, carrier usage accounting server 154 (e.g., the carrier billing server) communicates (e.g., using secure communication techniques) with service usage reconciliation server function 158 to obtain reconciled service charging reports (e.g., reconciled billing reports) and/or enterprise service usage charging credit reports. In some embodiments, the reconciled service charging reports (e.g., reconciled billing reports) and/or enterprise service usage charging credit reports are processed by carrier usage accounting server 154 and reported as user usage record(s) 155 and/or enterprise usage record(s) 156. For example, mediating such charging and credit reports can be based on various factors as

described herein (e.g., by application, time of day/day of week, and/or other factors). For example, the service usage charges that occur due to communication with the servers or services that are part of enterprise network 170, including secure enterprise mobile services gateway server 172 and intranet servers 180, can be counted as an enterprise service usage credit.

[0071] In some embodiments, enterprise service design center 194 issues device provisioning instructions for the device credential list from the enterprise services device group, and for each of the credentials, a service control policy is set on enterprise firewall/secure gateway 171 to allow properly authorized devices to reach the desired destinations listed on the enterprise service activity policy set. The provisioning of enterprise firewall/secure gateway 171 with the enterprise service device group credentials and the enterprise service policy set is illustrated in Figure 1 by the "C" input designator.

[0072] In some embodiments, enterprise service design center UI 196 and enterprise service design center 194 are provided as shown in Figure 1. In some embodiments, enterprise service design center UI 196 and enterprise service design center 194 provide dedicated enterprise control of the network policy provisioning for configuring the service charging, accounting or billing allocation policies for differentiating between enterprise device service usage activities and consumer device service usage activities. Furthermore, in some embodiments, the portion of the enterprise network policy provisioning information that is needed to provision the carrier network elements to implement various techniques for allocating device service usage between enterprise and consumer activities is communicated between enterprise service design center 194 and carrier service design center 190.

[0073] A carrier provisioning system is typically not capable of providing direct access to an enterprise network administrator (e.g., carrier or enterprise personnel) for the purpose of provisioning such service charging capabilities. For example, such direct access is often not provided due to concerns related to the risk to the entire network that exists if network provisioning controls are made available to many different administrators to program charging allocation policies for many enterprises. However, as described herein, by isolating the required carrier network provisioning information to a secure service design center UI and policy configuration that only influences a small portion of the carrier network policy provisioning available to the carrier service design center and UI, the risk of causing such

problems with the carrier network configuration is significantly reduced. Additionally, the process of performing the carrier side of the necessary provisioning is simplified for an administrator or in some cases can be automated.

[0074] The service design centers (e.g., carrier service design center 190 and enterprise service design center 194) are shown in Figure 1 and various other figures as separate network elements in order to more clearly define and discuss the functions of the service design centers. In some embodiments, enterprise service design center 194 is implemented in various other network elements (e.g., in enterprise network management apparatus, such as management functions of secure enterprise mobile services gateway server 172 or other enterprise network management apparatus). In some embodiments, enterprise service design center 194 is implemented as a securely partitioned and managed device group interface to a subset of the provisioning capabilities of carrier network service design center 190. In some embodiments, enterprise service design center 194 is implemented as a securely partitioned and managed device group interface to a subset of the provisioning capabilities of a cloud-based secure enterprise mobile services network that is run by a centralized enterprise services provider such as an ASP or MVNO. As would be appreciated by one of ordinary skill in the art in view of the various embodiments described herein, enterprise service design center 194 can be implemented using various network and software/hardware architectures while providing for secure and controlled access as described herein.

[0075] In some embodiments, the enterprise service design center administrator creates or imports the enterprise service device group credentials and the enterprise service policy set using enterprise service design center UI 196. In some embodiments, the information included in the enterprise service device group credentials and the enterprise service policy set is also communicated from enterprise service design center 194 to carrier service design center 190 via the "C" connection designator as shown. For each of the device credentials listed in the enterprise services device group, carrier service design center 190 determines the information it needs to properly provision carrier gateway/home agent 152 with the proper access policy allowances and service usage charging policies to provide enterprise service access and usage credit for communications from device 110 to the enterprise network destination addresses specified in the enterprise service policy set. Programming of this provisioning information to carrier gateway/home agent 152 is indicated by the "A" information connector from carrier service design center 190 to carrier gateway/home agent 152. In some embodiments, this

provisioning (e.g., programming) information sent via provisioning communication link "A" to carrier gateway/home agent 152 includes information to facilitate programming the enterprise device group credentials to: (i) receive the desired access service policy permissions, and (ii) implement the desired service usage accounting/charging policy settings. From the enterprise device group credentials list and the enterprise service activity policy set information provided in "C," carrier service design center 190 determines the information needed to properly provision the service usage reconciliation server function 158. Programming of this provisioning information to service usage reconciliation server function 158 is indicated by the "B" information connector from carrier service design center 190 to service usage reconciliation server function 158. In some embodiments, service usage reconciliation function 158 is part of the carrier network, and service usage reconciliation function 158 implements the charging reconciliation rules to determine how much of the recorded device 110 service usage to place on the user's usage record or service bill (e.g., consumer service usage cost allocation) and how much to place on the enterprise's usage record or service bill (e.g., enterprise service usage cost allocation).

[0076] An enterprise may wish to allow consumer services on an end-user device that also allows an employee to access enterprise services over the access network. In some such embodiments, service design center 190 specifies one or more service plans from which the device user can select, and these service plan selection options are configured into a configuration interface on a device software application (e.g., user data app 111, user voice app 112 or service processor framework program 139 (shown, e.g., in Figure 16)) that allows users to select from one or more service plans, for example, one or more plans with both consumer and enterprise allocations, and/or an enterprise-only service plan. In some embodiments, the configuration interface is made available directly on the device via a device client that provides a service plan selection user interface that displays one or more service plan options configured in service design center 190 or enterprise service design center 194. In some embodiments, the configuration interface is presented directly on the device user interface (UI) when the user attempts an access service usage activity that requires a service plan to be activated or purchased. In some embodiments, the configuration interface presented to the device UI accepts a user response and assists in sending the user response to a carrier network element responsible for provisioning a new user service plan that in turn activates the service plan chosen by the user, possibly after confirming service payment credit for the user or enterprise entity. In some embodiments, the carrier network element responsible for provisioning a new

user service plan is carrier usage accounting server 154. In some embodiments, the carrier network element responsible for provisioning a new user service plan is consumer Internet services elements 162. In some embodiments, the carrier network element responsible for provisioning a new user service plan is a carrier gateway/home agent 152. In some embodiments, the carrier network element responsible for provisioning a new user service plan is a billing system or service plan provisioning system. In some embodiments, the configuration interface is made available to the user in the form of a web site that provides a service plan selection user interface that displays one or more service plan options configured in service design center 190 or enterprise service design center 194.

[0077] In some embodiments, the initial configuration of device 110 includes one or more enterprise access service plans that allow the user to access certain applications or network destinations associated with enterprise access services, and the user can choose from one or more additional consumer-oriented service plans offered directly on the device UI by a device software application (e.g., user data app 111, user voice app112, or service processor framework program 139) in communication with a carrier network element responsible for provisioning a new user service plan that in turn activates the service plan chosen by the user, possibly after confirming service payment credit for the user or enterprise entity. In some embodiments, these access service plan options are configured using service design center 190. In some embodiments, these access service plan options are configured using enterprise service design center 194.

[0078] In some embodiments in which a user has selected a consumer-oriented service plan in addition to an enterprise service plan, service usage reconciliation function 158 distinguishes between data usage within the enterprise service plan and data usage within the consumer-oriented service plan. In some embodiments, the enterprise does not pay for, backhaul, process, or police data usage associated with the consumer-oriented plan. In some embodiments, service usage reconciliation function 158 determines how much data usage by device 110 is enterprise data usage, and how much data usage by device 110 is consumer data usage. In some embodiments, service usage reconciliation function 158 allocates data usage associated with applications and/or services specified by the enterprise service plan to the enterprise, and data usage associated with applications and/or services specified by the consumer-oriented data plan to the consumer.

[0079] The various embodiments described herein with respect to Figure 1 support a variety of techniques for allocating service usage accounting or billing between enterprise services and consumer services. For example, service usage reconciliation function 158 can report measured total usage, measured consumer usage, and/or measured enterprise usage to carrier usage accounting server 154. In some embodiments, the reconciliation service usage function (e.g., provided by service usage reconciliation function 158 and/or another element/function) implements the business rules that determine how much of the service usage to charge the user (e.g., a consumer service usage allocation) and how much of the service usage to charge the enterprise (e.g., an enterprise service usage allocation). In some embodiments, the service usage reconciliation service usage function records total device service usage, records total enterprise service activity service usage, and then subtracts the enterprise service usage from the total device service usage to determine a consumer service usage (e.g., a consumer service usage allocation). In some embodiments, service usage reconciliation function 158 passes on the enterprise service usage as a credit to the consumer account. In some embodiments, this credit is accounted for by the carrier billing the user at a reduced amount according to the credit and billing the enterprise for an increased amount according to the credit. In some embodiments, the credit is accounted for by communicating the credit to the enterprise so the enterprise can reimburse the consumer (e.g., generating an expense reimbursement for the credit to the consumer as an employee or contractor of the enterprise, directly paying the enterprise allocation of the carrier bill for the consumer, and/or various other approaches as described herein). In some embodiments, the credit is reported to the enterprise so that the enterprise can seek payment for the non-enterprise service usage (e.g., consumer service usage allocation) from the consumer (e.g., who can be an employee or contractor of the enterprise).

[0080] As another example, an enterprise allocation can also include providing an allowance for a certain level of monthly usage of data and/or voice. In some embodiments, carrier usage accounting server 154 generates a bill for the associated consumer account (e.g., associated with device 110, such as based on the device/user credentials) that reflects the cost of the service usage allocated to consumer service usage and a credit for the cost of service usage allocated to enterprise service usage (e.g., to offset the cost of the enterprise service usage, which can be billed to the enterprise account associated with the enterprise service usage for the device 110). As described herein, based on an allocation of enterprise and consumer service usage, various techniques for billing/charging and generating credits/reporting (e.g., the enterprise can generate the user/employee monthly expense reimbursements to compensate the

user/employee for the determined cost of the enterprise service usage and/or other approaches as described herein) can be provided using the network architecture 100 and/or other network architectures, as described herein.

[0081] In some embodiments, an enterprise manager manages service usage by specifying an access network service usage limit for a service usage activity (such as data service, voice service, text service, a roaming service, or a more detailed classification of data service such as one or more websites or one or more device applications), and, when that usage limit is reached for a device that is managed by the enterprise manager, a service usage notification message is generated. In some embodiments, the service usage notification message is configured through enterprise service design center UI 196. In some embodiments, the service usage notification message is delivered to device 110. In some embodiments, the service usage notification message is presented to the user via a user interface of device 110.

[0082] In some embodiments, the service usage notification message provides information about data usage or the status of device 100. In some embodiments, the service usage notification message is triggered by an event, e.g., detection that device 110 reaches a data usage ceiling, determination that device 110 is roaming, etc. In some embodiments, the service usage notification message provides real-time or near-real-time information about data usage. In some embodiments, the service usage notification message provides information about remaining data usage availability or entitlement. In some embodiments, the service usage notification message comprises a detailed report of enterprise usage by user, user group, device, device group, or location.

[0083] In some embodiments, secure enterprise mobile services gateway server 172 is a dedicated enterprise application server for a particular enterprise (e.g., company, government organization, school/university, or another entity). In some embodiments, secure enterprise mobile services gateway server 172 is a carrier or a third party service provider (e.g., a carrier for wireless network services, such as AT&T, Sprint, T-Mobile, and/or various other wireless network service providers/carriers or third party service providers) controlled/managed application server that performs the application server functions for various different enterprises (e.g., as a service/outsourced IT services model). In some embodiments, device 110 is partitioned (e.g., associated with a particular enterprise/MVNO partition and associated enterprise account) based on device credentials and/or VPN to determine a service plan for

managing (e.g., to determine how to allocate enterprise/consumer service usage for) device 110. In some embodiments, based on the partition determination of device 110, and the associated service plan for managing device 110, appropriate service usage monitoring and classification can be determined for providing an enterprise and consumer allocation for service usage activities of device 110 based on the associated service plan(s).

[0084] For example, by programming the business rules in service usage reconciliation function 158 that determine the service usage accounting allocation between enterprise services and consumer services, many approaches can be provided for creating a service that provides an enterprise service to a device when the device user has selected a consumer service plan or elected to pay for a consumer service plan. As an example, if the device user has chosen a service plan, the enterprise service usage accounted for in enterprise usage record 156 can be billed to the enterprise rather than the consumer. As another example, if the device user has chosen a service plan, the consumer service usage accounted for in user usage record 155 can be billed to the device user rather than the enterprise. As yet another example, if the device user has selected a service plan, the enterprise service usage can be communicated to the enterprise (e.g., and/or the device user), and the enterprise can issue a reimbursement to the device user for the enterprise portion of the user's bill, or pay the carrier directly for a portion of the user's bill, thus reducing the amount the user must pay. In some embodiments, the business rules in service usage reconciliation function 158 are programmed to provide the device user with a certain amount of service usage that may or may not be directly related to enterprise services.

[0085] For example, the user can be allocated a certain amount of general purpose browsing that includes network destinations that are not specified in the enterprise service activity policy set. In some embodiments, there is a cap to such general purpose browsing, and carrier service design center 190 can provision the network and/or the device to alert the user regarding how much of the enterprise sponsored browsing remains or when the enterprise sponsored internet browsing cap is reached or exceeded. In some embodiments, the business rules in service usage reconciliation function 158 are programmed to deduct the service usage associated with the enterprise sponsored general purpose browsing, up to the specified cap, from the user's bill. In this way, the user can be allocated an allowance for services that either the enterprise sponsors to account for enterprise related service usage that may not be included in the

enterprise service activity policy set or that the enterprise simply desires to sponsor to reduce the device user's consumer service plan billing.

[0086] In a similar manner, services other than browsing that are not necessarily associated with enterprise service usage can also be sponsored by the enterprise by properly provisioning the business rules in service usage reconciliation function 158. For example, a catch-all enterprise sponsored allowance (e.g., or cap) for "bulk" internet usage can be provided. The fact that the user is provided with such an allowance may be pointed out to the user if the user disputes how much of his or her device service usage cost should be covered by the enterprise and how much the user should cover personally. Another example is to provide a certain amount of voice minutes to any phone number or to phone numbers not in the enterprise service activity policy set.

[0087] In some embodiments, the business rules in service usage reconciliation function 158 are provisioned so that the enterprise specifically does not allow, sponsor, or pay for certain device service usage activities. In some embodiments, these service usage activities can include access to network destinations, applications, or services that pose security risks to enterprise data stored on device 110 or pose security risks to enterprise network 170. In some embodiments, these activities include access to network destinations, applications, or services that the enterprise does not wish to sponsor or that are potentially associated with user activity that violates enterprise policy or laws. For example, the business rules may be configured to allow only transmission of business data on approved networks, e.g., excluding free or unknown WiFi hotspots, or only when device 110 is connected to the network via a VPN. In some embodiments, such service usage activities that violate enterprise security policies or other service usage policies are blocked by the business rules programmed into the network or the device as specified in the enterprise service activity policy set.

[0088] By programming the business rules in service usage reconciliation function 158 that determine the service usage accounting allocation between enterprise services and consumer services, many approaches can be provided for creating a service that provides an enterprise service to a device when the device user has not selected a consumer service plan or elected to pay for a consumer service plan. For example, if the device user has not chosen to select or pay for a consumer service plan, carrier gateway/home agent 152 can be programmed to allow service usage for the enterprise service policy set but deny all other access until the user

chooses a consumer service plan. In some embodiments, when/if the consumer chooses a consumer service plan then access would be expanded beyond just the enterprise services, because when the service plan activation occurs, consumer service policy set in carrier gateway/home agent 152 will be updated to allow service (e.g., as the carrier administrator user of carrier service design center 190 programs a different set of consumer service access policies for each consumer service plan that can be chosen). In some embodiments, the user is allocated a certain amount of general purpose data access or voice minutes as described above even though the user does not have a consumer data plan. Another example is to provide the user with a certain monetary allowance that is sponsored by the enterprise rather than a service usage amount.

[0089] Although enterprise service design center 194 is shown provisioning mobile server usage counter 179 (e.g., shown in Figure 5) and enterprise firewall/secure gateway 171, it should be understood that not all device provisioning connections as shown from secure enterprise mobile services gateway/server 172 to device 110 are shown for device functions including secure mobile services application access, communication link provisioning (e.g., cryptographic encryption keys, VPN settings, and various other security/communication provisioning), security programs, service control programs, and program settings for enterprise service applications, such as email, calendar, contacts, mobile synchronization services, and traffic control. As shown, the labeled provisioning connections are provided as exemplary embodiments to assist in identifying the network elements that are provisioned for network access control and network service usage charging reporting. Those of ordinary skill in the art will appreciate that these additional device provisioning functions are not necessarily specifically called out with provisioning connection labels in each figure, and it will be apparent to one of ordinary skill in the art which of these device provisioning functions and connections are needed from enterprise service design center 194 and device 110. It will also be apparent to one of ordinary skill in the art in view of the various embodiments described herein that the various device provisioning connections and device element programming configurations needed to provision these device functions can be managed by secure enterprise mobile services gateway/server 172 via a device management communications link. It will also be apparent to one of ordinary skill in the art that, in some embodiments, the flow of policy provisioning information for the various device elements that participate in establishing service usage monitoring and reporting policies or service access control policies starts in enterprise service design center 194 and flows through secure enterprise mobile services

gateway/server 172 over a device management link, and through the device management link on device 110 to the device 110 functional elements that need to be provisioned. In various embodiments described herein, the device elements that are provisioned in some embodiments to set up enterprise services, service usage monitoring and reporting policies, or service usage access control policies include one or more of enterprise data application 124, enterprise voice application 126, secure mobile enterprise application environment 120 (shown, e.g., in Figure 8), secure network interface 128 (shown, e.g., in Figure 8), secure enterprise mobile services application 125 (shown, e.g., in Figure 13), virtual machine #2 secure enterprise application environment 118 (shown, e.g., in Figure 14), enterprise application secured hardware execution partition 106 (shown, e.g., in Figure 15), device service usage monitor 119 (shown, e.g., in Figure 17), service processor framework program 139 (shown, e.g., in Figure 16), and/or service processor kernel program 138 (shown, e.g., in Figure 16).

[0090] In some embodiments, service usage reconciliation function 158, or secure enterprise mobile services gateway/server 172, or another similar network function, is programmed to review traffic usage patterns of mobile device 110 for the purpose of determining if the device may have fallen into unauthorized hands or if the device secure enterprise communications and data management software may have been hacked or tampered with in a way that endangers enterprise security or causes the enterprise to be billed for usage that is not enterprise usage. For example, service usage reconciliation function 158 (e.g., or secure enterprise mobile services gateway/server 172) can be programmed to monitor "bulk" enterprise service usage for the enterprise device group and trigger a fraud detection alert for a device that exhibits enterprise usage that is higher than a pre-determined "normal" limit. As another example, service usage reconciliation function 158 can be programmed to monitor "bulk" enterprise service usage for the enterprise device group and trigger a fraud detection alert for a device that exhibits enterprise usage access patterns that are determined to be outside of "normal" limits. Examples of usage patterns can include usage as a function of time of day, duration of usage, usage above a certain limit for a subset of service usage activities, and/or usage above a certain limit for all service usage activities.

[0091] In some embodiments, enterprise service design center 194 is configured to receive or accept a specification for an access network service usage limit (e.g., a service amount in minutes, bytes, or cost) for a service usage activity (such as a data service, a voice service, a text service, a roaming service, or a more detailed classification of a data service, such as one

or more websites or one or more device applications), and the service usage limit is applied to one or more devices 110 or device groups (or users or user groups) managed by enterprise service design center 194. In some embodiments, enterprise service design center 194 is further configured to receive service usage records for device 110, which is managed by enterprise service design center 194, from a network element configured to monitor and report device 110 service usage (e.g., carrier usage accounting server 154, enterprise firewall/security gateway 171, or another network element), and when the usage limit is reached, to generate a service usage notification message. In some embodiments, enterprise service design center 194 is configured to deliver the service usage notification message to enterprise service design center UI 196. In some embodiments, enterprise service design center 194 is configured to deliver the service usage notification message to a software application of device 110 (e.g., service processor framework program 139 or user data app 111) for presentation to the device user through a user interface of device 110.

[0092] In some embodiments, enterprise service design center 194 is configured to receive or accept a specification for an access network service notification event consisting of a network access pattern achieved or attempted by device 110 that belongs to a device group (or user group) managed by enterprise service design center 194, wherein the network access pattern is access attempted or achieved by one or more pre-defined device applications, or access attempted or achieved by device 110 to one or more network destinations, websites or network servers. In some embodiments, enterprise service design center 194 is further configured to receive service usage records for device 110, which is managed by enterprise service design center 194, from a network element configured to monitor and report device 110 service usage (e.g., carrier usage accounting server 154, enterprise firewall/security gateway 171, or another network element), and when the service usage indicates that the network access pattern has occurred, enterprise service design center 194 is further configured to send a notification message to enterprise service design center UI 196.

Carrier Managed Billing Allocation With Service Usage Monitoring In Carrier Network and Enterprise Firewall/Gateway

[0093] **Figure 2** illustrates a functional diagram of another network architecture 101 for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments. Network architecture 101 of

Figure 2 is similar to network architecture 100 of Figure 1, except that in network architecture 101 of Figure 2, service usage reconciliation function158 receives service usage information from enterprise firewall/secure gateway 171 in addition to carrier gateway/home agent 152. This allows for various techniques that augment the capabilities of carrier gateway/home agent 152. For example, in networks in which it is impractical or infeasible for carrier gateway/home agent 152 to keep track of the service usage accounting allocation between the enterprise service policy set and consumer services for the devices in the device group, service usage reconciliation function 158 can receive total device service usage from carrier gateway/home agent 152, and receive the enterprise service usage from enterprise firewall/secure gateway 171. With this information, service usage reconciliation service usage function 158 can perform the allocation between enterprise service usage and consumer service usage without any detailed service usage reports from carrier gateway/home agent 152.

[0094] There are several reasons that the carrier network may not support numerous enterprise service customers with an enterprise/consumer allocation architecture that requires carrier gateway/home agent 152 to perform the necessary traffic classification or service usage classification as in the Figure 1 embodiment. For example, these reasons can include: (i) carrier gateway/home agent 152 does not have the detailed service usage classification capability (e.g., deep packet inspection function(s)) required to allocate service usage between the enterprise service policy set and consumer services for the devices in the device group, (ii) carrier gateway/home agent 152 is capable of performing the service monitoring required but can only do it for a limited number of devices (e.g., scaling issues), and/or (iii) there are too many device groups being managed by enterprise partners of the carrier creating a situation where the number of specialized profiles that must be supported by carrier gateway/home agent 152 is larger than can be accommodated by the profile management capacity of the gateway system (e.g., scaling issues). As would now be apparent to those of ordinary skill in the art in view of the embodiments described herein, there are other reasons that can make it advantageous to provide the enterprise service usage from the enterprise network.

[0095] In some embodiments, provisioning with the service design centers and UIs for the embodiment shown in Figure 2 is similar to that of Figure 1. In some embodiments, the billing allocation capabilities of the two embodiments are similar if carrier gateway/home agent 152 is fully capable of differentiating service usage between the enterprise service policy set and the

consumer services, but if not, then as discussed above, the billing allocation capabilities of the Figure 2 embodiment can be preferable in such environments.

[0096] Because the enterprise service usage is monitored by the enterprise network elements in the embodiments depicted in Figure 2, various service accounting or billing policies are available to the enterprise or carrier. For example, the amount of service usage resulting from enterprise services that occur during roaming conditions can be accounted for even when the carrier network does not receive detailed classification of service usage from roaming network partners. The business rules programmed into service usage reconciliation function 158 that are determined by the enterprise service activity policy set can break-out enterprise-service-related roaming charges separately from consumer-service-related roaming charges so that the enterprise-service-related roaming charges are sponsored or paid by the enterprise and consumer roaming service usage activities are not subsidized or are only partially subsidized. In addition, in some embodiments, secure enterprise mobile services gateway/server 172 includes the capability to determine if device 110 is roaming so that the access control policies specified in the enterprise service activity policy set can include modification or denial of access to enterprise network 170 services allowed by enterprise firewall/secure gateway 171 or secure enterprise mobile services gateway/server 172 during roaming conditions even though the access is not controlled by the carrier home network.

[0097] In some embodiments, an active network detection function is included on the device to assist the network policy enforcement elements to determine the type of network the device is connected to or to determine if the device is on a home or roaming network, as described herein. For example, the service usage policy allowances provided by the enterprise service activity policy set can be programmed so that the allowances change depending on the availability of a particular network or set of networks, the time of day, the congestion state of a network, or the current cost of service on the network. For example, if the carrier home network is not available and only a roaming network is available, the allowance may be decreased or removed. As another example, if a certain network type is not available but another network type is (e.g., 2G is available instead of 3G or 3G is available instead of 4G), then the allocation can be reduced. As yet another example, if a variable charging policy is in place with the carrier for access when the network is busy or during certain times of day, then the enterprise sponsored allowance can be reduced during times of higher charging.

Enterprise Managed Billing Allocation With Service Usage Monitoring in Carrier Network And Enterprise Firewall/Gateway

[0098] **Figure 3** illustrates a functional diagram of another network architecture 102 for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments. Network architecture 102 of Figure 3 is similar to network architecture 101 of Figure 2, except that in network architecture 102 of Figure 3, service usage reconciliation function 158 receives overall device service usage information from carrier usage accounting server 154 and also receives enterprise device service usage information from enterprise firewall/secure gateway 171. In some embodiments, there is no interaction between the provisioning of the carrier network and the provisioning of the enterprise network, and it is assumed that service usage reconciliation function 158 and enterprise usage accounting server 159 are both under the control of the enterprise administrator. This approach allows for various techniques that provide for enterprise allocation of consumer service usage and enterprise service usage without the need to interface to the carrier network other than to get the overall usage summary. For example, service usage reconciliation function 158 can receive total or "bulk" usage from carrier usage accounting server 154, receive enterprise service usage from enterprise firewall/secure gateway 171, and determine the amount of consumer service usage, enterprise service usage, and/or an enterprise service usage credit.

[0099] In some embodiments, provisioning with the service design centers and UIs for the embodiment shown in Figure 3 is similar to that of Figure 1 except that no provisioning of enterprise service parameters is required in the carrier network. The billing allocation capabilities are also similar if carrier gateway/home agent 152 is fully capable of differentiating service usage between the enterprise service policy set and the consumer services, but if not, then as discussed above, the billing allocation capabilities of the Figure 3 embodiment can be preferable in such environments. For example, using network architecture 102, the enterprise can deal directly with its employees without the need to bring the carrier into the consumer-versus-enterprise allocation process. As an example, the enterprise could have a policy in which consumers purchase their own mobile device services and then get credit for enterprise mobile device services at the end of each billing period. This credit can be provided back to the employee in the form of an expense reimbursement or an increase in their next paycheck.

Enterprise Usage Credit With Service Usage Monitoring in Enterprise Firewall/Gateway

[00100] **Figure 4** illustrates a functional diagram of another network architecture 103 for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments. Network architecture 103 of Figure 4 is similar to network architecture 102 of Figure 3, except that in network architecture 103 of Figure 4, service usage reconciliation server function 158 receives no overall device service usage information from the carrier network. As shown in Figure 4, the source of service usage information is enterprise network 170 (e.g., via the enterprise firewall/secure gateway 171). In some embodiments, there is no interaction between the provisioning of the carrier network and the provisioning of the enterprise network, and it is assumed that service usage reconciliation function 158 and enterprise usage accounting server 159 could both be under the control of the enterprise administrator. For example, network architecture 103 of Figure 4 can be less dependent on the carrier than network architecture 102 of Figure 3 in that no billing information feed is provided. Using various techniques described herein, an enterprise service usage credit can be determined, and the determined enterprise service usage credit can be reimbursed to the device user.

Carrier Managed Billing Allocation With Service Usage Monitoring In Carrier Gateway/Home Agent And Enterprise Mobile Services Gateway Server

[00101] **Figure 5** illustrates a functional diagram of another network architecture 200 for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments. Network architecture 200 of Figure 5 is similar to network architecture 101 of Figure 2, except that in network architecture 200 of Figure 5, secure enterprise mobile services gateway/server 172 includes mobile server usage monitor 179, and the enterprise service usage reports from this function are sent to service usage reconciliation function 158 instead of usage reports being sent from enterprise firewall/secure gateway 171. In some embodiments, various specialized needs of monitoring, recording, and reporting enterprise service usage are confined to the special-purpose secure enterprise mobile services gateway/server 172 rather than requiring the often more general-purpose enterprise firewall/secure gateway 171 to perform these functions.

Enterprise Managed Billing Allocation With Service Usage Monitoring in Carrier Network And Enterprise Mobile Services Gateway Server

[00102] **Figure 6** illustrates a functional diagram of another network architecture 201 for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments. Network architecture 201 of Figure 6 is similar to network architecture 102 of Figure 3, except that in network architecture 201 of Figure 6, secure enterprise mobile services gateway/server 172 includes mobile server usage monitor 179, and the enterprise service usage reports from this function are sent to service usage reconciliation function 158 instead of usage reports being sent from enterprise firewall/secure gateway 171. For example, this approach allows for the specialized needs of monitoring, recording, and reporting enterprise service usage to be performed by the special-purpose secure enterprise mobile services gateway/server 172 rather than requiring the often more general-purpose enterprise firewall/secure gateway 171 to perform such functions.

Enterprise Usage Credit With Service Usage Monitoring in Enterprise Mobile Services Gateway Server

[00103] **Figure 7** illustrates a functional diagram of another network architecture 202 for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments. Network architecture 202 of Figure 7 is similar to network architecture 103 of Figure 4, except that in network architecture 202 of Figure 7, secure enterprise mobile services gateway/server 172 includes mobile server usage counter 179, and the enterprise service usage reports from this function are sent to service usage reconciliation function 158 instead of usage reports being sent from enterprise firewall/secure gateway 171. For example, this approach allows for the specialized needs of monitoring, recording and reporting enterprise service usage to be performed by the special-purpose secure enterprise mobile services gateway/server 172 rather than requiring the often more general-purpose enterprise firewall/secure gateway 171 to perform such functions.

Carrier Managed Billing Allocation With Device Mobile Enterprise Services Application Environment and Service Usage Monitoring In Carrier Network

[00104] **Figure 8** illustrates a functional diagram of another network architecture 300 for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments. As shown, secure mobile enterprise application environment 120 and secure network interface 128 within secure mobile enterprise application environment 120 are included in device 110. Also, server secure

network interface 127 is included in secure enterprise mobile services gateway/server 172. In some embodiments, secure mobile enterprise application environment 120 protects sensitive enterprise information that is stored on device 110 (e.g., email text and downloads, calendar information, contacts, intranet data, or any other enterprise data) and provides a secure communication channel function to allow for authentication with server secure network interface 127 on secure enterprise mobile services gateway/server 172. As also shown, a user services application environment in device 110 includes various user applications, such as user data application 111 and user voice application 112.

[00105] In some embodiments, provisioning of the various network architecture elements to facilitate the allocation between enterprise service usage accounting or billing and consumer service usage accounting or billing is established as follows. The device portion of secure network interface 128 and the enterprise server portion of server secure network interface 127 are provisioned with connection "E." In some embodiments, this provisioning operation with the connection labeled "E" includes programming information for secure network interface 128 to direct enterprise network 170 access traffic associated with application functions running in secure mobile enterprise application environment 120 to enterprise network 170 destinations that are to be sponsored (and, in some embodiments, possibly intermediate network routes) according to the enterprise services policy set, including, for example, the addresses (e.g., IP, IP/port or other higher layer address identifiers) of secure enterprise mobile services gateway/server 172 or enterprise intranet servers 180. In some embodiments, the provisioning operation designated with the connection label "E" also establishes the parameters required for the secure communication of information between secure network interface 128 and server secure network interface 127. In some embodiments, this provisioning step sets up the policies for the authentication process, data encryption, and cryptographic key exchange processes take place to establish secure communication between secure mobile enterprise application environment 120 and secure enterprise services gateway/server 172.

[00106] In some embodiments, the enterprise network destinations that are to be sponsored according to the enterprise services policy set identified by provisioning connection "E" are also communicated to carrier service design center 190. For example, this allows carrier service design center 190 to determine and transmit the proper provisioning information to establish the access control policies or service usage accounting policies for these aspects of

the enterprise services policy set. Carrier service design center provisioning connections "A" communicate the provisioning information (programming) to carrier gateway/home agent 152. Carrier service design center provisioning connections "B" communicate the provisioning information (programming) to service usage reconciliation function 158.

[00107] In some embodiments, the provisioning operation associated with the provisioning connection label "C" provisions enterprise firewall/secure gateway 171 to admit devices 110 with device credentials or application credentials that belong to the desired enterprise services device group associated with the enterprise service policy set. In some embodiments, the provisioning information labeled as "C" includes enterprise network 170 destinations that are to be sponsored (and, in some embodiments, possibly intermediate network routes) according to the enterprise services policy set. In some embodiments, the provisioning information labeled as "C" includes only the network destinations for secure enterprise mobile services gateway/server 172, and devices 110 are not allowed access to other parts of enterprise network 170.

[00108] In some embodiments, network architecture 300 for providing enterprise and consumer billing allocation for wireless communication device service usage activities includes executing an enterprise application as a secure enterprise data application 124 in secure mobile enterprise application environment 120 of device 110 in which the secure applications are in network communication (e.g., secure network communication, such as via a virtual private network (VPN) or other secure network communication techniques) with secure enterprise mobile services gateway/server 172 (e.g., executing an enterprise server side of the enterprise authorized/sponsored applications, such as an enterprise email server, an enterprise calendar server, an enterprise contacts server, and/or an enterprise network access server) of the enterprise. In some embodiments, the secure enterprise mobile services gateway/server 172 performs application monitoring that includes counting application service usage (e.g., bytes used in communicating with the device's execution of secure enterprise application 124). In some embodiments, secure enterprise mobile services gateway/server 172 performs application monitoring that further includes classifying application service usage (e.g., classifying secure enterprise application 124 by application/service usage activity such as based on application name or using signed code/hash techniques, by time of day/day of week, enterprise server, destinations, enterprise intranet, and/or other factors).

Carrier Managed Billing Allocation With Device Mobile Enterprise Services Application Environment and Mobile Services Gateway Server With Service Usage Monitoring In Carrier Network

[00109] **Figure 9** illustrates a functional diagram of another network architecture 301 for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments. Network architecture 301 of Figure 9 is similar to network architecture 300 of Figure 8, except that in network architecture 301 of Figure 9, secure enterprise mobile services gateway/server 172 is located between the Internet 160 and enterprise network 170. For example, this approach allows for server secure network interface 127 of secure enterprise mobile services gateway/server 172 to restrict access to enterprise network 170 and enterprise intranet servers 180 based on device authentication and/or various other security techniques (e.g., secure access, authentication, and/or communication techniques), as would be apparent to one of ordinary skill in the art in view of the various embodiments described herein.

Carrier Managed Billing Allocation With Device Mobile Enterprise Services Application Environment and Mobile Services Gateway Server With Service Usage Monitoring In Carrier Network And Mobile Services Gateway Server

[00110] **Figure 10** illustrates a functional diagram of another network architecture 302 for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments. Network architecture 302 of Figure 10 is similar to network architecture 301 of Figure 9, except that in network architecture 302 of Figure 10, secure enterprise mobile services gateway/server 172 includes mobile service usage monitor 179 that reports enterprise service usage to the service usage reconciliation function 158. In some embodiments, various specialized needs of monitoring, recording, and reporting enterprise service usage are confined to the special-purpose enterprise mobile services gateway/server 172 rather than requiring the often more general-purpose enterprise firewall/secure gateway 171 and/or other network elements/functions to perform such functions.

Enterprise Managed Billing Allocation With Device Mobile Enterprise Services Application Environment and Mobile Services Gateway Server With Service Usage Monitoring In Mobile Services Gateway Server

[00111] **Figure 11** illustrates a functional diagram of network architecture 303 for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments. Network architecture 303 of Figure 11 is similar to network architecture 302 of Figure 10, except that network architecture 303 of Figure 11 includes another carrier usage accounting server 154B that reports service usage to service usage reconciliation function 158. In some embodiments, carrier usage accounting server 154B receives overall or bulk service usage data from carrier gateway/home agent 152 and forwards such information to service usage reconciliation function 158. Service usage reconciliation function 158 reconciles the overall or bulk service usage received from carrier accounting server 154B and the enterprise service usage received from mobile server usage monitor 179 and provides such reconciled service usage information to carrier usage accounting server 154A.

Enterprise Usage Credit With Device Mobile Enterprise Services Application Environment and Mobile Services Gateway Server With Service Usage Monitoring In Mobile Services Gateway Server

[00112] **Figure 12** illustrates a functional diagram of network architecture 304 for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments. Network architecture 304 of Figure 12 is similar to network architecture 303 of Figure 11, except that in network architecture 304 of Figure 12, the only service usage reported to service usage reconciliation function 158 is the enterprise service usage received from mobile server usage monitor 179. In some embodiments, service usage reconciliation function 158 reconciles the enterprise service usage received from mobile server usage monitor 179 and provides such reconciled service usage information to carrier usage accounting server 154, which generates enterprise service usage record(s) 156.

Device Configurations Without Service Usage Monitoring and Reporting

[00113] **Figure 13** illustrates a functional diagram of a secure device application architecture for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments. As shown, device 110 includes an operating system application space 131, operating system lower layers 130 including network stack 121, and access modem (e.g., wireless modem) 129. As also shown, operating

system application space 131 includes various user applications, such as user data application 111 and user voice application 119, and service usage monitor 119. Operating system application space 131 also includes secure enterprise mobile services application 125, which includes various enterprise applications, such as email, synchronization, contacts, calendar communications, and intranet. Secure enterprise mobile services application 125 also includes secure network interface 128 (e.g., for securely communicating with an enterprise network).

[00114] **Figure 14** illustrates a functional diagram of another secure device virtual machine architecture for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments. Figure 14 is similar to Figure 13, except that in Figure 14 the user applications are executed/stored within virtual machine (VM) #1 consumer application environment117, and secure enterprise mobile services application 125 is included within virtual machine (VM) #2 secure enterprise application environment 118. Device 110 also includes virtual machine operating system 115 that includes virtual OS instantiation #1 117A for VM #1 consumer application environment 117 and virtual OS instantiation #2 118A for VM #2 secure enterprise application environment 118. As also shown, virtual machine operating system 115 includes virtual machine OS network stack 116.

[00115] **Figure 15** illustrates a functional diagram of another secure device hardware execution partition architecture for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments. Figure 15 is similar to Figure 14, except that in Figure 15 hardware partitions are provided instead of virtual partitions. As shown, the user applications are executed/stored within user application secured hardware execution partition 105 and secure enterprise mobile services application 125 is included within enterprise application secured hardware execution partition 106. Device 110 also includes secured hardware partition for OS 115 that includes secure hardware partition manager #1 107 for user application secured hardware execution partition 105 and secure hardware partition manager #2 108 for enterprise application secured hardware execution partition 106. As also shown, secured hardware partition for OS 115 includes OS network stack 116.

[00116] **Figure 16** illustrates a functional diagram of another secure device service processor architecture for providing enterprise and consumer billing allocation for wireless

communication device service usage activities in accordance with some embodiments. As similarly described herein with respect to various embodiments, the device architecture of Figure 16 includes service processor framework program 139 (e.g., framework space agent/function) and network stack framework components 137 in operating system framework space 133, and service processor kernel program 138 (e.g., kernel space agent/function) and network stack kernel components 135 in operating system kernel space 132. In some embodiments, the service processor functions provide a user interface function to communicate to a user of device 110 whether or not a service usage activity is an approved/authorized service usage activity, or whether it is a disallowed service usage activity for device 110 (e.g., the enterprise has disallowed the usage of device 110 for such service usage activities, such as online gaming and/or certain other online activities or certain long distance calling or voice usage during certain days, such as weekends) or whether such would/will be charged/billed to the user as a consumer under the user's consumer plan. In some embodiments, the service processor functions provide a user interface function to communicate to a user of device 110 an associated cost of certain service usage activities allocated to consumer service usage. In some embodiments, the service processor functions provide a user interface function to communicate to a user of device 110 an associated credit of certain service usage activities allocated to enterprise service usage. In some embodiments, the service processor functions provide a user interface function to communicate to a user of device 110 various other information as described herein with respect to providing an enterprise and consumer allocation for service usage activities. In some embodiments, the service processor shown in Figure 16 communicates with a service controller, such as described herein with respect to various embodiments.

Carrier Managed Billing Allocation With Device Mobile Enterprise Services Application Environment and Mobile Services Gateway Server With Service Usage Monitoring In Carrier Network And On Device

[00117] **Figure 17** illustrates a functional diagram of another network architecture 400 for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments. Network architecture 400 of Figure 17 is similar to network architecture 302 of Figure 10, except that as shown in Figure 17, device 110 also includes service usage monitor 119 (e.g., agent/function) in secure mobile enterprise application environment 120. In some embodiments, service usage monitor 119

performs application monitoring that includes counting application service usage for secure data application 124 and secure voice application 126 (and, in some embodiments, for also counting application service usage for user applications that are not enterprise or secure enterprise applications 124 or 126). In some embodiments, counting application service usage includes counting bytes or network connection time used in communicating via carrier access network 150 during the device's execution of monitored data applications. In some embodiments, counting application service usage includes counting voice network connection time used in communicating via carrier access network 150 during the device's execution of monitored voice applications. In some embodiments, service usage monitor 119 performs application monitoring that further includes classifying application service usage for secure enterprise applications 124, 126 (e.g., classifying various secure enterprise applications 124, 126 and in some embodiments, including ambient services classification/determination, by application/service usage activity such as based on application name or using signed code/hash techniques, by time of day/day of week, enterprise server, destinations, enterprise intranet, and/or other factors).

[00118] In some embodiments, carrier usage accounting server 154 communicates (e.g., using secure communication techniques) with service usage monitor 119 to mediate billing/charging and credit reports, for example, using the various approaches and techniques as described herein.

[00119] In some embodiments, service usage monitor 119 and/or another function/agent executed in secure mobile enterprise application environment 120 of device 110 blocks user access for non-enterprise activities that the user has not agreed to pay for.

[00120] Because the enterprise service usage is monitored by the device network elements in the embodiments depicted in Figure 17, various service accounting or billing policies are available to the enterprise or carrier. For example, the amount of service usage resulting from enterprise services that occur during roaming conditions may be accounted for even when the carrier network does not receive detailed classification of service usage from roaming network partners. The business rules programmed into service usage reconciliation function 158 that are determined by the enterprise service activity policy set can break-out enterprise service related roaming charges separate from consumer service related roaming charges. In addition, in some embodiments, the device secure mobile enterprise environment includes an access

control function so that the access control policies specified in the enterprise service activity policy set can be enforced on roaming networks that have access that is not controlled by the carrier home network.

[00121] For example, the allowances provided by the enterprise service activity policy set can be programmed so that the allowances change depending on the availability of a particular network or set of networks, the time of day, the congestion state of a network, or the current cost of service on the network. As another example, if the carrier home network is not available and only a roaming network is available, the allowance can be decreased or removed. As yet another example, if a certain network type is not available but another network type is (e.g., 2G is available instead of 3G or 3G is available instead of 4G), then the allocation can be reduced. As yet a further example, if a variable charging policy is in place with the carrier for access when the network is busy or during certain times of day, then the enterprise sponsored allowance can be reduced during times of higher charging. As described herein, in some embodiments, an active network detection function can be included on the device to assist the network policy enforcement to determine the type of network the device is connected to or to determine if the device is on a home or roaming network. As also described herein, in some embodiments, a network busy state monitor function can be included on the device to assist the network policy enforcement to determine the network busy state or state of network congestion.

Carrier Managed Billing Allocation With Device Mobile Enterprise Services Application Environment and Mobile Services Gateway Server With Service Usage Monitoring In Carrier Network, On Device, And In Enterprise Mobile Services Gateway Server

[00122] **Figure 18** illustrates a functional diagram of another network architecture 401 for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments. Network architecture 401 of Figure 18 is similar to network architecture 400 of Figure 17, except that in network architecture 401 of Figure 18, secure enterprise mobile services gateway/server 172 includes mobile server usage counter 179, and the enterprise service usage reports from this function are sent to service usage reconciliation function 158. In some embodiments, various specialized needs of monitoring, recording, and reporting enterprise service usage are confined to the special-purpose secure enterprise mobile services gateway/server 172.

Enterprise Managed Billing Allocation With Device Mobile Enterprise Services Application Environment and Mobile Services Gateway Server With Service Usage Monitoring On Device And In Enterprise Mobile Services Gateway Server

[00123] **Figure 19** illustrates a functional diagram of another network architecture 402 for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments. Network architecture 402 of Figure 19 is similar to network architecture 401 of Figure 18, except that network architecture 402 of Figure 19 does not include the service usage feed from carrier gateway/home agent 152, and service usage reconciliation function 158 relies solely on a device service usage feed from device 110 usage monitors 119 and secure enterprise mobile services gateway/server 172 mobile service usage monitor 179. In some embodiments, service usage reconciliation function 158 and enterprise service usage accounting server 159 are under the control of the enterprise or the carrier. For example, an enterprise entity can establish enterprise service and consumer service usage allocation accounting without the need to tie into the carrier network for usage feeds and usage accounting. Using various techniques described herein, an enterprise service usage credit can be determined, and the determined enterprise service usage credit can be reimbursed to the device user.

Enterprise Managed Billing Allocation With Device Mobile Enterprise Services Application Environment and Mobile Services Gateway Server With Service Usage Monitoring On Device

[00124] **Figure 20** illustrates a functional diagram of another network architecture 403 for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments. Network architecture 403 of Figure 20 is similar to network architecture 402 of Figure 19, except that in network architecture 403 of Figure 20, service usage reconciliation function 158 receives feeds from device 110 service usage monitors 119 and there is no feed from the secure enterprise mobile services gateway server.

Enterprise Usage Credit With Device Mobile Enterprise Services Application Environment and Mobile Services Gateway Server With Service Usage Monitoring On Device And In Enterprise Mobile Services Gateway Server

[00125] **Figure 21** illustrates a functional diagram of another network architecture 404 for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments. Network architecture 404 of Figure 21 is similar to network architecture 402 of Figure 19, except that in network architecture 404 of Figure 21, there is no service usage monitor function 119 in user services application environment 122 providing service usage reports/information to service usage reconciliation function 158, and enterprise usage accounting server 159 only generates enterprise usage records 156.

Enterprise Usage Credit With Device Mobile Enterprise Services Application Environment and Mobile Services Gateway Server With Usage Monitoring On Device

[00126] **Figure 22** illustrates a functional diagram of another network architecture 405 for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments. Network architecture 405 of Figure 22 is similar to network architecture 404 of Figure 21, except that network architecture 405 of Figure 22 does not include mobile server usage monitor 179 providing enterprise service usage reports/information to service usage reconciliation function 158.

Device Configurations With Service Usage Monitoring and Reporting

[00127] In some embodiments, secure enterprise mobile services application 125 and network stack 121 can be implemented in access modem 129, as described below with respect to Figures 23 through 26.

[00128] **Figure 23** illustrates a functional diagram of a secure device application architecture with device-based service usage monitoring (and in some embodiments, access control) for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments. Figure 23 is similar to Figure 13 except that in Figure 23 usage monitor 119 is provided as shown, and secure enterprise mobile services application 125 and network stack 121 can be implemented in access modem 129 as also shown.

[00129] **Figure 24** illustrates a functional diagram of a secure device virtual machine architecture with device-based service usage monitoring (and in some embodiments, access control) for providing enterprise and consumer billing allocation for wireless communication

device service usage activities in accordance with some embodiments. Figure 24 is similar to Figure 14 except that in Figure 24, usage monitor 119 is provided as shown, and secure enterprise mobile services application 125 and virtual machine OS network stack 116 can be implemented in access modem 129 as also shown.

[00130] **Figure 25** illustrates a functional diagram of a secure device hardware execution partition architecture with device-based service usage monitoring (and in some embodiments access control) for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments. Figure 25 is similar to Figure 15 except that in Figure 25 usage monitor 119 is provided as shown, and secure enterprise mobile services application 125 and virtual machine OS network stack 116 can be implemented in access modem 129 as also shown.

[00131] **Figure 26** illustrates a functional diagram of a secure device service processor architecture with device based service usage monitoring (and in some embodiments, access control) for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments. Figure 263 is similar to Figure 16 except that in Figure 26 usage monitor 119 is provided as shown, and secure enterprise mobile services application 125, service processor framework 139, and service processor kernel program 138, can be implemented in the access modem 129 as also shown.

[00132] In some embodiments, service processor framework program 139 (or service processor kernel program 138) interacts with network stack framework components 137 or network stack kernel components 135 to inspect traffic for service usage classification and service policy enforcement (e.g., access control policy enforcement, traffic control policy enforcement, service usage accounting, charging policy enforcement, or service notification policy enforcement) purposes. In some embodiments, one or more of network stack framework components 137 and network stack kernel components 135 provides classification information on one or more traffic flows to service processor framework program 139 (or service processor kernel program 138). In some embodiments, service processor framework program 139 (or service processor kernel program 138) seeks to match the classification information to one or more classification parameters contained in the service policy definitions in order to determine the service policy enforcement actions that may be required for a traffic flow. In some embodiments, a traffic flow is a flow of data packets. In some embodiments, a

traffic flow is a flow of one or more data packets that are associated with a device application, the association of a traffic flow to a device application being identified by network stack framework components 137 or network stack kernel components 135 or service processor framework program 139 (or service processor kernel program 138). In some embodiments, the service usage classification determines that the traffic flow is associated with a combination of one or more of: a device application, a network destination, a traffic type, a content type, a QoS level, a roaming network, a home network.

[00133] In some embodiments, the association of traffic flow to a specific device application is used to determine a service policy enforcement action that is dependent on the specific device application. In some embodiments, a specific device application identifier (e.g., an application name, application signature, application hash or application certificate) forms an application credential that is used to index a service policy enforcement action that is intended to be implemented following a service usage activity or attempted service usage activity by the specific device application. In some embodiments, a specific device application is verified as consistent with an application credential in order to ensure that an application service policy enforcement action intended to be applied to the specific device application is applied to the correct application. In some embodiments, the verification that a specific application is consistent with an application credential associated with a service policy enforcement action is performed in service processor framework program 139 (or service processor kernel program 138) to ensure that ensure that an application service policy enforcement action intended to be applied to the specific device application is applied to the correct application. In some embodiments, the verification that a specific application is consistent with an application credential associated with a service policy enforcement action is performed in network stack framework components 137 or network stack kernel components 135, and service processor framework program 139 (or service processor kernel program 138) ascertains the application credential verification to ensure that ensure that an application service policy enforcement action intended to be applied to the specific device application is applied to the correct application.

[00134] In some embodiments, the association of traffic flow to a specific device application is used to determine a service policy enforcement action that is dependent on the specific device application, and service processor framework program 139 (or service processor kernel program 138) instructs network stack framework components 137 or network stack kernel

components 135 to implement the service policy enforcement action on the traffic flow associated with the specific device application. In some embodiments, the association of traffic flow to a specific device application is used to determine a service policy enforcement action that is dependent on the specific device application, and service processor framework program 139 (or service processor kernel program 138) implements the service policy enforcement action. In some embodiments, a traffic flow is buffered pending classification (e.g., buffered in one or more of network stack framework components 137, network stack kernel components 135, service processor framework program 139, or service processor kernel program 138). In some embodiments, upon classification of the traffic flow (e.g., determination of an association of the traffic flow to a specific device application), a service policy enforcement action that is dependent on the specific device application is determined by service processor framework program 139 (or service processor kernel program 138) and implemented in one or more of network stack framework components 137, network stack kernel components 135, service processor framework program 139, and service processor kernel program 138. In some embodiments, the service policy enforcement action for the traffic flow is implemented in service processor framework program 139 (or service processor kernel program 138). In some embodiments, service processor framework program 139 (or service processor kernel program 138) instructs a device UI program that displays a device service notification (e.g., a service usage notification, a service plan offer notification, or an indication of a service usage event or attempted service usage event that requires a user notification) to implement the service policy enforcement action for the traffic flow. In some embodiments, service processor framework program 139 (or service processor kernel program 138) instructs a service usage monitor (e.g., accounting traffic to bulk classification or a more detailed classification of service usage) to implement the service policy enforcement action for the traffic flow.

[00135] In some embodiments, the network destination of a traffic flow is used to determine if a service policy enforcement action that is dependent on a specific network destination should be applied to the traffic flow. In some embodiments, a traffic flow is inspected by network stack framework components 137 or network stack kernel components 135, and one or more traffic characteristics (e.g., an address, a socket/flow tuple, a layer-7 packet information, or a packet header string) are passed to service processor framework program 139 (or service processor kernel program 138), wherein the one or more traffic characteristics are matched against one or more classification parameters contained in a service policy definition,

and if a match is present then a service policy enforcement action is implemented for the traffic flow. In some embodiments, a traffic flow is inspected by service processor framework program 139 (or service processor kernel program 138), and one or more traffic characteristics (e.g., an address, a socket/flow tuple, a layer-7 packet information, or a packet header string) are matched against one or more classification parameters contained in a service policy definition, and if a match is present then a service policy enforcement action is implemented for the traffic flow. In some embodiments, the service policy enforcement action for the traffic flow is implemented in service processor framework program 139 (or service processor kernel program 138). In some embodiments, service processor framework program 139 (or service processor kernel program 138) instructs network stack framework components 137 or network stack kernel components 135 to implement the service policy enforcement action for the traffic flow. In some embodiments, the service policy enforcement action for the traffic flow is implemented by a device UI program that displays a device service notification (e.g., a service usage notification, a service plan offer notification, or an indication of a service usage event or attempted service usage event that requires a user notification). In some embodiments, the service policy enforcement action for the traffic flow is implemented by a service usage monitor (e.g., accounting traffic to bulk classification or a more detailed classification of service usage).

[00136] In some embodiments, an enterprise manger can define or select service plan policies that confine enterprise-sponsored access services to a pre-defined list of device applications. For example, an enterprise manager might choose to define or select a service plan wherein only corporate applications may be accessed (e.g., email, contacts, intranet services, text, and/or voice). In such embodiments, enterprise service design user interface 196 may be used by the enterprise manager to define or select the allowable applications that are to have access. In some embodiments, an enterprise access manager may define or select a different set of applications to be accessible when device 110 is roaming than when device 110 is on a home network or on a WiFi network. In some embodiments, an enterprise manager may define or select a set of applications that are to be not allowed access when a device is on a certain network (e.g., a roaming network). For example, many modern smart phone, tablet, and laptop operating systems have background services that have the potential to incur large roaming charges during roaming conditions (e.g., Google Android "gallery" functions that share device data with the Google network, Microsoft "system" functions that do the same, software update programs, etc.). In such cases, enterprise service design center 194 may be used to specify the

device applications that are not allowed to access the network during certain network conditions.

[00137] In some embodiments, the identification and network access control for a device application is performed with a device software program or agent (e.g., service processor framework program 139 or service processor kernel program 138), and enterprise service design center 194 programs the device agent with the application identification parameters and associated access policies. In some embodiments, the device agent identifies the application using an application name, certificate, signature, or hash for an application running on the device and a policy instruction stored on the device.

[00138] In some embodiments, the identification and network access control for a device application is performed with one or more network access policy enforcement elements (e.g., carrier gateway/home agent 152, carrier usage accounting server 154, enterprise firewall/security gateway 171), and enterprise service design center 194 causes the one or more network access policy enforcement elements to be provisioned with the application identification parameters and associated access policies. In some embodiments, the one or more network access policy enforcement elements identify an application by observing the traffic headers inserted by the application. In some embodiments, the one or more network access policy enforcement elements identify an application by observing the network destinations or destination patterns accessed by the application. In some embodiments, the one or more network access policy enforcement elements identify an application by routing or tunneling the application traffic to one or more network gateways or servers associated with the application (e.g., APN routes, dedicated application addressing, or a device agent that steers the application traffic to a server). In some embodiments, the device assists in this routing or tunneling with a device agent that is programmed to route or re-direct the traffic for an application.

[00139] In some embodiments, an enterprise manger can define or select service plan policies that confine enterprise-sponsored access services to a pre-defined list of network destinations, servers, or resources. For example, an enterprise manager might choose to define or select a service plan wherein only corporate network destinations may be accessed (e.g., email server, contacts server, intranet servers, text service servers, and VOIP servers). In some embodiments, enterprise service design center interface 196 may be used by an enterprise

manager to define or select the allowable network destinations that device 110 may access. In some embodiments, the enterprise access manager may define or select a different set of network destinations when device 110 is roaming than when device 110 is on a home network or on a WiFi network. In some embodiments, an enterprise manager may define or select a set of network destinations that device 110 cannot access when device 110 is on a certain network (e.g., a roaming network). For example, many websites and enterprise services exhibit network access service usage behavior that can incur large roaming charges during roaming conditions (e.g., software update websites or servers, contact database synchronization websites, email download synchronization websites, video conference websites, etc.). In such cases, enterprise service design center 194 may be used to specify the device applications, services, and/or websites that are not to be accessed or used during certain network connection conditions.

[00140] In some embodiments, a device agent identifies the network destination and applies the appropriate access policy by comparing traffic characteristics with pre-defined characteristics in the access policy instructions provisioned on device 110, and then applies the corresponding traffic control rule, and enterprise service design center 194 performs the provisioning of the device agent. In some embodiments, the identification and network access control for a network destination is performed with one or more network access policy enforcement elements (e.g., carrier gateway/home agent 152, carrier usage accounting server 154, enterprise firewall/security gateway 171) and enterprise service design center 194 performs the provisioning of the one or more network elements.

[00141] In some embodiments, enterprise service design center 194 is configured to receive or accept a specification for an access network service usage limit (e.g., a service amount in minutes, bytes, or cost) for a service usage activity (such as a data service, a voice service, a text service, a roaming service, or a more detailed classification of data service such as one or more websites or one or more device applications), and the service usage limit is applied to one or more devices 110 or device groups (or users or user groups) managed by enterprise service design center 194. In some embodiments, enterprise service design center 194 is further configured to receive service usage records for device 110, which is managed by enterprise service design center 194, from a device-based element that monitors and reports device 110 service usage (e.g., one or more device usage monitors 119, device service processor framework program 139, or service processor kernel program 138, network stack 134, or

access modem 151), and when the usage limit is reached a service usage notification message is generated. In some embodiments, enterprise service design center 194 is configured to deliver the service usage notification message to enterprise service design center UI 196. In some embodiments, enterprise service design center 194 is configured to deliver the service usage notification message to a device 110 software application (e.g., service processor framework program 139 or user data app 111) for presentation to the device user via a user interface.

[00142] In some embodiments, enterprise service design center 194 is configured to receive or accept a specification for an access network service usage limit (e.g., a service amount in minutes, bytes, or cost) for a service usage activity (such as a data service, a voice service, a text service, a roaming service, or a more detailed classification of data service such as one or more websites or one or more device applications), and the service usage limit is applied to one or more devices 110 or device groups (or users or user groups) managed by enterprise service design center 194. In some embodiments, enterprise service design center 194 is further configured to receive service usage records for device 110, which is managed by the enterprise service design center 194, from a device-based element configured to monitor and report device 110 service usage (e.g., one or more device usage monitors 119, device service processor framework program 139 or service processor kernel program 138, network stack 134, or access modem 151), and when the usage limit is reached a restriction or limitation on further usage is applied by the service design center by provisioning one or more network elements responsible for enforcing network access policy (e.g., carrier gateway/home agent 152, carrier usage accounting server 154, enterprise firewall/security gateway 171). In some embodiments, enterprise service design center 194 is configured to send the user a notification message or a message to contact an enterprise manager.

[00143] In some embodiments, secure network interface 128 on device 110 is configured with a VPN device client function to securely communicate between one or more approved enterprise applications (e.g., enterprise data app 124, enterprise voice app 126, secure enterprise mobile services app 125) and a counterpart VPN function that secures access to enterprise network 170 (e.g., enterprise firewall/security gateway 171 or server secure network interface 127). In some embodiments, a device software application or agent (e.g., service processor framework program 139 or service processor kernel program 138, secure network interface 128, secure hardware partition manager 108) is configured to identify network access

activity associated with individual applications and allow network access to one or more approved enterprise applications when a VPN device client function is in operation, or not allow network access to one or more approved enterprise applications when a VPN device client function is not in operation. In some embodiments, service design center 190 or enterprise service design center 194 is configured to provision a device 110 software application or agent (e.g., service processor framework program 139 or service processor kernel program 138, secure network interface 128, secure hardware partition manager 108) with application access policy rules to identify network access activity associated with individual applications and allow network access to one or more approved enterprise applications when a VPN device client function is in operation, or not allow network access to one or more approved enterprise applications when a VPN device client function is not in operation. In this manner, enterprise applications that might be subject to spoofing by network elements, websites, servers, or programs operating outside the secure enterprise environment are not placed in communication with such network elements.

[00144] In some embodiments, a device software application or agent (e.g., service processor framework program 139 or service processor kernel program 138, secure network interface 128, secure hardware partition manager 108) is configured to identify network access activity associated with individual applications and not allow network access to one or more non-approved applications when a VPN device client function is in operation, or allow network access to one or more non-approved applications when a VPN device client function is not in operation. In some embodiments, service design center 190 or enterprise service design center 194 is configured to provision a device 110 software application or agent (e.g., service processor framework program 139 or service processor kernel program 138, secure network interface 128, secure hardware partition manager 108) with application access policy rules to identify network access activity associated with individual applications and not allow network access to one or more non-approved applications when a VPN device client function is in operation, or allow network access to one or more enterprise applications when a VPN device client function is not in operation. In this manner, applications that might maliciously access enterprise network resources when the VPN is running are not permitted to do so.

[00145] In some embodiments, the application access policy rules are enforced by allowing or not allowing an application to access the network. In some embodiments, the application access policy rules are enforced by allowing or not allowing the application to run. In some

embodiments, the identification of approved enterprise applications associated with traffic flows is confirmed or secured by identifying the application certificate and comparing it to an application signature or hash on the device. In some embodiments, the identity of an approved enterprise application is confirmed by inspecting an application certificate, signature or hash that is provided by service design center 190 or enterprise service design center 194.

[00146] In some embodiments, secure network interface 128 is configured with a split-tunnel VPN device client function, wherein an enterprise side of the split tunnel is configured to securely communicate between one or more enterprise applications (e.g., enterprise data app 124, enterprise voice app 126, secure enterprise mobile services app 125) and a counterpart VPN function that secures access to the enterprise network 170 (e.g., enterprise firewall/security gateway 171 or server secure network interface 127), and a consumer side of the split tunnel is configured to communicate without encryption for access network services provided to consumer applications on the device. In some embodiments, a device software application or agent (e.g. service processor framework program 139 or service processor kernel program 138, secure network interface 128, secure hardware partition manager 108) is configured to identify network access activity associated with individual applications and route or direct traffic associated with one or more enterprise applications to the enterprise side of the split VPN tunnel, and route or direct traffic associated with one or more consumer applications to the consumer side of the VPN tunnel. In some embodiments, service design center 190 or enterprise service design center 194 is configured to provision a device 110 software application or agent (e.g., service processor framework program 139 or service processor kernel program 138, secure network interface 128, secure hardware partition manager 108) with application access policy rules to identify network access activity associated with individual applications and specify which applications are to be routed or directed to the enterprise side of the VPN tunnel and which applications are to be routed or directed to the consumer side of the VPN tunnel. In some embodiments, the identification of applications associated with traffic flows is secured by identifying the application certificate and comparing it to an application signature or hash on the device. In some embodiments, the application certificate, signature or hash is provided by service design center 190 or enterprise service design center 194.

[00147] In some embodiments, the policy rules only enable secure applications on device 110 to access enterprise data. In some embodiments, an enterprise manager sets policy rules that do not allow secure applications on device 110 to upload data to unsecure destinations.

[00148] In some embodiments, service design center 190 is configured to provide enterprise service design center 194. In some embodiments, enterprise service design center 194 comprises a policy management system configured to select a set of access network policies to be enforced for one or more device groups (or user groups) where the set of access network policies consists of a subset of the full set of access network policies capable of being enforced by the access network policy enforcement elements. In some embodiments, the subset of the full set of policies capable of being enforced by the access network policy enforcement elements comprises a pre-defined subset of the policy configuration capabilities. In some embodiments, the enterprise service design center policy management subset limitations for enterprise service design center 194 provide the ability to define and manage one or more of the policies that define a service policy set or service plan that is applied to a given device, user, device group or user group. In some embodiments, the enterprise service design center policy management subset limitations for enterprise service design center 194 can provide the ability to enroll a device, user, device group or user group in a set limited to one or more pre-defined service policy configurations or service plans.

[00149] As an example embodiment, the enterprise service design center policy management subset limitations for enterprise service design center 194 may provide the following policy definition and management capabilities for a device (or user) or device group (or user group): specify service usage limits (caps) for bulk access service or for a specific classification of access service activities, require all traffic or certain traffic associated with enterprise-critical applications or content to be communicated via an enterprise VPN, define controls for which applications that can access the network or certain defined destinations on the network, specify network destinations that are allowed or not allowed, specify roaming service limitations, specify WiFi networks that are allowed or not allowed, specify security settings in the device access control or I/O access control ports, specify service usage notification triggers and notification content associated with the triggers (e.g., warnings when a specified service usage activity occurs, access is not allowed for a given attempted service usage activity, or service usage reaches a limit), and other such examples that are allowed to be managed under the

policy management subset limitations. In some embodiments, the charging rates for such services may not be allowed to be managed under the policy management subset limitations.

[00150] In some embodiments, enterprise service design center 194 has an allowable subset of the full set of policies capable of being enforced by the access network policy enforcement elements that comprises a pre-defined set of one or more access network policy configurations (e.g., service plans). As an example embodiment, the set of pre-configured service plans may be defined for a certain implementation of enterprise service design center 194 comprising multiple pre-defined service plans, each of which provides variations in one or more of service notification policy, access control policy, service classification policy, service QoS policy, or service charging policy.

[00151] In some embodiments, enterprise service design center 194 is configured to allow a service design administrator to select one or more pre-configured access network policy configurations (or service plans) to be applied to a device, a user, a device group or a user group.

[00152] In some embodiments, enterprise service design center 194 comprises a device enrollment management system configured to enroll a device credential into a device group (or a user credential into a user group), where the set of device credentials (or user credentials) that enterprise service design center 194 is capable of managing is a subset of the device credentials (or user credentials) allowed on the access network. In some embodiments, the subset of device credentials (or user credentials) that are subject to management by enterprise service design center 194 is defined using service design center 190.

[00153] As an example embodiment, the set of pre-defined service plans that are made available to a first enterprise service design center 194 implementation managed by a first enterprise entity might consist of three service plans, wherein the first service plan comprises network policies (e.g., access policies, charging policies, or notification policies) that provide for limited or restricted home network access service but do not provide for roaming access services, the second service plan comprises network policies that provide for unlimited or unrestricted home network access service and also provide for limited roaming access services, and the third service plan comprises network policies that provide for unlimited or unrestricted home network access service and also provide for unlimited or unrestricted roaming access services. In another example embodiment, on the same carrier access network as the previous

example, a second enterprise service design center 194 implementation managed by a second enterprise entity might consist of two service plans, wherein the two service plans might be the same as two of the service plans from the previous example embodiment, or they might be completely different.

[00154] Given these examples, it will now be understood and appreciated by one of ordinary skill in the art that enterprise service design center 194 provides a convenient means of designing and distributing custom service plans to different enterprise entities that meet the needs of each enterprise entity, wherein the various policy definition capabilities disclosed herein can be used in a large number of combinations to create the service plans, with the number of combinations of service plan design capabilities being too numerous to list here. It will also now be understood and appreciated by one of ordinary skill in the art that each enterprise can effectively manage its devices (or users) and device groups (or user groups) to provide the appropriate level of policy control needed by the enterprise in a simplified manner, without the need to manage all the full policy capabilities of the access network.

[00155] For example, the embodiments of service design center 190 and enterprise service design center 194 disclosed herein support a carrier network business process wherein a carrier network manager utilizes service design center 190 to create a set of access network policies that consist of a subset of the full set of access network policies capable of being enforced by the access network policy enforcement elements (referred to as specialized enterprise service plans), and the specialized enterprise service plans are designed and offered to meet the special needs of one or more enterprise entities. In some embodiments, an enterprise manager uses enterprise service design center 194 to apply the one or more specialized enterprise service plans to one or more devices (or users) or device groups (or user groups) that belong to the enterprise entity's mobile device inventory (or employee list). The different needs of various employee groups (or device types) can be among the factors that determine which service plan is assigned to a given user group (or device group). The specific needs of an employee can assist in determining which user group (or device group) the employee should be assigned to. The carrier manager can also create other specialized enterprise service plans for other enterprise entities to meet varied needs among enterprise market customers.

[00156] In some embodiments, an enterprise manager controls access network usage, costs, and access limits for an employee user group (e.g., a group of devices that could be as small as

a single device or as large as all devices under the enterprise manager's control). In some embodiments, the enterprise manager establishes at least two user groups and establishes and manages different network-access policies for different employee user groups. For example, the enterprise manager may set and manage different policies for data usage on WiFi, 3G, 4G, or other networks for different employee user groups. Likewise, the enterprise manager may set different roaming privileges for different employee user groups.

[00157] In some embodiments, an enterprise manager sets expenditure ceilings by limiting allowed data usage for secure business applications to enforce security rules. In some embodiments, an enterprise manager tracks enterprise data access to improve compliance records. For example, the enterprise manager can track enterprise data usage by employee, device, application, location, network, or time of day.

[00158]

Process Flows For Providing Enterprise And Consumer Billing Allocation For Wireless Communication Device Service Usage Activities

[00159] **Figure 27** illustrates a flow diagram for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments. At 402, the process begins. At 404, a service usage activity of a wireless communication device (e.g., application based service usage that uses a wireless network in which the wireless communication device has an associated service plan) is performed. In some embodiments, the monitoring is performed on the wireless communication device. In some embodiments, the monitoring is performed by a network element, such as a secure application server for monitoring enterprise applications, as described herein with respect to various embodiments. At 406, an enterprise/consumer allocation is determined. In some embodiments, the monitored service usage activity is reported to a network element that determines the enterprise/consumer allocation based on the associated service plan that includes a defined enterprise/consumer allocation based on various factors, such as can be performed by a carrier billing server as described herein with respect to various embodiments. At 408, an associated consumer account is billed for the consumer service usage. At 410, the consumer account is credited for the enterprise service usage. At 412, the process is completed.

[00160] **Figure 28** illustrates another flow diagram for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments. At 502, the process begins. At 504, a service usage activity of a wireless communication device (e.g., application based service usage that uses a wireless network in which the wireless communication device has an associated service plan) is performed. At 506, an enterprise/consumer allocation is determined. At 508, an associated enterprise account is billed for the enterprise service usage. At 510, the enterprise account is credited for the consumer service usage. At 512, the process is completed.

[00161] **Figure 29** illustrates another flow diagram for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments. At 602, the process begins. At 604, a service usage activity of a wireless communication device (e.g., application based service usage that uses a wireless network in which the wireless communication device has an associated service plan) is performed. At 606, an enterprise/consumer allocation is determined. At 608, the enterprise service usage is reported. At 610, an expense reimbursement for the enterprise service usage is generated (e.g., by the enterprise for the consumer, who is, for example, an employee of the enterprise). At 612, the process is completed.

[00162] **Figure 30** illustrates another flow diagram for providing enterprise and consumer billing allocation for wireless communication device service usage activities in accordance with some embodiments. At 702, the process begins. At 704, a service usage activity of a wireless communication device (e.g., application based service usage that uses a wireless network in which the wireless communication device has an associated service plan) is performed. At 706, the monitored service usage is reported. At 708, an enterprise/consumer allocation is determined. At 710, a bill/charge based on the enterprise/consumer allocation is generated. At 712, the process is completed.

[00163] Although the foregoing embodiments have been described in some detail for purposes of clarity of understanding, the invention is not limited to the details provided. There are many alternative ways of implementing the invention. The disclosed embodiments are illustrative and not restrictive. In particular, many of the embodiments are not limited to supporting an enterprise/consumer split. As would be appreciated by one of ordinary skill in the art, the disclosed embodiments may be applied, for example, when a sponsor entity

subsidizes a cost associated with an end-user device's use of a sponsored (or ambient) data service or application, and the user pays for the end-user device's use of non-sponsored (or non-ambient) data services or applications. The sponsor entity may use enterprise service design center 194 to configure devices that may use the sponsored service, policies applicable to the sponsored service, etc. Moreover, the disclosed embodiments may be applied when a first sponsor subsidizes a cost associated with an end-user device's use of a first sponsored data service or application, a second sponsor subsidizes a cost associated with the end-user device's use of a second sponsored data service or application, and the user pays for the end-user device's use of non-sponsored data services or applications. The sponsor entities may use one or more enterprise service design centers to configure aspects of the sponsored services. As would be appreciated by one of ordinary skill in the art, there are many other environments in which the disclosed embodiments are useful or applicable.

[00164] Several advantageous combination embodiments are now disclosed for allocating enterprise service usage accounting and personal service usage accounting. These combinations are for example purposes, are not meant to be exhaustive or limiting in any way; as will be apparent to one of ordinary skill in the art, these combinations represent only a fraction of the embodiments provided herein.

[00165] In some embodiments, a network system for classifying the accounting of access network service usage for an end user device comprises (i) a first service design center configured to receive an accounting split classification policy defining the classification rules for dividing an overall access network service usage into an enterprise service usage allocation and a personal service usage allocation, (ii) a network provisioning instruction translator configured to receive the accounting split classification policy and translate it to a set of network service usage classification and reporting instructions for one or more network elements responsible for classifying service usage, (iii) a network provisioning system for communicating the set of network service usage classification and reporting instructions to the one or more network elements responsible for classifying service usage, (iv) the one or more network elements responsible for classifying service usage configured to classify service usage to determine the enterprise service usage allocation and the personal service usage allocation, and generate service usage reports, and (v) a service usage accounting system that receives the service usage reports and (a) accrues the enterprise service usage allocation, and (b) accrues the personal service usage allocation.

[00166] In some embodiments, the network system for classifying the accounting of access network service usage for an end user device can be augmented wherein the first network access notification message policy is associated with a first device group defined by a first list of device credentials or a first user group defined by a first list of user credentials, and the service design center is further configured to obtain a second network access notification message policy comprising a plurality of second network access trigger conditions and, for each of the plurality of second network access trigger conditions, an associated second network access notification message, the second network access notification message policy associated with a second device group defined by a second list of device credentials or a second user group defined by a second list of user credentials.

[00167] In some embodiments, the network system for classifying the accounting of access network service usage for an end user device further comprises a master service design center configured to define a first notification policy design capability set for the first service design center, the first notification policy design capability set comprising a first subset of a master policy capability set. This embodiment can be further augmented wherein the master service design center is further configured to define a second notification policy design capability set for a second service design center, the second notification policy design capability set comprising a second subset of the master policy capability set, the second subset of the master policy capability set either identical to or different from the first subset of the master policy capability set.

[00168] In some embodiments, the network system for classifying the accounting of access network service usage for an end user device is further augmented wherein the first service design center is hosted on an operator network. In some embodiments, the network system for classifying the accounting of access network service usage for an end user device is optimized for smaller enterprise data center deployments wherein the first service design center is hosted on an enterprise business network.

[00169] In some embodiments, the network system for classifying the accounting of access network service usage for an end user device can be augmented wherein the enterprise service usage allocation comprises a classification of service usage that specifies one or more enterprise device software applications. In some embodiments, the enterprise applications can be one or more of email, calendar, contacts, enterprise intranet (e.g., a secure intranet browser

with a secure SSL connection or other secure connection to enterprise services), mobile device synchronization or mobile enterprise communications.

[00170] In some embodiments, the network system for classifying the accounting of access network service usage for an end user device can be augmented wherein the enterprise service usage allocation comprises a classification of service usage that specifies one or more enterprise network destinations.

[00171] In some embodiments, the network system for classifying the accounting of access network service usage for an end user device can be augmented wherein the enterprise service usage allocation comprises a classification of service usage that specifies one or more enterprise network destinations and the one or more enterprise network destinations comprise an address or identifier for a secure enterprise gateway. In some embodiments, the enterprise gateway comprises a VPN server.

[00172] In some embodiments, the network system for classifying the accounting of access network service usage for an end user device can be augmented wherein the enterprise service usage allocation comprises a classification of service usage that specifies one or more enterprise network destinations and the one or more enterprise network destinations comprise an address or identifier for one or more secure enterprise mobile services gateways or servers comprising one or more of an email server, a calendar server, a contacts server, an enterprise intranet access server, a mobile device synchronization services server or a mobile enterprise communication server.

[00173] In some embodiments, the network system for classifying the accounting of access network service usage for an end user device can be augmented wherein the one or more network elements responsible for classifying service usage and generating service usage reports comprises a service usage monitor located in a wireless operator network.

[00174] In some embodiments, the network system for classifying the accounting of access network service usage for an end user device can be augmented wherein the one or more network elements responsible for classifying service usage and generating service usage reports comprises a service usage monitor located in an enterprise access network.

[00175] In some embodiments, the network system for classifying the accounting of access network service usage for an end user device can be augmented wherein the one or more

network elements responsible for classifying service usage and generating service usage reports comprises a service usage monitor located on a wireless device.

[00176] In some embodiments, the network system for classifying the accounting of access network service usage for an end user device can be augmented wherein the service usage accounting system is located in an enterprise network.

[00177] In some embodiments, the network system for classifying the accounting of access network service usage for an end user device can be augmented wherein the service usage accounting system is managed by an enterprise manager under the control of the entity that manages an enterprise business.

[00178] In some embodiments, the network system for classifying the accounting of access network service usage for an end user device can be augmented wherein the service usage accounting system is located in an operator network.

[00179] In some embodiments, the network system for classifying the accounting of access network service usage for an end user device can be augmented wherein the service usage accounting system is managed by an operator manager under the control of the entity that manages a network operator.

[00180] In some embodiments, the network system for classifying the accounting of access network service usage for an end user device can be augmented wherein the service usage accounting system is further configured to credit a user account with a service usage credit or monetary credit associated with the accrued enterprise service usage allocation.

[00181] In some embodiments, the network system for classifying the accounting of access network service usage for an end user device can be augmented wherein the service usage accounting system is further configured to debit a user account with a service usage debit or monetary cost associated with the accrued personal service usage allocation.

[00182] In some embodiments, the network system for classifying the accounting of access network service usage for an end user device can be augmented wherein the service usage accounting system is further configured to credit an enterprise account with a service usage credit or monetary credit associated with the accrued personal service usage allocation.

[00183] In some embodiments, the network system for classifying the accounting of access network service usage for an end user device can be augmented wherein the service usage accounting system is further configured to debit an enterprise account with a service usage debit or monetary cost associated with the accrued enterprise service usage allocation.

[00184] In some embodiments, the network system for classifying the accounting of access network service usage for an end user device can be augmented by further configuring the service design center to: (i) receive a personal service plan offer comprising one or more service plans for personal network access services accounted to the personal service usage allocation, (ii) configure a device user interface service plan offer notification message, (iii) communicate the device user interface service plan offer notification message to one or more device groups comprising a collection of devices identified by device credentials, (iv) receive a service plan selection option from an end user device user in response to the device user interface service plan offer notification message, and (v) cause one or more network elements responsible for activating service plans to activate the service plan selection chosen by the end user device user.

[00185] In some embodiments the end-user device system in communication with the network system for classifying the accounting of access network service usage comprises: (i) a device software application environment comprising: (a) an enterprise application execution environment configured with: (1) an enterprise application execution memory and data memory to support secure execution of enterprise software applications, the enterprise software applications comprising applications approved to execute in the secure execution environment and to communicate with secure enterprise services, (2) a secure enterprise communication link configured to provide communication between the enterprise software applications and enterprise network services, the enterprise network services comprising enterprise network resources and servers, (b) a personal application execution environment configured with execution memory and data memory to support execution of personal software applications not approved to execute in the secure execution environment, (ii) a personal service plan selection user interface comprising a notification software agent configured to receive personal service plan offer from a network element and display the service plan offers, the personal service plan offer comprising one or more service plans for personal network access services accounted to a personal service usage allocation, and receive a service plan selection option from an end user device user and forward the service plan selection option to a network element.

[00186] In some embodiments, the end-user device system can be augmented wherein the secure enterprise communication link comprises a VPN client in communication with an enterprise VPN gateway.

[00187] In some embodiments, the end-user device system can be augmented wherein the enterprise network services comprise access to one or more secure enterprise mobile services gateways or servers comprising one or more of an email server, a calendar server, a contacts server, an enterprise intranet access server, a mobile device synchronization services server or a mobile enterprise communication server.

[00188] In some embodiments, the end-user device system can be augmented wherein the enterprise application execution environment is further configured to: (i) acquire a device software application signature prior to allowing execution of the device software application in the virtual machine operating environment, (ii) compare the signature to an approved list of signatures, (iii) allow the application to execute if it is on the list, and (iv) not allow the application to execute if it is not on the list.

[00189] In some embodiments, the end-user device system can be augmented wherein enterprise application execution environment comprises a virtual machine operating environment.

[00190] In some embodiments, the end-user device system can be augmented wherein enterprise application execution environment comprises a secure CPU hardware execution partition.

[00191] In some embodiments, the end-user device system can be augmented wherein enterprise application execution environment comprises a secure operating system execution partition.

[00192] In some embodiments, the end-user device system can be augmented wherein enterprise application execution environment comprises a secure memory area protected by an enterprise application software program that encrypts the enterprise data stored on device memory and runs a secure encrypted communication protocol for communication with a secure mobile enterprise services gateway server.

[00193] Several advantageous combination embodiments are now disclosed for providing enterprise control of network access service to an end user device. These combinations are for example purposes, are not meant to be exhaustive or limiting in any way; as would be appreciated by one of ordinary skill in the art, these combinations represent only a fraction of the advantageous embodiment combinations provided herein.

[00194] In some embodiments, a network system for providing network access service control for an end user device comprising: (i) a first service design center configured to receive from an administrator user or a configuration file a first network access policy comprising a first set of network access service permissions associated with an end user device or end user device user, (ii) a network provisioning instruction translator configured to receive the first network access policy and translate it to a set of network access policy enforcement instructions for one or more network elements responsible for controlling network access, (iii) a network provisioning system for communicating the set of network access policy enforcement instructions to the one or more network elements responsible for controlling network access, (iv) the one or more network elements responsible for controlling network access configured to execute the set of network access policy enforcement instructions to enforce network access service permissions and limits.

[00195] In some embodiments, the network system for providing network access service control can be augmented wherein the first network access policy is associated with a first device group defined by a first list of device credentials or a first user group defined by a first list of user credentials, and the service design center is further configured to obtain a second network access policy comprising a second set of network access service permissions and, the second network access policy associated with a second device group defined by a second list of device credentials or a second user group defined by a second list of user credentials.

[00196] In some embodiments, the network system for classifying the accounting of access network service usage for an end user device further comprises a master service design center configured to define a first network access policy design capability set for the first service design center, the first network access policy design capability set comprising a first subset of a master policy capability set. This embodiment can be further augmented wherein the master service design center is further configured to define a second network access policy design capability set for a second service design center, the second network access policy design

capability set comprising a second subset of the master policy capability set, the second subset of the master policy capability set either identical to or different from the first subset of the master policy capability set.

[00197] In some embodiments, the network system for providing network access service control can be augmented wherein the first network access policy defines a set of one or more service usage limits or service cost limits.

[00198] In some embodiments, the network system for providing network access service control can be augmented wherein the first network access policy defines a set of one or more roaming network service usage limits or service cost limits.

[00199] In some embodiments, the network system for providing network access service control can be augmented wherein the first network access policy defines a set of one or more network type restrictions, wherein a network type comprises one or more of a cellular network, a 2G network, a 3G network, a 4G network, a WiFi network, a particular WiFi network APN, roaming cellular network, a particular cellular operator network.

[00200] In some embodiments, the network system for providing network access service control can be augmented wherein the first network access policy defines a set of one or more device application software network access restrictions.

[00201] In some embodiments, the network system for providing network access service control can be augmented wherein the first network access policy defines a set of one or more network destination access restrictions.

[00202] In some embodiments, the network system for providing network access service control can be augmented wherein the first network access policy defines a set of one or more enterprise network destination allowances or restrictions.

[00203] In some embodiments, the network system for providing network access service control can be augmented wherein the first network access policy defines a set of one or more enterprise network destination allowances or restrictions communicated over a secure VPN communication link.

[00204] In some embodiments, the network system for providing network access service control can be augmented wherein the first network access policy defines a set of one or more

application or network destination allowances or restrictions communicated over a non-secure communication link.

[00205] In some embodiments, the network system for providing network access service control can be augmented wherein the first network access policy defines a set of one or more personal application or network destination allowances or restrictions.

[00206] In some embodiments, the network system for providing network access service control can be augmented wherein the first network access policy defines a set of one or more geographic location allowances or restrictions.

[00207] In some embodiments, the network system for providing network access service control can be augmented wherein the one or more network elements responsible for controlling network access comprises a service usage monitor located in a wireless operator network.

[00208] In some embodiments, the network system for providing network access service control can be augmented wherein the one or more network elements responsible for controlling network access comprises a service usage monitor located in an enterprise access network. In some embodiments, the one or more network elements responsible for controlling network access comprises a service usage monitor located in an enterprise access network comprise a VPN gateway wherein all device traffic is communicated from the device to the VPN gateway configured to control the device traffic. In some embodiments, the VPN gateway performs service usage classification to identify and control enterprise traffic. In some embodiments, the VPN gateway performs service usage classification to identify and control personal traffic.

[00209] In some embodiments, the network system for providing network access service control can be augmented wherein the one or more network elements responsible for controlling network access comprises a service usage monitor located on a wireless device.

CLAIMS

1. A network system for providing network access service notification messages containing information about a network access activity of an end-user device, the network system comprising:

a first service design center configured to:

obtain a first network access notification message policy comprising a first network access trigger condition and an associated first network access notification message, the first network access trigger condition comprising one or more current or requested end-user device network access activities, the first network access notification message comprising notification information to be presented to a user through a user interface,

receive a trigger condition indication from a network element,

associate the trigger condition indication with the first network access notification message, and

present the notification information to the user through the user interface;

a network provisioning instruction translator configured to:

receive, from the first service design center, the first network access trigger condition, and

determine, based on the first network access trigger condition, one or more network access trigger identification instructions; and

a network provisioning system configured to communicate the one or more network access trigger identification instructions to one or more network elements responsible for monitoring the service usage, the one or more network elements responsible for monitoring the service usage configured to:

execute the one or more network access trigger identification instructions to identify when the first network access trigger condition occurs, and

send the trigger condition indication to the first service design center.

2. The network system recited in claim 1, further comprising a master service design center configured to define a first notification policy design capability set for the first service design center, the first notification policy design capability set comprising a first subset of a master policy capability set.

3. The network system of claim 2, wherein the master service design center is further configured to define a second notification policy design capability set for a second service

design center, the second notification policy design capability set comprising a second subset of the master policy capability set, the second subset of the master policy capability set either identical to or different from the first subset of the master policy capability set.

4. The network system recited in claim 1, wherein the first network access trigger condition comprises a period of time since a previous network access trigger condition, and the first network access notification message comprises a real-time or near-real-time measure of an amount of service usage or a cost of service usage.

5. The network system recited in claim 1, wherein the first network access trigger condition comprises an amount of service usage or a cost of service usage, and the first network access notification message comprises a real-time or near-real-time measure of an aggregate service usage or an aggregate cost.

6. The network system recited in claim 1, wherein the service design center is further configured to send a user notification message to a user of the end-user device based on the first network access notification message.

7. The network system recited in claim 1, wherein the first service design center is hosted on an operator network.

8. The network system recited in claim 1, wherein the first service design center is hosted on an enterprise network.

9. The network system recited in claim 1, wherein the first network access trigger condition comprises a service usage limit or a specified amount of accrued cost.

10. The network system recited in claim 1, wherein the first network access trigger condition comprises a roaming service usage limit or specified amount of accrued roaming service cost.

11. The network system recited in claim 1, wherein the one or more network elements responsible for monitoring the service usage are configured to classify service usage by device

application, and the first network access trigger condition comprises one or more device application access activities.

12. The network system recited in claim 1, wherein the one or more network elements responsible for monitoring service usage are configured to classify service usage by network destination, and the first network access trigger condition comprises one or more device network destination access activities.

13. The network system recited in claim 1, wherein the one or more network elements responsible for monitoring service usage comprise a service usage monitor located in a wireless operator network.

14. The network system recited in claim 1, wherein the one or more network elements responsible for monitoring service usage comprise a service usage monitor located in an enterprise access network.

15. The network system recited in claim 1, wherein the one or more network elements responsible for monitoring service usage comprise a service usage monitor located on a wireless device.

16. The network system recited in claim 1, wherein the first network access notification message policy is associated with a first device group defined by a first list of device credentials or a first user group defined by a first list of user credentials, and the service design center is further configured to obtain a second network access notification message policy comprising a plurality of second network access trigger conditions and, for each of the plurality of second network access trigger conditions, an associated second network access notification message, the second network access notification message policy associated with a second device group defined by a second list of device credentials or a second user group defined by a second list of user credentials.

17. The network system recited in claim 16, wherein the first network access notification message policy comprises a subset of the second network access notification message policy.

18. A network system for classifying an accounting of access network service usage by an end-user device, the network system comprising:

a first service design center configured to:

obtain a first accounting split classification policy defining classification rules for dividing an overall access network service usage into an enterprise service usage allocation and a personal service usage allocation;

a network provisioning instruction translator configured to:

receive the first accounting split classification policy from the first service design center, and

determine, based on the first accounting split classification policy, one or more network service usage classification and reporting instructions;

a network provisioning system configured to communicate the one or more network service usage classification and reporting instructions to one or more network elements responsible for classifying the service usage, the one or more network elements responsible for classifying the service usage configured to:

execute the one or more network service usage classification and reporting instructions to determine the enterprise service usage allocation and the personal service usage allocation, and

generate a service usage report; and

a service usage accounting system configured to receive the service usage report and, based on the usage report, accrue the enterprise service usage allocation and accrue the personal service usage allocation.

19. The network system as recited in claim 18, further comprising a master service design center configured to define a first accounting policy design capability set for the first service design center, the first accounting policy design capability set comprising a first subset of a master policy capability set.

20. The network system of claim 19, wherein the master service design center is further configured to define a second accounting policy design capability set for a second service design center, the second accounting policy design capability set comprising a second subset of the master policy capability set, the second subset of the master policy capability set either identical to or different from the first subset of the master policy capability set.

21. The network system recited in claim 1, wherein the first accounting split classification policy is associated with a first device group defined by a first list of device credentials or a first user group defined by a first list of user credentials, and the service design center is further configured to obtain a second accounting split classification policy, the second accounting split classification message policy associated with a second device group defined by a second list of device credentials or a second user group defined by a second list of user credentials.

22. The network system recited in claim 21, wherein the first accounting split classification policy comprises a subset of the second accounting split classification policy.

23. A communications device comprising:

a secure enterprise application execution environment comprising:

memory configured to support secure execution of an enterprise software application, the enterprise software application approved by an enterprise to execute in the secure enterprise application execution environment and to access one or more secure enterprise services, and

a secure enterprise communication link configured to provide communication between the enterprise software application and one or more network resources and servers associated with at least one of the one or more secure enterprise services, and

a personal application execution environment comprising memory to support execution of personal software applications not approved by the enterprise to execute in the secure enterprise application execution environment or to access the one or more secure enterprise services; and

one or more device agents configured to:

receive a personal service plan offer from a network element, the personal service plan offer comprising one or more service plans to enable the communications device to access available network services accounted to a personal service usage allocation,

present the personal service plan offer to a user of the communications device through a user interface of the communications device,

obtain a user response to the personal service plan offer through the user interface of the communications device, and

send the user response to the network element.

24. A network system for providing network access service control for an end-user device, the network system comprising:

a first service design center configured to obtain a first network access policy comprising one or more network access service permissions associated with the end-user device or a user of the end-user device;

a network provisioning instruction translator configured to:

receive, from the first service design center, the first network access policy, and

determine, based on the first network access policy, one or more network access policy enforcement instructions; and

a network provisioning system configured to communicate the one or more network access policy enforcement instructions to one or more network elements responsible for controlling network access, the one or more network elements responsible for controlling the service usage configured to:

execute the one or more network access policy enforcement instructions to enforce network access service permissions and limits.

25. The network system recited in claim 24, further comprising a master service design center configured to define a first control policy design capability set for the first service design center, the first control policy design capability set comprising a first subset of a master policy capability set.

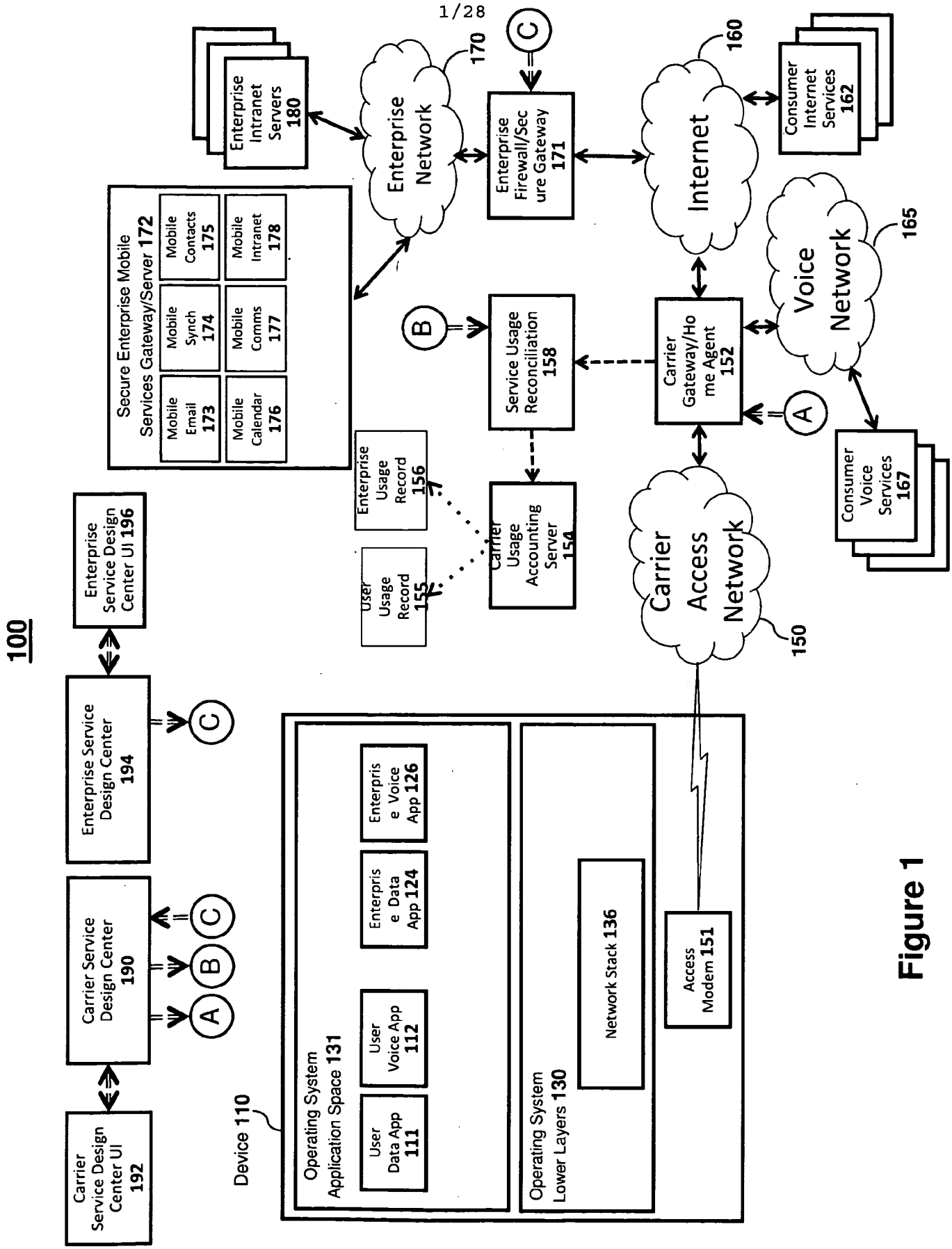
100
Carrier Service Design Center UI 192
Carrier Service Design Center 190
Enterprise Service Design Center 194
Enterprise Service Design Center UI 196
A
B
C
Device 110
Operating System Application Space 131
User Data App 111
User Voice App 112
Enterpris e Data App 124
Enterpris e Voice App 126
Operating System Lower Layers 130
Network Stack 136
Access Modem 151
Carrier Access Network 150
Carrier Usage Accounting Server 154
User Usage Record 155
Enterprise Usage Record 156
Service Usage Reconciliation 158
Carrier Gateway/Ho me Agent 152
Secure Enterprise Mobile Services Gateway/Server 172
Mobile Email 173
Mobile Calendar 176
Mobile Synch 174
Mobile Comms 177
Mobile Contacts 175
Mobile Intranet 178
Enterprise Network 170
Enterprise Intranet Servers 180
Enterprise Firewall/Sec ure Gateway 171
Internet 160
Consumer Internet Services 162
Voice Network 165
Consumer Voice Services 167

Figure 1

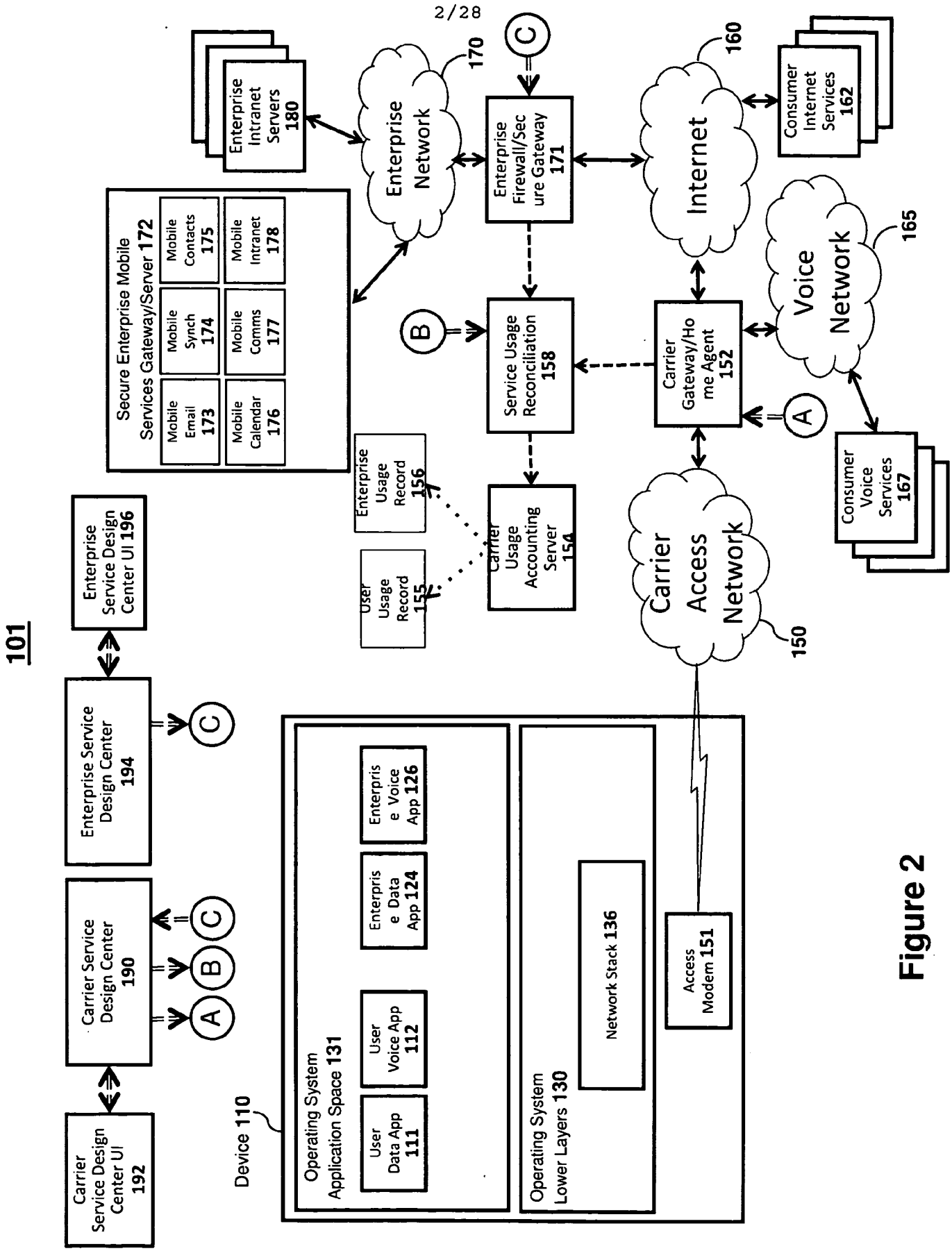
101
Carrier Service Design UI 192
Carrier Service Design Center 190
Enterprise Service Design Center 194
Enterprise Service Design Center UI 196
A
B
C
Device 110
Operating System Application Space 131
User Data App 111
User Voice App 112
Enterpris e Data App 124
Enterpris e Voice App 126
Operating System Lower Layers 130
Network Stack 136
Access Modem 151
Carrier Access Network 150
Carrier Usage Accounting Server 154
User Usage Record 155
Enterprise Usage Record 156
Service Usage Reconciliation 158
Carrier Gateway/Ho me Agent 152
Secure Enterprise Mobile Services Gateway/Server 172
Mobile Email 173
Mobile Synch 174
Mobile Contacts 175
Mobile Calendar 176
Mobile Comms 177
Mobile Intranet 178
Enterprise Intranet Servers 180
Enterprise Network 170
Enterprise Firewall/Sec ure Gateway 171
Internet 160
Consumer Internet Services 162
Voice Network 165
Consumer Voice Services 167

Figure 2

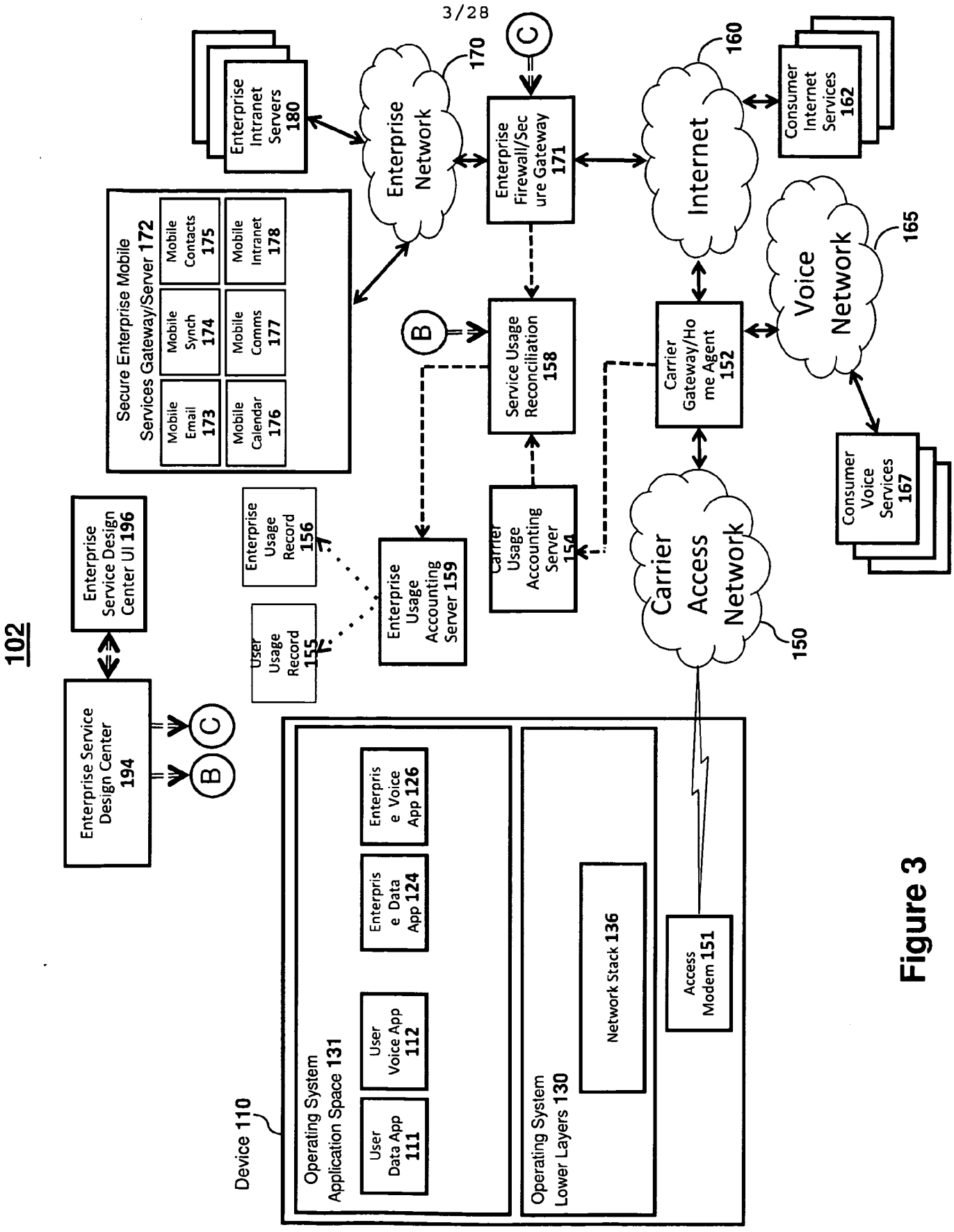
102
Enterprise Service Design Center 194
Enterprise Service Design Center UI 196
B
C
Device 110
Operating System Application Space 131
User Data App 111
User Voice App 112
Enterpris e Data App 124
Enterpris e Voice App 126
Operating System Lower Layers 130
Network Stack 136
Access Modem 151
Carrier Access Network 150
User Usage Record 155
Enterprise Usage Record 156
Enterprise Usage Accounting Server 159
Carrier Usage Accounting Server 154
Service Usage Reconciliation 158
Carrier Gateway/Ho me Agent 152
Secure Enterprise Mobile Services Gateway/Server 172
Mobile Email 173
Mobile Calendar 176
Mobile Synch 174
Mobile Comms 177
Mobile Contacts 175
Mobile Intranet 178
Enterprise Network 170
Enterprise Intranet Servers 180
Enterprise Firewall/Sec ure Gateway 171
Internet 160
Consumer Internet Services 162
Voice Network 165
Consumer Voice Services 167

Figure 3

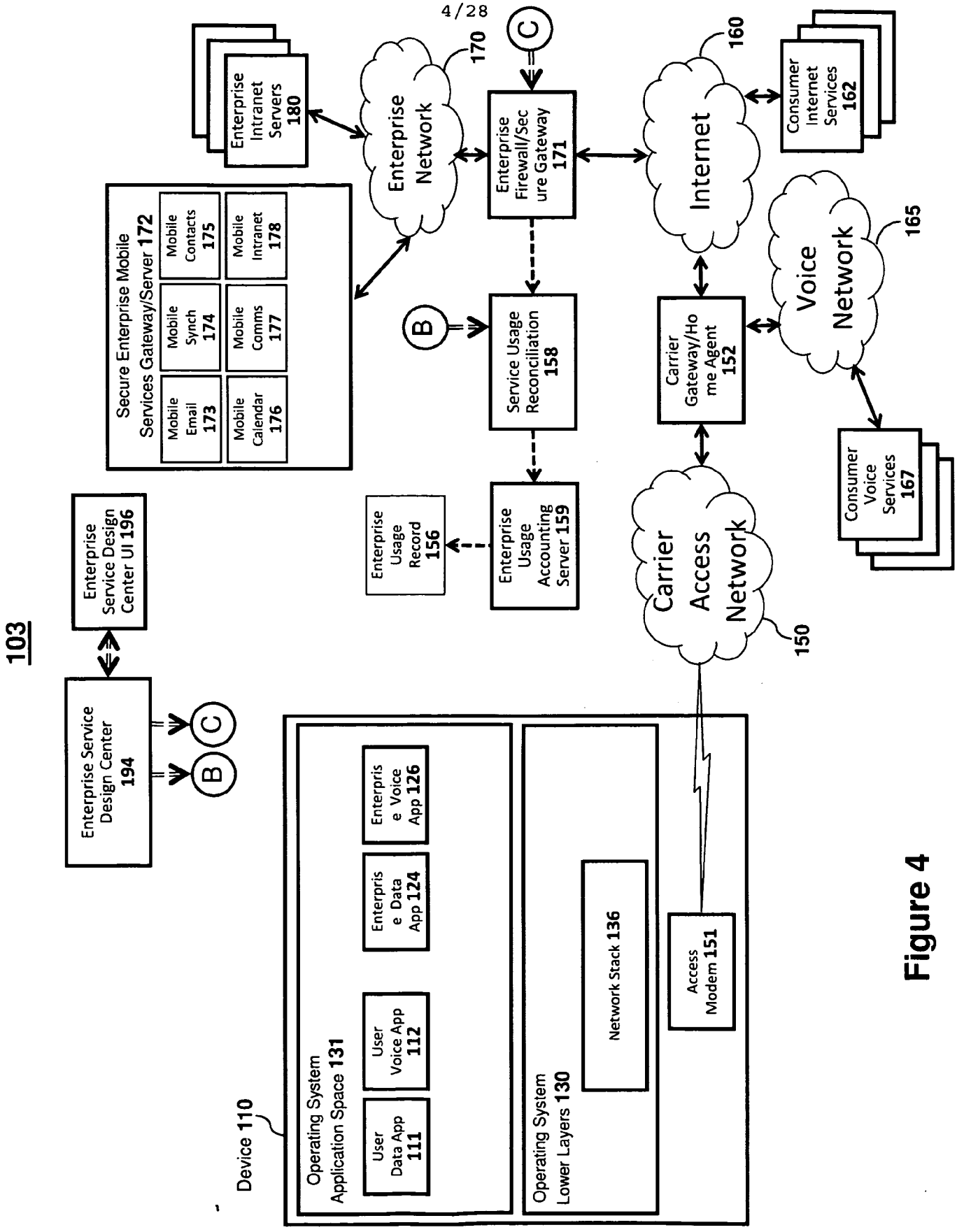
103
Enterprise Service Design Center 194
Enterprise Service Design Center UI 196
B
C
Device 110
Operating System Application Space 131
User Data App 111
User Voice App 112
Enterpris e Data App 124
Enterpris e Voice App 126
Operating System Lower Layers 130
Network Stack 136
Access Modem 151
Carrier Access Network 150
Secure Enterprise Mobile Services Gateway/Server 172
Mobile Email 173
Mobile Calendar 176
Mobile Synch 174
Mobile Comms 177
Mobile Contacts 175
Mobile Intranet 178
Enterprise Intranet Servers 180
Enterprise Network 170
Enterprise Firewall/Sec ure Gateway 171
Service Usage Reconciliation 158
Enterprise Usage Record 156
Enterprise Usage Accounting Server 159
Carrier Gateway/Ho me Agent 152
Internet 160
Consumer Internet Services 162
Voice Network 165
Consumer Voice Services 167

Figure 4

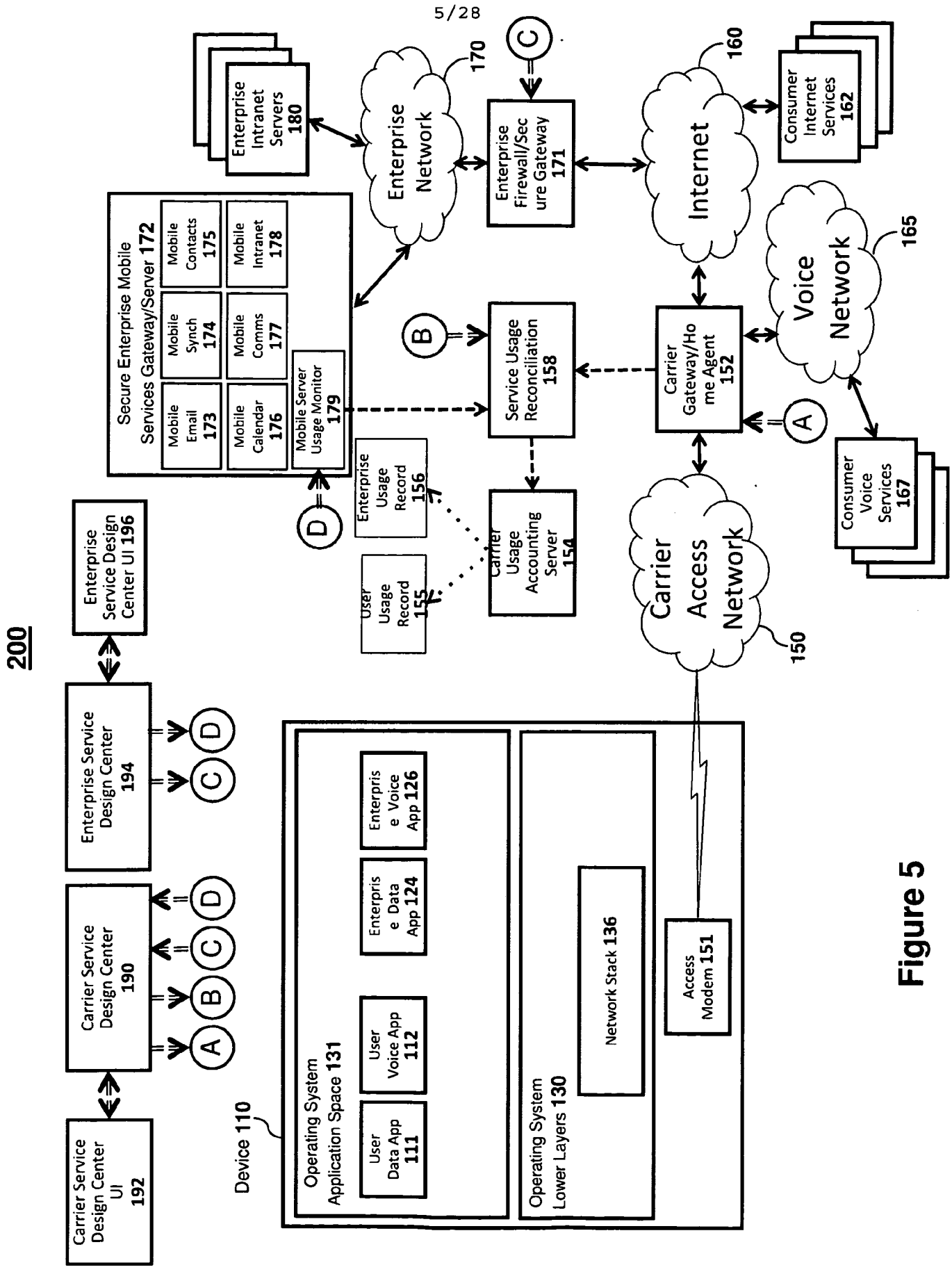
200
Carrier Service Design Center UI 192
Carrier Service Design Center 190
Enterprise Service Design Center 194
Enterprise Service Design Center UI 196
A
B
C
D
Device 110
Operating System Application Space 131
User Data App 111
User Voice App 112
Enterpris e Data App 124
Enterpris e Voice App 126
Operating System Lower Layers 130
Network Stack 136
Access Modem 151
Carrier Access Network 150
Secure Enterprise Mobile Services Gateway/Server 172
Mobile Email 173
Mobile Calendar 176
Mobile Server Usage Monitor 179
Mobile Synch 174
Mobile Comms 177
Mobile Contacts 175
Mobile Intranet 178
Enterprise Usage Record 156
User Usage Record 155
Carrier Usage Accounting Server 154
Service Usage Reconciliation 158
Carrier Gateway/Ho me Agent 152
Enterprise Network 170
Enterprise Intranet Servers 180
Enterprise Firewall/Sec ure Gateway 171
Internet 160
Consumer Internet Services 162
Voice Network 165
Consumer Voice Services 167

Figure 5

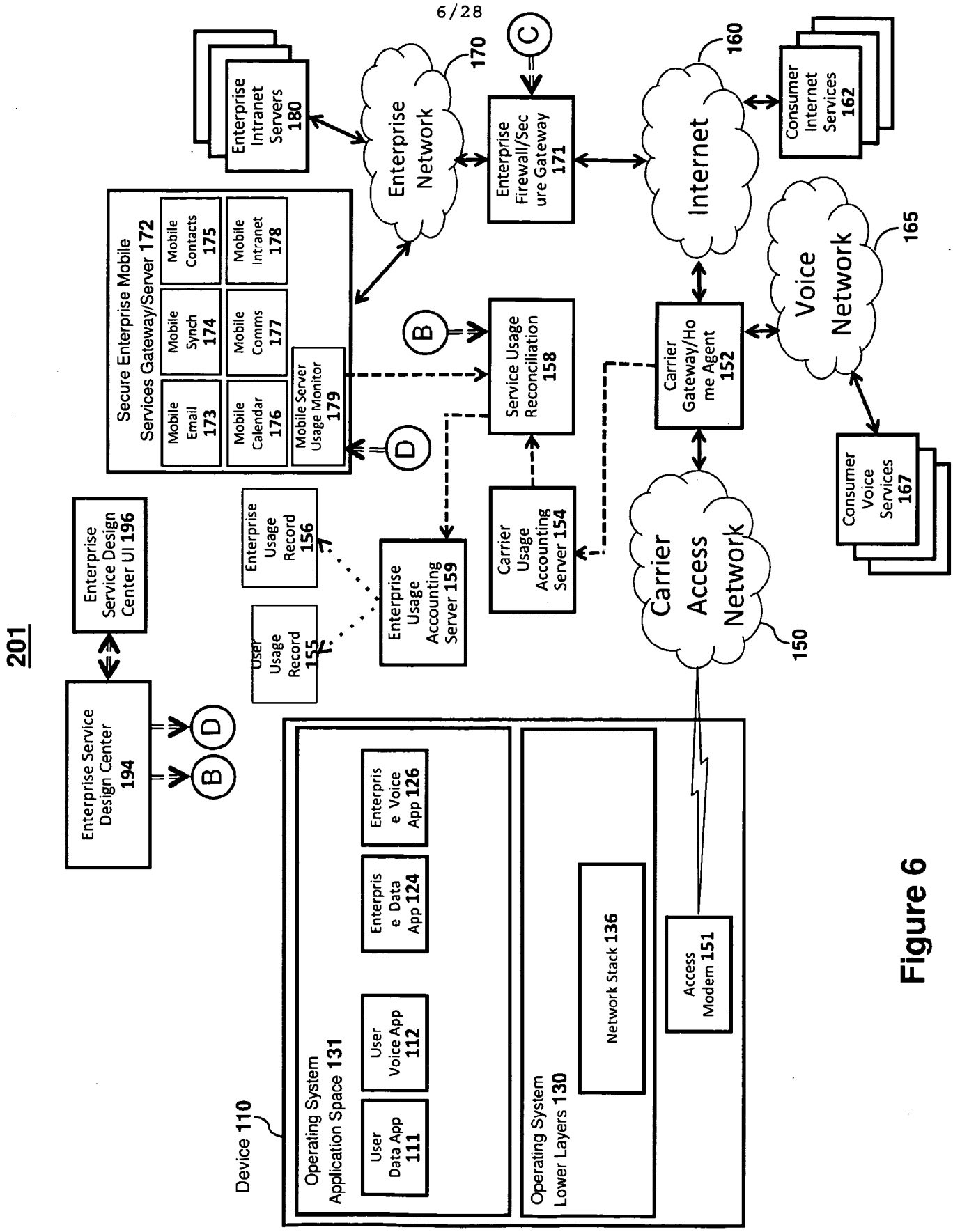
201
Enterprise Service Design Center 194
Enterprise Service Design Center UI 196
Device 110
Operating System Application Space 131
User Data App 111
User Voice App 112
Enterpris e Data App 124
Enterpris e Voice App 126
Operating System Lower Layers 130
Network Stack 136
Access Modem 151
Carrier Access Network 150
Enterprise Usage Record 156
User Usage Record 155
Enterprise Usage Accounting Server 159
Carrier Usage Accounting Server 154
Service Usage Reconciliation 158
Secure Enterprise Mobile Services Gateway/Server 172
Mobile Email 173
Mobile Calendar 176
Mobile Server Usage Monitor 179
Mobile Synch 174
Mobile Comms 177
Mobile Contacts 175
Mobile Intranet 178
Enterprise Network 170
Enterprise Intranet Servers 180
Enterprise Firewall/Sec ure Gateway 171
Internet 160
Consumer Internet Services 162
Carrier Gateway/Ho me Agent 152
Voice Network 165
Consumer Voice Services 167
A
B
C
D

Figure 6

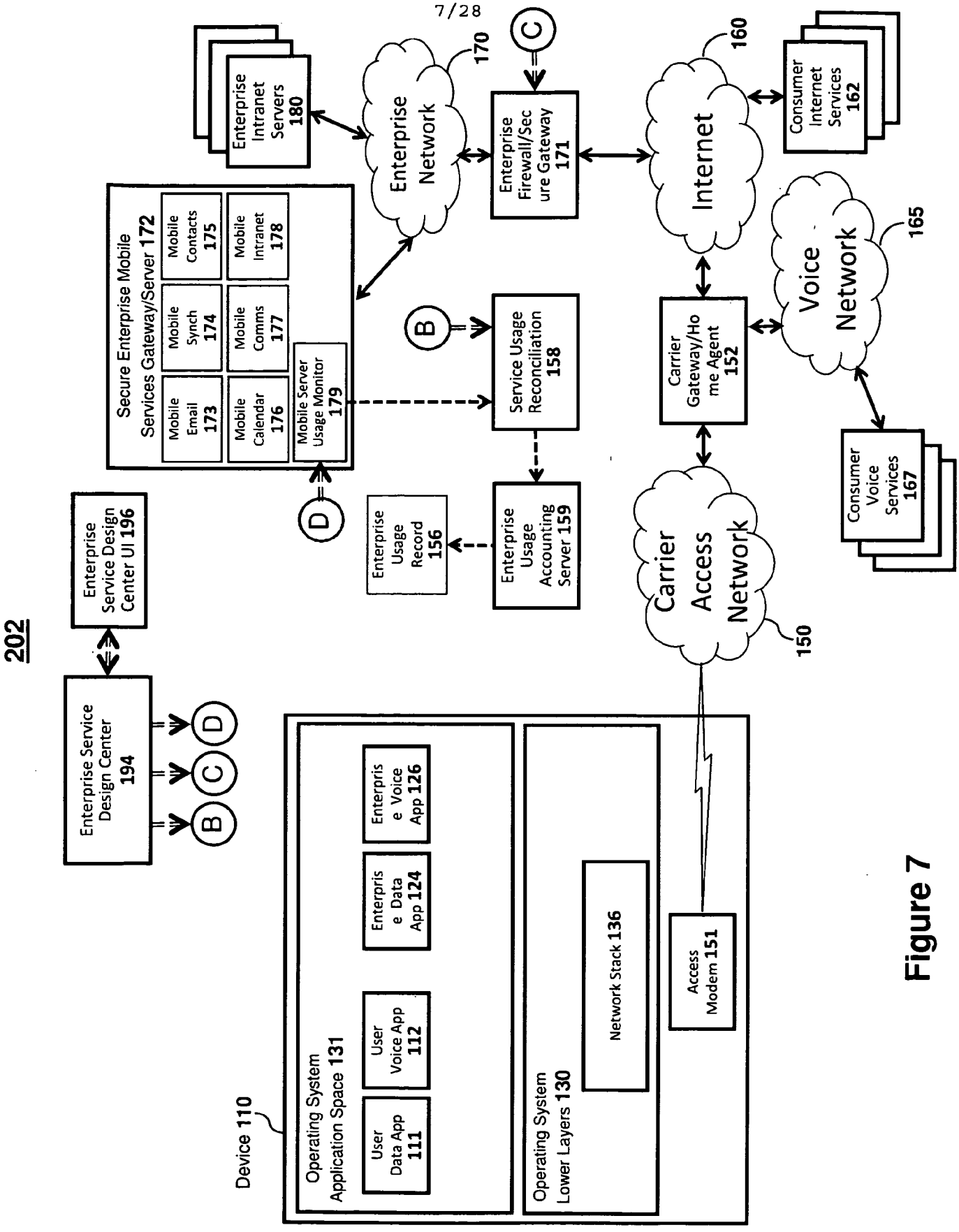
202
Enterprise Service Design Center 194
Enterprise Service Design Center UI 196
Device 110
Operating System Application Space 131
User Data App 111
User Voice App 112
Enterpris e Data App 124
Enterpris e Voice App 126
Operating System Lower Layers 130
Network Stack 136
Access Modem 151
Carrier Access Network 150
Carrier Gateway/Ho me Agent 152
Voice Network 165
Consumer Voice Services 167
Internet 160
Consumer Internet Services 162
Enterprise Firewall/Sec ure Gateway 171
Enterprise Network 170
Enterprise Intranet Servers 180
Secure Enterprise Mobile Services Gateway/Server 172
Mobile Email 173
Mobile Synch 174
Mobile Contacts 175
Mobile Calendar 176
Mobile Comms 177
Mobile Intranet 178
Mobile Server Usage Monitor 179
Service Usage Reconciliation 158
Enterprise Usage Accounting Server 159
Enterprise Usage Record 156
A
B
C
D

Figure 7

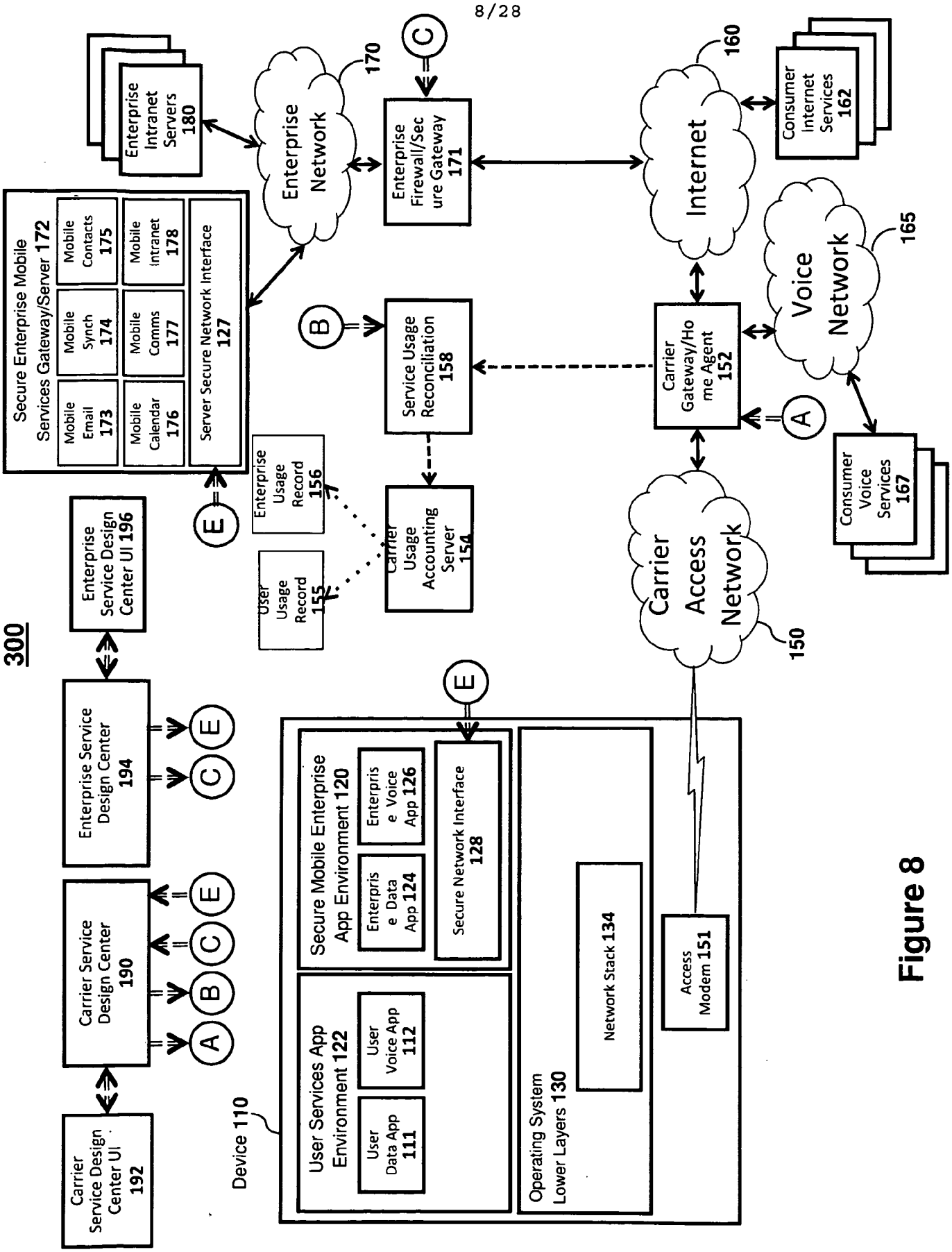
300
Carrier Service Design UI 192
Carrier Service Design Center 190
Enterprise Service Design Center 194
Enterprise Service Design Center UI 196
A
B
C
E
Device 110
User Services App Environment 122
User Data App 111
User Voice App 112
Secure Mobile Enterprise App Environment 120
Enterprise Data App 124
Enterprise Voice App 126
Secure Network Interface 128
Operating System Lower Layers 130
Network Stack 134
Access Modem 151
Carrier Access Network 150
Carrier Gateway/Home Agent 152
Carrier Usage Accounting Server 154
User Usage Record 155
Enterprise Usage Record 156
Service Usage Reconciliation 158
Secure Enterprise Mobile Services Gateway/Server 172
Mobile Email 173
Mobile Synch 174
Mobile Contacts 175
Mobile Calendar 176
Mobile Comms 177
Mobile Intranet 178
Server Secure Network Interface 127
Enterprise Intranet Servers 180
Enterprise Network 170
Enterprise Firewall/Secure Gateway 171
Internet 160
Consumer Internet Services 162
Voice Network 165
Consumer Voice Services 167

Figure 8

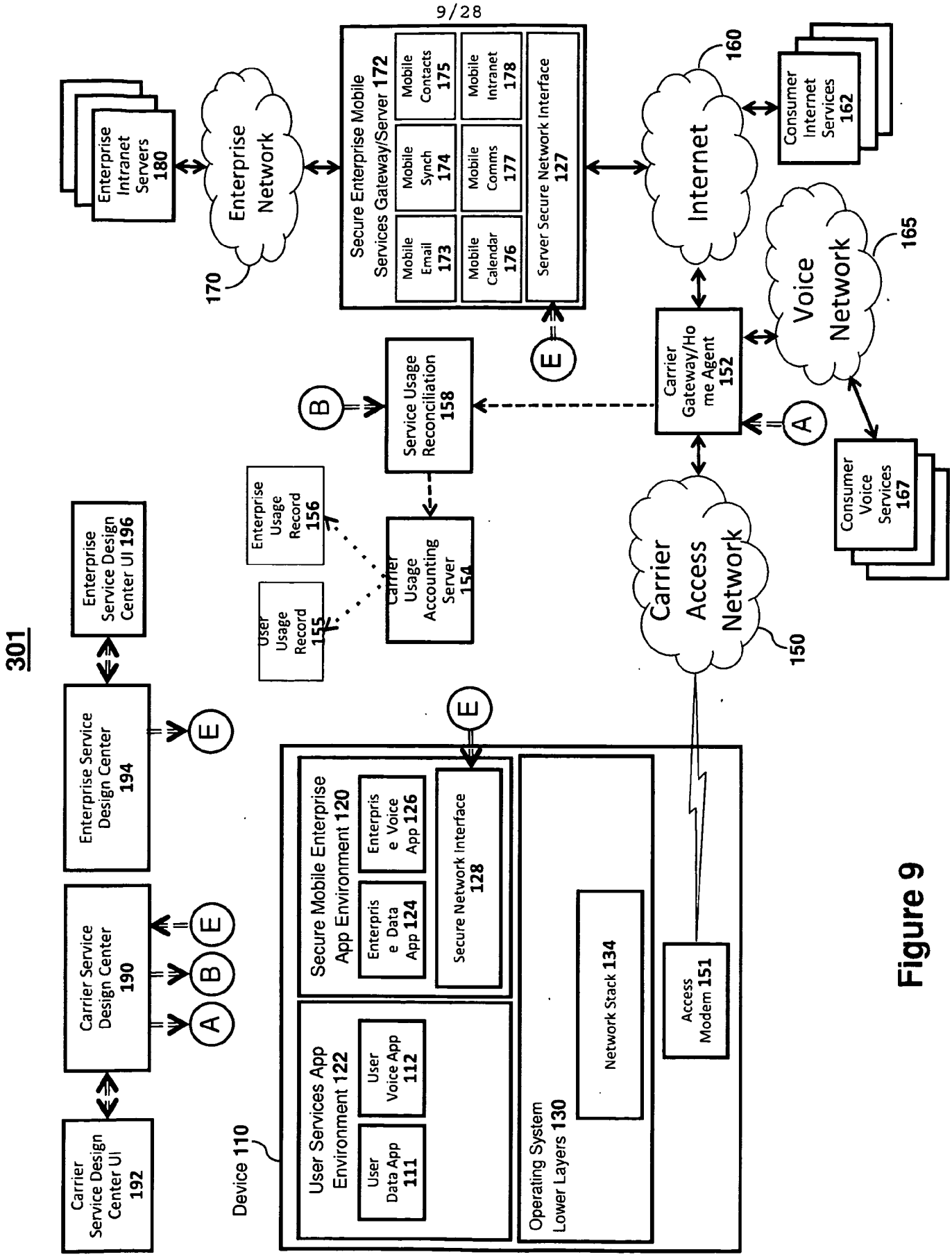
301
Carrier Service Design UI 192
Carrier Service Design Center 190
Enterprise Service Design Center UI 196
Enterprise Service Design Center 194
A
B
E
Device 110
User Services App Environment 122
User Data App 111
User Voice App 112
Secure Mobile Enterprise App Environment 120
Enterprise Data App 124
Enterprise Voice App 126
Secure Network Interface 128
Operating System Lower Layers 130
Network Stack 134
Access Modem 151
Carrier Access Network 150
Carrier Gateway/Home Agent 152
Carrier Usage Accounting Server 154
Service Usage Reconciliation 158
User Usage Record 155
Enterprise Usage Record 156
Enterprise Network 170
Enterprise Intranet Servers 180
Secure Enterprise Mobile Services Gateway/Server 172
Mobile Email 173
Mobile Synch 174
Mobile Comms 177
Mobile Contacts 175
Mobile Intranet 178
Mobile Calendar 176
Server Secure Network Interface 127
Internet 160
Consumer Internet Services 162
Voice Network 165
Consumer Voice Services 167

Figure 9

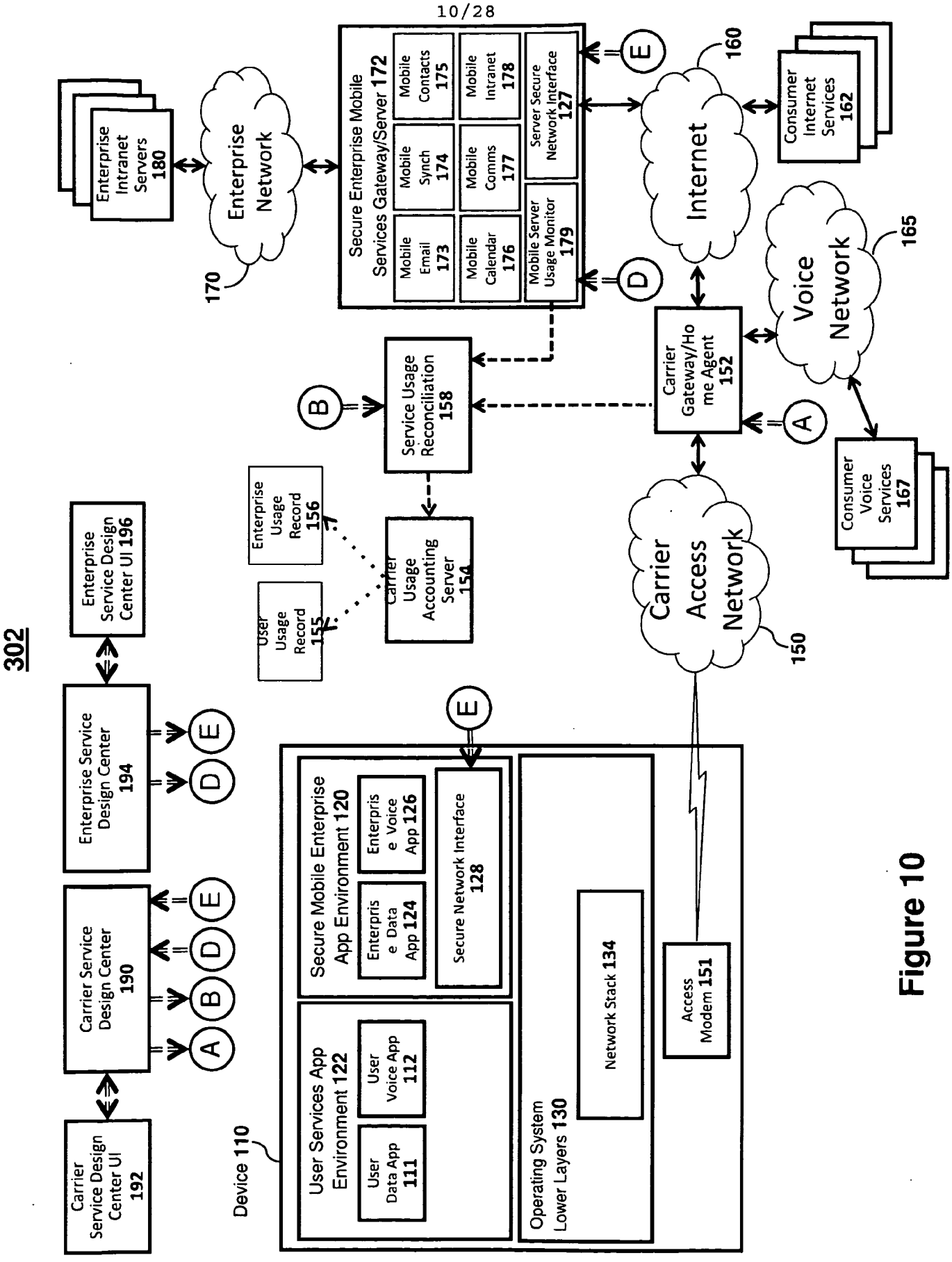
302
Carrier Service Design UI 192
Carrier Service Design Center 190
Enterprise Service Design Center UI 196
Enterprise Service Design Center 194
A
B
D
E
Device 110
User Services App Environment 122
User Data App 111
User Voice App 112
Secure Mobile Enterprise App Environment 120
Enterpris e Data App 124
Enterpris e Voice App 126
Secure Network Interface 128
Operating System Lower Layers 130
Network Stack 134
Access Modem 151
Carrier Access Network 150
Enterprise Usage Record 156
User Usage Record 155
Carrier Usage Accounting Server 154
Service Usage Reconciliation 158
Carrier Gateway/Ho me Agent 152
Voice Network 165
Consumer Voice Services 167
Internet 160
Consumer Internet Services 162
Secure Enterprise Mobile Services Gateway/Server 172
Mobile Email 173
Mobile Synch 174
Mobile Contacts 175
Mobile Calendar 176
Mobile Comms 177
Mobile Intranet 178
Mobile Server Usage Monitor 179
Server Secure Network Interface 127
Enterprise Network 170
Enterprise Intranet Servers 180

Figure 10

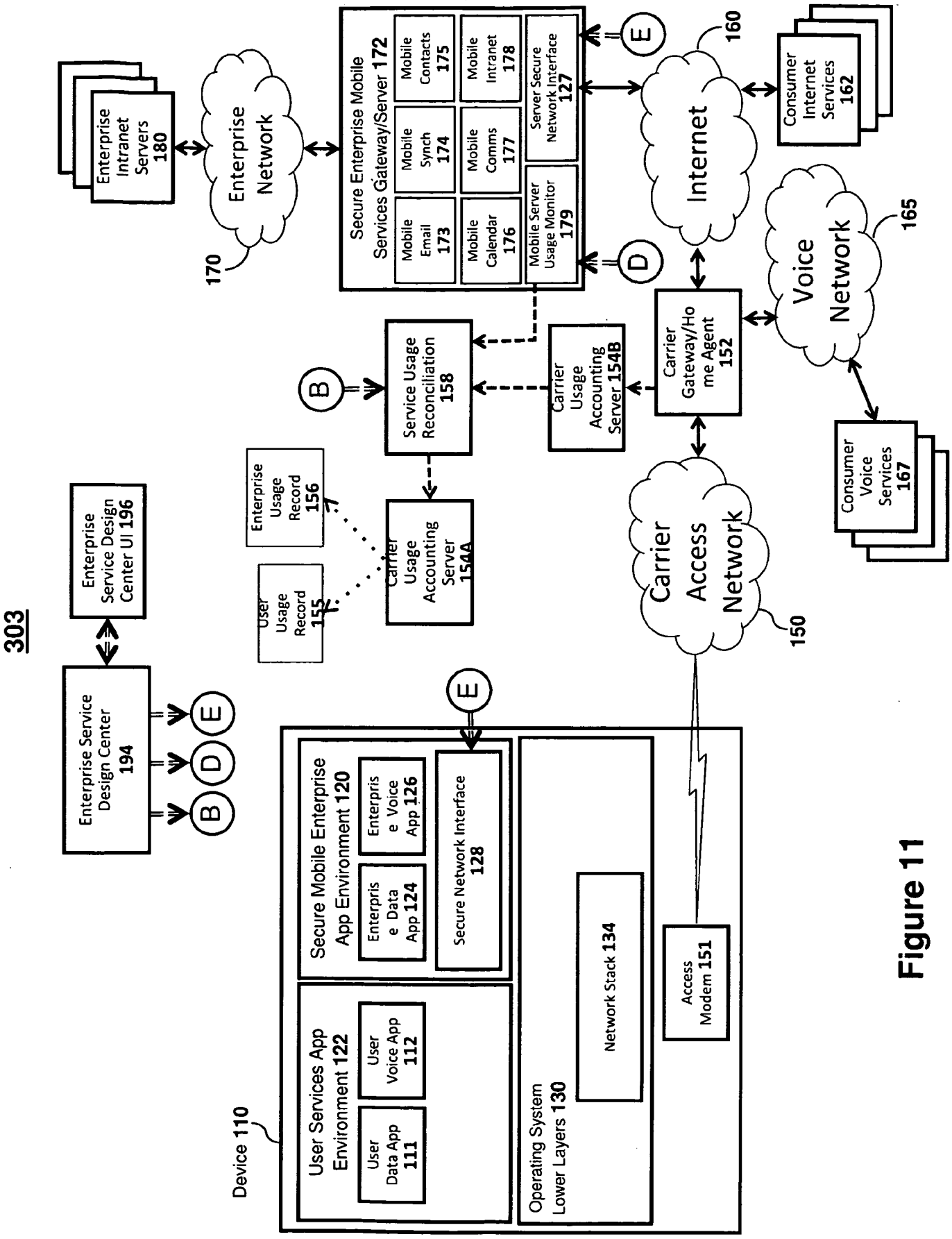
303
Enterprise Intranet Servers 180
Enterprise Network 170
Secure Enterprise Mobile Services Gateway/Server 172
Mobile Email 173
Mobile Synch 174
Mobile Contacts 175
Mobile Calendar 176
Mobile Comms 177
Mobile Intranet 178
Mobile Server Usage Monitor 179
Server Secure Network Interface 127
Internet 160
Consumer Internet Services 162
Voice Network 165
Consumer Voice Services 167
Carrier Gateway/Home Agent 152
Carrier Access Network 150
Service Usage Reconciliation 158
Carrier Usage Accounting Server 154B
Carrier Usage Accounting Server 154A
Enterprise Usage Record 156
User Usage Record 155
Enterprise Service Design Center UI 196
Enterprise Service Design Center 194
Device 110
User Services App Environment 122
User Data App 111
User Voice App 112
Secure Mobile Enterprise App Environment 120
Enterprise Data App 124
Enterprise Voice App 126
Secure Network Interface 128
Operating System Lower Layers 130
Network Stack 134
Access Modem 151
A
B
D
E

Figure 11

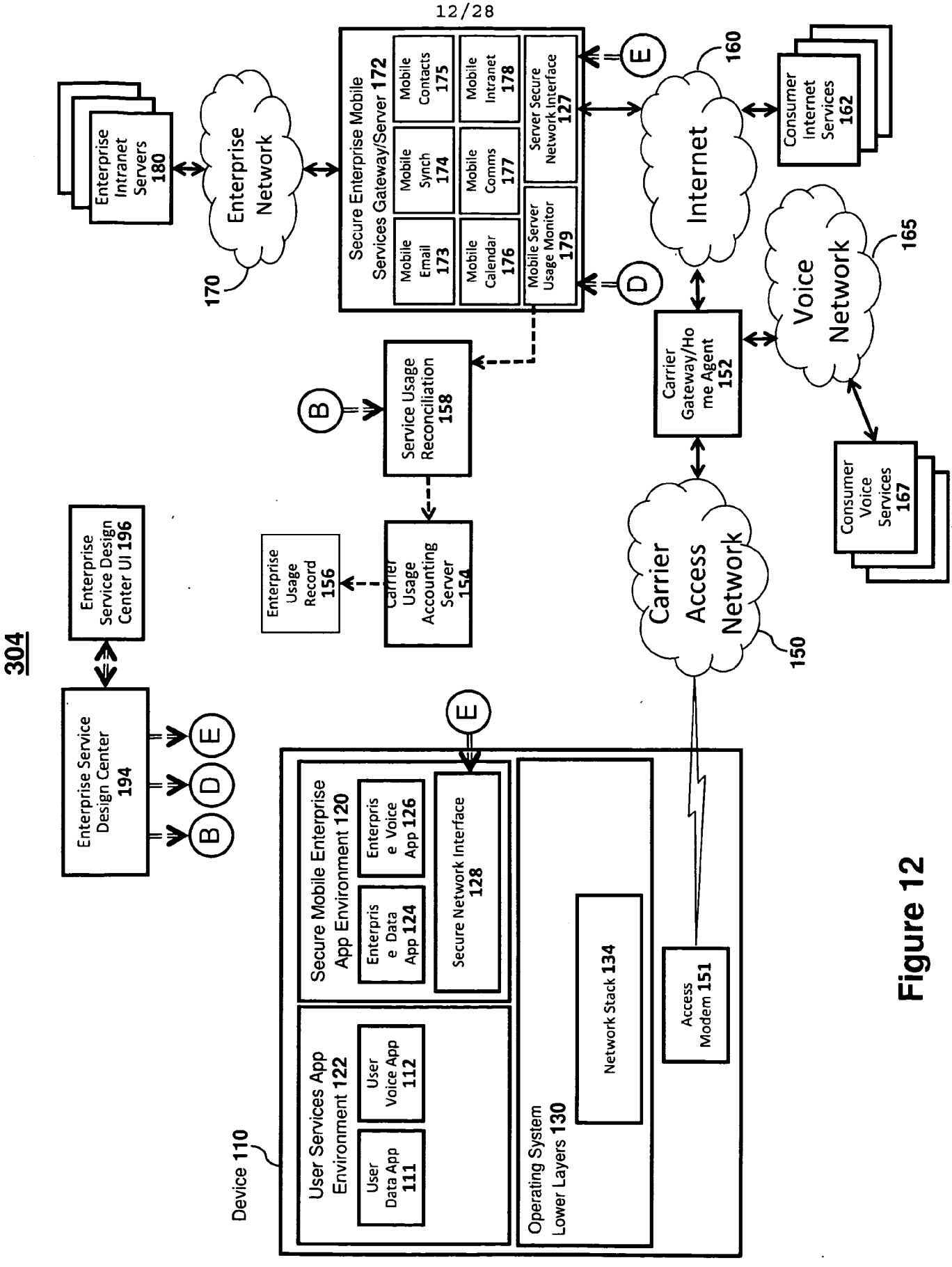
304
Enterprise Service Design Center 194
Enterprise Service Design Center UI 196
B
D
E
Device 110
User Services App Environment 122
User Data App 111
User Voice App 112
Secure Mobile Enterprise App Environment 120
Enterpris e Data App 124
Enterpris e Voice App 126
Secure Network Interface 128
Operating System Lower Layers 130
Network Stack 134
Access Modem 151
Carrier Access Network 150
Carrier Gateway/Ho me Agent 152
Carrier Usage Accounting Server 154
Enterprise Usage Record 156
Service Usage Reconciliation 158
Secure Enterprise Mobile Services Gateway/Server 172
Mobile Email 173
Mobile Synch 174
Mobile Comms 177
Mobile Contacts 175
Mobile Intranet 178
Mobile Calendar 176
Mobile Server Usage Monitor 179
Server Secure Network Interface 127
Enterprise Network 170
Enterprise Intranet Servers 180
Internet 160
Consumer Internet Services 162
Voice Network 165
Consumer Voice Services 167

Figure 12

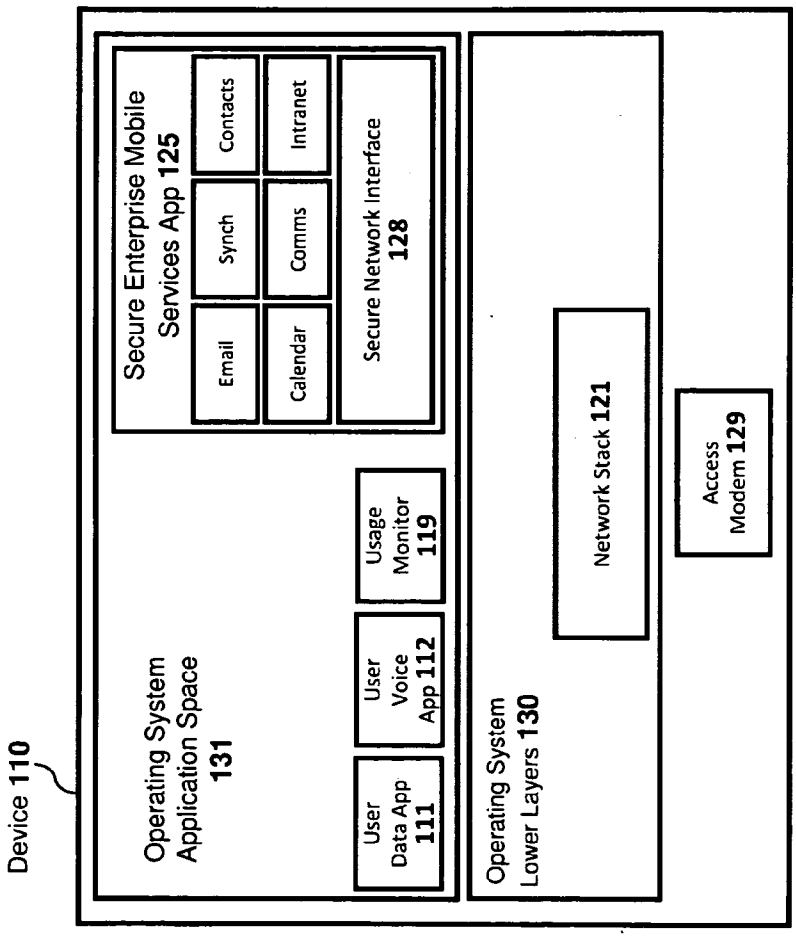
Device 110
Operating System Application Space 131
Secure Enterprise Mobile Services App 125
Email
Synch
Contacts
Calendar
Comms
Intranet
Secure Network Interface 128
User Data App 111
User Voice App 112
Usage Monitor 119
Operating System Lower Layers 130
Network Stack 121
Access Modem 129

Figure 13

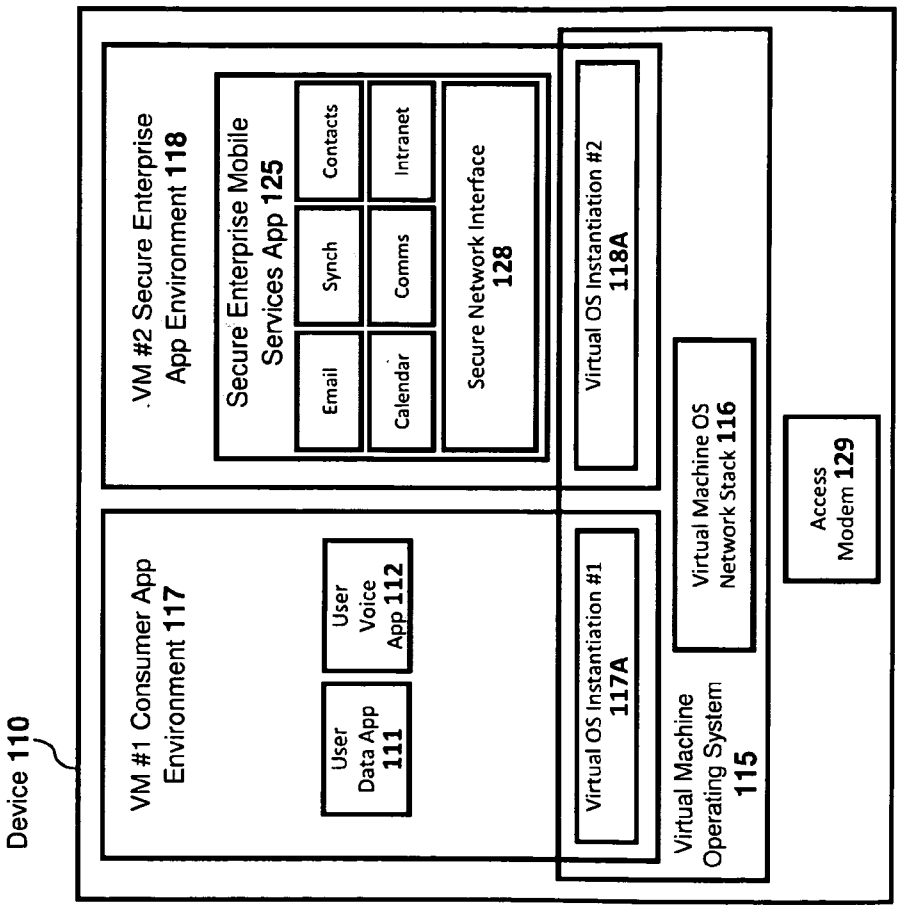
Device 110
VM #1 Consumer App Environment 117
User Data App 111
User Voice App 112
VM #2 Secure Enterprise App Environment 118
Secure Enterprise Mobile Services App 125
Email
Calendar
Synch
Comms
Contacts
Intranet
Secure Network Interface 128
Virtual OS Instantiation #1 117A
Virtual OS Instantiation #2 118A
Virtual Machine Operating System 115
Virtual Machine OS Network Stack 116
Access Modem 129

Figure 14

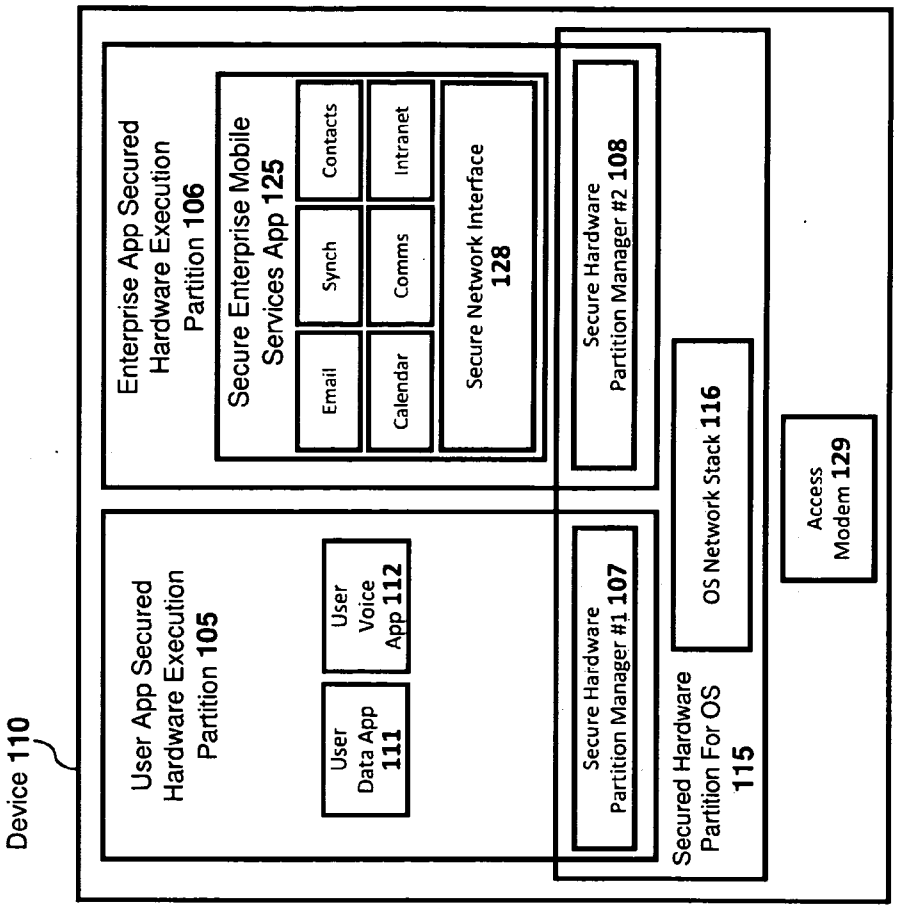
Device 110
User App Secured Hardware Execution Partition 105
User Data App 111
User Voice App 112
Enterprise App Secured Hardware Execution Partition 106
Secure Enterprise Mobile Services App 125
Email
Calendar
Synch
Comms
Contacts
Intranet
Secure Network Interface 128
Secure Hardware Partition Manager #2 108
Secure Hardware Partition Manager #1 107
Secured Hardware Partition For OS 115
OS Network Stack 116
Access Modem 129

Figure 15

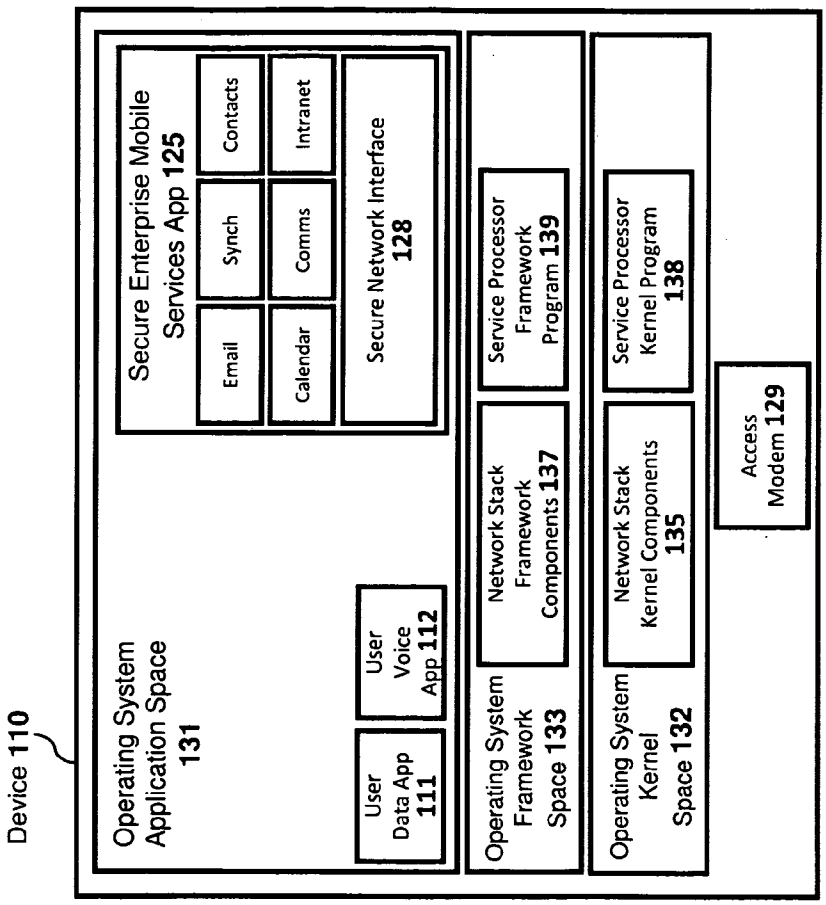
Device 110
Operating System Application Space 131
User Data App 111
User Voice App 112
Secure Enterprise Mobile Services App 125
Email
Calendar
Synch
Comms
Contacts
Intranet
Secure Network Interface 128
Operating System Framework Space 133
Network Stack Framework Components 137
Service Processor Framework Program 139
Operating System Kernel Space 132
Network Stack Kernel Components 135
Service Processor Kernel Program 138
Access Modem 129

Figure 16

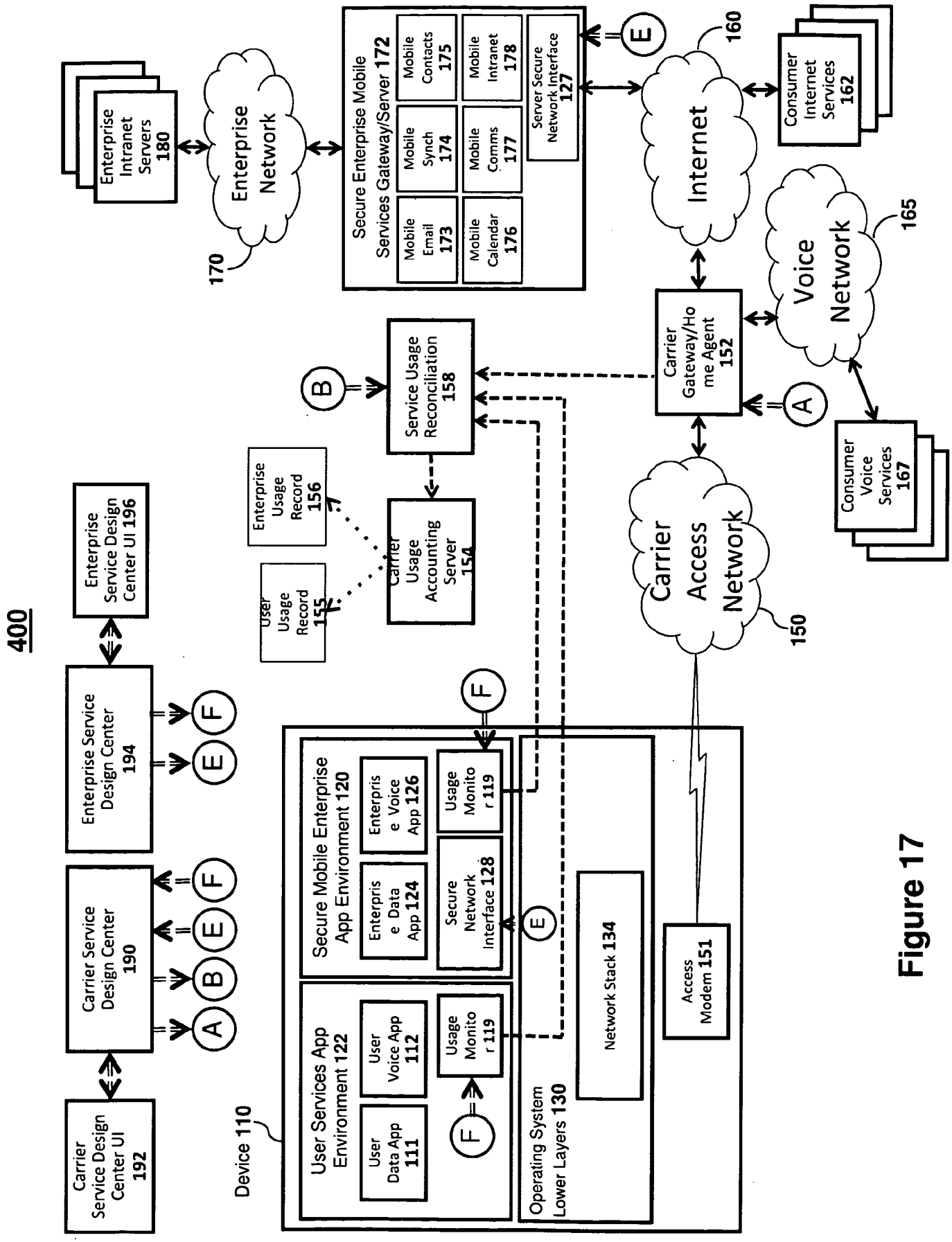
400
Carrier Service Design Center UI 192
Carrier Service Design Center 190
Enterprise Service Design Center 194
Enterprise Service Design Center UI 196
A
B
E
F
Device 110
User Services App Environment 122
User Data App 111
User Voice App 112
Usage Monitor 119
Secure Mobile Enterprise App Environment 120
Enterprise Data App 124
Enterprise Voice App 126
Secure Network Interface 128
Usage Monitor 119
Operating System Lower Layers 130
Network Stack 134
Access Modem 151
Carrier Access Network 150
Carrier Usage Accounting Server 154
User Usage Record 155
Enterprise Usage Record 156
Service Usage Reconciliation 158
Carrier Gateway/Home Agent 152
Voice Network 165
Consumer Voice Services 167
Internet 160
Consumer Internet Services 162
Secure Enterprise Mobile Services Gateway/Server 172
Mobile Email 173
Mobile Synch 174
Mobile Comms 177
Mobile Contacts 175
Mobile Intranet 178
Mobile Calendar 176
Server Secure Network Interface 127
Enterprise Network 170
Enterprise Intranet Servers 180

Figure 17

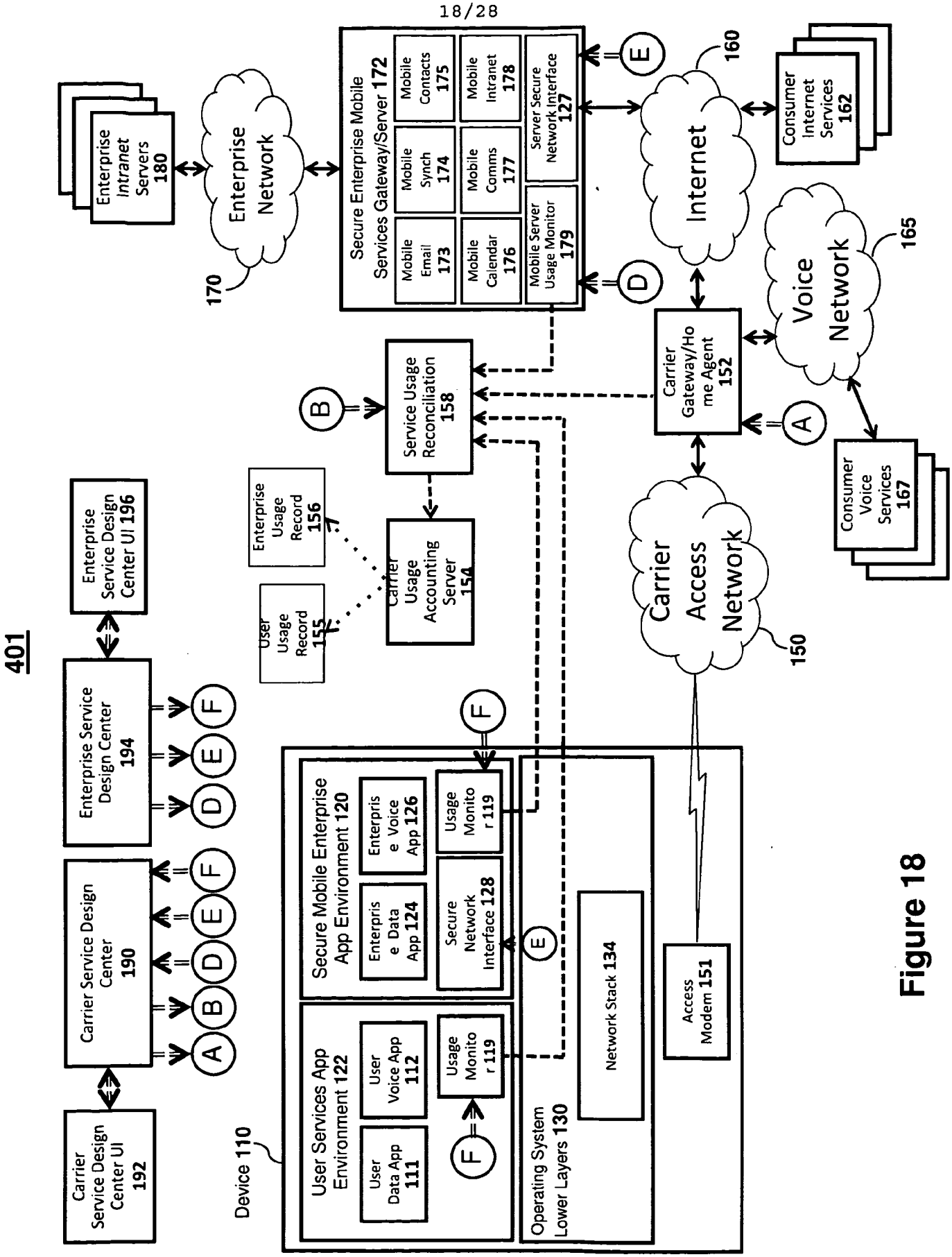
401
Carrier Service Design Center UI 192
Carrier Service Design Center 190
Enterprise Service Design Center UI 196
Enterprise Service Design Center 194
A
B
D
E
F
Device 110
User Services App Environment 122
User Data App 111
User Voice App 112
Usage Monitor 119
Secure Mobile Enterprise App Environment 120
Enterprise Data App 124
Enterprise Voice App 126
Usage Monitor 119
Secure Network Interface 128
Operating System Lower Layers 130
Network Stack 134
Access Modem 151
Carrier Access Network 150
Carrier Gateway/Home Agent 152
Service Usage Reconciliation 158
Carrier Usage Accounting Server 154
Enterprise Usage Record 156
User Usage Record 155
Secure Enterprise Mobile Services Gateway/Server 172
Mobile Email 173
Mobile Synch 174
Mobile Contacts 175
Mobile Calendar 176
Mobile Comms 177
Mobile Intranet 178
Mobile Server Usage Monitor 179
Server Secure Network Interface 127
Enterprise Intranet Servers 180
Enterprise Network 170
Internet 160
Consumer Internet Services 162
Voice Network 165
Consumer Voice Services 167

Figure 18

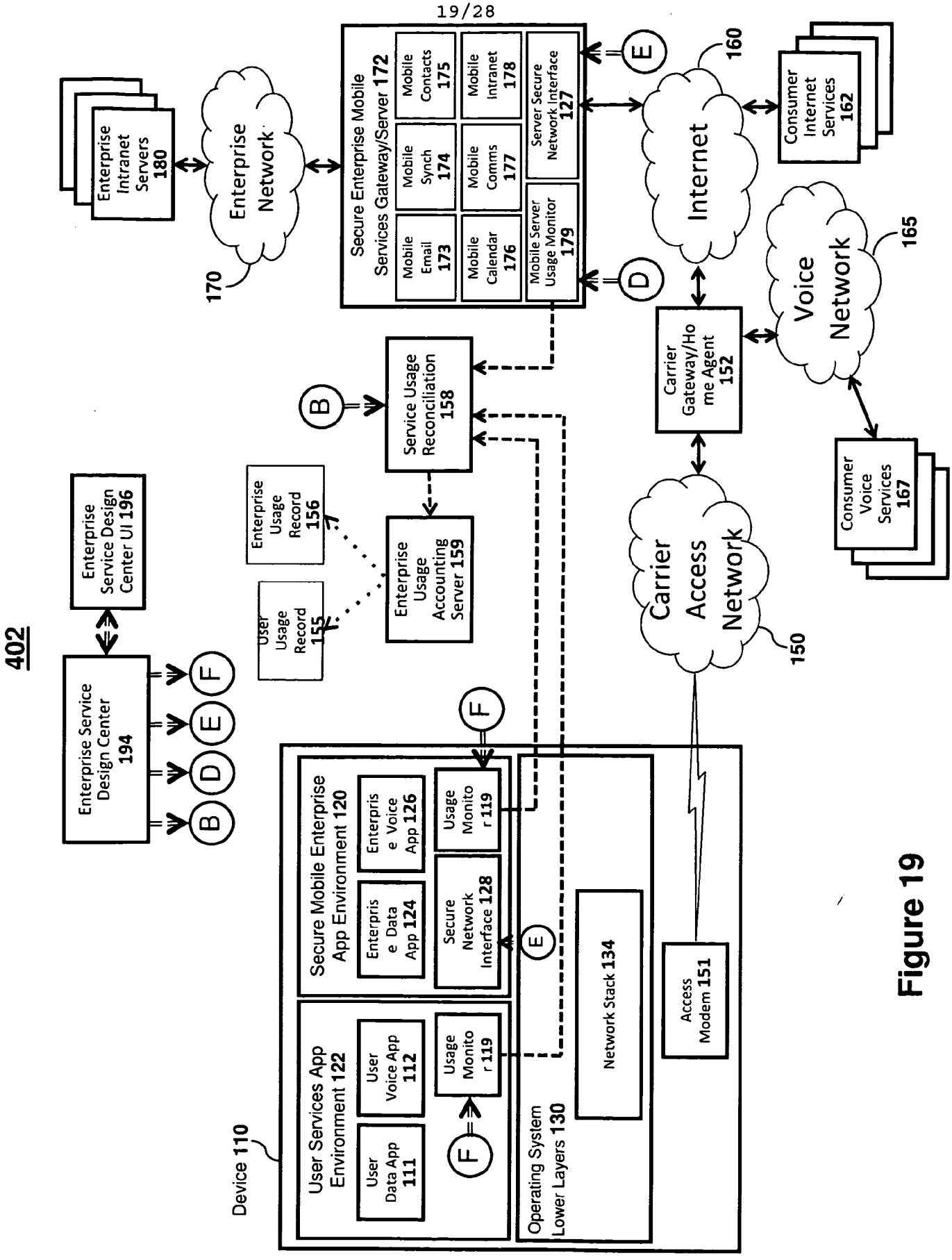
402
Enterprise Service Design Center 194
Enterprise Service Design Center UI 196
Enterprise Intranet Servers 180
Enterprise Network 170
Secure Enterprise Mobile Services Gateway/Server 172
Mobile Email 173
Mobile Synch 174
Mobile Contacts 175
Mobile Calendar 176
Mobile Comms 177
Mobile Intranet 178
Mobile Server Usage Monitor 179
Server Secure Network Interface 127
Internet 160
Consumer Internet Services 162
Voice Network 165
Consumer Voice Services 167
Carrier Gateway/Home Agent 152
Carrier Access Network 150
Service Usage Reconciliation 158
Enterprise Usage Record 156
User Usage Record 155
Enterprise Usage Accounting Server 159
Device 110
User Services App Environment 122
User Data App 111
User Voice App 112
Usage Monitor 119
Secure Mobile Enterprise App Environment 120
Enterprise Data App 124
Enterprise Voice App 126
Secure Network Interface 128
Operating System Lower Layers 130
Network Stack 134
Access Modem 151
A
B
C
D
E
F

Figure 19

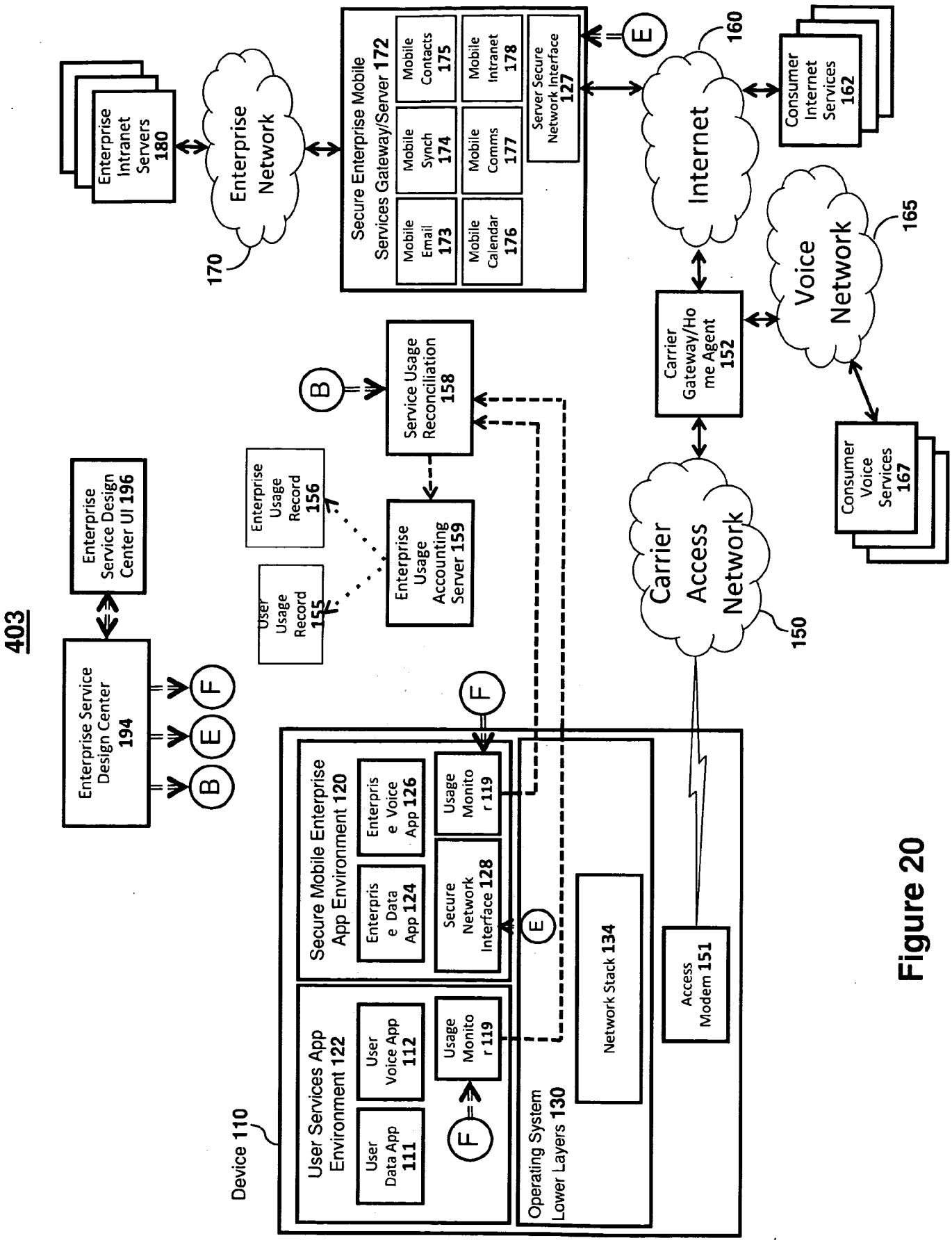
403
Enterprise Intranet Servers 180
Enterprise Network 170
Secure Enterprise Mobile Services Gateway/Server 172
Mobile Email 173
Mobile Synch 174
Mobile Comms 177
Mobile Contacts 175
Mobile Intranet 178
Mobile Calendar 176
Server Secure Network Interface 127
Internet 160
Consumer Internet Services 162
Voice Network 165
Carrier Gateway/Home Agent 152
Carrier Access Network 150
Consumer Voice Services 167
Service Usage Reconciliation 158
Enterprise Usage Record 156
User Usage Record 155
Enterprise Usage Accounting Server 159
Enterprise Service Design Center UI 196
Enterprise Service Design Center 194
Device 110
User Services App Environment 122
User Data App 111
User Voice App 112
Usage Monitor 119
Secure Mobile Enterprise App Environment 120
Enterprise Data App 124
Secure Network Interface 128
Enterprise Voice App 126
Usage Monitor 119
Operating System Lower Layers 130
Network Stack 134
Access Modem 151
A
B
C
D
E
F

Figure 20

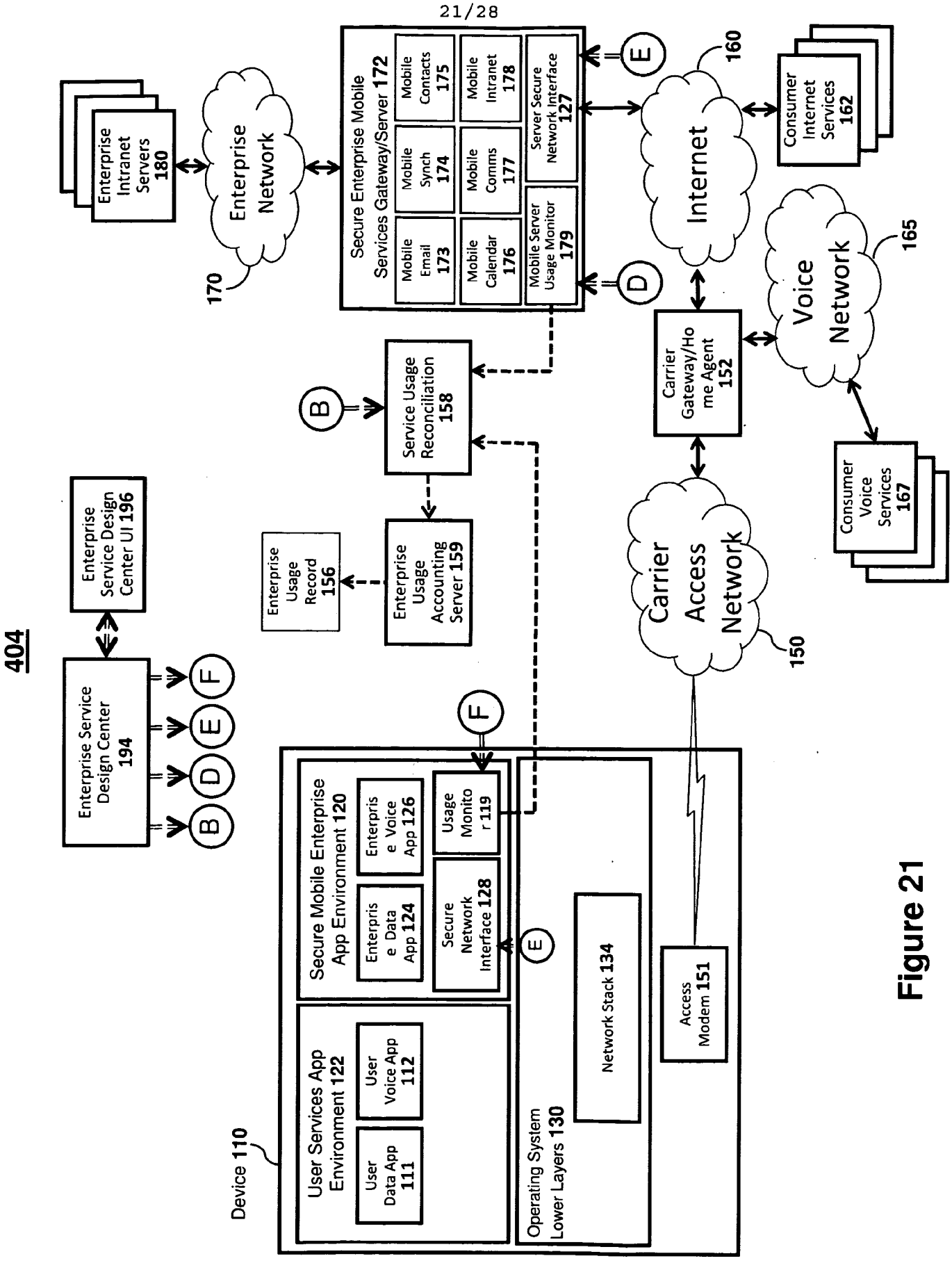
404
Enterprise Service Design Center 194
Enterprise Service Design Center UI 196
B
D
E
F
Device 110
User Services App Environment 122
User Data App 111
User Voice App 112
Secure Mobile Enterprise App Environment 120
Enterprise Data App 124
Enterprise Voice App 126
Secure Network Interface 128
Usage Monitor 119
Operating System Lower Layers 130
Network Stack 134
Access Modem 151
Carrier Access Network 150
Carrier Gateway/Home Agent 152
Voice Network 165
Consumer Voice Services 167
Internet 160
Consumer Internet Services 162
Service Usage Reconciliation 158
Enterprise Usage Accounting Server 159
Enterprise Usage Record 156
Enterprise Network 170
Enterprise Intranet Servers 180
Secure Enterprise Mobile Services Gateway/Server 172
Mobile Email 173
Mobile Synch 174
Mobile Contacts 175
Mobile Calendar 176
Mobile Comms 177
Mobile Intranet 178
Mobile Server Usage Monitor 179
Server Secure Network Interface 127

Figure 21

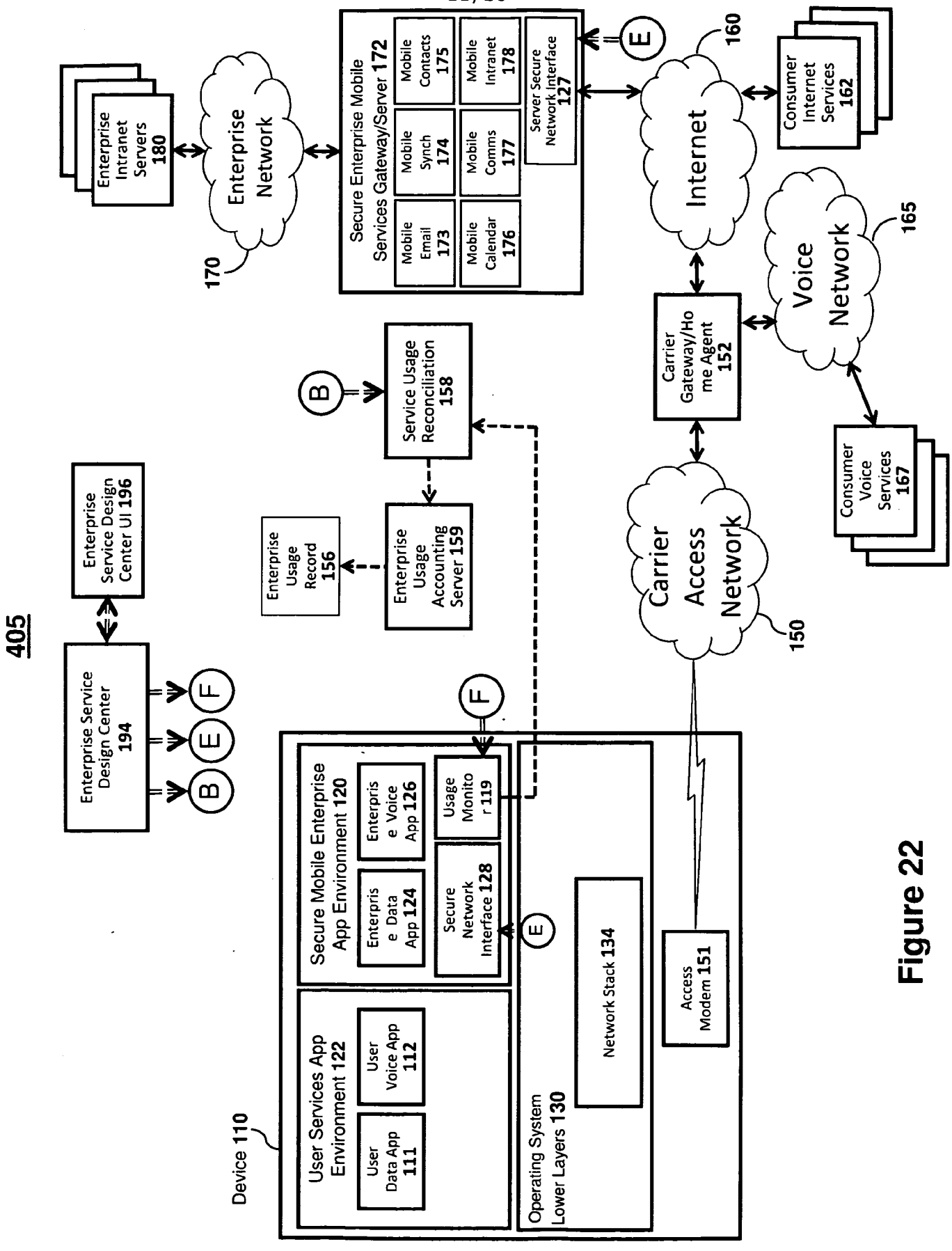
405
Enterprise Intranet Servers 180
Enterprise Network 170
Secure Enterprise Mobile Services Gateway/Server 172
Mobile Email 173
Mobile Synch 174
Mobile Contacts 175
Mobile Calendar 176
Mobile Comms 177
Mobile Intranet 178
Server Secure Network Interface 127
Internet 160
Consumer Internet Services 162
Voice Network 165
Consumer Voice Services 167
Carrier Gateway/Home Agent 152
Carrier Access Network 150
Service Usage Reconciliation 158
Enterprise Usage Accounting Server 159
Enterprise Usage Record 156
Enterprise Service Design Center UI 196
Enterprise Service Design Center 194
Device 110
User Services App Environment 122
User Data App 111
User Voice App 112
Secure Mobile Enterprise App Environment 120
Enterprise Data App 124
Enterprise Voice App 126
Secure Network Interface 128
Usage Monitor 119
Operating System Lower Layers 130
Network Stack 134
Access Modem 151
A
B
C
D
E
F

Figure 22

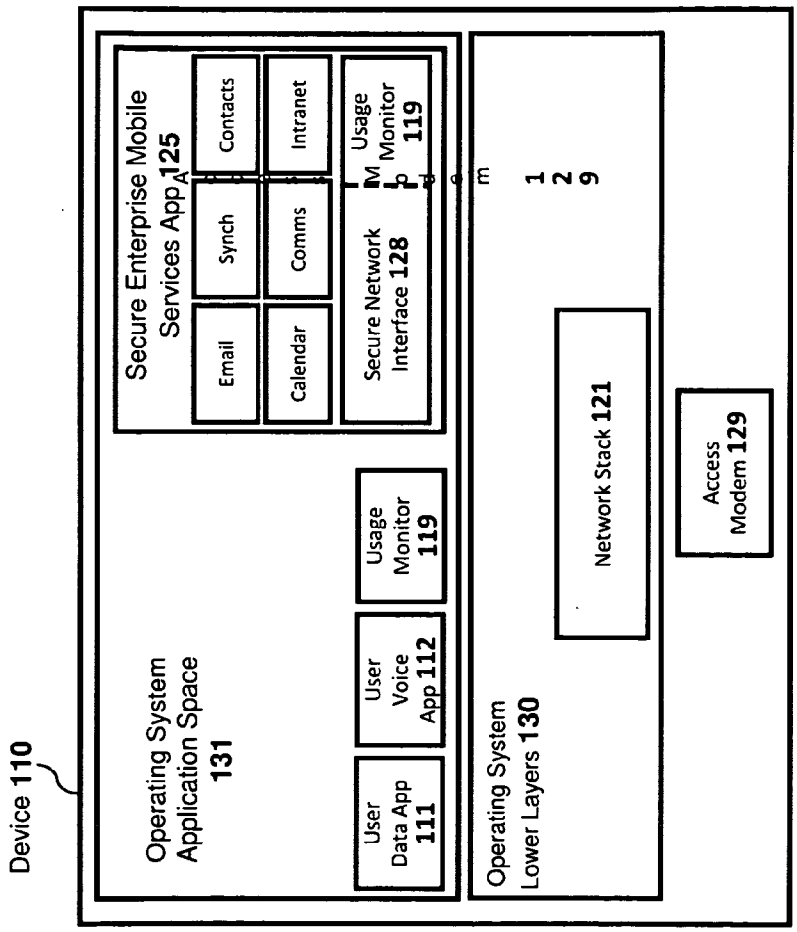
Device 110
Operating System Application Space 131
Secure Enterprise Mobile Services App 125
Email
Calendar
Synch
Comms
Contacts
Intranet
Secure Network Interface 128
Usage Monitor 119
User Data App 111
User Voice App 112
Usage Monitor 119
Operating System Lower Layers 130
Network Stack 121
Access Modem 129

Figure 23

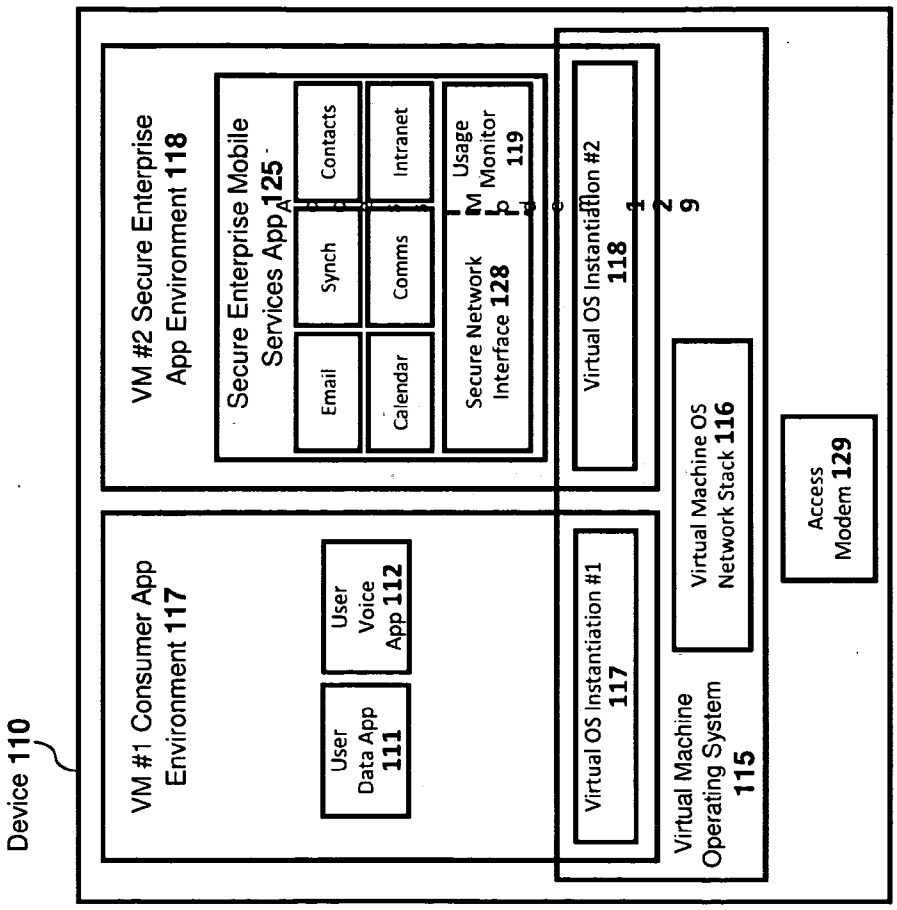
Device 110
VM #1 Consumer App Environment 117
User Data App 111
User Voice App 112
VM #2 Secure Enterprise App Environment 118
Secure Enterprise Mobile Services App 125
Email
Calendar
Synch
Comms
Contacts
Intranet
Secure Network Interface 128
Usage Monitor 119
Virtual Machine Operating System 115
Virtual OS Instantiation #1 117
Virtual OS Instantiation #2 118
Virtual Machine OS Network Stack 116
Access Modem 129

Figure 24

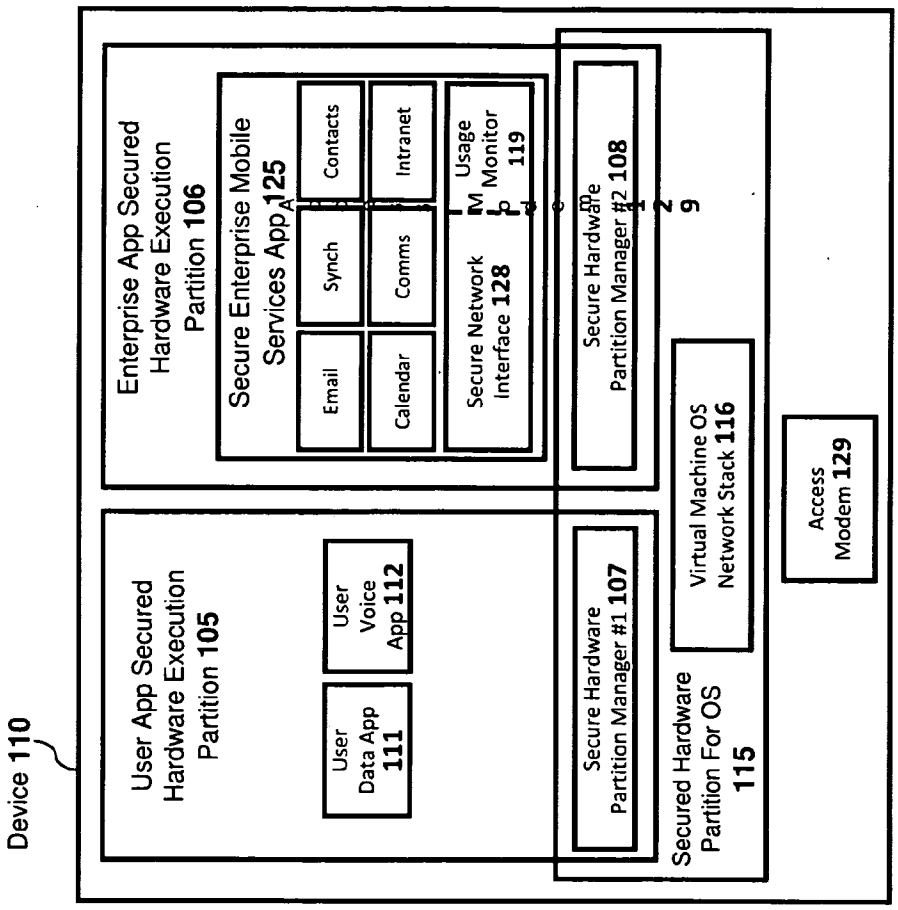
Device 110
User App Secured Hardware Execution Partition 105
User Data App 111
User Voice App 112
Enterprise App Secured Hardware Execution Partition 106
Secure Enterprise Mobile Services App 125
Email
Calendar
Synch
Comms
Contacts
Intranet
Secure Network Interface 128
Usage Monitor 119
Secure Hardware Partition Manager #1 107
Secure Hardware Partition Manager #2 108
Secured Hardware Partition For OS 115
Virtual Machine OS Network Stack 116
Access Modem 129

Figure 25

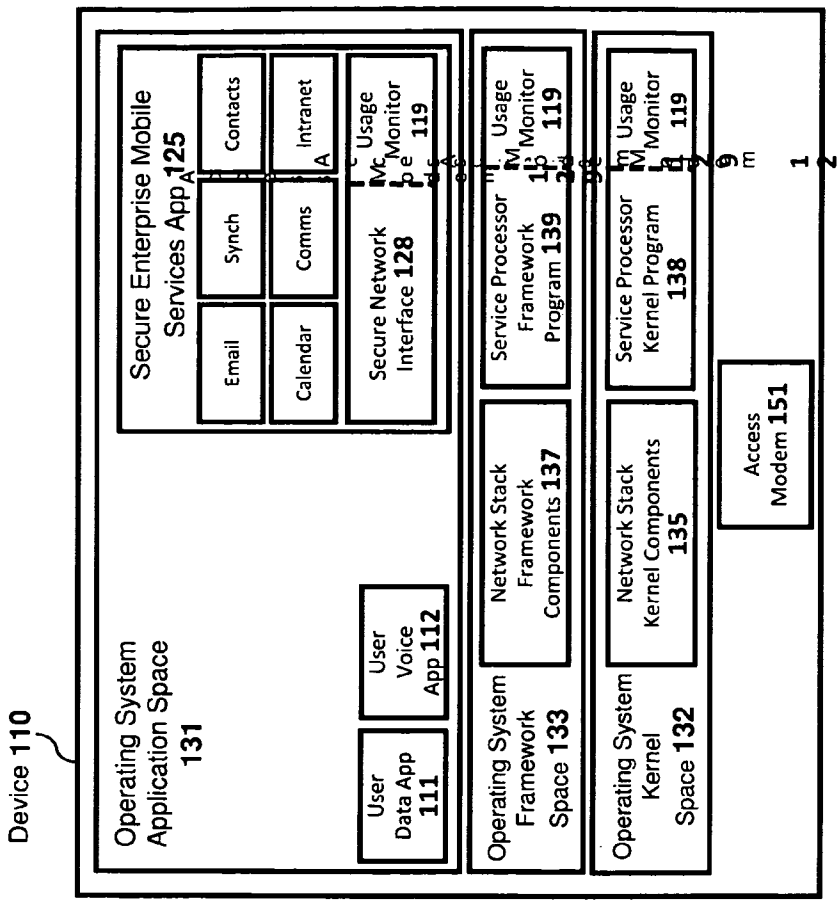
Device 110
Operating System Application Space 131
Secure Enterprise Mobile Services App 125
Email
Calendar
Synch
Comms
Contacts
Intranet
Secure Network Interface 128
Usage Monitor 119
User Data App 111
User Voice App 112
Operating System Framework Space 133
Network Stack Framework Components 137
Service Processor Framework Program 139
Usage Monitor 119
Operating System Kernel Space 132
Network Stack Kernel Components 135
Service Processor Kernel Program 138
Usage Monitor 119
Access Modem 151

Figure 26

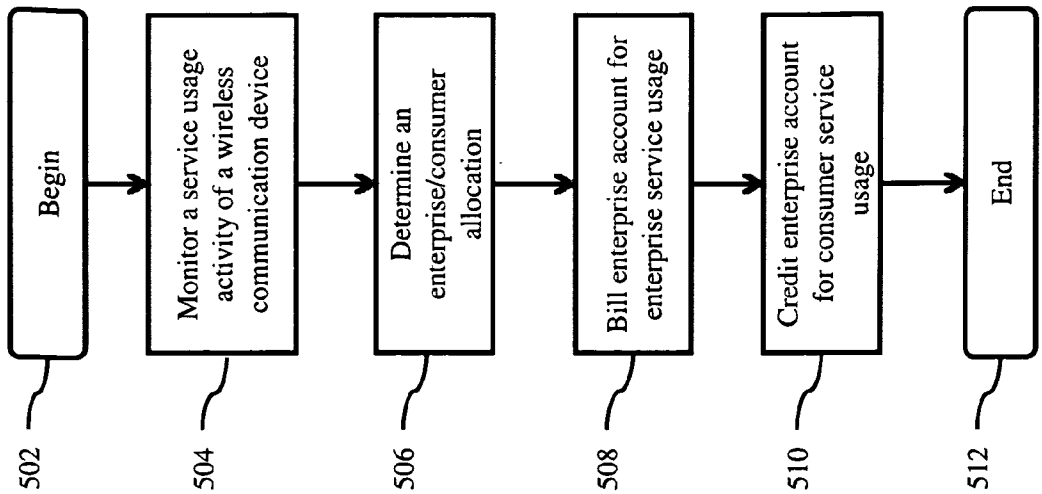

Figure 28

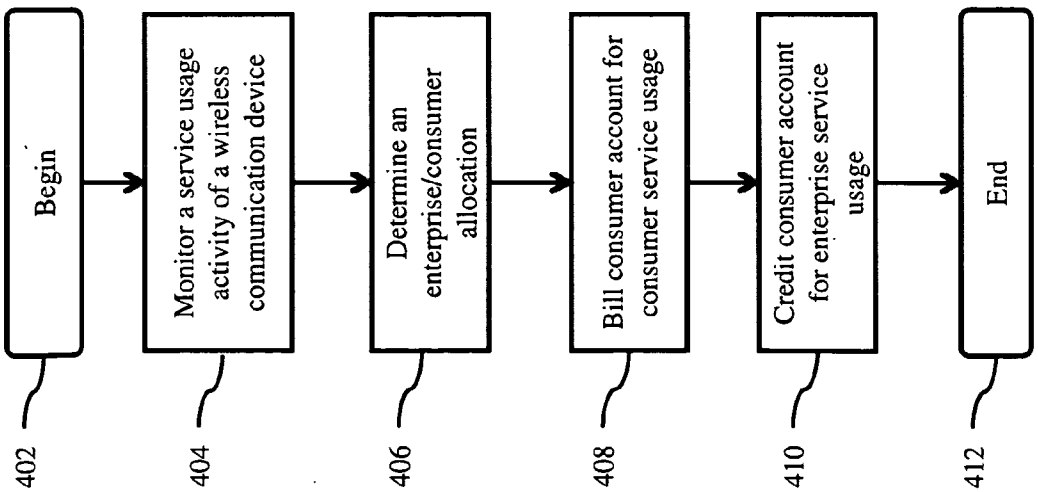

Figure 27

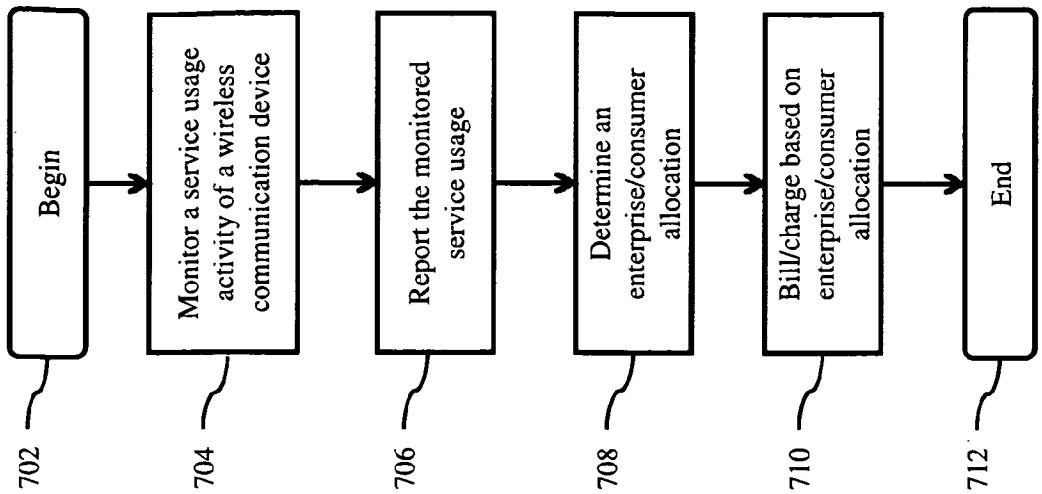

Figure 30

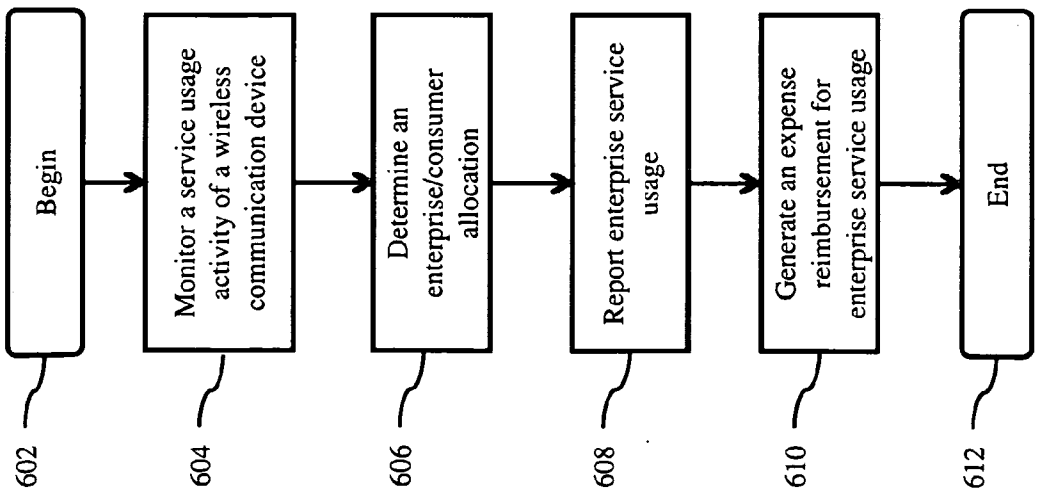

Figure 29

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 11/01683

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06F 17/00 (2011.01)
USPC - 726/1
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
USPC: 726/1

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC: 726/1-5 (keyword limited - see terms below)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
PubWEST(USPT,PGPB,EPAB,JPAB); Google
Search Terms: Monitor, tracking, usage, design, policy, enterprise, service, trigger, interface

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2010/0191612 A1 (Raleigh) 29 July 2010 (29.07.2010), para [0083], [0090], [0131], [0170], [0171], [0217], [0254], [0255], [0279], [0325], [0392], [0497]	1 - 25
A	US 2008/0319879 A1 (Carroll et al.) 25 December 2008 (25.12.2008), entire document	1 - 25
A	US 2008/0207167 A1 (Bugenhagen) 28 August 2008 (28.08.2008), entire document	1 - 25

☐ Further documents are listed in the continuation of Box C. ☐

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

Date of the actual completion of the international search	Date of mailing of the international search report
03 January 2012 (03.01.2012)	17 JAN 2012
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (July 2009)