

embodiment, the acknowledgement of receipt may be issued at the Network Driver Interface Specification (NDIS) driver level in the Microsoft Family of Windows Operating Systems.

At step 385 of illustrative method 360, the network stack 310a-310b receiving the false acknowledgment of receipt of the network packet from step 380 may in response to such receipt, may not execute, stop executing, or prevent from executing any one or more algorithms and operations providing one or more lossless characteristics of the lossless protocol. For example, in the embodiment of TCP as the lossless protocol, the network stack 310a-310b may not execute any one or more of the following with respect to the network packet, or the TCP connection: packet ordering, packet retransmission, a flow control algorithm, a sliding window algorithm, and/or a nagle's algorithm. In some embodiments, the false acknowledgment of receipt must be received on a packet by packet basis to prevent the lossless layer of the network stack 310a-310b from employing reliability algorithms. As such, the sending network stack 310a-310b can determine on a packet by packet basis which packets to apply the false acknowledgment techniques of the present invention to. There may be some lossless protocol network packets comprising the lossy protocol for which the reliability algorithms of the lossless protocol should be applied. In other embodiments, the false acknowledgment of receipt of the network packet may be received once for the lossless protocol connection to prevent employing reliability algorithms for any subsequent packets received during the lossless protocol session or connection.

At step 390, the illustrative method 360 communicates the lossless protocol packet having the lossless protocol payload via the network stacks 310a-310b. In one embodiment, the lossless protocol packet is communicated after step 385, or in other embodiments, before step 385. So, although the lossless protocol packet becomes lost in the network, no attempt is made to reclaim the packet as one would expect for a lossy protocol packet.

Although the illustrative embodiment of method 360 is discussed using a false acknowledgment of receipt of the network packet such as in TCP, any type and/or form of indication, request, or instruction may be communicated to the network stacks 310a-310b to prevent employing any reliability or lossless algorithms of the lossless protocol. In some embodiments, the lossless protocol layer of the network stack 310a-310b may be adapted or configured to have a configuration, flag, or instruction to not use the

reliability algorithms either on a packet by packet basis, or a session or connection basis. For example, the lossless protocol may have fields, such in a header of a lossless protocol packet, that indicates whether reliability should be discarded or avoided for the packet.

Referring now to Figure 3C, another embodiment of steps taken to transmit packets constructed according to a lossy protocol via a lossless protocol is shown by illustrative method 345, which may also be referred to as a payload shifting technique. In brief overview of illustrative method 345, at step 348, a first packet to be transmitted using an unreliable transport protocol is received by a first device, such as client 105. At step 350, the first device 105 creates a first TCP packet including a first payload of the received first packet and a first TCP header of information associated with a TCP connection established between the first device 105 and a second device. The first device 105 transmits the first TCP packet to the second device at step 352. At step 354, the first device 105 receives a second packet to be transmitted using an unreliable transport protocol, and at step 356, creates a second TCP packet including a second payload of the received second packet and the first TCP header information. At step 358, the first device transmits, before receipt of an acknowledgement of the receipt of the first payload from the second device, the second TCP packet to the second device.

Still referring to Figure 3C, and now in more detail, at step 348, a first packet to be transmitted using an unreliable transport protocol is received by a first device 105. In some embodiments, the packet is intended to be transmitted using a lossy protocol of UDP. In further embodiments, the packet comprises RDP over UDP. In other embodiments, the first packet is generated by an application program 338 executing in user mode 332. In some embodiments, the packet is generated by an application 338 executing in kernel mode 334. In other embodiments, the first packet is received by the first device 105 for retransmission. In still other embodiments, the first packet is intercepted by a filter process 322 before it reaches the network stack 310a-310b. The filter process 322 may execute in user mode 332 or in kernel mode 334. In some embodiments, the filter 322 is a mini-driver. In other embodiments, the filter 322 is an NDIS driver. In other embodiments, the filter 322 process uses application hooking to intercept the first packet. In further embodiments, the application hooking is implemented via an application programming interface (API). In one embodiment, the hooking of network packets occurs at the network layer of the network stack 310a-310n.

At step 350, the first device 105 creates a first TCP packet including a first payload of the received first packet and a first TCP header of information associated with a TCP connection established between the first device 105 and a second device. For example, the TCP connection may be established between the client 105 and a peer computing device 102b in one embodiment, and between the client 105 and the gateway 340 in another embodiment. In some embodiments, the first device 105 indicates that the TCP packet contains a payload of packets constructed to be transmitted via a lossy protocol by opening a specific TCP port. In other embodiments, the first device 105 indicates that the TCP packet contains a payload of packets constructed to be transmitted via a lossy protocol by setting a flag in the TCP header. The TCP header may include information regarding the source node, information regarding the destination node, or a sequence number particularly identifying the TCP packet.

At step 352, the first device 105 transmits the first TCP packet to the second device. In some embodiments, the second device may be a gateway 340. In other embodiments, the second device is a “peer” computing device 102b. The first TCP packet may be encrypted before transmission to the second device using, for example, SSL or TLS.

At step 354, the first device 105 receives a second packet to be transmitted using an unreliable transport protocol, such as UDP. The second packet may be received from the same application 338 that generated the first packet. At step 356, the first device 105 creates a second TCP packet including a second payload of the received second packet and the first TCP header information, as described above. At step 358, the first device 105 then transmits, before receipt of an acknowledgement of the receipt of the first payload from the second device, the second TCP packet to the second device. In some embodiments, when an acknowledgment is received from the second device, the first device 105 updates the TCP header information before transmitting the packet. In other embodiments, the first device 105 creates a third TCP packet with updated TCP header information and having the second payload. The first device then transmits the third TCP packet.

Upon receipt of the TCP packet, the second device decrypts it, if necessary, and determines that the payload is one or more packets constructed to be transmitted using a lossy protocol. The second device may determine this based on the port on which the

packet was received or by a flag in the TCP header information. Once determined, the second device strips the TCP header from the payload and delivers the payload.

In another aspect, the present invention is related to adjusting the reported maximum transmission unit (MTU) parameter to optimize network communications by reducing packet fragmentation for encrypted network packets. This technique may be applied on one or both network stacks 310a-310b of illustrative environment 300 of Figure 3A. Encrypting a payload of a network packet, such as any network packet processed according to the illustrative method 360 described above, may increase the size of the payload. That is, the size of the network packet may increase to account for the change in size of the unencrypted original payload to the encrypted payload.

Still referring to Figure 3A, the network stacks 310a-310b may comprise a maximum transmission unit 402a-402b (MTU) parameter to indicate the size of the largest unit of data that can be sent over a type of physical medium in a network, such as an Ethernet based network. In the embodiment of TCP/IP, the MTU 402a-402b indicates the largest datagram or packet that can be transmitted by an Internet Protocol (IP) layer interface, without the interface needing to break down or fragment the datagram into smaller units. An MTU parameter 402a-402b may be associated with a communications interface such as a network interface card. The default MTU size for Ethernet is 1,500 bytes, and IEEE 802.3 is 1,492 bytes. As one ordinarily skilled in the art will recognize and appreciate, the default MTU size will be based on the networking technologies such as Token Ring, FDDI, X.25, etc.

Referring now to Figure 4, a flow diagram depicts an illustrative embodiment of the MTU adjustment method 400 of the present invention. In brief overview, at step 405, a session between computing devices is established, such as between a first computing device 102a and a second computing device 102b. At step 410, one of the computing devices 102, such as the first computing device 102a, detects a network packet having an encrypted payload. At step 415, the computing device 102a-120b determines a setting for the MTU 402a-402b parameter of the network stack 310a-310b to account for the size of the encrypted portion of the payload. At step 420, the MTU 402a-402b parameter is decreased to account for the encrypted portion. If the MTU 402a-402b is requested or reported, the MTU 402a-402b will indicate a size smaller than the MTU size associated with the physical layer, such as 1,500 for Ethernet.

Using this technique, any device on the network 104 may communicate network packets to the network stack 310a-310b according to the decreased MTU size that can be encrypted along the route to the network stack 310a-310b and not be fragmented. If the network packet is encrypted it should still fit in the actual MTU size of the physical network layer medium, such as Ethernet. For example, the MTU parameter 402a-402b may be set to the default MTU size of 1,500 for Ethernet and in accordance with the illustrative method 400 decreased by a determined number of bytes, for example 100, to account for encryption overhead. A network packet may be transmitted from a server resource to the client comprising a size equal to the reported MTU 402a-402b size of 1,400. The network packet may traverse the gateway 340 and get encrypted via the SSL tunnel, which in turns increases the network packet size to 1,475. Since this size fits into the MTU size of the Ethernet physical medium, the network packet will not be fragmented.

At step 405 of illustrative method 400, any type and/or form of communication session between a first computing device 102a and a second computing device 102b, such as client 105b or gateway 340 of Figure 2A, may be established. In some embodiments, the session is established using the remote access client 120 on a first computing device. In one embodiment, the remote access client 120 establishes a session with the gateway 340, such as an SSL VPN session, or to another remote access client 120 on a peer computing device 102b.

In some embodiments of step 410, the remote access client 120 detects a network packet having an encrypted payload. In one embodiment, the packet capture mechanism 365 intercepts network packets and the agent 326 determines if the packet is encrypted. However, any other portion of the remote access client 120, such as the filter 322 or frame monitor 360 may determine if the packet is encrypted. In one embodiment, the entire payload of the network packet is encrypted, while in other embodiments, a portion of the payload is encrypted. The present invention may use any type and/or form of means or mechanism for determining if a packet has encryption. For example, in some cases, the remote access client 120 may check for a flag or field of the network packet indicating the payload is encrypted. In other embodiments, the remote access client 120 may check whether any portion of the payload is unintelligible, because it contains random data or noise from encryption. Additionally, the encrypted payload may be

encrypted in association with any layer of the network stack 310a-310b, such as layer 2, 3, 6 or 7 encryption.

In some embodiments of step 415, the illustrative method 400 of the present invention determines the adjustment to the reported MTU 402a-402b size on a packet by packet basis, or in other embodiments, on a connection or session basis, and at step 420 adjusts the MTU 402a-402b accordingly. In one embodiment, the MTU 402a-402b is decreased exactly by the amount of encryption overhead for the network packet. In some cases, the illustrative method 400 determines the MTU 402a-402b size adjustment once for the entire session or connection and decreases the size of the MTU 402a-402b to a value to account for encryption overhead for the entire session. For example, although network packets may have varying encryption overhead, the adjustment accounts for the largest encryption overhead. In further embodiments, the MTU 402a-402b may be adjusted to take into consideration encryption that may occur when the network packet leaves the network stack 310a-310b, such as encryption by a gateway 340 that may occur in the end-to-end network traversal of the network packet.

Additionally, the MTU 402a-402b size may be adjusted for other network performance factors in addition to the encryption overhead. In some embodiments, although the MTU 402a-402b is decreased due to encryption overhead, it may be further decreased to account for other overhead and factors related to network communication, as well as increased in other cases. For example, the MTU 402a-402b may have been previously adjusted for a factor not related to encryption and after using the techniques of the present invention the MTU 402a-402b is decreased to take into account encryption overhead. One ordinarily skilled in the art will recognize and appreciate that there may be other factors and considerations for adjusting the MTU besides or in addition to adjusting for encryption overhead in accordance with the techniques of the present invention.

Referring now to Figures 5A and 5B, the present invention, in an additional aspect, is related to client-side application-aware network communication prioritization techniques. The remote access client 120 of the present invention provides for the intelligent and client centric prioritization of application network communications on a client based on the type and/or priority of an application. As depicted in the system 500 of Figure 5A, the remote access client 105 of computing device 102 is connected to network 104. The client 105 may execute one or more applications 338a-338n, which

access the network 104 via the agent 326 and filter 322 of the remote access client 120. In some embodiments, the applications 338a-338n provide one or more real-time data communications, such as VoIP. In other embodiments, one or more of the applications 338a-338n may provide email, collaboration, online meeting, and/or desktop sharing related services or functionality.

As illustrated in Figure 5A, the packet capture mechanism 365, 365' may be included in the filter 322 or the agent 326 of the remote access client 120, for intercepting network traffic of any of the applications 338a-338n of the client 105. The remote access client 120 may comprise any queues 540a-540n for queuing and prioritizing network communications of the client 105. In one embodiment, the queues 540a-540n may be included in a network driver, such as an NDIS driver for the filter 322, and in other embodiments, may be included with or accessible by the agent 326. The queues 540a-540n may comprise any type and/or form of suitable means and/or mechanisms for storing and/or arranging network packets, such as network packets intercepted by the packet capture mechanism 365. In some embodiments, the queues 540a-540n may be associated with or assigned to network packets related to applications 338a-338n of the client 105. In other embodiments, the queues 540a-540n may be organized by levels of priority, such as high, medium, low, or numerically such as priority 1...10. One ordinarily skilled in the art will recognize and appreciate that number of queues 540a-540n may be based on any desired granularity of prioritization, such as 3, 5 or 10 levels of priority. Additionally, some of the queues 540a-540n may be used for receiving and/or transmitting network packets prior to being placed into and/or taken out of a priority based queue 540a-540n.

The remote access client 120 may also have, access, or use a routing table 538 for determining how to route network packets of the client via the agent 326, such as onto the network 104 via a gateway 340. In one embodiment, the agent 326 establishes and maintains an SSL VPN connection to the gateway 340, such as illustrated in Figure 1A for example. In one embodiment, the routing table 538 comprise information about a source computing device and a destination computing device to identify a communication path or connection between a source and destination communication points. The routing table 538 may include a source IP address and source port, and an destination IP address and destination port to identify a communication path on the network 104. For example, the source IP address and source port may represent the IP

address of the client 105 and the port by which an application 338a-338n on the client 105 communicates on the network 105. The destination IP address may represent the IP address of a peer computing device to which the application 338a-338n communicates with via the destination port used by the peer device.

Additionally, the remote access client 120 may have one or more policies 520 for specifying client-side prioritization of network communications related to applications 338a-338n running on application. These policies 520 may be specified by any suitable means and/or mechanisms. In some embodiments, the policies 520 may be specified by the name of the application 338a-338n and/or the type of application 338a-338n. In other embodiments, the policies 520 may be specified in accordance to the type of one or more protocols used by the applications 338a-338n and/or the size of the payload of the network packet. In another embodiment, the policies 520 define prioritization based on whether an application is running in the foreground or the background of the client 105. In yet another embodiment, policies 520 may indicate prioritization based on the destination network address, such as host name or IP address, and/or destination port number. Additionally, the policies 520 may be specified hierarchically to account for multiple applications 338a-338n and/or multiple protocols that may be executed on the client 105 at any point. Furthermore, the policies 520 may be specified conditionally, such as if one application 338a is running, a second application 338b may have a higher or lower priority. One ordinarily skilled in the art will recognize and appreciate the multitude of ways to define client-side application priorities.

The policies 520 may be accessible by the agent 326, configured into the agent 326, or loaded by the agent 326. For example, the policies 520 may be provided by or downloaded via the gateway 340. The policies 520 may comprise any type and format of syntax and/or language for specifying a policy, and may be provided via any type and/or form of medium, such as electronically by one or more network packets or via a file, such as an XML file. The policies 520 may be configurable by a user by any suitable means and/or mechanism. For example, the agent 326 may provide a configuration mechanism such as a user interface, graphical or otherwise, design and constructed for configuring or specifying the policies 520.

In view of the system 500 of Figure 5A and Figures 1A-1C, the prioritization technique of the present invention illustrated by method 550 in Figure 5B will be described. In brief overview, at step 555 of the illustrative method 550, the client 105

intercepts one or more network packets associated with an application 338a-338n on the client 105, and, at step 560, the network packets are stored to a queue 540a-540n. At step 565, a priority for the intercepted and queued network packet is determined based on the type and/or priority of the application 338a-338n. At step 570, the determined priority is indicated for the network packets, and, at step 575, the network packets are communicated according to the determined priority. As such, the outbound network packets generated by an application 338a-338n on the client 105 are prioritized by the client 105 prior to transmission based on the type and/or priority of the application 338a-338n. For example, the application 338a may generate real-time data of VoIP communications, such as RTP over UDP via a TCP/IP session of an SSL connection to the gateway 340. The client 105, using the techniques of the present invention, may prioritize the real-time data communications of application 338a ahead of other applications, such as non-real-time data communication applications. This technique may compliment Quality of Service (QOS) networks where network traffic prioritization occurs in intermediary network devices, such as switches and routers.

At step 555 of illustrative method 500, the client 105 may intercept network packets of one or more applications 338a-338n transparently to the application 338a-338n, the gateway 340, a peer computing device, and any of the network layers of a network stack. In this manner, the techniques of the present invention support any type of application 338a-338n on the client 105. In some embodiments, the network packets are intercepted by the packet capture mechanism 360 via agent 326 or filter 322. Any inbound and/or outbound network packets of an application 338a-338n may be intercepted by the remote access client 120 of the present invention.

At step 560, the network packets intercepted at step 555 may be stored in a queue 540a-540n. In one embodiment, the network packet is stored to a temporary queue 540a-540n prior to prioritizing the network packet at steps 565 and 570. In other embodiments, the network packet is stored to a determined priority queue 540a-540n or a queue 540a-540n associated with an application 338a-338n after the network packet is prioritized at steps 565 and/or step 570.

At step 565, the remote access client 120 of the present determines the association of network packets with applications 338a-338n in order to determine priorities and apply any priority based policies 520. The client 105, such as via agent 326, can associate network traffic with applications 338a-338n by any suitable means

and/or mechanisms. In some embodiments, the agent 326 identifies the network packet as generated from an application 338a-338n by any of the content of the network packet, such as any headers, fields, or the type and content of data in the payload of the network packet. In other embodiments, a network packet is associated with an application 338a-338n by matching information from the routing table 538, such as source and destination IP addresses and ports numbers with the IP addresses and ports numbers of the network packet. In some embodiments, the agent 326, such as via the frame monitor 360, may perform a checksum on the packet to verify that the identified application actually generated the packet.

Additionally, the remote access client 120 may determine whether the application 338a-338n associated with the network packet is running in the foreground or the background of the client 105. Furthermore, the remote access client 120 may determine any priorities, such as process task priority, assigned to the application 338a-338n by the operating system of the client 105. In other embodiments, the remote access client 120 may determine any other characteristics or statistics of the application 338a-338n such as size, memory usage, total execution time, and/or frequency of use. One ordinarily skilled in the art will recognize and appreciate the various characteristics of an application the present technique may use for providing client-side application-aware network communication prioritization.

At step 570, the remote access client 120 of the present invention indicates a priority for intercepted and queued network packets based on the application 338a-338n associated with the packet at step 565. In one embodiment, the agent 326 uses the policies 520 to apply a priority to network packets of applications 338a-338n in accordance with the prioritization rules specified or indicated by the policies 520. In some embodiments, the agent 326 may use characteristics of the application 338a-338n, such as running in the foreground or background, to indicate priority for a network packet of the application 338a-338n. In other embodiments, the agent 326 may use any combination of the policies 520 and characteristics of the application 338a-338n to indicate a priority for the network packets of the application 338a-338n.

In some embodiments, the agent 326 indicates the priority to the filter 322 for management of network packet queues 540a-540n to apply the indicated priorities. The agent 326 may communicate the priority of network packets to the filter 322 by any suitable means and/or mechanism such as via an application programming interface

(API), such as an IOCTL interface, or any other type and/or form of interface known to those ordinarily skilled in the art. In one embodiment, the filter 322 is not aware of the application 338a-338n by name but can associate priorities to network packets of applications 338a-338n via the routing table 538. An application 338a-338n corresponding to a network packet can be identified by any combination of source and destination identifiers, such as IP addresses and port numbers. As such, in some embodiments, the agent 326 indicates priorities to the filter 322 by routing information instead of application name. In other embodiments, the agent 326 provides to the filter 322 a mapping between applications 338a-338n, such as by application name or process id, to the routing information in a routing table 538.

Based on the indicated priorities for applications 338a-338n, in some embodiments, the filter 322 may place, arrange, or coordinate network packets into queues 540a-540n in support of the priorities. In one embodiment, the filter 322 may move network packets from temporary queues 540a-540n or from memory or other storage to a queue 540a-540n associated with the application 338a-338n, a queue 540a-540n associated with a priority, or a queue 540a-540n associated with both an application and a priority. For example, in one embodiment, all high priority network traffic may be placed in a high priority queue 540a and arranged in order based on an order of priority of the application 338a-338n, such as real-time data applications 338a-338n prior to other applications 338a-338n. In some embodiments, the network packets may be arranged in order in a priority queue 540a-540n based on the time the network packet was intercepted by the packet capture mechanism 365, such as in a FIFO manner. In yet a further embodiment, one queue 540a-540n may be used for prioritization by the filter 322. Each network packet may be placed and arranged in a priority order respective to all other intercepted network packets to provide a packet by packet prioritization across all applications 338a-338n and intercepted network packets. One ordinarily skilled in the art will recognize and appreciate that the network packets may be arranged in various priority queues 540a-540n, such as high, medium, low, or by any other granularity, and be placed or arranged in the queue in any suitable manner in practicing the operations of the present invention described herein.

In one embodiment, all network packets for an application 338a-338n are placed in a queue 540a-540n associated with the application 540a-540n. For example, intercepted network packets for an application communicating to a first destination IP

address, and a first destination port may be placed in a first queue 540a. In another embodiment, all network packets for a type of application 338a-338n, such as an email or voice application, or all network packets for a type of protocol used by the application 338a-338n, such as RTP or UDP, may be placed in a queue 540a-540n for prioritizing network packets for one or more applications. For example, online collaboration related applications 338a-338n may be placed and prioritized in a first queue 540a for collaboration related applications. A second queue 540b may be used for email related applications 338a-338n. In another example, a queue 540a may be used for applications 338a-338n communicating real-time data or communicating using the RTP and/or UDP protocol. In a further example, a queue 540a may be used for applications 338a-338n communicating using a remote display protocol, such as ICA or RDP.

Within each application associated queue 540a-540n organized by specific application 338a-338n, type or category of application 338a-338n, or by protocol, the network packets may be further prioritized by the characteristic of the application 338a-338n generating them, e.g., a foreground application, the size of the network packet, or the time the network packet was intercepted. In some embodiments, one or more queues 540a-540n may be used for network packets intercepted but not prioritized because a policy 520 does not exist or apply to the network packet, or the policies 520 indicate to ignore or not process the network packet for prioritization. One ordinarily skilled in the art will recognize and appreciate the various ways network packets may be placed and arranged in a priority based manner in queues 540a-540n associated with the application 338a-338n, the type of application 338a-338n or the protocol used by the application 338a-338n, and that the priority may be based on the policies 520 specified for the client 105.

At step 575 of illustrative method 550, the network packets are communicated from the queues 540a-540n according to the determined priorities for the network packets. In some embodiments, the network packets are organized into priority queues 540a-540b so that the network packets of the highest priority queue 540a-540n are communicated first, and then the next highest priority queue 540a-540n second, and so on. In other embodiments, the queues 540a-540n are organized by application 338a-338n, and therefore, at step 575, the present invention communicates network packets from the queue 540a-540n based on the respective priorities of the applications 338a-338n. Regardless of the queue 540a-540n organization and management, one ordinarily

skilled in the art will recognize and appreciate that the remote access client of the present invention will communicate the network packets from the queues in a manner according to or consistent with the determined priorities, which in turn, may be based or derived from the policies 520 of the client.

In some embodiments, the remote access client 120 of the present invention considers other network factors in determining what network packets to communicate from what queue. For example, the remote access client 120 may receive an indication of network congestion, such as receiving a window size of zero for a TCP connection related to an application 338a-338n. In another example, the remote access client 120 may recognize a high number of retransmits to a particular destination. As such, in some embodiments, the remote access client 120 may throttle back or not communicate network packets related to other networks factors, such as congestion, even though the network packets may have a higher priority than other network packets in a queue 540a-540n. Thus, the client 105 controls and manages the prioritization of network communications of the client 105 on an application 338a-338n basis and in accordance with any policies 520 for the client 105 and in further view of any network statistics and other factors occurring on the network.

In yet a further aspect and referring now to Figures 6A and 6B, the present invention is related to providing a network disruption shielding technique for persistent and reliable connectivity. Figure 6A illustrates environment 300 as discussed above in conjunction with Figure 3A. The environment 300 illustrates network stacks 310a and 310b, which may represent network stacks of computing devices 102a-120b or gateway 340, such as any of the computing devices 102 and the gateway 340 illustrated in Figures 1A-1C, 2A, or 5A. Each network stack 310a-310b may comprise one or more networks layers, such as a TCP/IP network layer on top of the frame network layer as one ordinarily skilled in the art will recognize and appreciate. Although the network stacks 310a-310b are illustrated in environment 300 of Figure 6A with a certain set of network layers, one ordinarily skilled in the art will recognize and appreciate that the network stacks 310a-310b may have any type and/or form of network layers, in any suitable combination, and each of the network stacks 310a-310b may have different forms of each layer in relation to the other network stack.

The network stacks 310a-310b may be considered to have a first portion 605a-605b of the network stack, and a second portion 610a-610b of the network stack. As

illustrated in the example network stacks 310a-310b of Figure 6A, the first portion 605a-605b of the network stack comprises the network layers at and below the TCP network layer. The second portion 610a-610b may comprise those network layers above the TCP network layer, such as a UDP over SSL protocol layer. Although the first portion 605a-605b and the second portion 610a-610b are shown as portioned, segmented, or otherwise divided at the TCP layer, the first portion and second portion may be formed at a higher or lower dividing layer in practicing the network disruption shielding technique of the present invention as one ordinarily skilled in the art will recognize and appreciate.

The network stacks 310a-310b illustrated in Figure 6A may represent an application 338a-338n on client 105, such as the client depicted in Figure 5A, establishing a peer-to-peer SSL VPN connection to a second computing device 102b or, alternatively, a gateway 340. The client 105 may be a mobile client, such as a notebook, personal digital assistant (PDA), a smart phone, or any type of mobile computing or telecommunication device. The client 105 may communicate real-time data such as VoIP communication via the UDP protocol or RTP over UDP via the SSL session established to the peer device 102b or gateway 340. In one embodiment, the agent 326 of the remote access client 120 establishes and maintains the SSL or SSL VPN session to the gateway 340 or to peer computing device 102b. The agent 326 may operate in user-mode 332, and may handle any network layer and protocol processing related to the second portion 610a-610b of the network stack 310a-310b, along with any application layer protocols. As a TCP/IP based network 104, the UDP over SSL session of the second portion 610a-610b of the network stack 310a-310b may be communicated over a TCP/IP stack forming the first portion 605a-605b of the network stack 310a-310b. In view of the remote access client 120 of the present invention, such as illustrated in Figure 1A or 5A, the filter 322 may be a network driver operating in kernel-mode 332 within the first portion 605a-605b of the network stack 310a-310b.

The present invention uses a network disruption shielding technique as depicted by illustrative method 650 in Figure 6B to maintain the second portion 610a-610b of the network stack 310a-310b through a network level connection interruption, such as any type and/or form of network disruption to the first portion 605a-605b of the network stack 310a-310b. The network disruption shielding technique of the present invention may be performed transparently to an application 338a-338n of the client 105, a user of the client 105, any one or more network layers above the first portion

605a-605b, and the gateway 340 or peer computing device 102b, and any portion of their respective network stacks 310a-310b. In one embodiment, the network disruption is shielded without notification to the user of the client that the network was disrupted or a session was interrupted.

In brief overview of illustrative method 650, at step 665, a client 105 establishes a session via at least a first protocol over a network connection between the client and another device, such as a peer computing device or gateway. As such, a network stack 310a-310b is established or used on the client 105. The network stack 310a-310b has a first portion 605a-605b and a second portion 610a-610b. At step 660, a disruption in the network connection is detected causing the first portion 605a-605b of the network stack 310a-310b to be disestablished, or otherwise disrupted from being used or continued to be used. At step 665, the present invention maintains the second portion 610a-610b of the network stack 310a-310b during the disruption and maintaining a session, or sessions, associated with the network layers of the second portion 610a-610b.

During the disruption, at step 670, any network packets related to the second portion 610a-610b of the network stack 310a-310b may be queued. At step 675, the first portion 605a-605b of the network stack 310a-310b is reestablished or otherwise received from the network disruption. While the first portion 605a-605b of the network stack 310a-310b is reestablished, the present invention maintains the second portion 610a-610b, and sessions thereof, allowing at step 680, to continue with the session by linking or re-associating the second portion 610a-610b with the first portion 605a-605b of the network stack 310a-310b. The network connection and/or the session may automatically be re-authenticated at step 680. At step 685, the illustrative method may communicate any queued network packets and continue with the session transparently as if the network disruption did not occur.

In an embodiment of illustrative step 655, a first computing device 102a may establish a network connection with a second device, such as a peer computing device 102b or a gateway 340, by any suitable means and/or mechanism and using any type and/or form of connection based protocol. For example, the network connection may be established via a TCP connection on a TCP/IP network or by an SPX connection on an IPX/SPX network. In some embodiments, the network connection may be initiated by any of the applications 338a-338n on the client, such as any application illustrated in

Figure 5A. For example, a remote display client, such as an ICA client of Citrix Systems, Inc. or a Remote Display Client of Microsoft Corporation may initiate or establish the network connection. In other embodiments, the network connection of illustrative step 665 may be initiated and/or established via the agent 326, filter 322, or any other portion of the remote access client 120. In one embodiment, the establishing of the network connection forms the first portion 605a-605b of the network stack 310a-310b. In other embodiments, the first portion 605a-605b of the network stack 310a-310b, or portion thereof, is established via connection to a network 104 upon startup of the client 105.

In some embodiments, the second portion 610a-610b of the network stack 310a-310b is formed by establishing one more sessions, such as an SSL session, via any type and/or form of protocol over the network connection, such as a remote display protocol of ICA or RDP. The session may be established via any application 338a-338n or the remote access client 120 of the client. In one embodiment, the session may correspond to a tunneling or gateway session with a peer computing device 102b or a gateway 340. In another embodiment, the session may be any type of interactive session such as a media session established via a signaling protocol, SIP for example. For example, the session of the second portion 610a-610b of the network stack 310a-310b may comprise a VoIP communication session, such as one established by illustrative method 260 of Figure 2B. Additionally, there may be multiple sessions associated with the second portion 610a-610b of the network stack 310a-310b. For example, an SSL or SSL VPN session may form one session, while a second session, such as media session via RTP over UDP may form a second session. Additionally, at any application layer of the network stack 310a-310b one or more applications 338a-338n on the client 105 may establish an application level session with a peer computing device 102b. In one embodiment, the agent 326 of the remote access client 120 is responsible for establishing and maintaining the second portion 610a-610b of the network stack 310a-310b and one or more of the associated sessions.

At step 660 of the illustrative method 650 of the present invention, a disruption in network connection is detected. In one embodiment, the network disruption may be caused by a mobile client 105 roaming between networks and networks segments, which, in some embodiments, causes the client 105 to obtain a new network IP address and/or host name. In some embodiments, the disruption disrupts the first portion 605a-

605b of the network stack 310a-310b, such as, for example, causing a TCP or SPX connection to be disconnected. In one aspect, the disruption causes the first portion 605a-605b, or any portion thereof, of the network stack 310a-310b to be disestablished, or otherwise needing to be re-established, reconnected, reconfigured or rebuilt. For example, in some embodiments, the IP layer of the network stack may maintain intact while the TCP layer is reestablished. In one embodiment, any TCP related drivers may need to be re-started. In other embodiments, the TCP/IP layer be intact even though the network connection is disrupted, and only a new TCP connection needs to be established. In other embodiments, the TCP/IP layer is intact but needs to reconfigure itself for a new network or network segment, such as changing the IP address of the client 105. One ordinarily skilled in the art will recognize and appreciate the various ways a network connection may be disrupted and impact or affect a first portion of the network stack.

In some embodiments, the agent 326, or any other portion of the remote access client 120 may detect the network disruption by any suitable means and/or mechanisms. In one embodiment, the agent 326 may determine a network disruption by receiving an error message or failure upon calling or executing an API call to the first portion 605a-605b of the network stack 310a-310b. For example, the SSL session maintained by the agent 326 for the second portion 610a-610b relies or depends on the TCP connection of the first portion 605a-605b of the network stack 310a-310b. As the agent 326 transacts via the SSL session, the agent 326 may receive an error or failure message indicating a problem with the TCP connection. In other embodiments, the agent 326 may receive an event or message from any network layer of the first portion 605a-605b of the network stack 310a-310b indicating a network disruption. One ordinarily skilled in the art will recognize and appreciate the various ways the network disruption may be detected.

At illustrative step 665, in some embodiments, upon detection of the network disruption, the agent 326 or any other portion of the remote access client 120 of the present invention maintains the second portion 610a-610b of the network stack 310a-310b during the disruption. For example, although the SSL based session maintained by the agent 326 depends on an underlying TCP connection, the agent 326 keeps the SSL session open or active through the disruption to the TCP connection. As there may multiple sessions associated with one or more layers of the second portion 610a-610b of the network stack, the agent 326, in some embodiments, keeps one or more, or all, of the

multiple sessions open or active although the first portion 605a-605b of the network stack 310a-310b is disrupted.

At step 670 of illustrative method 650, the remote access client 120 of the present invention, in some embodiments, queues one or more network packets of any of the protocols related to the second portion 610a-610b of the network stack 310a-310b during the network disruption. The remote access client 120 may use any type and/or form of queuing mechanisms, such as any of the queues 540a-540n illustrated in Figure 5A. In other embodiments, the remote access client 120 may discard network packets during the disruption, such any packets related to a lossy protocol, such as RTP over UDP for voice communications. In some cases, it may be desirable to discard packets, such as UDP packets, to reduce latency and quality issues, such as in voice communications. In further embodiments, the remote access client 120 may queue some network packets and discard other network packets. In an additional embodiment, the remote access client 120 may queue the network packets, and discard some or all of the network packets after a predetermined period of time. The remote access client 120 may use the policies 520 to determine which network packets to queue and/or discard. For example, a network packet of a first application 338a may be queued while a network packet of a second application 338n is discarded. In other embodiments, the remote access client 120 may use any network statistics or any network traffic inspection techniques, for example stateful inspection, as known to those skilled in the art to determine whether to queue and/or discard network packets during the disruption.

At step 675 of illustrative method 650, the first portion 605a-605b of the network stack 310a-310b is reestablished while the second portion 610a-610b of the network stack 310a-310b is maintained along with maintaining any desired session or sessions of the second portion 610a-610b of the network stack 310a-310b. The first portion 605a-605b of the network stack 310a-310b may be reestablished by any suitable means and/or mechanisms. For example, the client 105 may reestablish the TCP/IP connection to the network 104, such as by logging into a new network for a roaming mobile client 105. In other embodiments, the remote access client 120, such as via the agent 326 or the filter 322, reestablishes the first portion 605a-605b of the network stack 310a-310b. For example, the agent 326 may initiate and establish a new TCP connection. Upon reestablishing the first portion 605a-605b, the second portion 610a-610b of the network stack 310a-310b is linked with, re-associated with or starts to use or continue to use the

first portion 605a-605b to reestablish the network stack 310a-310b. In some embodiments, the agent 326 may be notified by an event of any network layer that the first portion 605a-605b has been reestablished or in other embodiments, may poll by any predetermined frequency to determine the first portion 605a-605b is reestablished. For example, the agent 326 may check if the TCP connection is active or can be reconnected.

In some embodiments, at step 680, the remote access client 120, such as the agent 326, may automatically re-authenticate the client 105 or a user of the client 105 for the network connection, such as a TCP connection for the first portion 605a-605b of the network stack 610a-610b. For example, the remote access client 120 may automatically re-authenticate the client 105 to a network 104 using any network related credentials of a user of the client 105. Additionally, the remote access client 120 may automatically re-authenticate the client 105 or a user of the client 105 for any session associated with the second portion 610a-610b of the network stack 310a-310b. For example, the SSL session between the agent 326 and the gateway 340 or peer computing device 102c may be re-authenticated.

In another example, an application 338a may be accessing a host service, web server, or application server that uses authentication credentials for access. The agent 326 may automatically re-authenticate the application 338a to the corresponding service or server using application related authentication credentials. In some embodiments, the remote access client 120 may re-authenticate the client and/or user of the client 105 at multiple levels, such as for network access and/or TCP connection, SSL or SSL VPN session, and/or any application level sessions, such as a media interactive user session, for example, a VoIP telephone session. Furthermore, the remote access client 120 may re-authenticate at any time prior to step 685, during step 685, for example, after communicating queued network packets but before continuing other communications, or after step 865, in response to a request to authenticate from a peer computing device, such as a server or the gateway 340.

At step 685 of illustrative method 650, the remote access client 120 of the present invention continues to use the session or sessions of the second portion 610a-610b of the network stack. If any network packets have been queued or remain queued at step 670, the remote access client 120 communicates the queued network packets and continues communicating any network packets of the client 105, such as network

packets generated by or sent to the one more applications 338a-338n of the client 105. As such, the network disruption shielding technique of the present invention provides a seamless and transparent solution to nomadic mobile computing solutions and for generally providing reliable and persistent network connectivity and access.

In the example of a VoIP communications, the illustrative method 650 of the present invention will reduce the number of telephone call drops due to network disruptions and improve the usage of and experience with VoIP. A VoIP user will not need to reconnect the telephone call due to temporary network disruptions in network availability as the remote access client 120 of the present invention will automatically maintain the session and reconnect to the network. Additionally, the remote access client 120 of the present invention will automatically re-authenticate the connection and sessions for providing security after the network disruption. Furthermore, the network shielding technique of the present invention is useful for 1) continuing transactions, commands, or operations automatically through the network disruption, 2) maintaining session related context and cache through the network disruption, and 3) automatically handling change in network address of the client due to changes in the network.

By providing a reliable and persistent connection, the present invention also avoids interruptions to transactions, commands or operations as part of the functionality exercised between the a first computing device 102a and a second computing device 102b, such as client 105a and 105b in Figures 1C. For example, a file copy operation using Windows Explorer has not been designed to continue working after there is a disruption in a network connection. A user on the client 105 may use the file copy feature of Windows Explorer to copy a file from the client 105 to a server 102c. Because of the size of the file or files, this operation may take a relatively extended period of time to complete. If during the middle of the operation of the copy of the file to the server, there is an interruption in the network connection between the client 105 and the server, the file copy will fail. Once the network connection is re-established, the user will need to start another file copy operation from Windows Explorer to copy the file from the client 105 to the server. Under the present invention, the user would not need to start another file copy operation. The network connection would be re-established in accordance with the network disruption shielding technique of the present invention as illustrated in Figure 6B. As such, the file copy of Windows Explorer would not get notified of the interruption in the network connection and therefore, would not

fail. The remote access client 120 would re-establish any connections and transmits any queued data so that operation can continue without failure. The remote access client 120 would maintain a queue of the data related to the file copy operations that has not been transferred to the server because of the interruption in the network connection. Once the network connection is re-established, the remote access client 120 can transmit the queued data and then continue on with transferring the data related to the file copy operation in due course.

Although this aspect of the invention is described in terms of a file copy operation example, one ordinarily skilled in the art will recognize that any operation, transaction, command, function call, etc. transacted between a first computing device 102a and a second computing device 102b, can be maintained and continued without failure from the network connection disruption, and, furthermore, without the client 105 or user of the client 105 recognizing there was a disruption or having notice of the disruption. Additionally, the transaction or operation can be maintained and continued transparently to the application 338, the gateway 340, second computing device 102c, and any part of the second portion 610a-610b of the network stack 310a-310b.

By providing the client 105 with a reliable and persistent connection to a peer computing device 102b or gateway 340, the present invention avoids the process of opening a new user session with an application 338 on the peer, such as a host service on server, by maintaining the user session through network connection interruptions. For each user session between peer computing device, each computing device may maintain session specific context and caches, and other application specific mechanisms related to that instance of the user session. For each new user session established, these session specific context and caches need to be re-populated or re-established to reflect the new user session. For example, a user on the client 105 may have an http session with a server 102c having a web server or web application. The server 102c may keep context specific to providing this instance of the http session with the client 105. The context may be stored in the memory of the server, in files of the server, a database or other component related to providing the functionality of the server 102c. Also, the client 105 may have local context specific to the instance of the http session, such as a mechanism for keeping track of an outstanding request to the web server. This context may be stored in memory of the client 105, in files on the client 105, or other software component interfaced with the client 105. If the connection between the client 105 and

the server 102c is not persistent, then a new user session needs to be established with new session specific context on the server 102c and the client 105. The present invention maintains the session so that a new session, and therefore new specific session context, does not need to be re-established.

The present invention maintains the user session through network level connection interruptions and without notification to the user of the client that the session was interrupted. In operation of this aspect of the invention, the client 105 establishes the connection to the peer computing devices. Via the connection, a session between the client 105 and the server is established. The remote access client 120 can store and maintain any session related information such as authentication credentials, and client 105 and host server 102c context for the established session. Upon detection of a disruption in network connection, the remote access client 120 can re-establish the first portion 605a-605b of the network stack 310a-301b while maintaining the second portion 610a-610b of the network stack. The network connection disruption may cause an interruption to the underlying TCP/IP connection used by the session between the client 105 and the server 102c. However, since the second portion 610a-610b of the network stack 310a-310b is maintained, the session can be re-established and/or continued after the network connection is re-established without the user on the client 105 having notification that the session was interrupted. Thus, the interruption of the session caused by the network connection disruption is effectively hidden from the user using the network disruption shielding techniques of the present invention.

Furthermore, by providing a reliable and persistent connection, the present invention also enables a client 105 to traverse through different network topologies without re-starting a session or an application 338 on the client 105. For example, the client 105 may be a computer notebook with a wireless network connection. As the client 105 moves from a first wireless network to a second wireless network, the client's network connection may be temporarily disrupted from the first wireless network as a network connection is established with the second wireless network. The second wireless network may assign a new network identifier, such as a host name or internet protocol address, to the client 105. This new network identifier may be different than the network identifier assigned to the client 105 by the first wireless network. In another example, the client 105 may be physically connected through an Ethernet cable to a port on the network. The physical connection may be unplugged and the client 105 moved to

another location to plug into a different port on the network. This would cause a disruption into the network connection and possibly a change in the assigned network identifier. Without the present invention, any sessions between peer computing devices may need to be restarted due to the change in the network topology, the disruption to the network connection, and/or the change in the assigned network identifier. By the method and systems described herein, the remote access client 120 of the present invention maintains the network connection for the client and automatically re-established the client's 105 network connection including handling changes in the network topology and network identifier. The client 105, and any applications or sessions on the client 105, can continue to operate as if there was not a network connection disruption or a change in the network identifier. Furthermore, the user on the client 105 may not recognize there were any interruptions or changes, and the client 105 may not receive any notice of such interruptions.

In an additional aspect, any of the techniques of the present invention, such as the illustrative methods of Figures 2B, 3B, 3C, 4, 5B and 6B, can be practiced in one or more combinations with each other. In one embodiment, the peer-to-peer routing technique may be practiced with the false acknowledgement and/or MTU adjustment techniques. This would provide a client communicating real-time data, such as VoIP, to connect to the peer via a more optimal and direct route and to communicate the real-time data via UDP over a secure SSL/TCP/IP connection, while avoiding any latency due to any reliability mechanism of TCP and reduce fragmentation due to the encryption overhead. Additionally, this embodiment may be further combined with the client-side application-aware prioritization technique and/or the network disruption shielding technique. As such, the secure real-time data communications can be communicated from the client at higher priorities than other applications of the client to improve the quality of the real-time experience, such as VoIP. The network disruption technique would allow a mobile VoIP phone, such as a soft phone of a notebook, roam between network access points and automatically continue with the session.

The techniques of the present invention are complimentary to each other for network communication optimizations, such as for example in VoIP communications over a SSL VPN gateway. As such, each of the 1) peer-to-peer routing technique, 2) the false acknowledgement technique, 3) payload shifting technique, 4) the MTU adjustment technique, 5) the client-side application-aware technique, and 5) the network

disruption shielding technique of the present invention may be practiced with one or more of the following techniques and optimization of the present invention: 1) the peer-to-peer routing technique, 2) the false acknowledgement technique, 3) payload shifting technique, 4) the MTU adjustment technique, 5) the client-side application-aware technique, and/or 5) the network disruption shielding technique.

In one further illustrative example of the present invention, an online meeting, collaboration and/or desktop sharing service, such as the hosted service of GoToMeeting.com, WebEx.com, or LiveMeeting.com may use the techniques of the present invention in one or more combinations. The host service may use a gateway 340, and the techniques of illustrative method 260 to facilitate a peer-to-peer connection between a first computing device of a meeting presenter and a second computing device of a meeting attendee. The computing devices of the meeting presenter and attendees may download via the host service the remote access client 120, or any portions thereof. Once the meeting presenter and the meeting attendee establish a peer-to-peer connection, the peer computing devices may use any of the optimization techniques of the present invention to optimize their communications, such as the MTU adjustment technique, client-side application aware technique, or the network disruption shielding technique. Along with the peer-to-peer routing, the optimization techniques of the present invention, will improve the performance, efficiency and user experience of the online meeting, collaboration, or desktop sharing.

In yet a further aspect and in view of Figure 2A, for example, the remote access client 120 of the present invention can distribute Dynamic Host Configuration Protocol (DHCP) IP addresses of the client 105 or the publicly visible IP addresses to the telecommunication device 210a-210b, such as either a hardware or software based VoIP telephone. The gateway 340 of the present invention facilitates the discovery of the public IP addresses of the client, such as client 105b illustrated in Figure 2A. As such, the techniques of the present invention enables protocols that communicate their IP address over the protocol to continue to function.

Many alterations and modifications may be made by those having ordinary skill in the art without departing from the spirit and scope of the invention. Therefore, it must be expressly understood that the illustrated embodiments have been shown only for the purposes of example and should not be taken as limiting the invention, which is defined by the following claims. These claims are to be read as including what they set forth

literally and also those equivalent elements which are insubstantially different, even though not identical in other respects to what is shown and described in the above illustrations.

We claim:

1. A method for establishing a peer to peer communication session between a first computing device on a first network and a second computing device on a second network, the first network disconnected from and not routable to the second network, the method comprising the steps of:

(a) establishing, by the first computing device, a first tunneling session with a third computing device, and establishing, by the second computing device, a second tunneling session with the third computing device;

(b) initiating, by the first computing device, a communication session to the second computing device via the third computing device;

(c) receiving, by a server, a signal to establish the communication session;

(d) communicating, by the server, to the first computing device a first network address comprising a network address of the second computing device associated with the second tunneling session;

(e) communicating, by the first computing device, a request to initiate a connection with the second computing device using the first network address;

(f) intercepting, by the third computing device, the request, and providing the first computing device a second network address for the second computing device, the second network address comprising a public network address associated with the second computing device; and

(g) communicating, by the third computing device, a request to the second computing device to allow a connection from the first computing device using the second network address.

2. The method of claim 1, wherein at least a portion of one of the first tunneling session or the second tunneling session comprises one of a Secure Socket Layer or a virtual private network

3. The method of claim 1, wherein the third computing device comprises a remote access gateway.

4. The method of claim 1, wherein the second computing device is located behind a firewall associated with the second network address.

5. The method of claim 1, comprising providing, by the third computing device, the second network address to the first computing device by communicating an out of band signal to the first computing device via the first tunneling session.
6. The method of claim 1, comprising providing, by the second computing device, a forward hole in a firewall for the first computing device to communicate to the second computing device using the second network address.
7. The method of claim 1, comprising communicating, by the third computing device, a key to the first computing device and the second computing device.
8. The method of claim 7, comprising communicating, by the first computing device, the key to the second computing device.
9. The method of claim 8, comprising checking, by the first computing device, that the key received from the second computing device matches the key of the first computing device before transmitting data to the second computing device.
10. The method of claim 7, comprising communicating, by the second computing device, the key to the first computing device.
11. The method of claim 10, comprising checking, by the second computing device, that the key received from the first computing device matches the key of the second computing device before transmitting data to the second computing device.
12. The method of claim 1, associating a first telecommunication device with the first computing device, and associating a second telecommunication device with the second computing device.
13. The method of claim 12, wherein one of the first telecommunication device or the second telecommunication device comprises one of a software component or a hardware component.

14. The method of claim 12, comprising establishing a telecommunication session between the first telecommunication device and the second telecommunication device via the connection.

15. The method of claim 15, comprising communicating between the first telecommunication device and the second telecommunication device over the telecommunication session without traversing the to the first computing device

16. The method of claim 1, comprising communicating a remote display protocol via the connection between the first computing device and the second computing device.

17. The method of claim 16, wherein the remote desktop protocol comprises one of an Independent Computing Architecture protocol or a Remote Desktop Protocol.

18. The method of claim 1, comprising sharing a screen view of the first computing device with the second computing device via the connection.

19. In a gateway, a method for establishing a peer to peer communication session between a first computing device on a first network and a second computing device on a second network, the first network disconnected from and not routable to the second network, the method comprising the steps of:

(a) establishing a first tunneling session with the first computing device on a first network;

(b) establishing a second tunneling session with the second computing device on the second network;

(c) receiving a request by the first computing device to initiate a communication session with the second computing device;

(d) providing to the first computing device a first network address for contacting the second computing device, the first network address comprising a network address of the second computing device associated with the second tunneling session;

(e) receiving a request by the first computing device to initiate a connection with the second computing device using the first network address;

(f) intercepting the request to initiate the connection, and providing the first computing device a second network address for the second computing device, the second network address comprising a public network address associated with the second computing device; and

(g) communicating to the second computing device a request to allow the connection from the first computing device to the second computing device using the second network address.

20. The method of claim 19, wherein at least a portion of one of the first tunneling session or the second tunneling session comprises one of a Secure Socket Layer or a virtual private network.

21. The method of claim 19, wherein the second computing device is located behind a firewall associated with the second network address.

22. The method of claim 19, comprising providing the second network address to the first computing device by communicating an out of band signal to the first computing device via the first tunneling session.

23. The method of claim 19, comprising communicating a key to the first computing device.

24. The method of claim 19, comprising communicating a key to the second computing device.

25. A system for establishing a peer to peer communication session between a first computing device on a first network and a second computing device on a second network via a third computing device, the first network disconnected from and not routable to the second network, the system comprising:

a first computing device on the first network;

a second computing device on the second network;

a third computing device establishing a first tunneling session with the first computing device and a second tunneling session with the second computing device;

a server accessible via the third computing device;

wherein:

the server communicates via the third computing device to the first computing device a first network address comprising a network address of the second computing device associated with the second tunneling session;

the first computing device communicates via the third computing device a first request to initiate a connection with the second computing device using the first network address;

the third computing device intercepts the first request, and provides the first computing device a second network address for the second computing device, the second network address comprising a public network address associated with the second computing device; and

the third computing device communicates a second request to the second computing device to allow a connection from the first computing device using the second network address.

26. The system of claim 25, wherein at least a portion of one of the first tunneling session or the second tunneling session comprises one of a Secure Socket Layer or a virtual private network.

27. The system of claim 25, wherein the third computing device comprises a remote access gateway.

28. The system of claim 25, wherein the second computing device is located behind a firewall associated with the second network address.

29. The system of claim 25, wherein the third computing device provides the second network address to the first computing device by communicating an out of band signal via the first tunneling session.

30. The system of claim 25, wherein the second computing device provides a forward hole in a firewall for the first computing device to communicate to the second computing device using the second network address.

31. The system of claim 25, wherein the third computing device communicates a key to the first computing device and the second computing device.

32. The system of claim 31, wherein the first computing device communicates the key to the second computing device.

33. The system of claim 32, wherein the first computing device checks that the key received from the second computing device matches the key of the first computing device before transmitting data to the second computing device.

34. The system of claim 31, wherein the second computing device communicates the key to the first computing device.

35. The system of claim 34, wherein the second computing device checks that the key received from the first computing devices matches the key of the second computing device before transmitting data to the second computing device.

36. The system of claim 25, comprising a first telecommunication device associated with the first computing device, and a second telecommunication associated with the second computing device.

37. The system of claim 36, wherein one of the first telecommunication device or the second telecommunication device comprises one of a software component or a hardware component.

38. The system of claim 37, wherein the first telecommunication device establishes a telecommunication session with the second telecommunication device via the connection.

39. The system of claim 38, wherein the first telecommunication device communicates with the second telecommunication device over the telecommunication session without traversing the third computing device.

40. The system of claim 25, wherein the first computing device and the second computing device communicate a remote display protocol via the connection.

41. The system of claim 25, wherein the remote desktop protocol comprises one of an Independent Computing Architecture protocol or a Remote Desktop Protocol.

42. The system of claim 25, wherein the first computing device shares a screen view with the second computing device via the connection.

43. A gateway for establishing a peer to peer communication session between a first computing device on a first network and a second computing device on a second network, the first network disconnected from and not routable to the second network, the gateway comprising:

- a means for establishing a first tunneling session with the first computing device on a first network;

- a means for establishing a second tunneling session with the second computing device on the second network;

- a means for receiving a request by the first computing device to initiate a communication session with the second computing device;

- a means for providing to the first computing device a first network address for contacting the second computing device, the first network address comprising a network address of the second computing device associated with the second tunneling session;

- a means for receiving a request by the first computing device to initiate a connection with the second computing device using the first network address;

- a means for intercepting the request to initiate the connection, and providing the first computing device a second network address for the second computing device, the second network address comprising a public network address associated with the second computing device; and

- a means for communicating to the second computing device a request to allow the connection from the first computing device to the second computing device using the second network address.

44. The system of claim 43, wherein at least a portion of one of the first tunneling session or the second tunneling session comprises one of a Secure Socket Layer or a virtual private network.
45. The system of claim 43, wherein the second computing device is located behind a firewall associated with the second network address.
46. The system of claim 43, comprising a means for providing the second network address to the first computing device by communicating an out of band signal to the first computing device via the first tunneling session.
47. The system of claim 43, comprising a means for communicating a key to the first computing device.
48. The system of claim 43, comprising a means for communicating a key to the second computing device.
49. A method for communicating via a lossless protocol a packet constructed for transmissions via a lossy protocol, the method comprising the steps of:
- (a) establishing a connection between a first computing device and a second computing device via a lossless protocol;
 - (b) detecting, by the first computing device, a lossless protocol packet comprising a payload having one or more packets constructed in accordance with a lossy protocol;
 - (c) communicating, by the first computing device, a false acknowledgement of receipt of the lossless protocol packet to one of the first computing device or the second computing device; and
 - (d) communicating, by the first computing device, the lossless protocol packet to the second computing device.
50. The method of claim 49, comprising encrypting, by the first computing device, the one or more packets using a key.

51. The method of claim 50, comprising providing the encryption key to the first computing device via an out of band transport security layer session between the first computing device and the second computing device.
52. The method of claim 49, comprising encrypting the one or more packets on a packet by packet basis.
53. The method of claim 49, further comprising performing step (c) before step (d).
54. The method of claim 49, wherein the second computing device is a gateway.
55. The method of claim 49, comprising, in response to receiving the false acknowledgement of receipt of the lossless protocol packet by one of the first computing device or the second computing, preventing a network stack of one of the first computing device or the second computing from executing an operation associated with providing a lossless characteristic of the lossless protocol.
56. The method of claim 49, wherein the lossless protocol comprises a transport control protocol.
57. The method of claim 56, comprising preventing the network stack of one of the first computing device or the second computing device from executing one or more of the following in connection with the lossless protocol: a retransmit, an ordering, a flow control algorithm, a nagle's algorithm, and a sliding window algorithm.
58. The method of claim 49, wherein the lossy protocol comprises a user datagram protocol.
59. The method of claim 49, comprising communicating, by the first computing device, the lossless protocol packet via one of a secure socket layer or a transport security layer tunnel to the second computing device.

60. The method of claim 49, wherein the one or more packets comprises a real-time protocol.

61. The method of claim 49, comprising communicating by the first computing device one of real-time voice, audio, or data to the second computing device via the one or more packets.

62. A system for communicating via a lossless protocol a packet constructed for transmissions via a lossy protocol, the system comprising:

- a means for establishing a connection between a first computing device and a second computing device via a lossless protocol;

- a means for detecting, by the first computing device, a lossless protocol packet comprising a payload having one or more packets constructed in accordance with a lossy protocol;

- a means for communicating, by the first computing device, a false acknowledgement of receipt of the lossless protocol packet to one of the first computing device or the second computing device; and

- a means for communicating, by the first computing device, the lossless protocol packet to the second computing device.

63. The system of claim 62, comprising a means for encrypting, by the first computing device, the one or more packets using a key.

64. The system of claim 63, comprising a means for providing the encryption key to the first computing device via an out of band transport security layer session between the first computing device and the second computing device.

65. The system of claim 63, comprising a means for encrypting the one or more protocol packets on a packet by packet basis.

66. The system of claim 62, further comprising a means for communicating the false acknowledgement of receipt of the lossless protocol packet before communicating the

lossless protocol packet.

67. The system of claim 62, wherein the second computing device is a gateway.

68. The system of claim 62, comprising a means, in response to receiving the false acknowledgement of receipt of the lossless protocol packet by one of the first computing device or the second computing, for preventing a network stack of one of the first computing device or the second computing from executing an operation associated with providing a lossless characteristic of the lossless protocol.

69. The system of claim 62, wherein the lossless protocol comprises a transport control protocol.

70. The system of claim 69, comprising a means for preventing the network stack of one of the first computing device or the second computing device from executing one or more of the following in connection with the lossless protocol: a retransmit, an ordering, and a flow control algorithm.

71. The system of claim 62, wherein the lossy protocol comprises a user datagram protocol.

72. The system of claim 62, comprising a means for communicating, by the first computing device, the lossless protocol packet via one of a secure socket layer or a transport security layer tunnel to the second computing device.

73. The system of claim 62, wherein the one or more packets comprises a real-time protocol.

74. The system of claim 62, comprising a means for communicating by the first computing device one of real-time voice, audio, or data to the second computing device via the one or more packets.

75. A method for transmitting packets from an application using an unreliable

transport protocol over a TCP connection, comprising:

- receiving, at a first device, a first packet to be transmitted using an unreliable transport protocol;
- creating a first TCP packet including a first payload of the received first packet and a first TCP header of information associated with a TCP connection established between the first device and a second device;
- transmitting, by the first device, the first TCP packet to the second device;
- receiving, at the first device, a second packet to be transmitted using an unreliable transport protocol;
- creating a second TCP packet including a second payload of the received second packet and the first TCP header information; and
- transmitting, by the first device, before receipt of an acknowledgement of the receipt of the first payload from the second device, the second TCP packet to the second device.

76. The method of claim 75, comprising establishing the TCP connection with a port number associated with the unreliable transport protocol.

77. The method of claim 75, comprising dynamically determining, by the first device, the first TCP packet and second TCP packet comprise an unreliable transport protocol.

78. The method of claim 75, wherein the unreliable transport protocol is UDP.

79. The method of claim 75, comprising further:

- receiving the first TCP packet and second TCP packet on the first device by intercepting the first TCP packet and second TCP packet using a packet capturing mechanism.

80. The method of claim 75, comprising establishing, by the first device, the TCP connection with a VPN gateway device.

81. The method of claim 75, comprising establishing peer-to-peer communications between the first device and the second device via the TCP connection.

82. The method of claim 75, comprising encrypting, by the first device, the first and second TCP packets, and decrypting, by the second device, the encrypted first and second TCP packets.

83. A method for transmitting packets from an application using an unreliable transport protocol over a TCP connection, comprising:
intercepting, at a second device, a first TCP packet created on a first device and received on the second device, the first TCP packet including a first payload of a first packet generated by an application using an unreliable protocol and a first TCP header of information associated with a TCP connection established between the first device and the second device, the intercepting occurring before the first TCP packet is provided to a TCP stack on the second device;
identifying, responsive to the TCP header of information, that the first payload is a packet generated by an application using an unreliable transport protocol;
stripping the TCP header of information from the first TCP packet; and
forwarding the first payload to an application using the unreliable data protocol.

84. The method of claim 83, wherein the unreliable protocol is UDP.

85. The method of claim 83, wherein the step of identifying comprises identifying the TCP header information includes a port number associated with the unreliable transport protocol.

86. The method of claim 83, comprising further:
intercepting, by the second device, the first TCP packet using a packet capture driver.

87. The method of claim 83, wherein the first device is a client device and the

second device is a VPN gateway.

88. The method of claim 87, comprising further:
performing Network Address Translation (NAT) on the second device prior to forwarding the first payload to the application.

89. A system for transmitting packets from an application using an unreliable transport protocol over a TCP connection, the system comprising:
a first device, the first device comprising:
an application generating a first and second packet, the first and second packet intended to be transmitted using an unreliable transport protocol;
a filter process, the filter process intercepting the first and second packets from the application and forwarding the intercepted packets to a tunnel process; and
a tunnel process, the tunnel process requesting the opening of a TCP connection between the first device and a second device, the request to open the TCP connection indicating to the first and second device that the TCP connection will transport packets intended to be transmitted with an unreliable transport protocol, the tunnel process forwarding the first and second packets as payloads in a first and second TCP packet to the second device, the tunnel process sending the second TCP packet after sending the first TCP packet and prior to receiving an acknowledgement for the first TCP packet ; and
a second device in communication with the first device, the second device comprising:
a second tunnel process opening the TCP connection requested by the first device, the second tunnel process identifying and forwarding the source address of the TCP connection to a second filter process; and
the second filter process, the second filter process intercepting packets from the application received at the second device with the TCP connection source address in a header, the second filter process stripping the TCP header from the received packets and forwarding the stripped packets,

circumventing the TCP/IP stack on the second device, to an intended destination.

90. The system of claim 89, wherein the filter process on the first device comprises a packet capture driver.

91. The system of claim 89, wherein the second filter process on the second device comprises a packet capture driver.

92. The system of claim 89, wherein the first device is a client device and the second device is a VPN gateway device.

93. The system of claim 89, further comprising:
a third device to which the stripped packets are transmitted.

94. The system of claim 93, wherein the second device comprises further:
a Network Address Translation (NAT) table used to perform network address translation prior to transmitting the stripped packets to a third device.

95. The system of claim 89, wherein the unreliable data protocol is UDP.

96. A method for adjusting the maximum transmission unit of a secure network communication to reduce network fragmentation, the method comprising the steps of:

(a) establishing a session between a first computing device and a second computing device, the first computing device having a first network stack;

(b) detecting, by the first computing device, a network packet having an encrypted payload;

(c) determining, by the first computing device, a setting for a maximum transmission unit parameter of the first network stack to reduce the maximum transmission unit size by at least a size associated with the encrypted portion of the payload; and

(d) altering the maximum transmission unit parameter of the first network stack to the determined setting.

97. The method of claim 96, comprising communicating the network packet via one of a secure socket layer or a transport layer security tunnel to the second computing device.

98. The method of claim 96, wherein the payload comprises a real-time protocol.

99. The method of claim 96, further comprising altering the maximum transmission unit parameter via a network driver interface specification level mechanism of the first network stack

100. The method of claim 96, further comprising determining the setting of the maximum transmission unit parameter dynamically per session between the first computing device and the second computing device.

101. The method of claim 96, comprising establishing the session between the first computing device and the second computing device via a gateway.

102. The method of claim 96, communicating by the first computing device one of real-time voice, audio, or data to the second computing device via the payload of the network packet.

103. The method of claim 96, comprising communicating a false acknowledgement of receipt of the network packet to one of the first computing device or the second computing device before communicating the network packet.

104. The method of claim 96, further comprising establishing the session between the first computing device and the second computing device via an agent of the first computing device.

105. The method of claim 104, comprising communicating, by the agent, via an IOCTL application programming interface to the first network stack to alter the

maximum transmission unit parameter to the determined setting.

106. A system for adjusting the maximum transmission unit of a secure network communication to reduce network fragmentation, the system comprising:

a means for establishing a session between a first computing device and a second computing device, the first computing device having a first network stack;

a means for detecting, by the first computing device, a network packet having an encrypted payload;

a means for determining, by the first computing device, a setting for a maximum transmission unit parameter of the first network stack to reduce the maximum transmission unit size by at least a size associated with the encrypted portion of the payload; and

a means for altering the maximum transmission unit parameter of the first network stack to the determined setting.

107. The system of claim 106, comprising a means for communicating the network packet via one of a secure socket layer or a transport layer security tunnel to the second computing device.

108. The system of claim 106, wherein the payload comprises a real-time protocol.

109. The system of claim 106, wherein the payload comprises a representation of one of real-time voice, audio, or data.

110. The system of claim 106, further comprising a means for altering the maximum transmission unit parameter of the first computing device via a network driver interface specification level mechanism of the first network stack

111. The system of claim 106, further comprising a means for determining the setting of the maximum transmission unit parameter dynamically per session between the first computing device and the second computing device.

112. The system of claim 106, comprising a means for establishing the session

between the first computing device and the second computing device via a gateway.

113. The system of claim 106, comprising a means for communicating by the first computing device one of real-time voice, audio, or data to the second computing device via the payload of the network packet.

114. The system of claim 106, comprising a means for communicating a false acknowledgement of receipt of the network packet to one of the first computing device or the second computing device before communicating the network packet.

115. The system of claim 106, wherein the network packet comprises a lossless protocol packet.

116. The system of claim 115, wherein the lossless protocol packet comprises a transport control protocol.

117. The system of claim 106, wherein the payload comprises a lossy protocol packet.

118. The system of claim 117, wherein the lossy protocol packet comprises a user datagram protocol.

119. The system of claim 106, comprising an agent of the first computing device for establishing the session between the first computing device and the second computing device.

120. The system of claim 119, wherein the agent communicates via an IOCTL application programming interface to the first network stack to alter the maximum transmission unit parameter to the determined setting.

121. A method for a client to prioritize network communications of the client associated with an application of the client, the method comprising the steps of:

(a) intercepting, by the client, one or more network packets associated with one or more applications of the client;

- (b) storing, by the client, the one or more network packets to a queue;
- (c) determining, by the client, the queued one or more network packets is associated with a first application of the client;
- (d) indicating, by the client, a priority for the determined one or more network packets to place the determined one or more network packets ahead of at least one network packet in the queue associated with a second application of the client; and
- (e) providing the prioritized one or more network packets for communications via a network stack of the client.

122. The method of claim 121, wherein the step of determining, by the client, further comprises determining the queued one or more networks packets of the first application comprises real-time data.

123. The method of claim 122, wherein the real-time data comprises one of the following: a real-time protocol, a user datagram protocol, and a representation of one of voice or audio.

124. The method of claim 121, comprising preventing, by the client, at least one network packet of the second application from being communicated via the network stack ahead of the one or more network packets of the first application.

125. The method of claim 121, comprising holding, by the client, in the queue a network packet associated with the second application, and releasing the held network packet upon communication of the one or more network packets associated with the first application prioritized ahead of the held network packet.

126. The method of claim 121, comprising intercepting, by the client, the one or more network packets transparently to the one or more applications on the client.

127. The method of claim 121, comprising running the first application in the foreground, and the second application in the background.

128. The method of claim 121, comprising associating a priority with the first

application higher than a priority associated with the second application.

129. The method of claim 128, comprising specifying, by a user, the priority of one of the first application or the second application.

130. The method of claim 121, comprising receiving, by the client, the one or more network packets from a computing device.

131. The method of claim 121, comprising providing, by the one or more applications, the one or more network packets for communicating from the client to a computing device.

132. A client for prioritizing network communications of the client associated with an application of the client, the client comprising:

- a mechanism for intercepting one or more network packets of the client associated with one or more applications of the client, and

- a network driver for storing the one or more network packets to a queue and communicating the one or more network packets via a network stack of the client; and

- an agent for determining the one or more network packets is associated with a first application of the client, and indicating to the network driver a priority of the one or more network packets to place the determined one or more network packets ahead of at least one network packet in the queue associated with a second application of the client.

133. The client of claim 132, wherein the agent determines the one or more network packets of the first application comprises real-time data.

134. The client of claim 132, wherein the real-time data comprises one of the following: a real-time protocol, a user datagram protocol, and a representation of one of voice or audio.

135. The client of claim 132, wherein one of the agent or the network driver prevents at least one network packet of the second application from being communicated via the network stack ahead of the one or more network packets of the first application.

136. The client of claim 132, wherein the network driver holds in the queue a network packet associated with the second application, and releasing the held network packet upon communication of the one or more network packets associated with the first application prioritized ahead of the held network packet.

137. The client of claim 132, wherein the mechanism intercepts the one or more network packets transparently to the one or more applications on the client.

138. The client of claim 132, wherein the first application is running in the foreground, and the second application is running in the background.

139. The client of claim 132, wherein the first application has a priority higher than the second application of the client.

140. The client of claim 132, comprising a configuration mechanism for a user to specify the priority.

141. The client of claim 132, wherein the client receives the one or more network packets from a computing device.

142. The client of claim 132, wherein the one or more applications provides the one or more network packets for communicating from the client to a computing device.

143. The client of claim 132, wherein the network driver comprises a Network Driver Interface Specification (NDIS) driver.

144. The client of claim 132, wherein the network driver operates in kernel-mode of an operating system of the client.

145. The client of claim 132, wherein the agent operates in user-mode of an operating system of the client.

146. The client of claim 132, wherein one of the agent or the network driver comprises the mechanism for intercepting one or more network packets of the client.

147. A method for shielding from a network disruption a session established via a first protocol, the method comprising the steps of:

(a) establishing, via an agent of a client, a session via a first protocol over a network connection between the client and a device, the network connection associated with a network stack, a first portion of the network stack comprises one or more layers of the network stack below the layer of the first protocol, and a second portion of the network stack comprises a layer for the first protocol and one or more layers of the network stack above the first protocol;

(b) detecting a disruption in the network connection causing the first portion of the network stack to be disestablished;

(c) maintaining, by the agent, the session and the second portion of the network stack during the disruption; and

(d) re-establishing the second portion of the network stack and the network connection while maintaining the session and the second portion of the network stack.

148. The method of claim 147, comprising the step of:

(e) continuing the session with the maintained second portion of the network stack and the re-established first portion of the network stack.

149. The method of claim 147, comprising the step of

(e) dropping, by the second portion of the network stack, any network packets received
during the disruption.

150. The method of claim 147, wherein the device comprises one of a remote access gateway or a computing device.

151. The method of claim 147, further comprising establishing the session via the first protocol of one of the following: secure socket layer (SSL) protocol, a transport layer security (TLS) protocol, and a tunneling protocol.

152. The method of claim 147, comprising communicating, by the agent, real-time data via the session between the client and the device.
153. The method of claim 152, wherein the real-time data comprises a real-time protocol.
154. The method of claim 152, wherein the real-time data comprises a representation of one of voice or audio.
155. The method of claim 147, comprising operating the agent in user-mode of an operating system of the client.
156. The method of claim 147, wherein the first portion of the network comprises one of a transport control protocol or an internet protocol.
157. The method of claim 147, wherein the second portion of the network stack comprises one of an internet protocol, a user datagram protocol, or a voice over internet protocol.
158. The method of claim 147, comprising the client communicating with the device via a remote display protocol.
159. The method of claim 158, wherein the remote display protocol comprises one of an Independent Computing Architecture protocol or a Remote Desktop protocol.
160. The method of claim 147, comprising performing one of steps (b), (c) and (d) transparently to an application of the client communicating via the network connection.
161. The method of claim 147, comprising intercepting, by the agent, transparently to an application of the client one or more network packets associated with the application.
162. The method of claim 147, comprising intercepting, by a network driver

associated with the second portion of the stack, transparently to the application on the client one or more network packets associated with the application.

163. A system for shielding from a network disruption a session established via a first protocol, the system comprising

an agent of a client establishing a session between the client and a device over a network connection via a first protocol;

a network stack having a first portion and a second portion, the first portion of the network stack comprising one or more layers of the network stack below the layer of the first protocol, and the second portion of the network stack comprising a layer for the first protocol and one or more layers of the network stack above the first protocol; and

a detector for detecting a disruption in the network connection causing the second portion of the network stack to be disestablished;

wherein:

upon detection of the disruption by the detector, the agent maintains the session and the second portion of the network stack during the disruption; and

the client re-establishes the first portion of the network stack and the network connection while the agent maintains the session and the second portion of the network stack.

164. The system of claim 163, wherein the agent continues the session with the maintained second portion of the network stack and the re-established first portion of the network stack.

165. The system of claim 163, wherein one of the first portion or the second portion of the network stack drops any network packets received during the disruption.

166. The system of claim 163, wherein the device comprises one of a remote access gateway or a computing device.

167. The system of claim 163, wherein the first protocol comprises one of the following: secure socket layer (SSL) protocol, a transport layer security (TLS) protocol, and a tunneling protocol.

168. The system of claim 163, wherein the agent communicates real-time data via the session between the client and the device.

169. The system of claim 168, wherein the real-time data comprises one of a real-time protocol.

170. The system of claim 168, wherein the real-time data comprises a representation of one of voice or audio.

171. The system of claim 163, wherein the agent operates in user-mode of an operating system of the client.

172. The system of claim 163, wherein the first portion of the network stack comprises one of a transport control protocol or an internet protocol.

173. The system of claim 163, wherein the second portion of the network stack comprises one of an internet protocol, a user datagram protocol, or a voice over internet protocol.

174. The system of claim 163, wherein the first protocol comprises a remote display protocol.

175. The system of claim 174, wherein the remote display protocol comprises one of an Independent Computing Architecture protocol or a Remote Desktop protocol.

176. The system of claim 163, wherein the agent intercepts one or more network packets of an application of the client transparently to the application.

177. The system of claim 163, comprising a network driver associated with the second portion of the network stack, the network driver intercepts one or more network packets of an application of the client transparently to the application, and provides the one or more packets to the agent to communicate via the session.

178. The system of claim 177, wherein the network driver comprises a Network Driver Interface Specification (NDIS) driver.

179. The system of claim 177, wherein the network driver operates in kernel-mode of an operating system of the client.

1/15

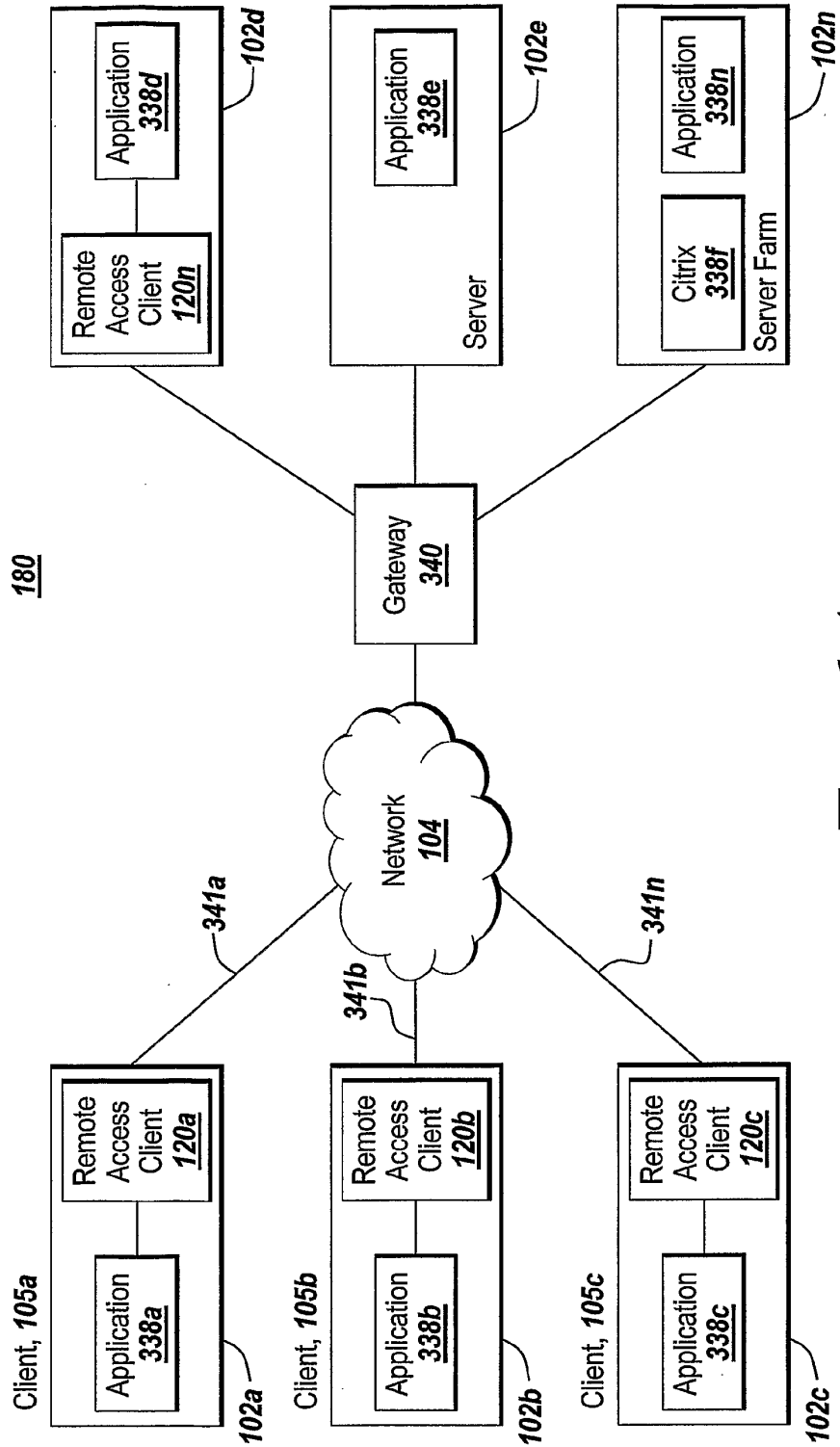
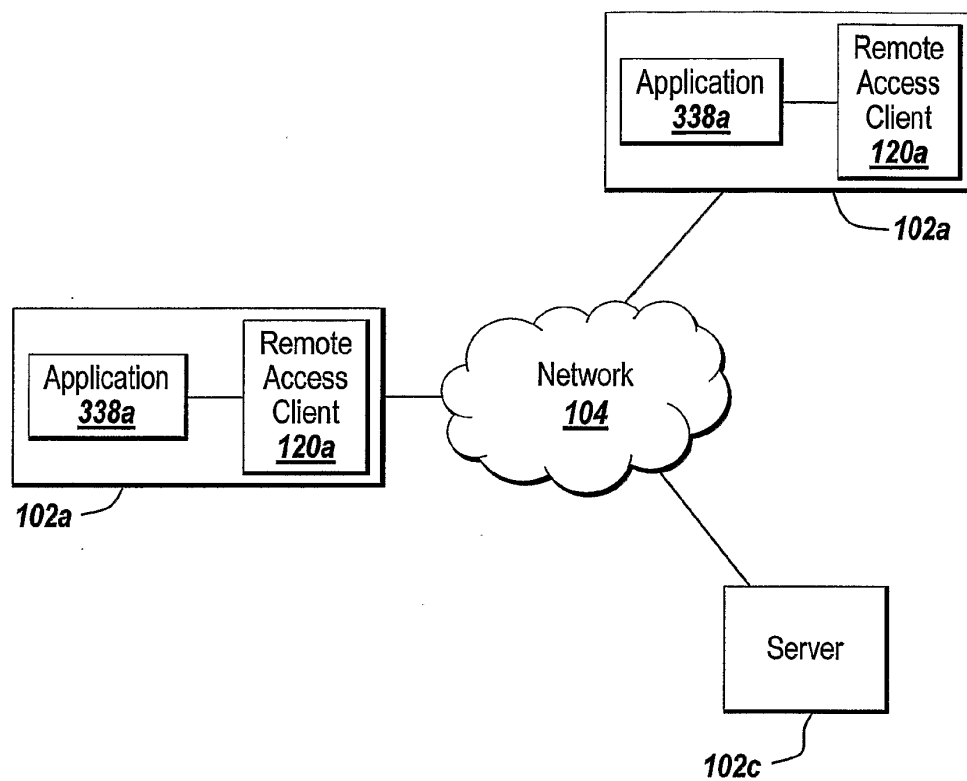
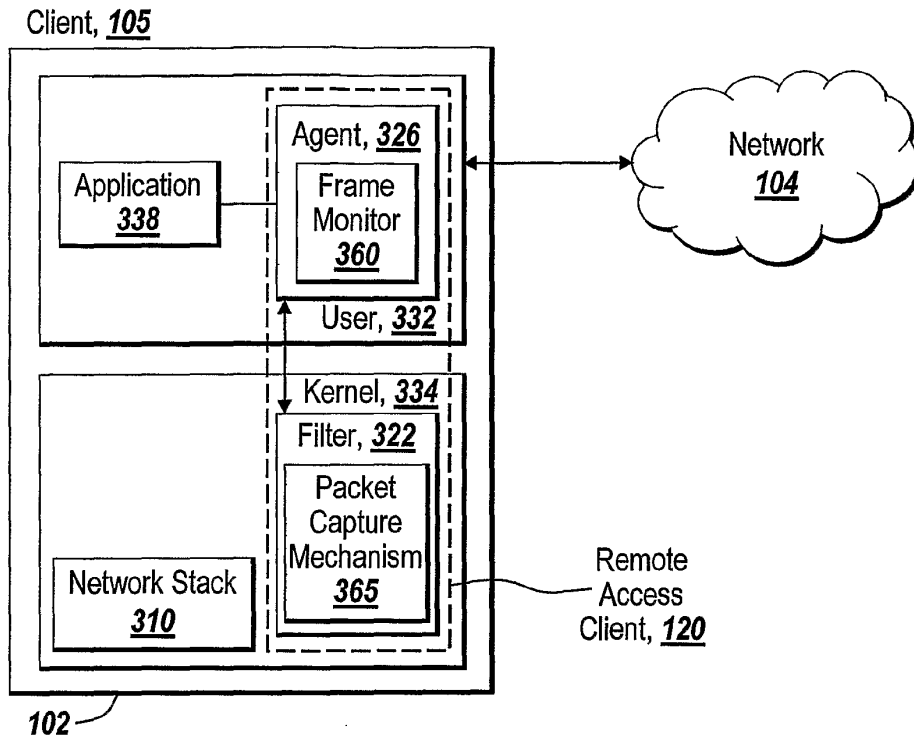


Fig. 1A

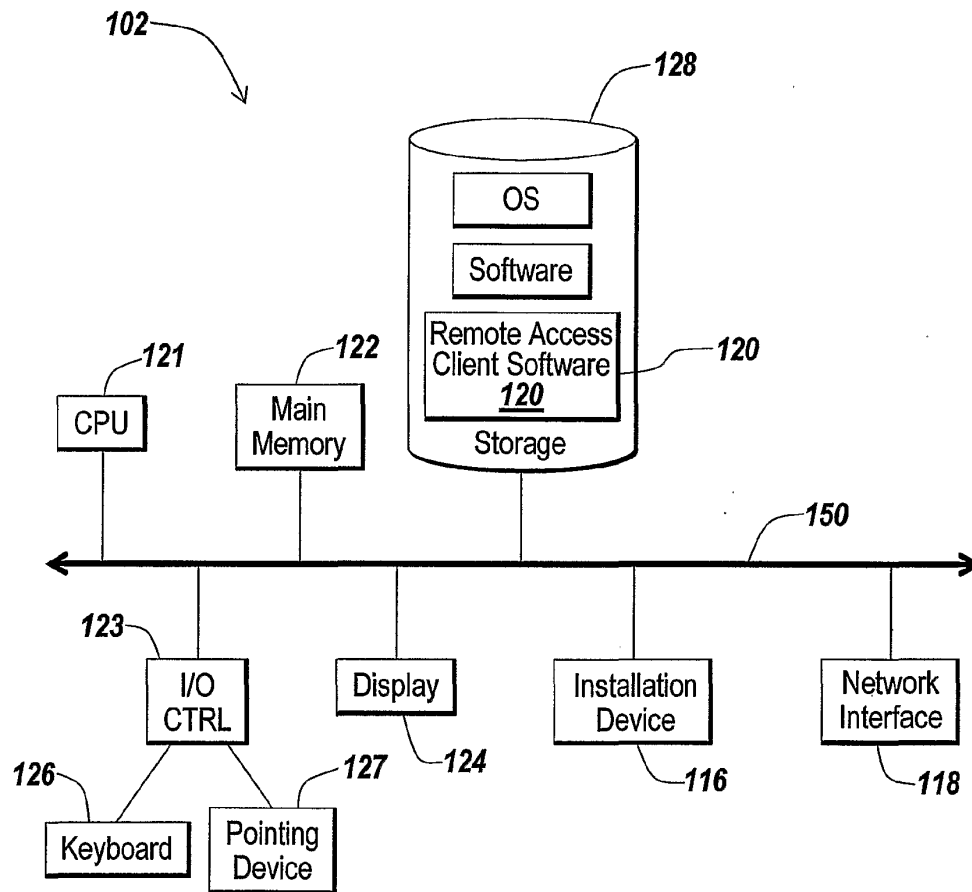
2/15

*Fig. 1B*

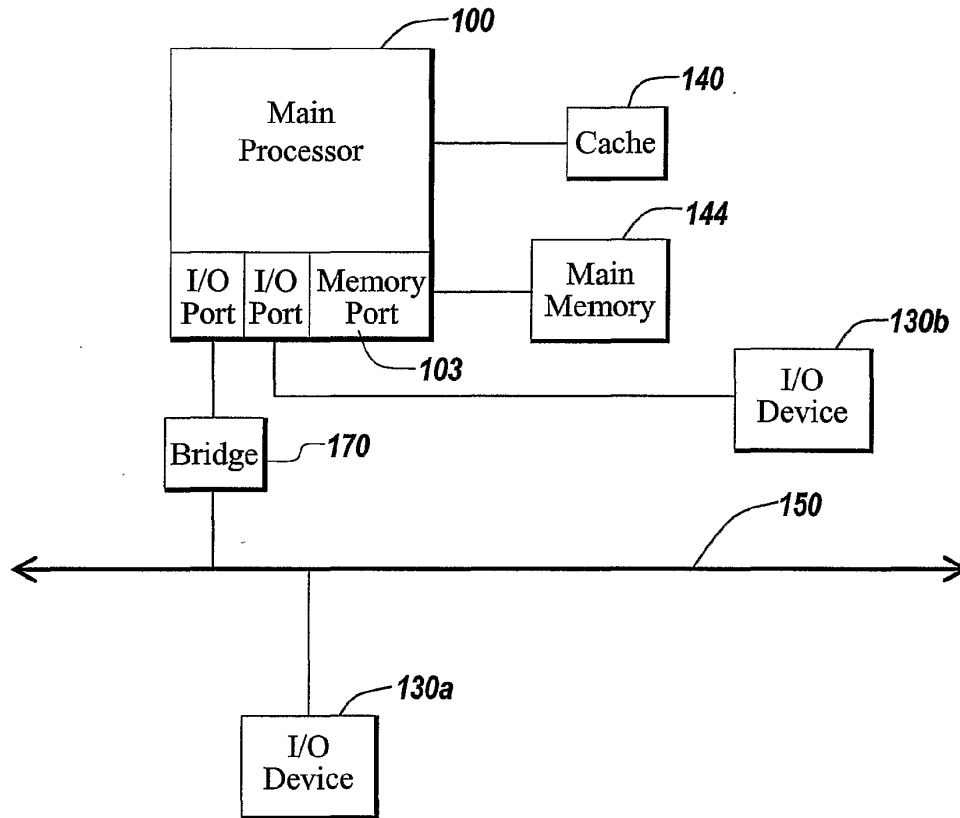
3/15

*Fig. 1C*

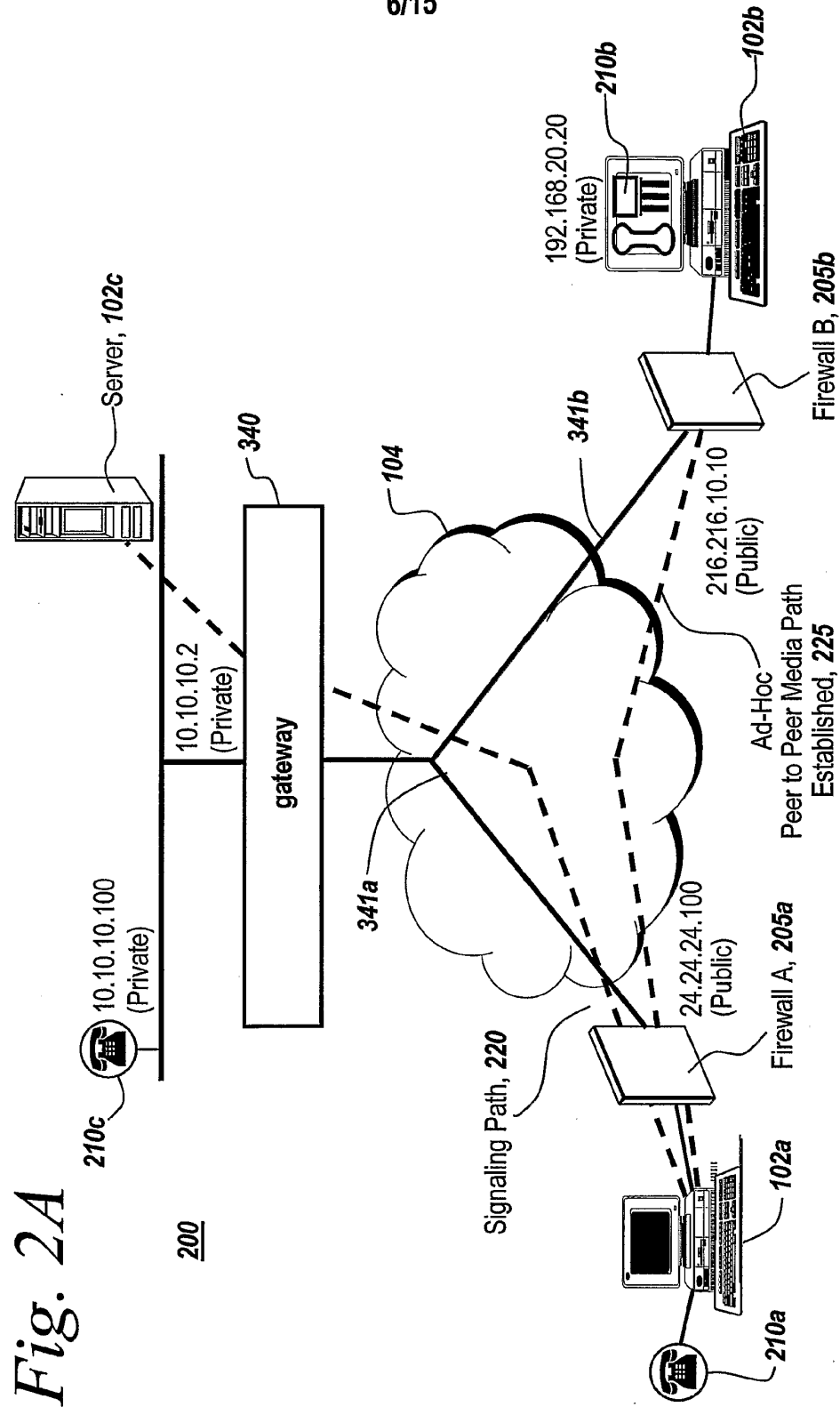
4/15

*Fig. 1D*

5/15

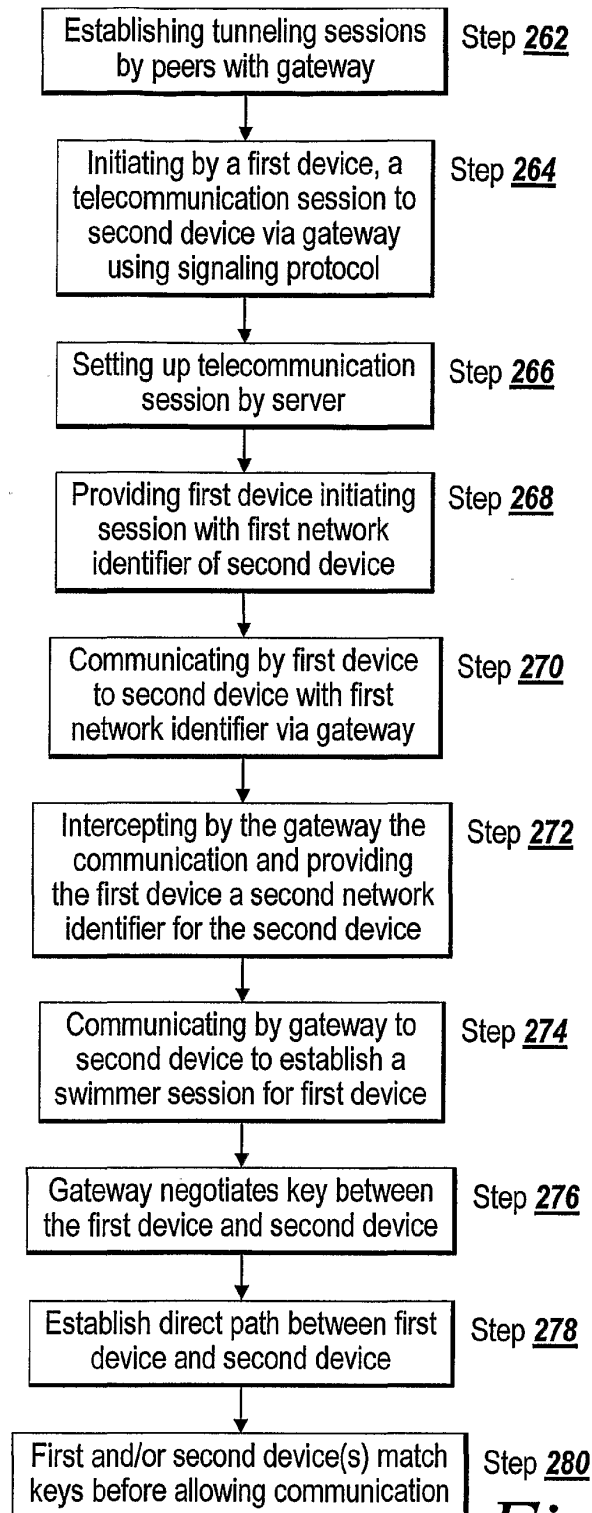
*Fig. 1E*

6/15



260

7/15

*Fig. 2B*

8/15

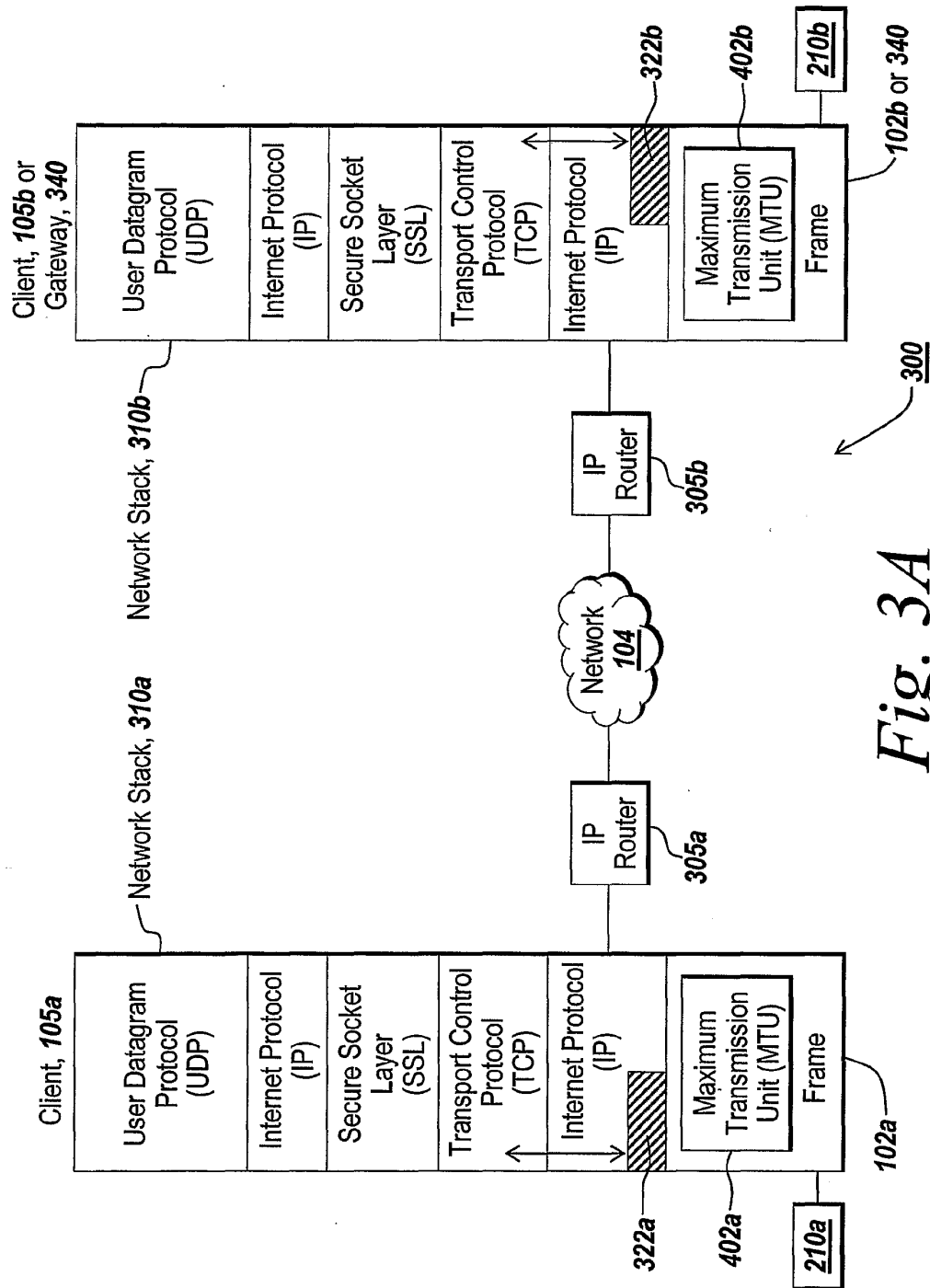
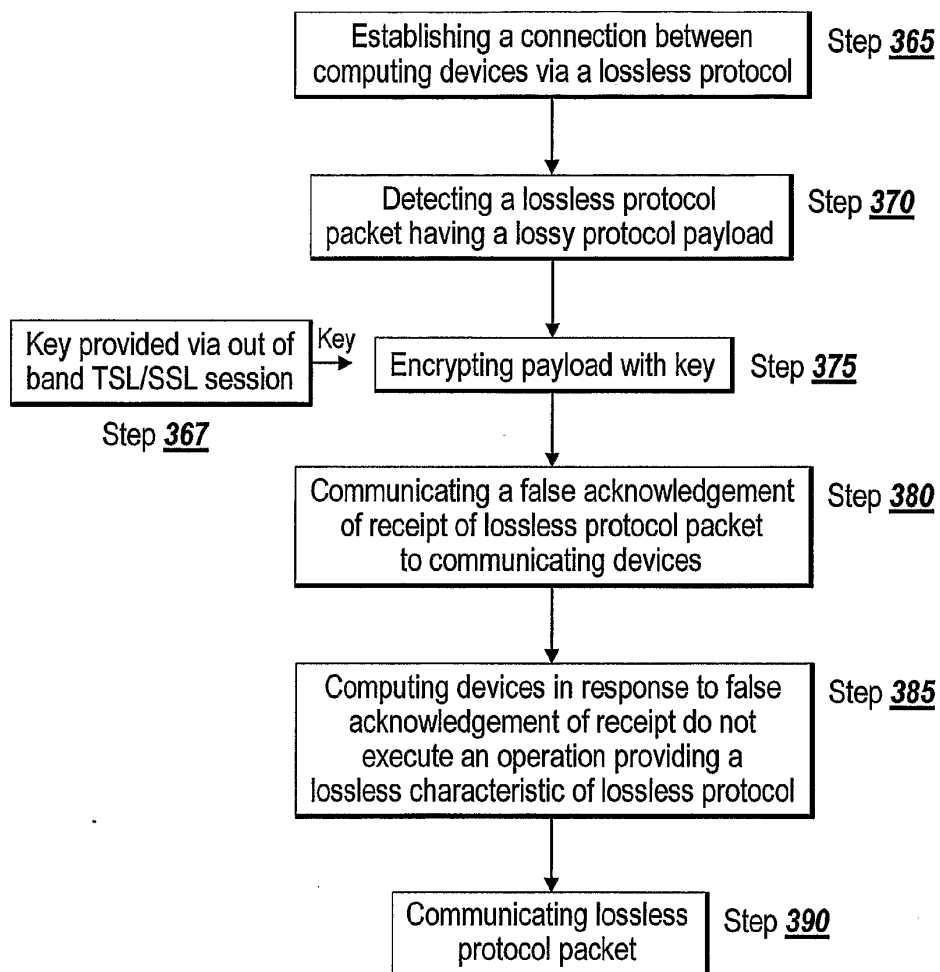
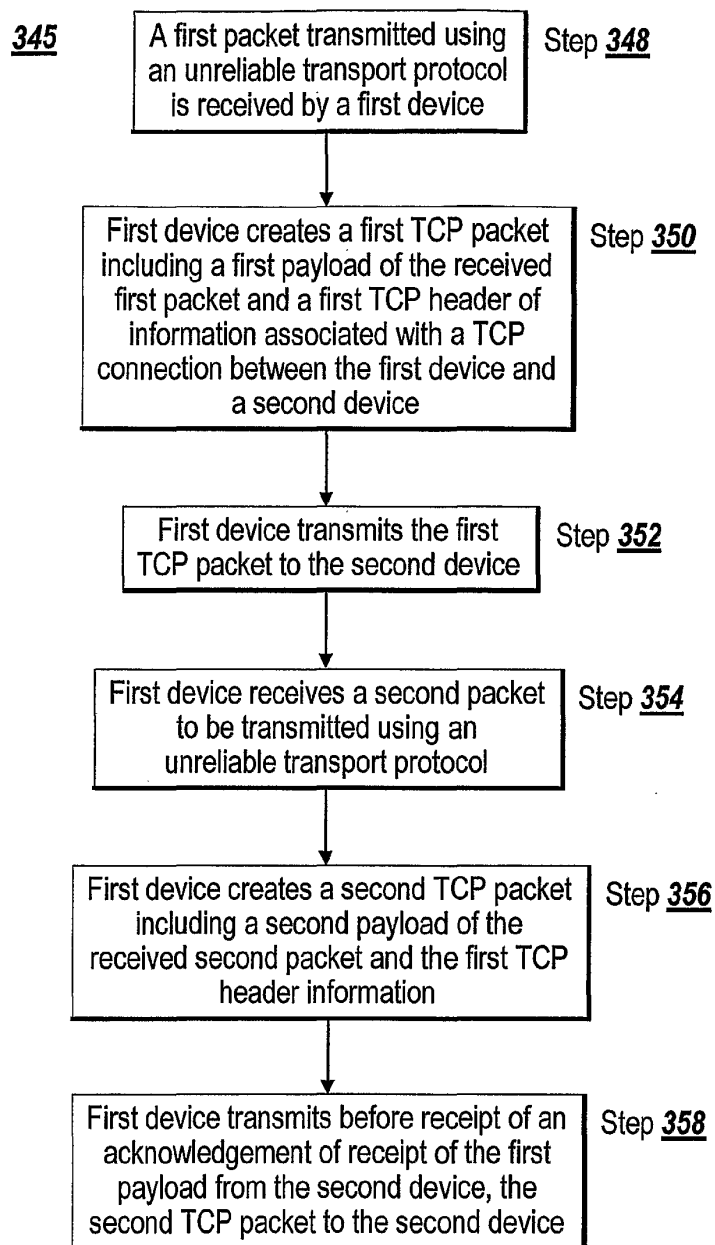


Fig. 3A

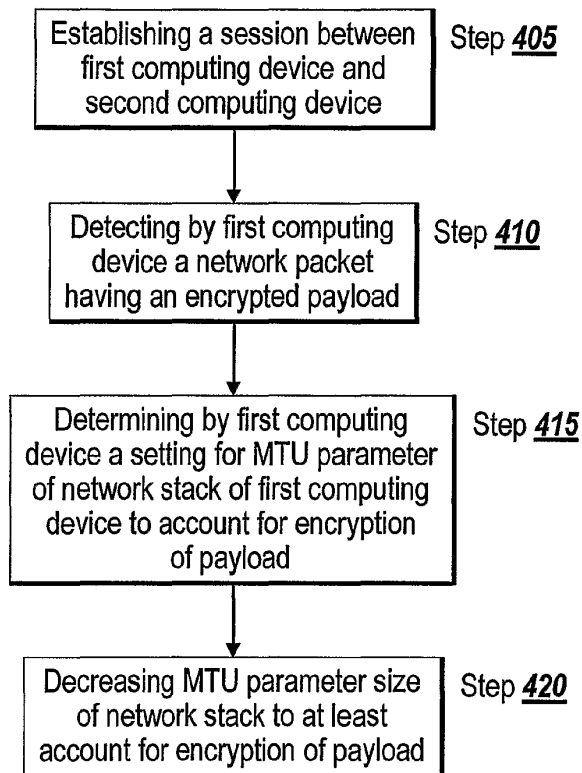
9/15

*Fig. 3B*

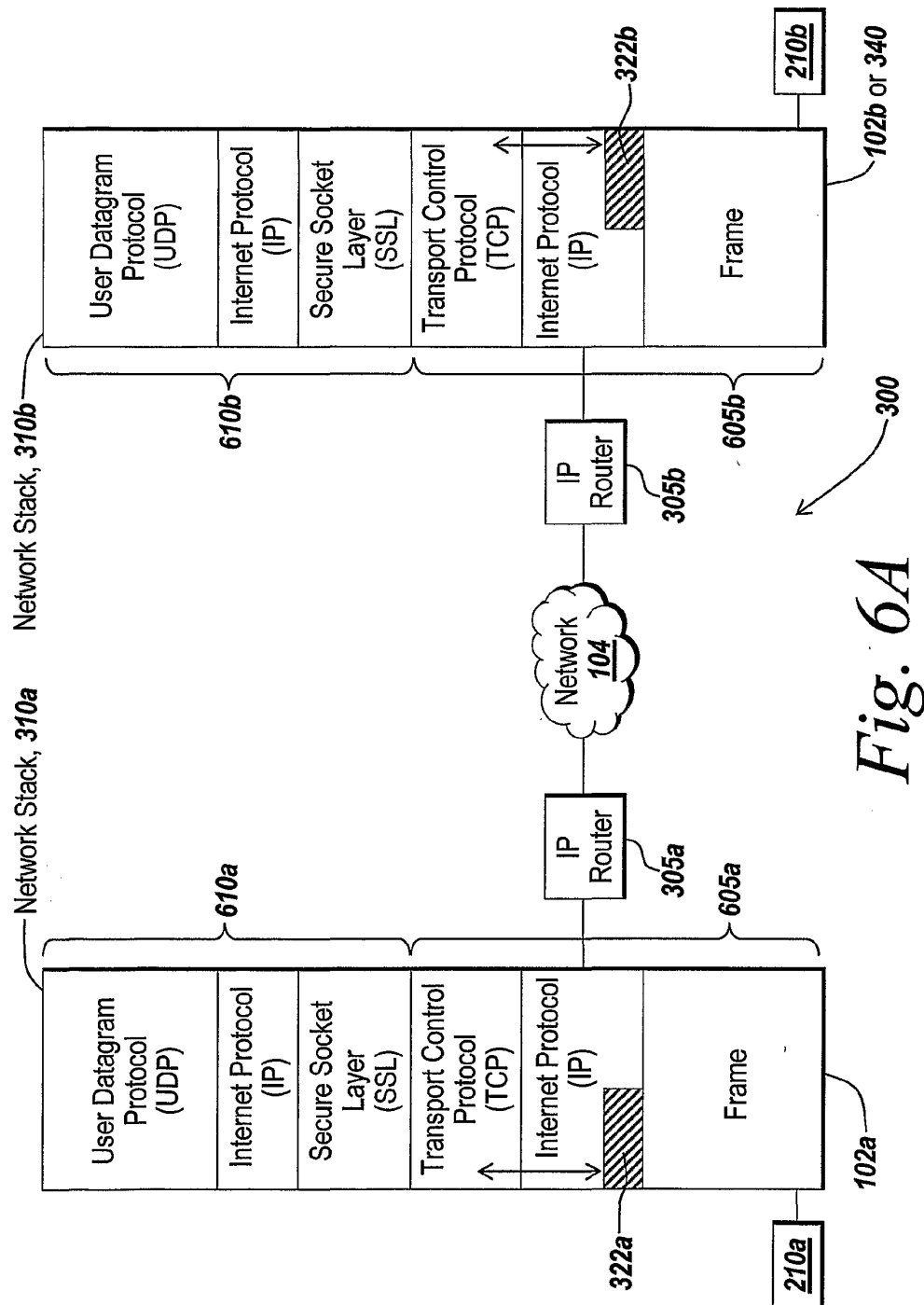
10/15

*Fig. 3C*

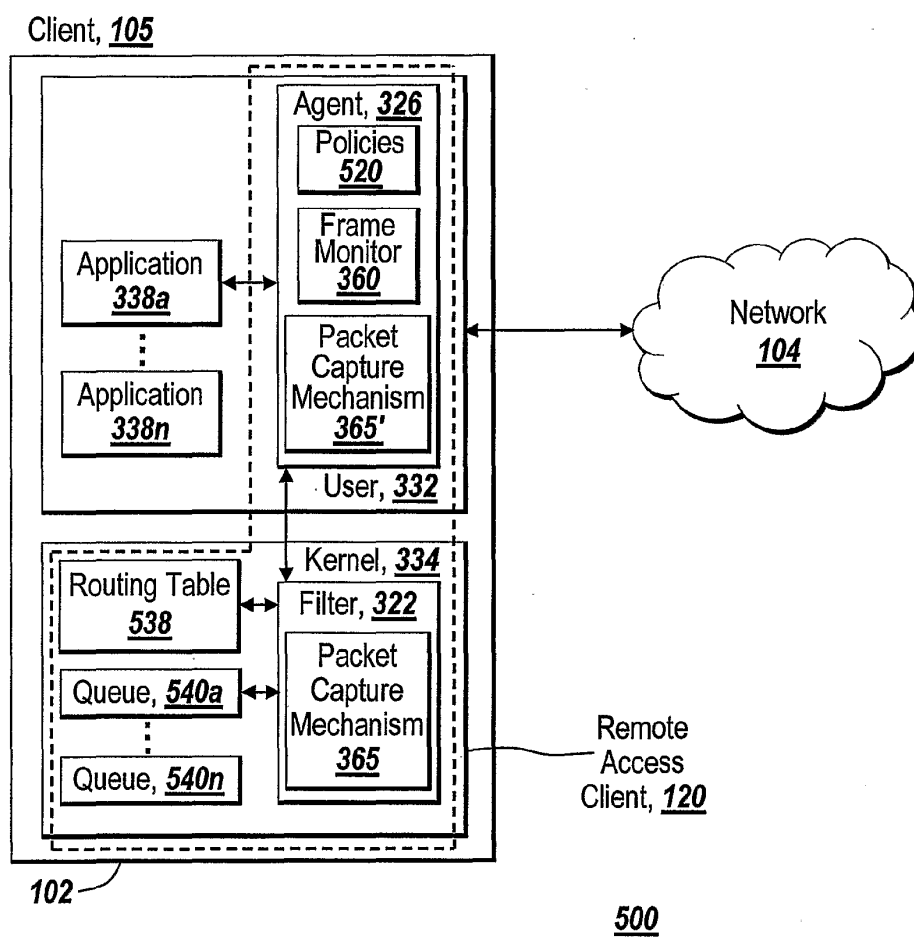
11/15

400*Fig. 4*

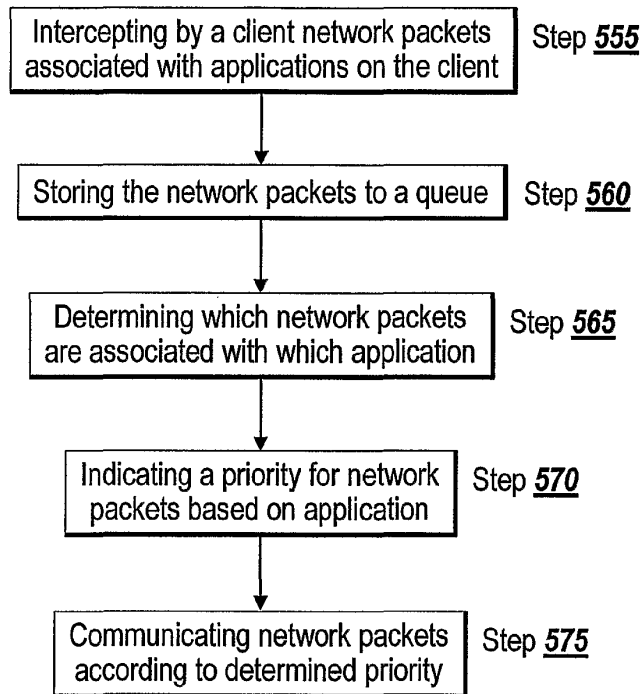
12/15

*Fig. 6A*

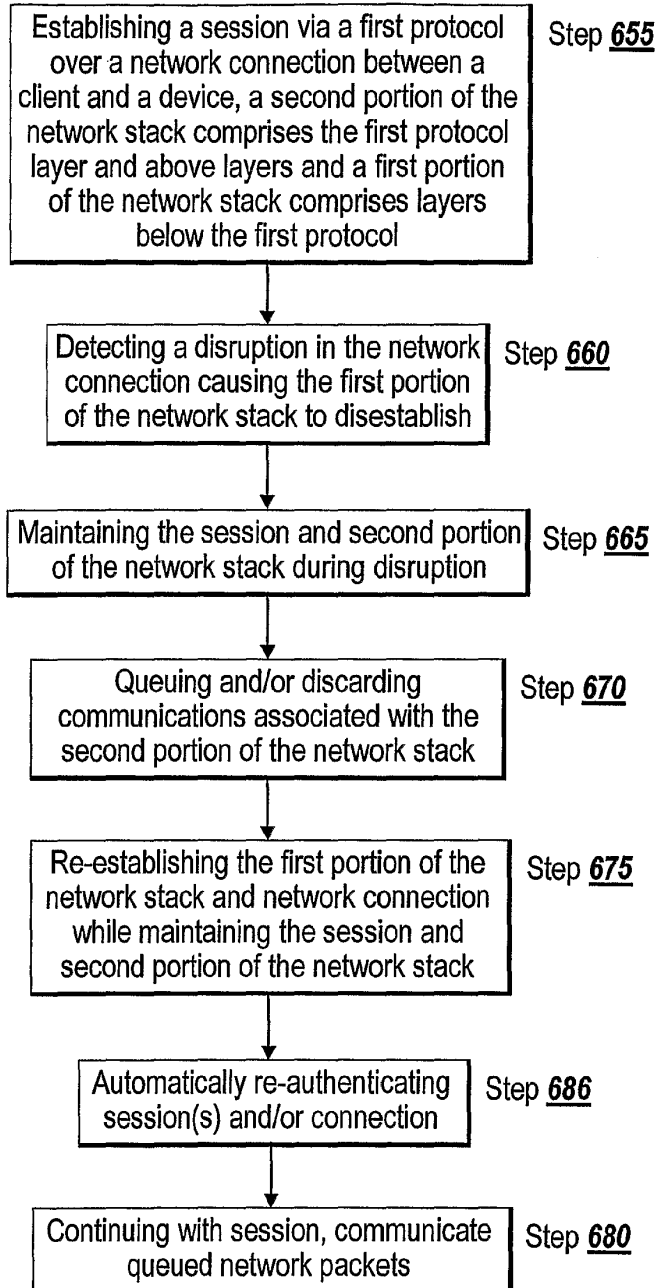
13/15

*Fig. 5A*

14/15

550*Fig. 5B*

15/15

650*Fig. 6B*

[19] 中华人民共和国国家知识产权局

[51] Int. Cl⁷
G06F 17/60



[12] 发明专利申请公开说明书

[21] 申请号 02156671.2

[43] 公开日 2004 年 6 月 30 日

[11] 公开号 CN 1508734A

[22] 申请日 2002.12.13 [21] 申请号 02156671.2

[71] 申请人 华人创意股份有限公司

地址 台湾省台北市

[72] 发明人 温世仁 吴鸿祺

[74] 专利代理机构 北京三幸商标专利事务所

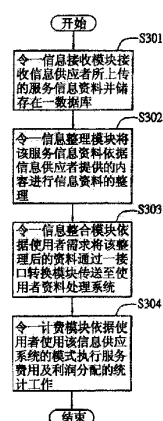
代理人 刘激扬

权利要求书 3 页 说明书 10 页 附图 3 页

[54] 发明名称 用以支持中小企业营运发展的信息
供应方法以及系统

[57] 摘要

一种用以支持中小企业营运发展的信息供应方法以及系统，令一信息接收模块接收信息供应者上传的服务信息资料并储存在数据库中；令一信息整理模块将该服务信息资料依据信息供应者提供的内容进行相关资料的整理；令一信息整合模块依据使用者输入的需求将该整理后且符合该需求的资料，通过一接口转换模块传送至使用者数据处理系统；最后，令一计费模块依据使用者使用系统的模式，执行服务费用的统计工作。通过该使用本发明，能够提供个人工作室、住家办公室及中小企业的经营者及其从业人员使用者通过单一网站即可获得所需的信息服务。



ISSN 1008-4274

1. 一种用以支持中小企业营运发展的信息供应方法，用以提供使用者借由一数据处理系统通过一网络通讯系统取得所需要的信息服务，其特征在于，该用以支持中小企业营运发展的信息供应方法包括：

5 令一信息接收模块接收信息供应者上传的服务信息资料并储存在一数据库中；

令一信息整理模块将该服务信息资料依据信息供应者所提供的内容进行信息资料的整理；

10 令一信息整合模块依据使用者所输入的需求，将该整理后且符合该需求的资料通过一接口转换模块传送至使用者数据处理系统；以及

令一计费模块依据使用者使用该用以支持中小企业营运发展的信息供应系统的模式，执行服务费用的统计与利润分配工作。

2. 如权利要求1所述的方法，其特征在于，该信息供应者上传的服务信息资料可以是文字资料、图像数据、声音资料、影像资料、以
15 超级链接方式所提供的网络协议地址及统一资源寻址器地址资料其中的一种。

3. 如权利要求1所述的方法，其特征在于，该信息供应者上传的服务信息资料可以是商业情报、商业机会、专业服务、专业规划、业务连接、行政程序及增值服务中的一种。
20

4. 如权利要求1所述的方法，其特征在于，该信息资料的整理步骤还包括将同一信息供应者及不同信息供应者其中任一者提供的相同、相似及不同信息的其中任一种信息，加以分类、归纳及结合的数据处理过程。

25 5. 如权利要求1所述的方法，其特征在于，该信息整合形式可以是数据库信息的搜寻、信息服务提供者网络资源的连接及提供线上实时的信息请求与响应中的任一种。

6. 如权利要求1所述的方法，其特征在于，该接口转换模块转换的通讯协议可以是国际互联网协议及无线应用软件协议中的任一种。

30 7. 如权利要求1所述的方法，其特征在于，使用该用以支持中小企业营运发展的信息供应系统的模式可以是使用者连接该网站的层次、连接的时间及信息服务的内容中的任一种。

8. 如权利要求1所述的方法，其特征在于，该数据处理系统可以是服务器、工作站、个人计算机、笔记本型计算机、掌上型计算机、

个人数字助理以及移动电话中的任一种。

9. 如权利要求 1 所述的方法, 其特征在于, 该网络通讯系统可以是国际互联网、企业内部互联网以及企业间互联网中的任一种。

10. 如权利要求 1 所述的方法, 其特征在于, 该网络通讯系统可以是
5 是有线通讯系统以及无线通讯系统中的任一种。

11. 如权利要求 1 所述的方法, 其特征在于, 该数据库是一关系型数据库。

12. 如权利要求 1 所述的方法, 其特征在于, 该信息接收模块、
信息整理模块、信息整合模块、接口转换模块及计费模块是一软件程
10 序。

13. 如权利要求 1 所述的方法, 其特征在于, 该使用者可以是个人工作室、住家办公室及中小企业的经营者及其从业人员中的任一种。

14. 一种用以支持中小企业营运发展的信息供应系统, 用以提供
使用者借由一数据处理系统通过一网络通讯系统取得所需要的信息服
15 务, 其特征在于, 该用以支持中小企业营运发展的信息供应系统包括:

一数据库, 用以储存至少包括信息提供者所提供的信息、信息整理的相关资料、信息需求者的信息资料、信息需求者及信息供应者间
信息服务整合的资料以及服务费用资料;

一信息接收模块, 用以接收信息提供者通过网络通讯系统提供的
20 信息;

一信息整理模块, 用以整合该信息接收模块接收该信息提供者所提供的信息内容;

一信息整合模块, 用以将该信息整理模块所整理的信息与使用者所提出的信息需求作一连接互通;

25 一接口转换模块, 用以依据不同的客户端数据处理系统提供符合该系统的资料传送、存取的规格; 以及

一计费模块, 用以依据使用者使用资源服务的模式计算其所需支付的服务费用, 以及信息供应者与用以支持中小企业营运发展的信息供应系统管理者的利润分配。

30 15. 如权利要求 14 所述的系统, 其特征在于, 该信息供应者提供的信息可以是文字资料、图像数据、声音资料、影像资料、以超级链接方式提供的网络协议地址及统一资源寻址器地址资料中的任一种。

16. 如权利要求 14 所述的系统, 其特征在于, 该信息供应者上传的服务信息资料可以是商业情报、商业机会、专业服务、专业规划、
35 业务连接、行政程序及增值服务中的任一种。

17. 如权利要求 14 所述的系统, 其特征在于, 该信息整理模块是将同一信息供应者及不同信息供应者中任一者提供的相同、相似及不同的信息中的任一种信息, 加以分类、归纳及结合的数据处理过程。

18. 如权利要求 14 所述的系统, 其特征在于, 该信息整合模块的
5 整合形式可以是数据库信息的搜寻、信息服务者网络资源的连接及提供线上实时的信息请求与响应中的任一种。

19. 如权利要求 14 所述的系统, 其特征在于, 该接口转换模块转换的通讯协议可以是国际互联网协议及无线应用软件协议中的任一种。

10 20. 如权利要求 14 所述的系统, 其特征在于, 使用该用以支持中小企业营运发展的信息供应系统的模式可以是使用者连接该网站的层次、连接的时间及信息服务的内容中的任一种。

21. 如权利要求 14 所述的系统, 其特征在于, 该数据处理系统可以是服务器、工作站、个人计算机、笔记本型计算机、掌上型计算机、
15 个人数字助理以及移动电话中的任一种。

22. 如权利要求 14 所述的系统, 其特征在于, 该网络通讯系统可以是国际互联网、企业内部互联网以及企业间互联网中的任一种。

23. 如权利要求 14 所述的系统, 其特征在于, 该网络通讯系统可以是有线通讯系统以及无线通讯系统中的任一种。

20 24. 如权利要求 14 所述的系统, 其特征在于, 该数据库是一关系型数据库。

25. 如权利要求 14 所述的系统, 其特征在于, 该信息接收模块、信息整理模块、信息整合模块、接口转换模块及计费模块是一软件程序。

25 26. 如权利要求 14 所述的系统, 其特征在于, 该使用者可以是个人工作室、住家办公室及中小企业的经营者及其从业人员中的任一种。

用以支持中小企业营运发展的信息供应方法以及系统

5 技术领域

本发明是关于一种用以支持中小企业营运发展的信息供应方法以及系统，特别是关于一种整合信息以提供使用者通过单一网站获取该整合信息的信息供应方法与系统。

10 背景技术

随着电子信息科技的蓬勃发展，诸如个人计算机、笔记本型计算机、平板计算机、掌上型计算机、个人数字助理乃至移动电话等具有数据处理功能的电子装置或系统，其在功能上愈来愈强大，除单纯进行数据处理外，这些设备已经能够提供使用者上网浏览、信息的上传
15 或下载、听音乐、编辑、播放影像信息等多元化的多媒体服务，来获取所需要的信息。另一方面由于有线及无线网络通讯技术的日益成熟，再加上这些电子装置或系统的体积愈来愈轻薄短小，便于使用者在行动中进行信息的取得。基于上述种种客观环境，使用者主观上也更乐意通过该具有网络连接与数据传输功能的电子装置或系统进行信息的
20 搜寻及取得。

但是当愈来愈多的使用者不再通过报纸、杂志，甚至广播电视等传统的媒体来取得信息，而是选择通过具有实时性的网络通讯系统来取得所需的信息时，网络信息供应商势必要考虑如何能够充分利用网络通讯系统的特性，提供有别于传统媒体所能够提供的信息。

25 现有通过网络通讯系统提供使用者信息的方法不一般是以下方法：由使用者通过浏览器联接门户网站，输入要搜寻信息的关键词等搜寻条件，通过该门户网站提供的搜寻引擎进行与该关键词相符及/或近似的网页资料，由使用者通过输入网址或借由超级链接的方式与该网址进行联接，通过浏览器进行资料的浏览或传输。

30 这种现有的信息搜寻方法，对于缺乏网络搜寻经验或是搜寻条件等相关信息不是十分充分的使用者而言，信息的寻找、取得有时就如同大海捞针。此外，若使用者要同时搜寻许多具有实质关联性、却不具有形式关联性的网站时，上述的搜寻方式恐怕无法有效解决使用者的需要。此时，使用者仍须通过一次次的搜寻才有可能找到所需要的

信息。即令使用者已经搜寻到所有的相关信息，但若缺乏有效率的资料筛选，则所搜集到的信息对于使用者而言不但无法有效的解决自身的需要，有时反而会成为庞大的负担。

另一方面，使用者在通过付费网站获取信息方面，通常所采用的方法有固定费率制，也就是缴纳一定的费用取得在一定期间内无限次的使用权；储值制，也就是购买一定的点数，再从所使用的信息对应的点数中加以扣除。除上述两种以外，再一种方法就是依据服务提供商所开列的价格，通过信用卡或转帐的方式支付费用。上述服务费用的支付方法均是依据固定的服务价目表收费，并不能够将使用者登录或连接的等级、范围甚或是服务内容作为服务费率调整的依据。

综上所述，如何能够为使用者提供一套具有整合多元信息、并能够更合理地保证信息服务提供商与信息需求方利益的方法，是亟需解决的问题。

15 发明内容

为克服现有技术的缺点，本发明的主要目的在于提供一种用以支持中小企业营运发展的信息供应方法以及系统，它能够提供一信息供应网站，让信息供应者通过该信息供应网站提供信息服务。

本发明的另一目的在于提供一种用以支持中小企业营运发展的信息供应方法以及系统，它能够对信息供应者提供的信息进行有效的整合，提高使用者查找所需信息的效率。

本发明的又一目的在于提供一种用以支持中小企业营运发展的信息供应方法以及系统，它能够提供使用者通过一信息服务整合的机制与信息供应者进行信息服务的交易。

25 本发明的再一目的在于提供一种用以支持中小企业营运发展的信息供应方法以及系统，它能够提供一计费机制，让信息供应者依据使用者使用信息服务的模式，进行服务费用的计算。

本发明的又再一目的在于提供一种用以支持中小企业营运发展的信息供应方法以及系统，它能够提供一接口转换机制，用以提供客户端的使用者可以借由不同类型的数据处理系统通过本发明获得信息服务。

为达成上述目的，本发明之用以支持中小企业营运发展的信息供应系统包括：一数据库，用以储存至少包括信息提供者所提供的信息、信息整理的相关资料、信息需求者的信息资料、信息需求者及信息供应者间信息服务整合的资料以及服务费用资料；一信息接收模块，用

以接收信息提供者通过网络通讯系统提供的信息；一信息整理模块，用以整合该信息接收模块接收该信息提供者所提供的信息内容；一信息整合模块，用以将该信息整理模块所整理的信息与使用者所提出的信息需求作一连接互通；一接口转换模块，用以依据不同的客户端数据

5 数据处理系统提供符合该系统的资料传送、存取的规格；以及一计费模块，用以依据使用者使用资源服务的模式计算其所需支付的服务费用，以及信息供应者与用以支持中小企业营运发展的信息供应系统管理者的利润分配。

通过该用以支持中小企业营运发展的信息供应系统，进行信息供应的方法是：令一信息接收模块接收信息供应者上传的服务信息资料并储存在一数据库中；令一信息整理模块将该服务信息资料依据信息供应者所提供的内容进行信息资料的整理；令一信息整合模块依据使用者所输入的需求，将该整理后且符合该需求的资料通过一接口转换模块传送至使用者数据处理系统；以及令一计费模块依据使用者使用该用以支持中小企业营运发展的信息供应系统的模式，执行服务费用的统计与利润分配工作。

与传统的信息供应方法以及系统比较，本发明通过整合信息供应者提供的信息机制、信息服务整合的机制、计费机制及接口转换机制借由一信息供应网站以供信息供应者通过该信息供应网站提供信息服务，它能对信息供应者提供的信息进行有效的整合，提高使用者查找所需信息的效率；同时能够提供使用者通过一信息服务整合的机制与信息供应者进行信息服务的交易，它所提供一计费机制，让信息供应者依据使用者使用信息服务的模式，进行服务费用的计算及收取。本发明提供的接口转换机制，能够让客户端的使用者可以借由不同类型的数据处理系统通过本发明获得其所需的信息服务。

附图说明

图 1 为一应用架构方块示意图，用以显示本发明之用以支持中小企业营运发展的信息供应系统的应用架构：

图 2 为一系统架构方块示意图，用以显示本发明之用以支持中小

图 3 为流程图,用以显示本发明之用以支持中小企业营运发展的信息供应方法的流程步骤。

35 具体实施方式

实施例

在以下实施例中，本发明用以支持中小企业营运发展的信息供应方法以及系统中所提供的信息包括文字资料、图像数据、影音资料以及其它无法由人类通过感官直接辨识的电磁记录资料，实际上能够通过本发明的用以支持中小企业营运发展的信息供应方法以及系统提供信息供应服务的，均适用于本发明的用以支持中小企业营运发展的信息供应方法以及系统。

请参阅图 1，如图所示，在本实施例中，本发明的用以支持中小企业营运发展的信息供应系统 100，是应用在现有的主从架构网络通讯系统 200 中，又该用以支持中小企业营运发展的信息供应系统 100 是建构在该网络通讯系统 200 的伺服器端，用以提供具有网络连接功能的网络终端装置 300 及网络终端装置 400 的客户端使用者，借由一浏览器应用程序通过该网络通讯系统 200，与建构在该伺服器端的用以支持中小企业营运发展的信息供应系统 100 相互连接，进行包括程序或资料的上传或下载、资料储存及数据管理等工作。其中，该网络通讯系统 200 可以是一国际互联网(Internet)、企业内部互联网(Intranet)或企业间互联网(Extranet)；该网络终端装置 300 及网络终端装置 400 可以是个人计算机(PC)、笔记本型计算机(NB)、工作站(Workstation)或其它具有数据处理功能的装置或系统；该浏览器应用程序可以是微软的网络探险家(Internet Explorer)或是网景的领航员(Netscape Navigator)等。上述的主从架构网络通讯系统 200、该网络终端装置及该浏览器应用程序均为现有的软、硬件架构，故在此不重复说明。

请参阅图 2，它显示了本发明的用以支持中小企业营运发展的信息供应系统 100 的系统架构，如图所示，该用以支持中小企业营运发展的信息供应系统 100 搭配至一网络服务器 210，该网络服务器 210 是提供该用以支持中小企业营运发展的信息供应系统 100，通过该网络通讯系统 200 与网络终端装置 300 及网络终端装置 400 相互连接，并提供该网络终端装置 300 及网络终端装置 400 响应使用者的指令或其它需求以进行资料存取之用。在本实施例中，该网络终端装置 300 及网络终端装置 400，是利用各该网络终端装置上的网络浏览器应用程序，如上述的微软的 IE 或是网景的 Navigator，通过网络通讯系统 200 经由该网络服务器 210，与该用以支持中小企业营运发展的信息供应系统 100 相互连接，以进行档案管理相关的工作。需特别说明的是，该用以支持中小企业营运发展的信息供应系统 100 还可以与一防火墙(Firewall)系统联接(未图标)，用以保护该用以支持中小企业营运发展的信息供应

系统 100。该用以支持中小企业营运发展的信息供应系统 100 包括：一数据库 220、一信息接收模块 230、一信息整理模块 240、一信息整合模块 250、一接口转换模块 260 以及一计费模块 270。

该数据库 220 是用来储存至少包括信息提供者所提供的信息、信息整合的相关资料、信息需求者的信息资料、信息需求者及信息供应者之间信息服务整合的资料以及服务费用等资料表。在本实施例中，为增加资料查询及检索的效率，该数据库 220 可以是一关系型数据库。其中，该信息提供者所提供的信息资料表，用来储存至少包括信息提供者所提供的文字资料、图像数据、影音资料以及其它能够以储存在该数据库的任何形式的资料等数据区位；该信息整合的相关资料表，用以储存至少包括信息类别资料、信息内容相互关系资料以及信息整合资料等数据区位；该信息需求者的信息资料表，用以储存至少包括使用者基本身分、使用者使用信息的权限以及使用者使用资源的记录等数据区位；该信息需求者及信息供应者之间信息服务整合的资料表，用以储存至少包括有信息服务整合类别资料以及信息服务整合历史记录资料等数据区位；该服务费用资料表，则用以储存至少包括信息供应者的收费模式、信息供应者所提供的信息被使用的计量以及信息供应者与该用以支持中小企业营运发展的信息供应系统管理者之间利润分配基础等数据区位。

通过这种关系型数据库的建立，当使用者输入上述任一种资料时，该用以支持中小企业营运发展的信息供应系统 100 即可快速的寻找对其对应的资料。需特别说明的是，上述的各该数据区位及其所属的资料表仅为举例而已，在实际情况下，其内容应更为明确详细。此外，各该数据区位的内容也有可能包括有其它的数据区位或是资料表，只是由于篇幅所限，以及为陈述上的简洁，仅显示与本发明的用以支持中小企业营运发展的信息供应方法以及系统有关的部分资料。另一方面，该关系型数据库的系统架构也有多种，应视使用者的需要加以建构，故也不再重复说明。

该信息接收模块 230 是用来接收信息提供者通过网络通讯系统 200 所提供的信息。在本实施例中，信息提供者可以是顾问咨询服务、专业规划服务、生活增值服务、知识增值服务、业务连接服务，甚至包括法人组织或政府机关的行政单位或对外服务窗口等任何自然人或法人构成的信息提供主体。该信息提供者可借由该网络终端装置通过该网络通讯系统 200，将提供的信息服务内容上传至该网络服务器 210，该信息接收模块 230 随即将接收到的信息服务相关资料加以储存至该

数据库 220 中。

需特别说明的是，信息提供者与该用以支持中小企业营运发展的信息供应系统 100 的管理者之间应建立一资料传送的协议，如以特定的识别号码或文字定义的特定的信息种类，当该信息接收模块 230 接收到具有该识别号码或文字的信息相关资料时，则应依据该识别号码或文字将该相关信息储存至该数据库 220 中对应的信息资料储存字段。

该信息整理模块 240 是对该信息接收模块 230 接受该信息提供者提供的信息内容，按照一定的规则进行整理。在本实施例中，由于信息提供者所提供的信息内容包罗万象，内容可能包括各个领域不同层次的内容，可能是民间企业或是政府机关。但是通常一种业务的处理流程可能包括许多不同的信息供应者才能完成。如专利的申请，其流程可能包括寻找专业的专利事务所讨论专利申请的相关信息，委托其办理如专利说明书的撰写或专利申请程序的代办，当完成专利说明书的撰写后，还必须送交专利局进行专利审查，最后再经由相关的作业程序才能确定是否获得专利权。

该信息整理模块 240 能够将与专利申请相关的信息服务内容作一整理，当使用者欲搜寻与专利申请相关的信息服务时，即可获取一连串有用且相关的信息服务。在整理手段上，可以通过上述由信息供应者与用以支持中小企业营运发展的信息供应系统管理者之间的协议，借由特定的识别号码或文字加以分类，以将前阶段由民间专利事务所提供的服务，与后阶段由政府机关的专利局提供的行政程序服务等加以连接。也就是当信息供应者提供的信息通过该信息接收模块 230 储存至该数据库 220 时，该信息整理模块 240 能够将该特定相关的信息加以整理，并以特定的关键内容如“专利申请”等储存至该数据库 220 中的特定数据区位中，以供该用以支持中小企业营运发展的信息供应系统 100 进行资料的存取。

该信息整合模块 250 用来将该信息整理模块 240 所整理出的信息与使用者所提出的信息需求作一个连接互通。在本实施例中，当使用者借由网络终端装置通过该网络通讯系统 200，与建构有该用以支持中小企业营运发展的信息供应系统 100 的网站相互连接时，该网站会提供一信息服务相关的搜寻机制，如请求使用者输入使用者基本身分、使用者使用信息的权限等个人识别资料，以及特定的信息搜寻关键识别号码或文字等，通过该信息整合模块 250 的搜寻功能，即能够将信息需求者所需的信息服务与该用以支持中小企业营运发展的信息供应系统 100 中所能够提供的相关信息服务相互结合。其结合方式包括提

供使用者以超级链接的方式与该信息供应者相互连接、以提供如统一资源寻址器(URL)等网络资源的连接及/或提供如线上实时视频会议(Net-Meeting)等线上实时的信息请求及响应。

该接口转换模块 260 会依据不同客户端的网络终端装置提供符合该系统资料传送存取的资料规格。在本实施例中,该网络终端装置 300 及 400 并不限定为现有的个人计算机或笔记本型计算机,还可包括任何能够通过网络通讯系统 200 连接至架构有该用以支持中小企业营运发展的信息供应系统 100 网站的系统或装置,如移动电话所适用的无线应用软件协议(WAP)等其它网页浏览格式。该接口转换模块 260 是为使用不同资料浏览或存取协议的系统或装置提供转换接口,使其均可连接到架构有该用以支持中小企业营运发展的信息供应系统 100 的网站,供使用不同浏览或存取协议的网络终端装置进行信息的搜寻或接受信息供应者所提供各种形式的信息服务。

该计费模块 270 是用以依据使用者使用资源服务的模式,计算其所应支付的服务费用。在本实施例中,该计费模块 270 除了依据信息供应者或该用以支持中小企业营运发展的信息供应系统 100 的管理者所确定的信息服务价目表,计算使用者所使用的信息服务内容所应支付的总服务费用外。还能够依据使用者使用该用以支持中小企业营运发展的信息供应系统 100 的模式及其历史记录,作为计算服务费用的标准。以上述的“专利申请”流程为例,使用者自搜寻相关专利事务所或专利局的信息时,该计费模块 270 随即开始记录使用者使用该网站的使用时间、点选次数或下载档案的资料量等行为模式、并加以记录,若该使用者与其中一家具有专利代理经验的信息供应者相互联系,并且双方进行了如线上实时咨询等信息服务时,该计费模块 270 随即记录使用者与该信息供应者之间服务与被服务的信息,若使用者再通过该网站与专利局进行信息需求与供应的服务时,该计费模块 270 仍会记录他们之间的有关信息。通过上述追踪记录使用者的行为模式、并加以记录的方式,能够以依据使用者利用该网站的不同层次(Level)作为计算服务费用的标准。

请参阅图 3,它显示通过上述的用以支持中小企业营运发展的信息供应系统 100,在实施该用以支持中小企业营运发展的信息供应方法的步骤是。

在步骤 S301 中,令该信息接收模块 230 接收信息供应者上传的服务信息资料并储存在该数据库 220 中。通过该信息接收模块 230 能够接收资料供应者所传送的信息资料,以超级链接的方式所提供的网络

协议地址及 / 或统一资源寻址器地址等资料。

承前所述，该信息提供者与该用以支持中小企业营运发展的信息供应系统 100 的管理者之间得建立一资料传送的协议，如以特定的识别号码或文字定义特定的信息种类，当该信息接收模块 230 接收到具有该识别号码或文字的信息等相关资料时，则能够依据该识别号码或文字将该相关信息储存至该数据库 220 中对应的信息资料储存字段中。

在本实施例中，若一专利事务所欲通过该用以支持中小企业营运发展的信息供应系统 100 作为一专利信息供应者，则其能够借由网络终端装置通过该网络通讯系统 200，将其所能提供的信息资料传送至该网络服务器 210，其中该传送的资料包括文字或影像信息资料，以超级链接方式所提供的网络协议地址及 / 或统一资源寻址器地址等资料。此外，还包括特定的识别号码或文字，如“0001”与“专利服务”等，该信息接收模块 230 在该网络服务器 210 接收到上述的资料时，即将该资料储存至该数据库 220 中符合该识别号码“0001”与识别文字“专利服务”的数据区位中，接着进行步骤 S302。

在步骤 S302 中，令该信息整理模块 240 将该服务信息资料依据信息供应者所提供的内容进行相关资料的归纳、整理。其过程包括将同一信息供应者或不同信息供应者所提供的相同、相似或不同的信息加以分类、归纳或结合等。

承前所述，除该专利服务的信息供应者能够传送相关信息资料外，设架构有该用以支持中小企业营运发展的信息供应系统 100 的网站还能够与政府机关、如上述的专利局等相互合作，提供诸如线上专利申请或咨询等服务。由于一专利的申请流程可能需通过包括专利事务所与专利局等信息服务提供者的协助才能顺利完成。则该信息整理模块 240 则应将专利事务所及专利局所提供的信息服务作一信息归类，当使用者登录架构有该用以支持中小企业营运发展的信息供应系统 100 的网站，且欲请求该网站提供“专利申请”的信息服务时，则能够轻易的搜寻到上述经归纳后的该专利事务所及专利局所提供的信息服务，接着进行步骤 S303。

在步骤 S303 中，令一信息整合模块 250 依据使用者输入的需求，将该整理后且符合该需求的资料通过一接口转换模块 260 传送至客户端网络终端装置。其整合的模式包括数据库 220 信息的搜寻、信息服务提供者网络资源的连接及/或提供线上实时的信息请求及响应等。

承前所述，当有“专利服务”信息需求的使用者登录该网站后，该网站能够提供使用者一输入该使用者相关信息的功能，如要输入使

用者的基本身份、使用者使用信息的权限等个人识别资料，以及特定的信息搜寻关键识别号码或文字，如识别号码“0001”与识别文字“专利服务”等，通过该信息整合模块 250 的搜寻功能，即能够将信息需求者所需要的“专利服务”的相关信息服务，与该用以支持中小企业营运发展的信息供应系统 100 中所能够提供的、经整合后的该专利事务所及专利局所提供的信息服务相互结合。

在本实施例中，使用者进行数据库 220 中相关资料的搜寻、与该专利事务所进行网络视频会议及上述假设的专利局线上的专利申请作业流程等信息服务，接着进行步骤 S304。

10 在步骤 S304 中，令一计费模块 270 依据使用者使用该用以支持中小企业营运发展的信息供应系统 100 的模式，执行服务费用的统计工作。它是依据使用者使用信息的模式，计算所需支付的费用以及信息供应者之间的利润分配。

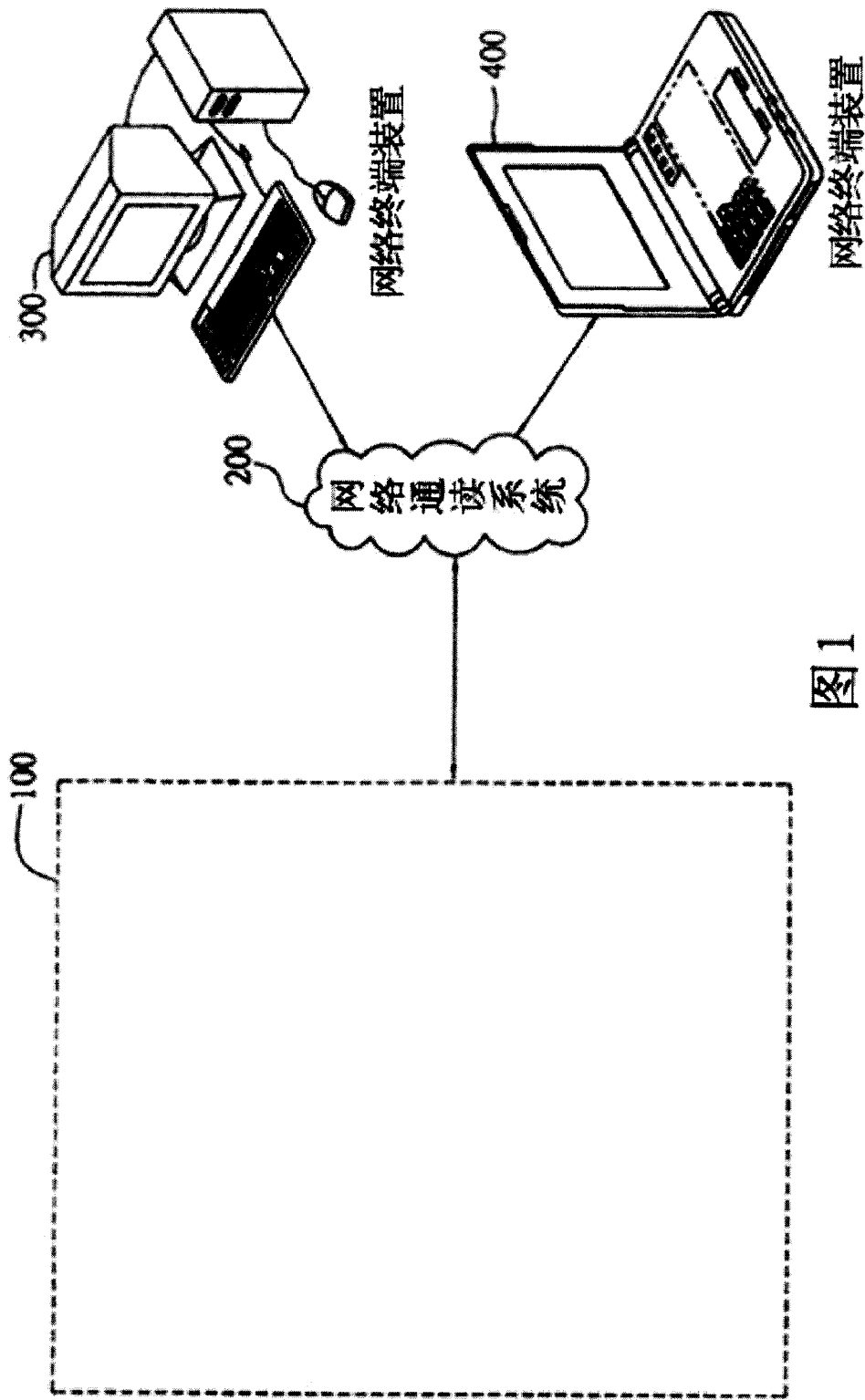
承前所述，在使用者通过上述的信息整合模块 250 取得该用以支持中小企业营运发展的信息供应系统 100 所提供的服务信息的过程中，15 该计费模块 270 会记录使用者与该信息供应者整合的信息，若使用者再通过该网站与专利局进行信息需求与供应的联系时，该计费模块 270 仍会记录其信息。

在本实施例中，以上述的“专利申请”流程为例，使用者自搜寻20 相关专利事务所或专利局的信息时，该计费模块 270 随即开始记录使用者使用该网站的使用时间、点选次数或下载档案的资料量等行为模式并加以记录，若该使用者与其中一具有专利代理经验的信息供应者相互联系，双方进行如线上实时咨询等信息服务时，该计费模块 270 随即记录使用者与该信息供应者之间的相关信息，若使用者再通过该25 网站与专利局进行信息需求与供应的联系时，该计费模块 270 仍会记录其有关信息。通过上述的信息记录，该计费模块 270 能够依据所记录该使用者连接该网站的层次、连接的时间及/或信息服务的内容等，计算出相对应的服务费用，其中，该服务费用的计算基准应视实际情况加以制定。此外，该计费模块 270 还能够依据信息提供者与该用以30 支持中小企业营运发展的信息供应系统 100 的管理者对于信息提供的利润分配基准，进行利润分配的计算。

综上所述，本发明之用以支持中小企业营运发展的信息供应方法以及系统，能够通过整合信息服务供应者所提供的信息服务供应机制、35 信息服务整合的机制、计费机制及接口转换机制，借由一信息供应网站以供信息服务供应者通过该信息供应网站提供信息服务。

本发明的用以支持中小企业营运发展的信息供应方法以及系统能够协助个人工作室、住家办公室及中小企业的经营者及其从业人员，在接取订单、增创营收、善用外部资源、进行委外服务、增加经营弹性、减少聘雇人员及办公室空间的需求、节省营运成本、降低创业门槛等方面提供帮助，进而达到解决失业问题及调整产业结构的目的。

5



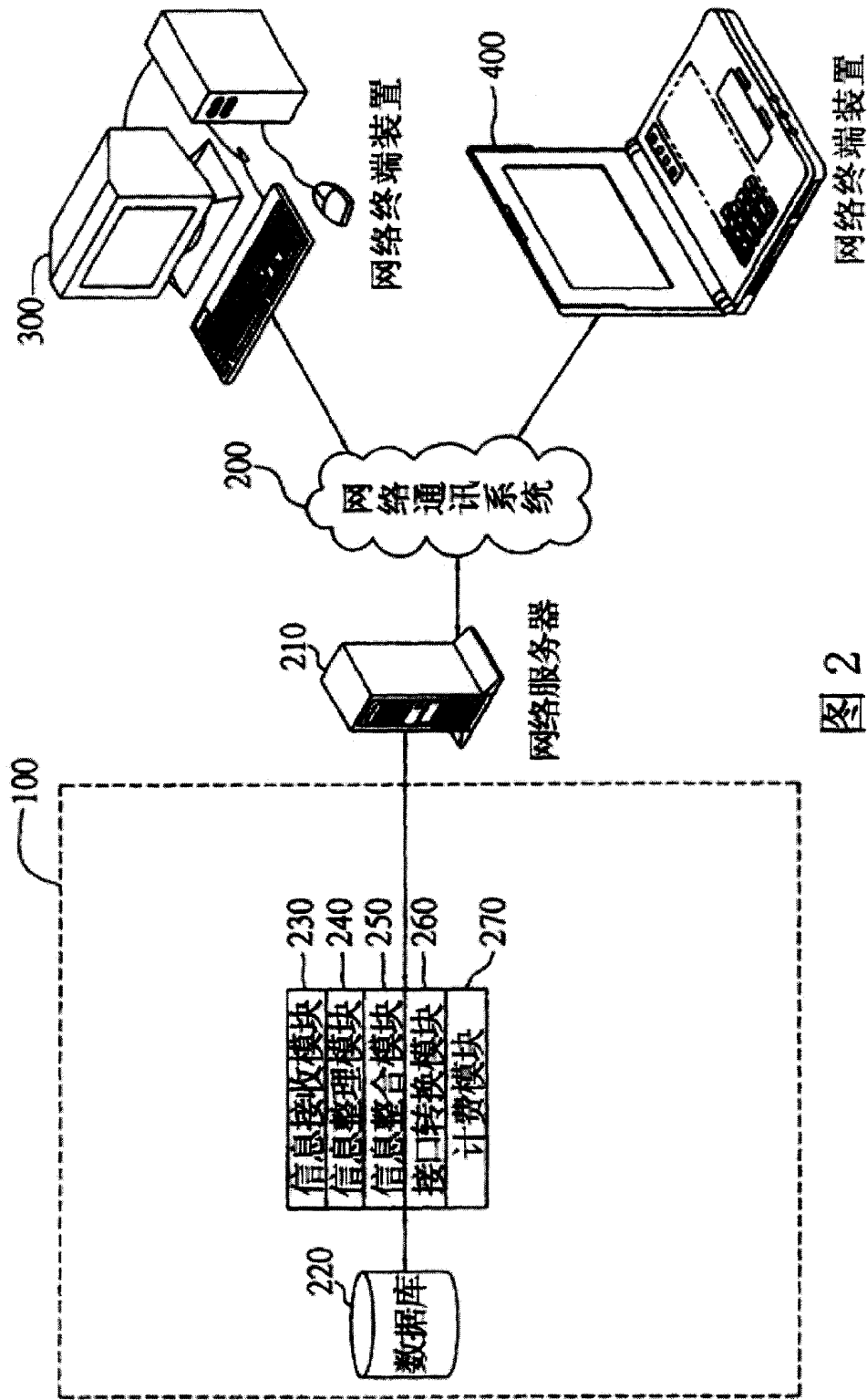


图 2

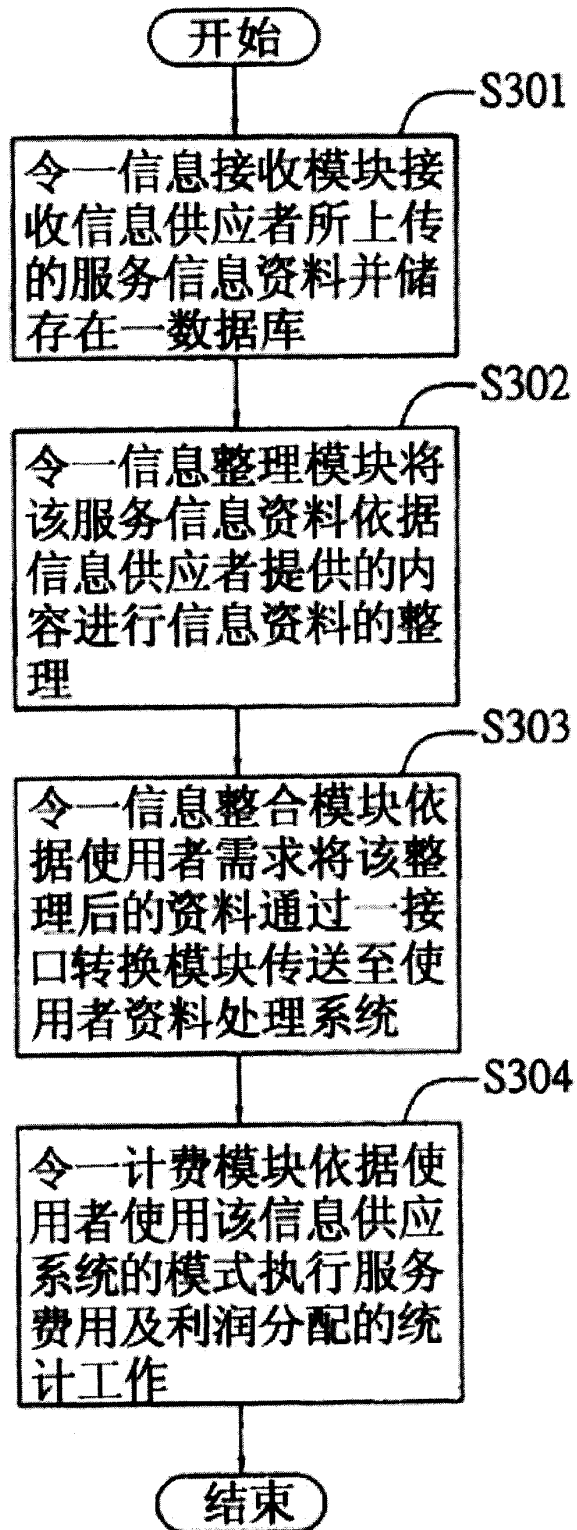


图 3

Patents

EnglishChinese

Find prior art

Discuss this application

View PDF

Download PDF

Method and system for providing information for supporting operation development of small-medium enterprises

CN 1508734 A

ABSTRACT

The invention is a kind of information supplying method and the system for supporting small and medium-sided enterprise development. A information receiving model receives the service information data uploaded by supplier and stores them in the databank; a information arranging model carries on the arrangement of relative data according to the content supplied by the supplier; a information integrating model transmits the proper data to the user data processing system through a interface converting model, finally, a charge calculating model calculates the charge according to the mode used by the user.

DESCRIPTION translated from Chinese

Supply methods to support the development of SMEs as well as operating system

Technical Field

The present invention relates to an operation to support the development of SMEs information provision method and system, especially with regard to an integrated information to provide users to access information through a single Web site that integrated information provision method and system.

Background

With the rapid development of electronic information technology, such as personal computers, notebook computers, tablet computers, palmtop computers, personal digital assistants and even mobile phones and other electronic devices or systems having a data processing function, its increasingly powerful in function. In addition to simple data processing, these devices have been able to provide users with Internet browsing, upload or download information, music, editing and playback of multimedia video information and other diversified services to get the information they need. On the other hand due to the wired and wireless network communications technologies become more sophisticated, the volume plus these electronic devices or systems increasingly compact size, ease of access to information in the user performs actions. Based on all these objective circumstances, users are more willing subjective electronic device or system that has a network connection and data transmission capabilities to search and access to information.

But when more and more users are no longer to obtain information through traditional media, newspapers, magazines and even radio and television, choosing instead to obtain the necessary information through the network communication system with real-time, online information provider bound to consider how to take full advantage of the characteristics of the network communications system, providing different from traditional media to provide information.

Existing methods provide user information through the network communication system is not generally the following methods: by the user through a browser connection portal, enter search keywords and other search criteria information

CLAIMS (26) translated from Chinese

An information provision method to support SME Business Development, to provide users with a data processing system by means of the information required to obtain services through a network communication system, wherein the means for support of the SME Business Supply method development include: make an information receiving module receives the information service provider information uploaded and stored in a database; make an information consolidation module based on the content of the service information provided by the information provider of information materials finishing; make an information integration module based on the needs of the user input, the finishing and meet the needs of data through a user interface conversion module is transferred to the data processing system; and to make a billing module according to the user to use the use to support the development of SMEs operating mode of information supply system, the implementation of service fees and profit distribution statistics work.

2. The method according to claim 1, characterized in that the information service provider information may be uploaded text data, image data, audio data, image data, network protocol address provided by hyperlinks and unified address information resource addressing one of them.

3. The method according to claim 1, characterized in that the service information This information can be uploaded provider of business intelligence, business opportunities, professional services, professional planning, business connections, administrative procedures and value-added services in one .

4. The method according to claim 1, characterized in that the finishing step also includes the same information will be different from the same information provider and wherein any one of the information provider provides, any of which is similar to and different information information, classify, summarize and combine the data processing.

5. The method according to claim 1, characterized in that the integration of information and forms can be connected to provide search and information services provider of database information online real-time network resource information request and response in

http://www.google.com/patents/CN1508734A?cl=en

1/7

Page 557 of 964

provided through the portal, and the search engine Keywords consistent and / or similar web information input by the user through the website or by way of hyperlinks connecting with the site, browse or transfer data through the browser.

This existing information search method, for lack of experience, or search Web search and related information is not very full of users, the information search, obtain sometimes like needle in a haystack. In addition, if the user to simultaneously search a number of substantive relevance, is not associated with a form of site, said search means could not be effectively addressed the needs of users. In this case, the user must still search through time and time again possible to find the information they need. And even if the user has to find all the relevant information, but if the lack of effective screening information, then the information gathered for the user not only can not effectively solve their own needs, sometimes it will become a huge burden.

On the other hand, users get to information through pay sites, typically used a fixed rate system, which is to pay a fee to obtain unlimited times within a certain period the right to use; stored value system, which is to buy a certain points, and then be deducted from the corresponding point information used in the. In addition to the two outside, then one approach is based on the service provider listed price, pay by credit card or debit way. The method of payment of the above services are based on a fixed fee service price list, the user is not able to log on or connect the level, the scope of services or even service rates as the basis for the adjustment.

In summary, how can we provide users with a set of integrated pluralistic information and the ability to more reasonable assurance that the information service provider and information needs of Fangli Yi approach is needed to solve problems.

DISCLOSURE

To overcome the disadvantages of the prior art, the main object of the present invention is to provide a support operation for the development of SMEs information provision method and system capable of providing an information provider website information provider to provide information so that the information supplied by website services.

Another object of the present invention is to provide a support operation for the development of SMEs information provision method and system that can provide information on the information provider for effective integration, improve the efficiency of users to find the information.

A further object of the present invention is to provide a support for the development of the SME Business information provision method and system, which can provide a user through an information service integration mechanisms and information provider of information services deals.

A further object of the present invention is to provide a support operation for the development of SMEs information provision method and system, which can provide an accounting mechanism to allow information providers to use information service based on user model to calculate the cost of services .

Again object of the present invention is to provide an operation to support the development of SMEs information provision method and system, which can provide an interface conversion mechanism for providing client user can borrow from the different types of data processing systems The present invention is to obtain information services.

To achieve the above objects, the present invention in order to support the development of SMEs operating information supply system comprising: a database for storing information providers including at least the information provided, the relevant data and information collated, the information needs of those information, information and data as well as those who need services cost

any one.

The method according to claim 6, wherein the interface conversion module converts the communication protocol may be Internet Protocol and wireless application protocol either.

7. The method according to claim 1, characterized in that, using this to support the development of SMEs operating mode information supply system may be a content level of the site's users to connect, the connection time and information services in the either.

8. The method according to claim 1, characterized in that the data processing system may be a server, workstations, personal computers, notebook computers, handheld computers, personal digital assistants and mobile phones either.

9. The method according to claim 1, characterized in that the network may be the Internet communication system between the Internet and corporate intranets any one.

10. The method according to claim 1, characterized in that the network communication system may be a wired communication systems and wireless communication system of any one.

11. The method according to claim 1, characterized in that the database is a relational database.

12. The method according to claim 1, characterized in that the message receiving module, information sorting module, information integration module, the interface conversion module and a billing module is a software program.

13. The method according to claim 1, characterized in that the user may be operators and their employees personal studio, home office and SME any one.

14. A method for supporting the development of the SME Business information supply system to provide users with borrowed by a data processing system to obtain the required information and services through a network communication system, wherein the means for support of the SME Business development of information supply system comprising: a database for storing at least include the information provided by those who provide information, relevant data and information collated, the information needs of those information, information needs and information providers who integrate data and information services Service cost information; an information receiving module for receiving information provider provides information through a network communication system; an information consolidation module to integrate the information receiving module receives information about the content of the information provided by the provider; an information integration module to the information needs of information consolidation module collated information submitted by the user to make a connection interworking; an interface converter module for different clients according to the data processing system to provide data transmission in line with the system, access specifications; and a billing module for computing services they need to pay the costs, as well as information provider and distribution of profits to support the development of SMEs operating information providing system administrators use of resources based on user-service model.

15. The system according to claim 14, characterized in that the information provider provides information may be text data, image data, audio data, image data, addresses in hyperlinks network protocol and provide uniform resource addressing address data in either.

16. The system of claim 14, wherein the service information provider uploaded the information may be business intelligence, business

data integration between information provider of information services; an information receiving module for receiving information provider provides information through a network communication system; an information consolidation module to integrate the information receiving module an information integration module to the information needs of information consolidation module collated information and user make a connection the proposed exchange;; an interface converter module for different customers based on the content of the information provided by the information provider end data processing system provides data transmission in line with the system specifications access; and a billing module for computing services they need to pay the costs, as well as information service providers based on user patterns and the use of resources to support SME Business Development Supply system administrator profit distribution.

The method by which to support the development of SMEs operating information supply system for the supply of information is: make an information receiving module receives information on the service provider information uploaded and stored in a database; an information consolidation module makes the service information provided in accordance with the content of the information provider to collate information; and make an information integration module based on the needs of the user input, the finishing and meet the needs of data transmission via an interface conversion module to the user data processing systems; and to make a billing module according to the user to use the development of SMEs to support operations information supply system mode, performing a service fee of statistical work and the distribution of profits.

Compared with the traditional supply methods and information systems, information mechanism of the present invention to provide by integrating information provider, the information service integration mechanisms, billing mechanism and interface conversion mechanism, through information supplied by a website to provide information by the information provider Supply website provides information services, information providers can provide information for effective integration, improve the efficiency of users to find the information required; at the same time be able to provide users with information and services through an integrated mechanism and information provider of information services transaction, it provides a billing mechanism, so that information providers use information service based on user patterns, calculate and charge for the services. Interface conversion mechanism of the present invention provides, allows the client user can borrow from the different types of data processing systems and services to get the information they need by the present invention.

Brief Description

Figure 1 is a block diagram of the application architecture, application architecture to show support for the operation of the present invention the development of SMEs information supply system; Figure 2 is a block diagram of the system architecture, the present invention is used to show support for SMEs operation and development of information systems architecture supply system; and Figure 3 is a flow chart, the process steps for information provision method of the present invention to support the development of SMEs operating display.

DETAILED DESCRIPTION

Example In the following examples, the present invention is to support the development of SMEs operating information supply method and an information system is provided including text data, image data, audio and video data as well as by other human senses can not be recorded by the direct identification of electromagnetic data actually able to provide information supply services through information provision method and system to support the operation and development of SMEs in the present invention are useful in the present invention, an information provision method and system to support the operation and development of SMEs.

See Figure 1, as shown in this embodiment, in order to support the operation and development of SMEs in the information supply system 100 of the invention, is used in the existing master-slave architecture network communication system 200, versus a to support the operation and development of SMEs in the information supply system 100 is constructed on the

opportunities, professional services, professional planning, business connections, administrative procedures and any value-added services species.

17. The system according to claim 14, characterized in that the module is the same as information of the same sort of information providers and different information provider provided by any one, any one of similar and different information in the information, classify, summarize and combine the data processing.

18. The system according to claim 14, characterized in that the form of the integration of information integration module may search a database of information, and providing on-line information services connected by network resources and real-time information request in response to any one of species.

19. The system of claim 14, wherein the interface conversion module converts the communication protocol may be Internet Protocol and wireless application protocol either.

20. The system of claim 14, characterized in that, using this to support the development of SMEs operating mode information supply system may be a content level of the site's users to connect, the connection time and information services in the either.

21. The system of claim 14, wherein the data processing system may be a server, workstations, personal computers, notebook computers, handheld computers, personal digital assistants and mobile phones either.

22. The system of claim 14 claim, characterized in that the network may be the internet communication system between the internet and corporate intranets any one.

23. The system of claim 14 claim, wherein the network communication system may be wired communication systems and wireless communications systems in any one.

24. The system according to claim 14, characterized in that the database is a relational database.

25. The system according to claim 14, characterized in that the message receiving module, information sorting module, information integration module, the interface conversion module and a billing module is a software program.

26. The system of claim 14 claim, characterized in that the user may be operators and their employees personal studio, home office and small and medium enterprises of any kind.

served end of the network communication system 200 for providing network terminal device has a network connection function client user network terminal device 300 and 400, made by a browser application 200, 100 interconnected with the construction of the served end to support the operation and development of SMEs in the information supply system via the network communication system for including a program or data upload or download, data storage and data management. Wherein the network communication system 200 may be a Internet (Internet), intranet (Intranet) or enterprises Internet (Extranet); the network terminal device 300 and a network terminal device 400 may be a personal computer (PC), notebook computer (NB), workstation (Workstation) or other device or system with data processing capabilities; the browser application may be Microsoft's Internet Explorer (Internet Explorer) or Netscape Navigator (Netscape Navigator) and so on. Said main are existing software and hardware architecture from architecture network communication system 200, the network terminal device and the browser application, so this will not be repeated.

See Figure 2, which shows the operation to support the development of SMEs information systems architecture supply system 100 of the invention, as shown in the operation to support the development of SMEs with information supply system 100 to a network server 210, the network server 210 is provided to support the operation and development of SMEs in the information supply system 100 through the network communication system 200 and the network terminal device 300 and a network terminal device 400 connected to each other, and to provide the network terminal device 300 and network the terminal apparatus 400 in response to user commands or other requirements for use of data access. In this embodiment, the network terminal device 300 and a network terminal device 400 is using a web browser application on each of the network terminal device, such as Microsoft's IE or Netscape Navigator as described above, through the network communication system 200 210, 100 connected to each other via the network server to support the development of SMEs operating information supply system for records management-related work. In particular, and it noted that the operation to support the development of SMEs information supply system 100 also may be a firewall (Firewall) system connections (not shown) to protect the operation to support the development of SMEs information supply system 100. The operation to support the development of SMEs information supply system 100 includes: a database 220, an information receiving module 230, an information consolidation module 240, an information integration module 250, an interface conversion module 260, and a billing module 270.

The database is used to store at least 220, including information provided by the information provided, the information related to the integration of data, information, information needs of those, who between information needs and information providers of information services and integrated information service expense sheet. In the present embodiment, in order to increase the efficiency of data query and retrieval, the database 220 may be a relational database. Among them, the information sheet provided by the information provider, used to store text data including at least provided information provider, image data, video and audio information and other data can be stored in any form of the databases and other data area bits; information integration related information table for storing information including at least category, information content and information integration relationship information data such as location information; the information needs of those information table for storing includes at least the basic user identity, user permission to use information and recording user data such as resource use location; the information needs of persons between information providers and information services to integrate the data sheet, including an information service for storing at least types of information integration and data information services into history data such as location; the service cost data tables, including at least information provider to store the charging mode, metering and information provider information provider the information provided is used to support the operation and development of SMEs Supply Profit distribution between basic data such as location system administrator.

Through this relationship database when a user enters any of the above information, which is used to support 100 to quickly find the information corresponding to its SME Business Development Supply System. In particular, and it noted that all the data and information on the location of the above table belongs only way of example only, in reality, its contents should be more clearly detailed. In addition, the contents of each bit of the data area may also include other data or information table location, but due to limited space, as well as a succinct statement on the show only to the present invention supports SME Business Development Supply methods and some of the information system related. On the other hand, the relational database system architecture also has many, depending on the needs of users should be construction, it is also not repeated.

The message receiving module 230 is used to receive network information provider through the communication system 200 to provide information. In this embodiment, the information provider may be consulting services, professional planning services, life value-added services, value-added knowledge services, business connectivity services, and even any natural or legal person or legal entity government administrative units or foreign service window, etc. Information provided constituted body. This information is provided by the network may, by the terminal device 200 via the network communication system, the information services to be provided to upload to the network server 210, the information receiving module 230 then the received information service related information to be saved to the database 220.

Need of special note is the establishment between information providers and managers to support the operation and development of the SME information supply system 100 a data transfer protocol, the particular type of information, such as specific identification number or text definition When 230 receives information related information having the identification

number or character of the information receiving module should be based on the identification number or text to the relevant information stored in the database 220 corresponding information storage field.

This information consolidation module 240 is receiving module 230 accepts the information content of the information providers, in accordance with certain rules finishing. In this embodiment, since the information content provided by the information provider all-inclusive, the content may include various fields at different levels of content, may be private companies or government agencies. But usually a business process flow may include a number of different information provider to complete. As a patent application, the process may include professional patent search firm to discuss patent applications related information for the execution of programs written or patent application as the patent specification of the charge d'affaires, after the completion of drafting patent specification must also be sent to the Patent patent examination Board, and finally by the relevant operating procedures in order to determine whether the franchise.

This information consolidation module 240 can be related applications and patent information services as a consolidation, when the user wants to search and patent applications related to information services, you can get a series of useful and related information services. On finishing means, said by agreement by the information provider and to support the development of SMEs operating information supply system between managers, to be borrowed by a particular identification number or text classification, to the front stage by private patent matters services provided, to be connected with the later stages of the administrative service provided by government agencies and other offices. That is when the information provider of information provided by the information receiving module 230 to 220 stored in the database, the information sorting module 240 can be related to the specific information received, and in particular the key elements as "patent application" and storage to the database 220 of location-specific data in order for the operation to support the development of SMEs information supply system 100 access data.

The information integration module 250 to the information needs of information consolidation module 240 to sort out information and users are asked to make a connection exchange. In this embodiment, when the user by the network terminal device 200 via the network communication systems, and construction has to support the operation and development of SMEs in the information supply system 100 is connected to each other at the site, the site will provide an information service relevant search mechanism, such as requesting the user to enter a personal identification data basic user identity, user permission to use the information, as well as specific information search key identification number, or text and so on, through the information integration module search function 250, that can The information requirements are needed for information services and related information services to support the operation and development of the SME information supply system 100 can offer combined with each other. Its combination of methods include providing users with hyperlinks connected to each other and the information provider to provide a unified resource addressing connector device (URL) and other network resources, and / or provide such as on-line real-time video conferencing (Net-Meeting) and other online real-time information requests and responses.

The interface conversion module 260 will be based on network unit to provide different clients in line with the specifications of the information system data transmission access. In this embodiment, the network terminal device 300 and 400 is not limited to existing personal computer or notebook computer, it may also include any communication system 200 connected via a network to have the infrastructure to support SME Business Development system or device information supply system 100 sites, such as mobile phones applies wireless applications protocol (WAP) and other browser formats. The interface conversion module 260 is to use a different browser or system or device data access protocol conversion interface is provided, it can be connected to architecture has to support the operation and development of SMEs in the information supply system 100 sites for different use Browse or access protocol network terminal devices to search for information or receive information providers are providing various forms of information services.

The billing module 270 is for the use of resources based on user mode services, computing services, they should pay the costs. In this embodiment, the billing module 270, in conformity with the information provider or manager to support the development of SMEs operating information providing system 100 of the determined price list information services, information services used to calculate the user Total service charges to be paid outside. It can also be based on the user to use the operation to support the development of SMEs information supply system model and its history of 100, as a standard computing service costs. In the aforementioned "patent application" process, for example, when a user from searching for relevant patent office or patent offices of information, the billing module 270 begins recording the user to use the site of use, click on the number or download files The amount of data and other behavior patterns, and recorded, if the user with one of the information provider has experienced patent agents interrelated, and both sides were as real-time online information and consulting service, the billing module 270 immediately recorded use between those and the information provider services and information to be served, if the user then the demand and supply of information services through the site with the Patent Office, the billing module 270 will still record information between them. It is recorded by the above-mentioned track record of user behavior patterns and the way the user can take advantage of different levels according to the website (Level) as a standard to calculate the cost of services.

See Figure 3, which shows through the above-mentioned operation to support the development of SMEs information supply system 100, the procedures described in the information supply method to support the operation and development

of SMEs in yes.

In step S301, so that the information service information receiving module 230 receives information provider uploaded and stored in the database 220. Information received by the information provider module 230 is capable of receiving data transmitted, the network protocol address provided by way of hyperlinks and / or uniform resource addressing address and other information.

Cheng said before, the information provider to support the operation and development of SMEs in the information supply system was set up a data transfer protocol between the 100 managers, such as a specific identification number or text to define specific types of information, when The information receiving module 230 receives the information and other related information with that identification number or text, it is possible according to the identification numbers or letters to the relevant information stored in the database 220 corresponding information storage field.

In this embodiment, if a patent office by the desire to support the operation and development of SMEs in the information supply system 100 as a provider of patent information, it can borrow from the network terminal device 200 via the network communication system, which it can provide information sent to the network server 210, wherein the transmission of data, including text or image information, network protocol addresses to hyperlinks provided and / or uniform resource addressing address and other information. Moreover, further comprising a specific identification number or text, such as "0001" and "Patent services", the information receiving module 230 at the network server 210 receives the information, then the information stored in the database 220 to meet the The identification number "0001" and recognized character "Patent Services" data location, followed by step S302.

In step S302, so that the information received from the service module 240 on the basis of information provided by the content information provider summarize the relevant information and organize. The process includes the same information the same provider or different information provided by suppliers, similar or different information to be classified, or a combination of induction and the like.

Cheng said before, in addition to the patent information service providers can communicate the relevant information, provided the architecture has to support the development of SMEs operating site information providing system 100 also with government agencies, such as the above-mentioned patent offices and other mutual cooperate in providing such as online and other patent applications or consulting services. Because of a patent application process may include assistance and other needs by the patent office and patent office information service providers in order to successfully complete. Then this information should be finishing module 240 information services Patent Office and the Patent Office provided information to make a classification, when the user logs architecture has to support the operation and development of the SME information supply system 100 sites, and wants When requesting the site to provide "patent application" of information services, it is possible to easily find the information and services that the patent office and summarized by the Patent Office after the above offer, followed by step S303.

In step S303, so that an information integration module 250 in accordance with the needs of the user input, the finishing and meet the needs of data through an interface conversion module 260 is transmitted to the client network terminal devices. Its integrated model includes a connection search, information services provider database 220 information network resources and / or provide real-time online information request and response and so on.

Before the bearing, when the "Patent Services" users log on to the information needs of the site, the site can provide users with an input of the user information related functions, such as the identity of the user to enter basic user usage information permissions and other personally identifiable information, as well as specific information search key identification number or character, such as the identification number "0001" and recognition of the word "patent services" through which information integration module search function 250, that person can demand the required information "patent" of related information services, and information services to support the operation and development of the SME information supply system 100 can be provided by the Patent Office and the Patent Office provided consolidated combined with each other.

In this embodiment, the user searches the database 220 relevant information, and the patent office video conferencing and network of offices above assumptions online patent application processes and other information services, followed by step S304.

In step S304, so that a billing module 270 according to the user to use this information to support the development of SMEs operating mode supply system 100, performing a service fee of statistics. It is based on the user using the information mode, calculate the required fees paid profits and the distribution of information between providers.

The front bearing, when the user 250 acquires service information to support the operation and development of the SME information supply system 100 is provided by the above process of information integration module, the billing module 270 will record the information supply Aggregated information, if the user further information contact the demand and supply through the site with the Patent Office, the billing module 270 will still record its information.

In this embodiment, the above-mentioned "patent application" process, for example, when users search for relevant patent office or patent offices of information from the billing module 270 begins recording the user to use the site of use, point When the selected frequency or amount of data downloaded file to record patterns of behavior and, if the user and the information provider which patent agency experience having contact with each other, the two sides as online real-time information and consulting services, the billing module 270 then record the relevant information and the user information between suppliers, if the user further information contact the demand and supply through the site with the Patent Office, the billing module 270 will continue to record their information. By the above information recording, the billing module 270 can connect the user based on the recorded level of the site, the connection time and / or information services and other content, calculate the corresponding service charges, which the service fees calculation basis should be developed as practicable. In addition, the billing module 270 can also provide the basis for information and managers to support the operation and development of SMEs in the information supply system 100 is provided baseline information for profit distribution, the calculated distribution of profits.

In summary, the present invention in order to support the development of the SME Business information provision method and system capable of information services through the integration of information mechanism provided by the service provider, information service integration mechanisms, billing mechanism and interface conversion mechanism , by the information supplied by a website to provide information and services provider to provide information services through the information provider sites.

Information provision method and system to support the operation and development of SMEs in the present invention can assist individuals studio, home office and SME managers and employees, in the next to take orders, to create revenue, use of external resources, conduct outsourcing services and increase business flexibility, reduce demand and office space, hiring staff, to save operating costs, reduce business barriers, such as providing help, and then to solve the unemployment problem and the purpose of the adjustment of industrial structure.

LEGAL EVENTS

Date	Code	Event	Description
Jun 30, 2004	C06	Publication	
Sep 8, 2004	C10	Request of examination as to substance	
Mar 21, 2007	C02	Deemed withdrawal of patent application after publication (patent law 2001)	

[Google Home](#) - [Sitemap](#) - [USPTO Bulk Downloads](#) - [Privacy Policy](#) - [Terms of Service](#) - [About Google Patents](#) - [Send Feedback](#)

Electronic Acknowledgement Receipt	
EFS ID:	23060786
Application Number:	14673625
International Application Number:	
Confirmation Number:	9085
Title of Invention:	Wireless end-user device with differentiated network access status for different device applications
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	James E. Harris/Ann Taylor
Filer Authorized By:	James E. Harris
Attorney Docket Number:	RALEP032C1C2
Receipt Date:	29-JUL-2015
Filing Date:	30-MAR-2015
Time Stamp:	16:17:59
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	P032C1C2_IDS.pdf	614287 432087b00987c25a0cc4e7a0be771ff2c70a238c	no	10

Warnings:

Information:

2	Foreign Reference	2063.pdf	2400276	no	21
			5c7adffc40b293a3442a4c140083d3fc5d876114		
Warnings:					
Information:					
3	Foreign Reference	2064.pdf	2345898	no	20
			db3b0051c6d9ab3dfa64f05d6324394e5fc54486		
Warnings:					
Information:					
4	Foreign Reference	2065.pdf	2381976	no	25
			7796f26254f7db3b899626b2e7332663eaff0633		
Warnings:					
Information:					
5	Foreign Reference	2066_Fujitsu.pdf	856885	no	22
			72e75495c5d83e30e4fbefee0e38a1bb25a5405f		
Warnings:					
Information:					
6	Foreign Reference	2067_Kyocera.pdf	641903	no	27
			024bbc366c4ffca0d6206fd9400790e51cab71c3		
Warnings:					
Information:					
7	Foreign Reference	2068_Citrix.pdf	14110049	no	118
			6b5308424d6052f222f99c6297e0f2cd005b02d2		
Warnings:					
Information:					
8	Foreign Reference	2069_CN1508734A.pdf	3021193	no	24
			c8818fe2ac00cd927bb1eb76517cffb16566e7c4		
Warnings:					
Information:					
9	Non Patent Literature	3040_Ahmed.pdf	698684	no	10
			312c9bfa74f55adbdbd7f0eeec7032be26a77e3ad5		
Warnings:					
Information:					
10	Non Patent Literature	3041_Kassar.pdf	840076	no	14
			1b87a4e38876abxc373a0c7a689d940a997ba013		
Warnings:					
Information:					

11	Non Patent Literature	3042_Kaufmann.pdf	3412131 987a5e9e6c5cadcf6cd5982f4c181ac27b6d afe7	no	283
Warnings:					
Information:					
12	Non Patent Literature	3043_Sadeh.pdf	1095284 adc744cb7b194a97b6f3ac3e1b28a65e042 abd9f	no	16
Warnings:					
Information:					
Total Files Size (in bytes):			32418642		
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>					



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/673,625	03/30/2015	Gregory G. Raleigh	RALEP032C1C2

CONFIRMATION NO. 9085

106963

Headwater Partners I LLC
555 Twin Dolphin Drive, Suite 310
Redwood Shores, CA 94065

PUBLICATION NOTICE



OC000000076456849

Title:Wireless end-user device with differentiated network access status for different device applications

Publication No.US-2015-0207760-A1

Publication Date:07/23/2015

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently <http://www.uspto.gov/patft/>.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently <http://pair.uspto.gov/>. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

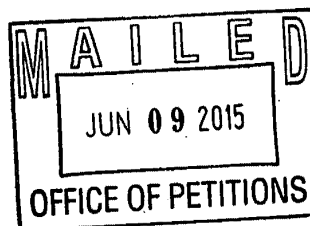
Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

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



UNITED STATES PATENT AND TRADEMARK OFFICE

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



HEADWATER PARTNERS I LLC
555 TWINB DOLPHIN DRIVE, SUITE 310
REDWOOD SHORES CA 94065

Doc Code: TRACK1.GRANT

Decision Granting Request for Prioritized Examination (Track I or After RCE)	Application No.: 14/673,625
<p>1. THE REQUEST FILED <u>3/30/15</u> IS GRANTED.</p> <p>The above-identified application has met the requirements for prioritized examination</p> <p>A. ☒ for an original nonprovisional application (Track I).</p> <p>B. ☐ for an application undergoing continued examination (RCE).</p> <p>2. The above-identified application will undergo prioritized examination. The application will be accorded special status throughout its entire course of prosecution until one of the following occurs:</p> <p>A. filing a <u>petition for extension of time</u> to extend the time period for filing a reply;</p> <p>B. filing an <u>amendment to amend the application to contain more than four independent claims, more than thirty total claims</u>, or a multiple dependent claim;</p> <p>C. filing a <u>request for continued examination</u>;</p> <p>D. filing a notice of appeal;</p> <p>E. filing a request for suspension of action;</p> <p>F. mailing of a notice of allowance;</p> <p>G. mailing of a final Office action;</p> <p>H. completion of examination as defined in 37 CFR 41.102; or</p> <p>I. abandonment of the application.</p> <p>Telephone inquiries with regard to this decision should be directed to Cheryl Gibson-Baylor at (571)272-3213, Office of Petitions. In his/her absence, calls may be directed to Brian W. Brown, (571)272-5338.</p> <p>Cheryl Gibson-Baylor /Cheryl Gibson-Baylor/ [Signature]</p> <p>Petitions Paralegal Specialist (Title)</p>	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625	
	Filing Date		2015-03-30	
	First Named Inventor	Raleigh		
	Art Unit	2642		
	Examiner Name	not yet assigned		
	Attorney Docket Number	RALEP032C1C2		

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					
If you wish to add additional U.S. Patent citation information please click the Add button.						Add
U.S.PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20020022472		2002-02-21	WATLER et al.	
	2	20020120540		2002-08-29	KENDE et al.	
	3	20020131404		2002-09-19	MEHTA et al.	
	4	20020138601		2002-09-26	PIPONIUS et al.	
	5	20020176377		2002-11-28	HAMILTON, Thomas E.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625
	Filing Date		2015-03-30
	First Named Inventor	Raleigh	
	Art Unit	2642	
	Examiner Name	not yet assigned	
	Attorney Docket Number	RALEP032C1C2	

	6	20020199001		2002-12-26	WENOCUR et al.	
	7	20030004937		2003-01-02	SALMENKAITA et al.	
	8	20030005112		2003-01-02	KRAUTKREMER, Todd Joseph	
	9	20030013434		2003-01-16	ROSENBERG et al.	
	10	20030018524		2003-01-23	FISHMAN et al.	
	11	20030046396		2003-03-06	RICHTER et al.	
	12	20030050070		2003-03-13	MASHINSKY et al.	
	13	20030050837		2003-03-13	KIM, Do Sik	
	14	20030088671		2003-05-08	KLINKER et al.	
	15	20030133408		2003-07-17	CHENG et al.	
	16	20030161265		2003-08-28	CAO et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625	
	Filing Date		2015-03-30	
	First Named Inventor	Raleigh		
	Art Unit	2642		
	Examiner Name	not yet assigned		
	Attorney Docket Number	RALEP032C1C2		

	17	20030182420		2003-09-25	JONES et al.	
	18	20030182435		2003-09-25	REDLICH et al.	
	19	20030220984		2003-11-27	JONES et al.	
	20	20030224781		2003-12-04	MILFORD et al.	
	21	20030229900		2003-12-11	REISMAN, Richard	
	22	20030236745		2003-12-25	HARTSELL et al.	
	23	20040019539		2004-01-29	RAMAN et al.	
	24	20040021697		2004-02-05	BEATON et al.	
	25	20040030705		2004-02-12	BOWMAN-AMUAH, Michel K.	
	26	20040044623		2004-03-04	WAKE et al.	
	27	20040047358		2004-03-11	CHEN et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625	
	Filing Date		2015-03-30	
	First Named Inventor	Raleigh		
	Art Unit	2642		
	Examiner Name	not yet assigned		
	Attorney Docket Number	RALEP032C1C2		

	28	20040073672		2004-04-15	FASCENDA, Anthony C.	
	29	20040082346		2004-04-29	SKYTT et al.	
	30	20040098715		2004-05-20	AGHERA et al.	
	31	20040103193		2004-05-27	PANDYA et al.	
	32	20040107360		2004-06-03	HERRMANN et al.	
	33	20040127200		2004-07-01	SHAW et al.	
	34	20040132427		2004-07-08	LEE et al.	
	35	20040168052		2004-08-26	CLISHAM et al.	
	36	20040198331		2004-10-07	COWARD et al.	
	37	20040236547		2004-11-25	RAPPAPORT et al.	
	38	20040249918		2004-12-09	SUNSHINE, Roger N.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625
	Filing Date		2015-03-30
	First Named Inventor	Raleigh	
	Art Unit	2642	
	Examiner Name	not yet assigned	
	Attorney Docket Number	RALEP032C1C2	

	39	20050021995		2005-01-27	LAL et al.	
	40	20050048950		2005-03-03	MORPER, Hans-Jochen	
	41	20050055291		2005-03-10	BEVENTE et al.	
	42	20050055309		2005-03-10	WILLIAMS et al.	
	43	20050060266		2005-03-17	DEMELLO et al.	
	44	20050097516		2005-05-05	DONNELLY et al.	
	45	20050107091		2005-05-19	VANNITHAMBY et al.	
	46	20050128967		2005-06-16	SCOBIE, Donald MacGregor	
	47	20050166043		2005-07-28	ZHANG et al.	
	48	20050183143		2005-08-18	ANDERHOLM et al.	
	49	20050198377		2005-09-08	FERGUSON et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625
	Filing Date		2015-03-30
	First Named Inventor	Raleigh	
	Art Unit	2642	
	Examiner Name	not yet assigned	
	Attorney Docket Number	RALEP032C1C2	

	50	20050216421		2005-09-29	BARRY et al.	
	51	20050228985		2005-10-13	YLIKOSKI et al.	
	52	20050238046		2005-10-27	HASSAN et al.	
	53	20050246282		2005-11-03	NASLUND et al.	
	54	20050250508		2005-11-10	GUO et al.	
	55	20050254435		2005-11-17	MOAKLEY et al.	
	56	20050266825		2005-12-01	CLAYTON, Steve	
	57	20050266880		2005-12-01	GUPTA, Vivek G.	
	58	20060014519		2006-01-19	MARSH et al.	
	59	20060019632		2006-01-26	CUNNINGHAM et al.	
	60	20060026679		2006-02-02	ZAKAS, Philip H.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625	
	Filing Date		2015-03-30	
	First Named Inventor	Raleigh		
	Art Unit	2642		
	Examiner Name	not yet assigned		
	Attorney Docket Number	RALEP032C1C2		

	61	20060034256		2006-02-16	ADDAGATLA et al.	
	62	20060040642		2006-02-23	BORIS et al.	
	63	20060045245		2006-03-02	AARON et al.	
	64	20060048223		2006-03-02	LEE et al.	
	65	20060072646		2006-04-06	FEHER, Kamilo	
	66	20060085543		2006-04-20	HRASTAR et al.	
	67	20060112016		2006-05-25	ISHIBASHI, Yoshihito	
	68	20060143098		2006-06-29	LAZARIDIS, Mihal	
	69	20060165060		2006-07-27	DUA, Robin	
	70	20060178917		2006-08-10	MERRIAM et al.	
	71	20060178918		2006-08-10	MIKURAK, Michael G.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625
	Filing Date		2015-03-30
	First Named Inventor	Raleigh	
	Art Unit	2642	
	Examiner Name	not yet assigned	
	Attorney Docket Number	RALEP032C1C2	

	72	20060183462		2006-08-17	KOLEHMAINEN, Mikko	
	73	20060190314		2006-08-24	HERNANDEZ, Rick	
	74	20060199608		2006-09-07	DUNN et al.	
	75	20060206904		2006-09-14	WATKINS et al.	
	76	20060218395		2006-09-28	MAES, Stephane H.	
	77	20060233108		2006-10-19	KRISHNAN, Murali R.	
	78	20060233166		2006-10-19	BOU-DIAB et al.	
	79	20060236095		2006-10-19	SMITH et al.	
	80	20060242685		2006-10-26	HEARD et al.	
	81	20060258341		2006-11-16	MILLER et al.	
	82	20060291477		2006-12-28	CROAK et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	14673625
	Filing Date	2015-03-30
	First Named Inventor	Raleigh
	Art Unit	2642
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1C2

	83	20070019670		2007-01-25	FALARDEAU, Eric	
	84	20070022289		2007-01-25	ALT et al.	
	85	20070036312		2007-02-15	CAI et al.	
	86	20070055694		2007-03-08	RUGE et al.	
	87	20070061243		2007-03-15	RAMER et al.	
	88	20070076616		2007-04-05	NGO et al.	
	89	20070093243		2007-04-26	KAPADEKAR et al.	
	90	20070100981		2007-05-03	ADAMCZYK et al.	
	91	20070101426		2007-05-03	LEE et al.	
	92	20070104126		2007-05-10	CALHOUN et al.	
	93	20070130315		2007-06-07	FRIEND et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625	
	Filing Date		2015-03-30	
	First Named Inventor	Raleigh		
	Art Unit	2642		
	Examiner Name	not yet assigned		
	Attorney Docket Number	RALEP032C1C2		

	94	20070140113		2007-06-21	GEMELOS, Steven	
	95	20070140275		2007-06-21	BOWMAN et al.	
	96	20070198656		2007-08-23	MAZZAFERRI et al.	
	97	20070220251		2007-09-20	ROSENBERG et al.	
	98	20070226225		2007-09-27	YIU et al.	
	99	20070243862		2007-10-18	COSKUN et al.	
	100	20070248100		2007-10-25	ZUBERI et al.	
	101	20070254675		2007-11-01	ZORLU OZER et al.	
	102	20070255848		2007-11-01	SEWALL et al.	
	103	20070259673		2007-11-08	WILLARS et al.	
	104	20070263558		2007-11-15	SALOMONE, Leonardo	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	14673625
	Filing Date	2015-03-30
	First Named Inventor	Raleigh
	Art Unit	2642
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1C2

	105	20070274327		2007-11-29	KAARELA et al.	
	106	20070282896		2007-12-06	WYDROUG et al.	
	107	20070294395		2007-12-20	STRUB et al.	
	108	20070298764		2007-12-27	CLAYTON, Steve	
	109	20080005285		2008-01-03	ROBINSON et al.	
	110	20080005561		2008-01-03	BROWN et al.	
	111	20080010452		2008-01-10	HOLTZMAN et al.	
	112	20080039102		2008-02-14	SEWALL et al.	
	113	20080049630		2008-02-28	KOZISEK et al.	
	114	20080052387		2008-02-28	HEINZ et al.	
	115	20080059474		2008-03-06	LIM, Keng	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625	
	Filing Date		2015-03-30	
	First Named Inventor	Raleigh		
	Art Unit	2642		
	Examiner Name	not yet assigned		
	Attorney Docket Number	RALEP032C1C2		

	116	20080059743		2008-03-06	BYCHKOV et al.	
	117	20080060066		2008-03-06	WYNN et al.	
	118	20080062900		2008-03-13	RAO, Bindu Rama	
	119	20080064367		2008-03-13	NATH et al.	
	120	20080066149		2008-03-13	LIM, Keng	
	121	20080066150		2008-03-13	LIM, Keng	
	122	20080082643		2008-04-03	STORRIE et al.	
	123	20080083013		2008-04-03	SOLIMAN et al.	
	124	20080095339		2008-04-24	ELLIOTT et al.	
	125	20080098062		2008-04-24	BALIA, Hinal K.	
	126	20080109679		2008-05-08	WRIGHT et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	14673625
	Filing Date	2015-03-30
	First Named Inventor	Raleigh
	Art Unit	2642
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1C2

	127	20080120688		2008-05-22	QIU et al.	
	128	20080127304		2008-05-29	GINTER et al.	
	129	20080130534		2008-06-05	TOMIOKA, Tazuko	
	130	20080130656		2008-06-05	KIM et al.	
	131	20080132268		2008-06-05	CHOI-GROGAN et al.	
	132	20080134330		2008-06-05	KAPOOR et al.	
	133	20080147454		2008-06-19	WALKER et al.	
	134	20080160958		2008-07-03	ABICHANDANI et al.	
	135	20080162637		2008-07-03	ADAMCZYK et al.	
	136	20080162704		2008-07-03	POPLETT et al.	
	137	20080164304		2008-07-10	NARASIMHAN et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	14673625
	Filing Date	2015-03-30
	First Named Inventor	Raleigh
	Art Unit	2642
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1C2

	138	20080167027		2008-07-10	GAUTIER et al.	
	139	20080167033		2008-07-10	BECKERS, Michel	
	140	20080168523		2008-07-10	ANSARI et al.	
	141	20080177998		2008-07-24	APSANGI et al.	
	142	20080183812		2008-07-31	PAUL et al.	
	143	20080184127		2008-07-31	RAFEY et al.	
	144	20080189760		2008-08-07	ROSENBERG et al.	
	145	20080207167		2008-08-28	BUGENHAGEN, Michael K.	
	146	20080212470		2008-09-04	CASTANEDA et al.	
	147	20080221951		2008-09-11	STANFORTH et al.	
	148	20080222692		2008-09-11	ANDERSSON et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625
	Filing Date		2015-03-30
	First Named Inventor	Raleigh	
	Art Unit	2642	
	Examiner Name	not yet assigned	
	Attorney Docket Number	RALEP032C1C2	

	149	20080225748		2008-09-18	KHEMANI et al.	
	150	20080229385		2008-09-18	FEDER et al.	
	151	20080229388		2008-09-18	MAES, Stephane H.	
	152	20080256593		2008-10-16	VINBERG et al.	
	153	20080268813		2008-10-30	MAES, Stephane H.	
	154	20080298230		2008-12-04	LUFT et al.	
	155	20080305793		2008-12-11	GALLAGHER et al.	
	156	20080311885		2008-12-18	DAWSON et al.	
	157	20080316923		2008-12-25	FEDDERS et al.	
	158	20080318547		2008-12-25	BALLOU et al.	
	159	20080318550		2008-12-25	DeATLEY, Dallas	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625
	Filing Date		2015-03-30
	First Named Inventor	Raleigh	
	Art Unit	2642	
	Examiner Name	not yet assigned	
	Attorney Docket Number	RALEP032C1C2	

	160	20080319879		2008-12-25	CARROLL et al.	
	161	20090005005		2009-01-01	FORSTALL et al.	
	162	20090013157		2009-01-08	BEAULE, Stephane	
	163	20090054030		2009-02-26	GOLDS, David	
	164	20090068984		2009-03-12	BURNETT, R. Alan	
	165	20090077622		2009-03-19	BAUM et al.	
	166	20090079699		2009-03-26	SUN, Jian	
	167	20090113514		2009-04-30	HU, Q. James	
	168	20090125619		2009-05-14	ANTANI, Snehal S.	
	169	20090180391		2009-07-16	PETERSEN et al.	
	170	20090197585		2009-08-06	AARON, Jeffrey A.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625	
	Filing Date		2015-03-30	
	First Named Inventor	Raleigh		
	Art Unit	2642		
	Examiner Name	not yet assigned		
	Attorney Docket Number	RALEP032C1C2		

	171	20090257379		2009-10-15	ROBINSON et al.	
	172	20090271514		2009-10-29	THOMAS et al.	
	173	20090286507		2009-11-19	O'NEIL et al.	
	174	20090287921		2009-11-19	ZHU et al.	
	175	20090288140		2009-11-19	HUBER et al.	
	176	20100017506		2010-01-21	FADELL, Anthony	
	177	20100042675		2010-02-18	FUJII, Hiroshi	
	178	20100043068		2010-02-18	VARADHAN et al.	
	179	20100071053		2010-03-18	ANSARI et al.	
	180	20100082431		2010-04-01	RAMER et al.	
	181	20100103820		2010-04-29	FULLER et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625
	Filing Date		2015-03-30
	First Named Inventor	Raleigh	
	Art Unit	2642	
	Examiner Name	not yet assigned	
	Attorney Docket Number	RALEP032C1C2	

	182	20100188975		2010-07-29	RALEIGH, Gregory G.	
	183	20100188990		2010-07-29	RALEIGH, Gregory G.	
	184	20100188992		2010-07-29	RALEIGH, Gregory G.	
	185	20100188994		2010-07-29	RALEIGH, Gregory G.	
	186	20100191576		2010-07-29	RALEIGH, Gregory G.	
	187	20100191612		2010-07-29	RALEIGH, Gregory G.	
	188	20100191846		2010-07-29	RALEIGH, Gregory G.	
	189	20100192170		2010-07-29	RALEIGH, Gregory G.	
	190	20100192212		2010-07-29	RALEIGH, Gregory G.	
	191	20100195503		2010-08-05	RALEIGH, Gregory G.	
	192	20100197268		2010-08-05	RALEIGH, Gregory G.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625
	Filing Date		2015-03-30
	First Named Inventor	Raleigh	
	Art Unit	2642	
	Examiner Name	not yet assigned	
	Attorney Docket Number	RALEP032C1C2	

	193	20100198698		2010-08-05	RALEIGH et al.	
	194	20100198939		2010-08-05	RALEIGH, Gregory G.	
	195	20100325420		2010-12-23	KANEKAR, Tushar	
	196	20110126141		2011-05-26	KING et al.	
	197	20080132201		2008-06-05	KARLBERG, Johan	
	198	20080081606		2008-04-03	COLE, Terry L.	
	199	20090248883		2009-10-01	SURYANARAYANA et al.	
	200	20100144310		2010-06-10	BEDINGFIELD, James Carlton	
	201	20080085707		2008-04-10	FADELL, Tony	
	202	20090046723		2009-02-19	RAHMAN, Reshad A. et al.	
	203	20080219268		2008-09-11	DENNISON, Larry R.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625
	Filing Date		2015-03-30
	First Named Inventor	Raleigh	
	Art Unit	2642	
	Examiner Name	not yet assigned	
	Attorney Docket Number	RALEP032C1C2	

	204	20080005285		2008-01-03	ROBINSON, James David et al.	
	205	20090315735		2009-12-24	BHAVANI, Neeraj S. et al.	
	206	20090219170		2009-09-03	CLARK, Ryan C. et al.	
	207	20090067372		2009-03-12	SHAH, Keyur C. et al.	
	208	20080262798		2008-10-23	KIM, Eun Ah et al.	
	209	20100103820		2010-04-29	FULLER, Randy et al.	
	210	20100153781		2010-06-17	HANNA, Stephen R.	
	211	20120029718		2012-02-02	DAVIS, Edward L.	
	212	20110241624		2011-10-06	PARK, Jun-seok et al.	
	213	20090307746		2009-12-10	DI, Jinwen et al.	
	214	20050009499		2005-01-13	KOSTER, Karl	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625
	Filing Date		2015-03-30
	First Named Inventor	Raleigh	
	Art Unit	2642	
	Examiner Name	not yet assigned	
	Attorney Docket Number	RALEP032C1C2	

	215	20010053694		2001-12-20	IGARASHI, Yoichiro et al.	
	216	20100041364		2010-02-18	LOTT, Robert Wayne et al.	
	217	20100027469		2010-02-04	GURAJALA, Ravindra Babu et al.	
	218	20090299857		2009-12-03	BRUBAKER, Curtis M.	
	219	20080051076		2008-02-28	O'Shaughnessy, John et al.	
	220	20080313730		2008-12-18	Iftimie, Sorin et al.	
	221	20110173678		2011-07-14	KAIPPALLIMALIL, John et al.	
	222	20080235511		2008-09-25	O'BRIEN, William G. et al.	
	223	20080240373		2008-10-02	WILHELM, Robert D.	
	224	20100027559		2010-02-04	LIN, Hung-Ming et al.	
	225	20020116338		2002-08-22	GONTHIER, Jean-Charles et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625
	Filing Date		2015-03-30
	First Named Inventor	Raleigh	
	Art Unit	2642	
	Examiner Name	not yet assigned	
	Attorney Docket Number	RALEP032C1C2	

	226	20070061878		2007-03-15	HAGIU, Costin et al. et al.	
	227	20100020822		2010-01-28	ZERILLO, Anthony J. et al.	
	228	20040203755		2004-10-14	BRUNET, Jeffrey et al.	
	229	20090172077		2009-07-02	ROXBURGH, David et al.	
	230	20080120668		2008-05-22	Yau, Frank Chuen-Foo	
	231	20030171112		2003-09-11	Lupper, Alfred et al.	
	232	20070300252		2007-12-27	Acharya, Swarup et al.	
	233	20050007993		2005-01-13	Chambers, Mahdi et al.	
	234	20020164983		2002-11-07	Raviv, Li-On et al.	
	235	20070280453		2007-12-06	Kelley, Sean S.	
	236	20100241544		2010-09-23	Benson, Dan et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625
	Filing Date		2015-03-30
	First Named Inventor	Raleigh	
	Art Unit	2642	
	Examiner Name	not yet assigned	
	Attorney Docket Number	RALEP032C1C2	

	237	20090157792		2009-06-18	Fiatal, Trevor	
	238	20070109983		2007-05-17	Shankar, Rohit et al.	
	239	20020049074		2002-04-25	Eisinger, Bernd et al.	
	240	20020161601		2002-10-31	Nauer, Bernhard et al.	
	241	20040132427		2004-07-08	Lee, Wan-Yeon et al.	
	242	20060068796		2006-03-30	Millen, Stephanie L. et al.	
	243	20010048738		2001-12-06	Baniak, Paul G. et al.	
	244	20070033197		2007-02-08	Scherzer, Shimon et al.	
	245	20110013569		2011-01-20	Scherzer, Shimon et al.	
	246	20110159818		2011-06-30	Scherzer, Shimon et al.	
	247	20120020296		2012-01-26	Scherzer, Shimon et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	14673625
	Filing Date	2015-03-30
	First Named Inventor	Raleigh
	Art Unit	2642
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1C2

	248	20120196644		2012-08-02	Scherzer, Shimon et al.	
	249	20120238287		2012-09-20	Scherzer, Shimon	
	250	20130058274		2013-03-07	Scherzer, Shimon et al.	
	251	20130084835		2013-04-04	Scherzer, Shimon et al.	
	252	20090005000		2009-01-01	Baker, Matthew et al.	
	253	20090006116		2009-01-01	Baker, Matthew et al.	
	254	20090006200		2009-01-01	Baker, Matthew et al.	
	255	20110081881		2011-04-07	Baker, Matthew Donald et al.	
	256	20110082790		2011-04-07	Baker, Matthew Donald et al.	
	257	20130029653		2013-01-31	Baker, Matthew Donald et al.	
	258	20130065555		2013-03-14	Baker, Matthew Donald et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625
	Filing Date		2015-03-30
	First Named Inventor	Raleigh	
	Art Unit	2642	
	Examiner Name	not yet assigned	
	Attorney Docket Number	RALEP032C1C2	

	259	20120155296		2012-06-21	Kashanian, Nematolah	
	260	20120330792		2012-12-27	Kashanian, Nematolah	
	261	20130030960		2013-01-31	Kashanian, Nematolah	
	262	20130095787		2013-04-18	Kashanian, Nematolah	
	263	20130117140		2013-05-09	Kashanian, Nematolah	
	264	20130183937		2013-07-18	Neal, Daniel John et al.	
	265	20060135144		2006-06-22	Jothipragasam, Premkumar	
	266	20080089295		2008-04-17	Keeler, James D. et al.	
	267	20080022354		2008-01-24	Grewal, Karanvir et al.	
	268	20040102182		2004-05-27	Reith, Lothar et al.	
	269	20030233332		2003-12-18	Keeler, James D. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	14673625
	Filing Date	2015-03-30
	First Named Inventor	Raleigh
	Art Unit	2642
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1C2

	270	20080250053		2008-10-09	Aaltonen, Janne et al.	
	271	20110195700		2011-08-11	Kukuchka, Robert et al.	
	272	20070155365		2007-07-05	Kim, Sung-Jun et al.	
	273	20130144789		2013-06-06	Aaltonen, Janne et al.	
	274	20100131584		2010-05-27	Johnson, William J.	
	275	20100080202		2010-04-01	Hanson, Mark	
	276	20070147324		2007-06-28	McGary, Faith	
	277	20130024914		2013-01-24	Ahmed, Shahid et al.	
	278	20130103376		2013-04-25	Gaddam, Venkat et al.	
	279	20130111572		2013-05-02	Gaddam, Venkat et al.	
	280	20130117382		2013-05-09	Gaddam, Venkat et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625	
	Filing Date		2015-03-30	
	First Named Inventor	Raleigh		
	Art Unit	2642		
	Examiner Name	not yet assigned		
	Attorney Docket Number	RALEP032C1C2		

	281	20130149994		2013-06-13	Gaddam, Venkat et al.	
	282	20070168499		2007-07-19	Chu, Jing-Long	
	283	20070025301		2007-02-01	Petersson, Justus et al.	
	284	20070140145		2007-06-21	Kumar, Surender et al.	
	285	20080120129		2008-05-22	Seubert, Michael et al.	
	286	20060174035		2006-08-03	Tufail, Mudassir	
	287	20110264923		2011-10-27	Kocher, Paul C. et al.	
	288	20080201266		2008-08-21	Chua, Huina et al.	
	289	20060156398		2006-07-13	Ross, Alan D. et al.	
	290	20060173959		2006-08-03	McKelvie, Samuel J. et al.	
	291	20100284327		2010-11-11	Miklos, Gyorgy	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625	
	Filing Date		2015-03-30	
	First Named Inventor	Raleigh		
	Art Unit	2642		
	Examiner Name	not yet assigned		
	Attorney Docket Number	RALEP032C1C2		

	292	20070033194		2007-02-08	Srinivas, Davanum M. et al.	
	293	20050079863		2005-04-14	Macaluso, Anthony G.	
	294	20060114832		2006-06-01	Hamilton, Thomas E. et al.	
	295	20040225898		2004-11-11	Frost, D. Gabriel et al.	
	296	20080070550		2008-03-20	Hose, David Alan	
	297	20110019574		2011-01-27	Malomsoky, Szaboles et al.	
	298	20030188117		2003-10-02	Yoshino, Kenji et al.	
	299	20040255145		2004-12-16	Chow, Jerry	
	300	20050055595		2005-03-10	Frazer, Mark et la.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add								
FOREIGN PATENT DOCUMENTS								Remove
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ² j	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625	
	Filing Date		2015-03-30	
	First Named Inventor	Raleigh		
	Art Unit	2642		
	Examiner Name	not yet assigned		
	Attorney Docket Number	RALEP032C1C2		

	1							☐
--	---	--	--	--	--	--	--	--------------------------

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

NON-PATENT LITERATURE DOCUMENTS								Remove
--	--	--	--	--	--	--	--	---------------

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

	1		☐
--	---	--	--------------------------

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

EXAMINER SIGNATURE			
---------------------------	--	--	--

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625
	Filing Date		2015-03-30
	First Named Inventor	Raleigh	
	Art Unit	2642	
	Examiner Name	not yet assigned	
	Attorney Docket Number	RALEP032C1C2	

CERTIFICATION STATEMENT

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

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

OR

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

☐ See attached certification statement.

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

☒ None

SIGNATURE

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

Signature	/James E. Harris/	Date (YYYY-MM-DD)	2015-04-29
Name/Print	James E. Harris	Registration Number	40013

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

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625	
	Filing Date		2015-03-30	
	First Named Inventor	Raleigh		
	Art Unit	2642		
	Examiner Name	not yet assigned		
	Attorney Docket Number	RALEP032C1C2		

U.S. PATENTS							Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	
	1						
If you wish to add additional U.S. Patent citation information please click the Add button.							Add
U.S. PATENT APPLICATION PUBLICATIONS							Remove
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	
	1	20070259656		2007-11-08	Jeong, Jong Woo		
	2	20080263348		2008-10-23	Zaltsman, Etai et al.		
	3	20080313315		2008-12-18	Karaoguz, Jeyhan et al.		
	4	20090282127		2009-11-12	LeBlanc, Michael et al.		
	5	20100167696		2010-07-01	Smith, Christopher David et al.		

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625
	Filing Date		2015-03-30
	First Named Inventor	Raleigh	
	Art Unit	2642	
	Examiner Name	not yet assigned	
	Attorney Docket Number	RALEP032C1C2	

	6	20030188006		2003-10-02	Bard, Steven R.	
	7	20060160536		2006-07-20	Chou, Joey	
	8	20060168128		2006-07-27	Sistla, Amber et al.	
	9	20040203833		2004-10-14	Rathunde, Dale F. et al.	
	10	20050186948		2005-08-25	Gallagher, Michael D. et al.	
	11	20070147317		2007-06-28	Smith, Brian K. et al.	
	12	20080270212		2008-10-30	Blight, Jeffrey et al.	
	13	20080056273		2008-03-06	Pelletier, Ghyslain et al.	
	14	20110110309		2011-05-12	Bennett, James D.	
	15	20100030890		2010-02-04	Dutta, Satadip et al.	
	16	20110238545		2011-09-29	Fanaian, Nabil Ruh et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625	
	Filing Date		2015-03-30	
	First Named Inventor	Raleigh		
	Art Unit	2642		
	Examiner Name	not yet assigned		
	Attorney Docket Number	RALEP032C1C2		

	17	20080025230		2008-01-31	Patel, Alpesh et al.	
	18	20040170191		2004-09-02	Guo, Zihua et al.	
	19	20020188732		2002-12-12	Buckman, Charles R. et al.	
	20	20080034419		2008-02-07	Mullick, Amarnath et al.	
	21	20080010379		2008-01-10	Zhao, Hang	
	22	20080139210		2008-06-12	Gisby, Doug et al.	
	23	20040243992		2004-12-02	Gustafson, James P. et al.	
	24	20070226775		2007-09-27	Andreasen, Flemming Stig et al.	
	25	20100235329		2010-09-16	Koren, David et al	
	26	20090254857		2009-10-08	Romine, Christopher et al.	
	27	20120101952		2012-04-26	Raleigh, Gregory G. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625	
	Filing Date		2015-03-30	
	First Named Inventor	Raleigh		
	Art Unit	2642		
	Examiner Name	not yet assigned		
	Attorney Docket Number	RALEP032C1C2		

	28	20080166993		2008-07-10	Gautier et al.	
	29	20040137890		2004-07-15	Kalke, Catherine	
	30	20070143824		2007-06-21	Shahbazi, Majid	
	31	20070266422		2007-11-15	Germano et al.	
	32	20090044185		2009-02-12	Krivopaltsev, Eugene	
	33	20040039792		2004-02-26	Nakanishi, Tomoaki	
	34	20050075115		2005-04-07	Corneille et al.	
	35	20050239447		2005-10-27	Holzman et al.	
	36	20070213054		2007-09-13	Han, Seung-Wook	
	37	20080032715		2008-02-07	Jia et al.	
	38	20090163173		2009-06-25	Williams, Timothy D.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625	
	Filing Date		2015-03-30	
	First Named Inventor	Raleigh		
	Art Unit	2642		
	Examiner Name	not yet assigned		
	Attorney Docket Number	RALEP032C1C2		

	39	20100075666		2010-03-25	Garner, Neil Robert	
	40	20080293395		2008-11-27	Matthews, Ajit et al.	
	41	20050245241		2005-11-03	Durand, Terry et al.	
	42	20080125079		2008-05-29	O'Neil, Douglas et al.	
	43	20050135264		2005-06-23	Popoff, Jeff et al.	
	44	20070165630		2007-07-19	Rasanen, Jorma	
	45	20100287599		2010-11-11	HE, Xianhui	
	46	20070060200		2007-03-15	Boris et al.	
	47	20060030306		2006-02-09	Kuhn, Brian Gerald	
	48	20060035631		2006-02-16	White et al.	
	49	20060206709		2006-09-14	Labrou et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625	
	Filing Date		2015-03-30	
	First Named Inventor	Raleigh		
	Art Unit	2642		
	Examiner Name	not yet assigned		
	Attorney Docket Number	RALEP032C1C2		

	50	20090046707		2009-02-19	Smires et al.	
	51	20100311402		2010-12-09	Srinivasan et al.	
	52	20110277019		2011-11-10	Pritchard Jr., John Russell	
	53	20050250536		2005-11-10	Deng et al.	
	54	20070192460		2007-08-16	Choi et al.	
	55	20080080457		2008-04-03	Cole, Terry L.	
	56	20090049518		2009-02-19	Roman et al.	
	57	20100248719		2010-09-30	Scholaert, Hugh	

If you wish to add additional U.S. Published Application citation information please click the Add button. [Add](#)

FOREIGN PATENT DOCUMENTS								Remove
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ² j	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1	1310401A	CN		2000-02-22	Wang, Di Xing		☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625	
	Filing Date		2015-03-30	
	First Named Inventor	Raleigh		
	Art Unit	2642		
	Examiner Name	not yet assigned		
	Attorney Docket Number	RALEP032C1C2		

	2	1878160A	CN		2006-12-13	Jiang, Yong		☐
	3	2012047275	WO		2012-04-19	Raleigh, Gregory G. et al.		☐
	4	101127988A	CN		2008-02-20	ZTE Corporation		☐
	5	1503548 A1	EP		2005-02-02	FG Microtec GmbH		☐
	6	3148713 B2	JP		2001-03-26	ATR Kankyo Tekio Tsushin Kenkyusho		☐
	7	2009-218773	JP		2009-09-24	Advanced Telecommunication Research Institute Inte		☐
	8	2006093961	WO		2006-09-08	Kyocera Wireless Corp.		☐
	9	2007-318354	JP		2007-12-06	Fujitsu Ten Ltd.		☐
	10	2007126352	WO		2007-11-08	Telefonaktiebolaget LM Ericsson		☐
	11	2009-212707	JP		2009-09-17	Fujitsu Ltd.		☐
	12	2008-301121	JP		2008-12-11	Kyocera Corp.		☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625
	Filing Date		2015-03-30
	First Named Inventor	Raleigh	
	Art Unit	2642	
	Examiner Name	not yet assigned	
	Attorney Docket Number	RALEP032C1C2	

If you wish to add additional Foreign Patent Document citation information please click the Add button				Add
NON-PATENT LITERATURE DOCUMENTS				Remove
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵	
	1	Dixon et al., "Triple Play Digital Services: Comcast and Verizon (Digital Phone, Television, and Internet), August 2007	☐	
If you wish to add additional non-patent literature document citation information please click the Add button				
EXAMINER SIGNATURE				
Examiner Signature		Date Considered		
*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.				
<small> ¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached. </small>				

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	14673625
	Filing Date	2015-03-30
	First Named Inventor	Raleigh
	Art Unit	2642
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1C2

CERTIFICATION STATEMENT

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

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

OR

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

☐ See attached certification statement.

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

☒ None

SIGNATURE

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

Signature	/James E. Harris/	Date (YYYY-MM-DD)	2015-04-29
Name/Print	James E. Harris	Registration Number	40013

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

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.

H04M 1/00 (2006.01)

H04M 1/21 (2006.01)

G04G 5/00 (2006.01)



[12] 发明专利申请公开说明书

[21] 申请号 200410099356.1

[43] 公开日 2006 年 7 月 12 日

[11] 公开号 CN 1801829A

[22] 申请日 2004.12.30

[21] 申请号 200410099356.1

[71] 申请人 昆达电脑科技(昆山)有限公司

地址 215300 江苏省昆山市昆山出口加工区

[72] 发明人 许世法

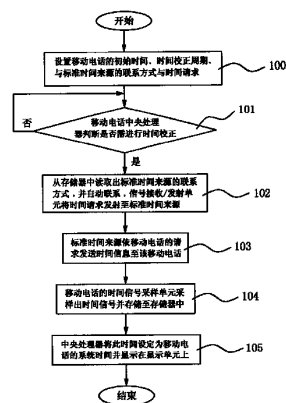
权利要求书 1 页 说明书 3 页 附图 2 页

[54] 发明名称

移动电话时间自动校正方法

[57] 摘要

本发明揭示一种移动电话时间自动校正方法，该移动电话包括接收信号与发射信号的信号接收/发射单元、从接收到的信号中采样出时间信号的时间信号采样单元、存储时间信息与设定信息的存储器、中央处理器及显示单元，该方法主要通过设置移动电话的初始时间、时间校正周期、与标准时间来源的联系方式与时间请求，当需进行时间校正时，该移动电话自动将时间请求发送至标准时间来源，并取得标准时间，而后将该标准时间设定为移动电话的系统时间，从而令移动电话使用一般的石英振荡器亦可满足较高的时间精度，从而利于降低移动电话成本，并不影响移动电话的体积。



1、一种移动电话时间自动校正方法，该移动电话包括接收信号与发射信号的信号接收/发射单元、从接收到的信号中采样出时间信息的时间信号采样单元、存储时间信息与设定信息的存储器、中央处理器及显示单元，其特征在于该时间自动校正方法包括如下步骤：

设置移动电话的初始时间、时间校正周期、与标准时间来源的联系方式与时间请求，并将此些数据存储于移动电话的存储器中；

移动电话中央处理器判断是否需进行时间校正，如否则继续判断；

如需进行时间校正，则移动电话自动发射请求信号至标准时间来源；

标准时间来源依请求发送时间信息至该移动电话；

移动电话的时间信号采样单元采样出时间信号并存储至存储器中；

中央处理器将该时间设定为移动电话的系统时间。

2、如权利要求1所述的移动电话时间自动校正方法，其特征在于：该方法还包括将移动电话的系统时间显示在显示单元上的步骤。

3、如权利要求1或2所述的移动电话时间自动校正方法，其特征在于：该标准时间来源为声询台。

4、如权利要求3所述的移动电话时间自动校正方法，其特征在于：该移动电话内设有语音产生单元与语音辨识单元，行动电话中预先设有的时间询问请求为询问时间的声音信号。

5、如权利要求4所述的移动电话时间自动校正方法，其特征在于：当移动电话呼叫声询台后，移动电话通过语音产生单元提出时间询问请求。

6、如权利要求5所述的移动电话时间自动校正方法，其特征在于：声询台依请求发送的时间信号至移动电话，该信号经过移动电话的语音产生单元发出，并且移动电话的语音辨识单元采样出时间信号并存储至存储器中。

7、如权利要求1或2所述的移动电话时间自动校正方法，其特征在于：该标准时间来源为移动电话服务供应网络。

8、如权利要求7所述的移动电话时间自动校正方法，其特征在于：该移动电话中预先设有的时间询问请求为询问时间的短信。

9、如权利要求8所述的移动电话时间自动校正方法，其特征在于：移动电话从存储器中读取标准时间来源的联系方式，并自动联系，信号接收/发射单元将询问时间的短信发射至移动电话服务供应网络。

10、如权利要求9所述的移动电话时间自动校正方法，其特征在于：移动电话服务供应网络以短信形式发送标准时间至该移动电话，移动电话的时间信号采样单元采样出时间信号并存储至存储器中。

移动电话时间自动校正方法

【技术领域】

本发明有关一种时间自动校正方法，尤其是应用于移动电话中的时间自动校正方法。

【背景技术】

随着通讯技术的发展，具有时钟功能的移动电话普及率日益提高，其中时钟的准确性在移动电话的实际使用中的重要性日益提高，如现在的备忘录、闹钟等功能的实现均依靠时钟的准确性。而目前时钟的精确性主要取决于时钟电路中使用的振荡器的精度，而目前多使用普通的石英振荡器，其频率误差在 $\pm 20-50\text{ppm}$ （百万分之20-50），如以 20ppm 的误差为例，每天产生的时间误差将为1.728秒，而一年的时间误差则累积为630.72秒，将达10.5分钟之久，故会给使用者带来一定的不便。

针对该问题，业界采取使用较高精度的石英振荡器或使用微调电容或类似的元件对普通振荡器的频率进行微调的二种方法。第一种方法的不足在于：即使使用高精度的石英振荡器，振荡电路的负载电容依存在差别，所以实际上不可能得到与石英振荡器相同的高精度，因此无论使用多么昂贵的元件，也不可能得到高准确度的时间。第二种方法的不足之处在于：虽然使用一般的石英振荡器成本不会太高，但是需要频率调节装置，如微调电容器，这引起了部件成本增加和令频率调节过程较为繁琐的缺陷，特别是元件数量的增加会导致对移动电话小型化的妨碍。

有鉴于此，实有必要提供一种既不会增加移动电话成本，且不影响移动电话体积的移动电话时间自动校正方法。

【发明内容】

本发明目的在于提供一种既不会增加移动电话成本，且不影响移动电话体积的移动电话时间自动校正方法。

为实现上述目的，实施本发明的移动电话包括接收信号与发射信号的信号接收/发射单元、从接收到的信号中采样出时间信号的时间信号采样单元、存储时间信息与设定信息的存储器、中央处理器及显示单元，本发明移动电话时间的自动校正方法包括以下步骤：

设置移动电话的初始时间、时间校正周期、与标准时间来源的联系方式与时间请求，并将此些数据存储于移动电话的存储器中；

移动电话中央处理器判断是否需进行时间校正，如否则继续判断；

如需进行时间校正，则移动电话自动发射请求信号至标准时间来源；

标准时间来源依请求发送时间信息至该移动电话；

移动电话的时间信号采样单元采样出时间信号并存储至存储器中；

中央处理器将该时间设定为移动电话的系统时间。

较佳地，该标准时间来源为声询台，移动电话通过呼叫声询台提出时间请求，并且声询台发送的时间信号至移动电话，该信号经过移动电话的语音产生单元发出，并且移动电话的语音辨识单元采样出时间信号并存储至存储器中。

较佳地，该标准时间来源为移动电话服务供应网络，移动电话通过发送短信至移动电话服务供应网络提出时间请求，并且移动电话服务供应网络发送标准时间至该移动电话，移动电话的时间信号采样单元采样出时间信号并存储至存储器中。

与现有技术相比较，本发明利用移动电话联系外部的标准时间来源定期对移动电话的系统时间进行校正，从而可定期将时间误差及时消除，因此即使移动电话的时钟电路采用一般的石英振荡器，也不会给使用者造成不便，如此不需采用较为昂贵的石英振荡器或其它的微调电容器等，因此不会增加移动电话的成本，并且也不会对移动电话的小型化形成妨碍。

为对本发明的目的、构造特征及其功能有进一步的了解，兹配合附图详细说明如下：

【附图说明】

图 1 为本发明移动电话的组成框图。

图 2 为本发明移动电话时间自动校正方法的流程图。

【具体实施方式】

以下将结合图 1 与图 2 对本发明的进行详细说明，在以下说明中是以行动电话为例进行说明，该技术领域的普通技术人员应可理解，实施本发明的电子装置并不局限于移动电话，如具有无线通信功能的智能电话及个人数字助理（PDA）均可应用本发明。

请参阅图 1 所示，实施本发明的移动电话 1 包括：

信号接收/发射单元 10，用于发射与接收无线通讯信号；

时间信号采样单元 11，与信号接收/发射单元 10 耦接，用以将接收信号中的时间信号采样出；

存储器 12，用以存储移动电话 1 的系统程序、时间校正周期、标准时间来源的联系方式及移动电话 1 的最初设定时间；

显示单元 14，用以显示移动电话 1 的系统时间；

中央处理器 13，与上述各单元耦接，用以控制以上不同单元的运作。

请参阅图 2 所示，本发明的移动电话 1 的时间自动校正方法包括以下步骤

:

设置移动电话的初始时间、时间校正周期、与标准时间来源的联系方式与时间请求，并将此些数据存储于移动电话 1 的存储器 12 中，其中时间校正周期可设定为一周或一个月，而标准时间来源可为声询台，如中国大陆的 114 查询台或中国台湾的 104 报时台（步骤 100）；

移动电话 1 中央处理器 13 判断是否需进行时间校正，即从最初设定的时间起，是否经过设定的时间校正周期的时间，如否则继续判断（步骤 101）；

如需进行时间校正，即从最初设定的时间起，已经过设定的时间校正周期的时间，则移动电话 1 的中央处理器 13 执行自动联系功能，即从存储器 12 中读取标准时间来源的联系方式，并自动联系，信号接收/发射单元 10 将时间请求发射至标准时间来源（步骤 102）；

标准时间来源依移动电话 1 的请求发送时间信息至该移动电话 1（步骤 103）；

移动电话 1 的时间信号采样单元 11 采样出时间信号并存储至存储器 12 中（步骤 104）；

中央处理器 13 将此时间设定为移动电话 1 的系统时间并显示在显示单元 14 上（步骤 105）。

较佳地，当该标准时间来源为声询台时，而移动电话 1 内设有语音产生单元与语音辨识单元，步骤 100 中包括预先在移动电话 1 内设定时间询问请求，如可为询问时间的声音信号，步骤 102 具体包括以下步骤：当移动电话 1 呼叫声询台后，移动电话 1 通过语音产生单元提出时间询问请求，而步骤 103 相应包括以下步骤：声询台依次请求发送的时间信号至移动电话 1，该信号经过移动电话 1 的语音产生单元发出，并且移动电话 1 的语音辨识单元采样出时间信号并存储至存储器 12 中。

较佳地，当该标准时间来源为移动电话服务供应网络，步骤 100 中包括预先在移动电话 1 内设定时间询问请求，如可为询问时间的短信，步骤 102 具体包括以下步骤：移动电话 1 从存储器 12 中读取标准时间来源的联系方式，并自动联系，信号接收/发射单元 10 将询问时间的短信发射至移动电话服务供应网络，而步骤 103 相应包括以下步骤：移动电话服务供应网络以短信形式发送标准时间至该移动电话 1，移动电话的时间信号采样单元 11 采样出时间信号并存储至存储器 12 中。

与现有技术相比较，本发明利用移动电话联系外部的标准时间来源定期对移动电话的系统时间进行校正，从而可定期将时间误差及时消除，因此即使移动电话的时钟电路采用一般的石英振荡器，也不会给使用者造成不便，如此不需采用较为昂贵的石英振荡器或其它的微调电容器等，因此不会增加移动电话的成本，并且也不会对移动电话的小型化形成妨碍。

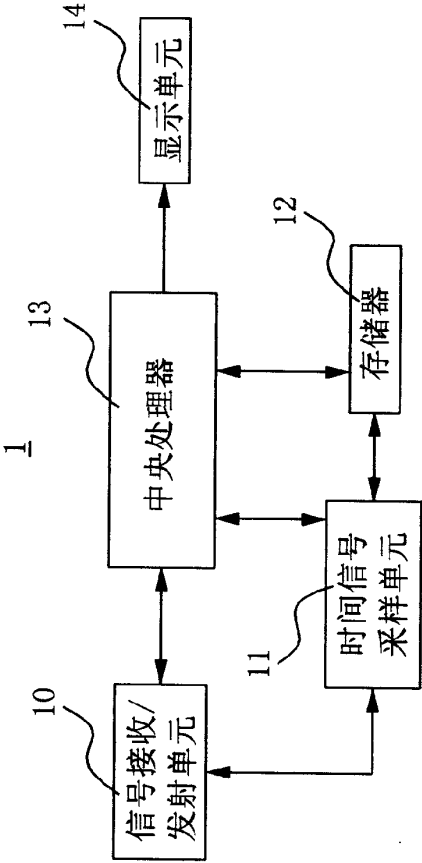


图1

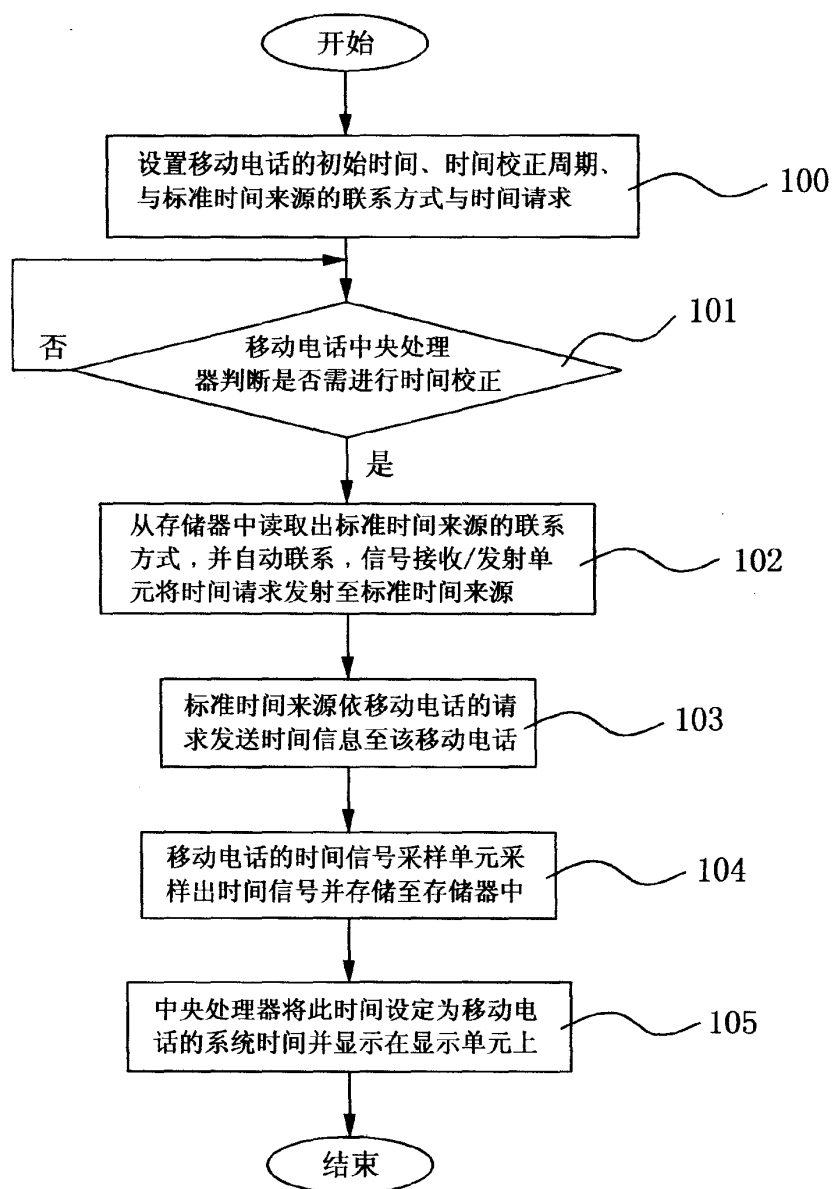


图2

Sign in

Patents

English

Chinese

Find prior art

Discuss this application

View PDF

Download PDF



Mobile phone time automatic correction method

CN 1801829 A

ABSTRACT

Said invention provides a mobile telephone time autocorrection method. It contains signal reception / transmitting unit, time signal sampling unit memory unit, central processing unit and display unit, said method mainly setting mobile telephone initial time, time adjustment cycle, and standard time source connection mode and time request, when need proceeding time correction, said mobile telephone automatically transmitting time request to standard time source and taking standard time then configuring said standard time as system time of mobile telephone to reach higher time precision by using normal quartz oscillator.

Publication number	CN1801829 A
Publication type	Application
Application number	CN 200410099356
Publication date	Jul 12, 2006
Filing date	Dec 30, 2004
Priority date	Dec 30, 2004
Inventors	许世法
Applicant	昆山电脑科技(昆山)有限公司
Export Citation	BiBTeX, EndNote, RefMan
Classifications (3), Legal Events (3)	
External Links: SIPO, Espacenet	

DESCRIPTION translated from Chinese

Mobile phone time automatic calibration method

TECHNICAL FIELD The present invention relates to a method of automatic correction of the time, especially for mobile phones in the automatic time correction method.

BACKGROUND OF THE INVENTION With the development of communication technology, mobile phone penetration has a clock function increasing importance of the accuracy of the clock and the actual use of mobile phones increasing, as now realize memo, alarm clock and other functions both rely on the accuracy of the clock. At present, the accuracy of the clock depends on the accuracy of the clock oscillator used in the circuit, and the current multi-use ordinary quartz oscillator frequency error at $\pm 20\text{-}50\text{ppm}$ ($20\text{-}50\text{ ppm}$), as to 20ppm error, for example, the time error will be generated every 1.728 seconds, while the one-year time error accumulation is 630.72 seconds, to reach 10.5 minutes long, it will bring some inconvenience to users.

To solve this problem, the industry adopted the use of high precision quartz oscillator or use a trimmer capacitor or similar elements of the common oscillator frequency tuning of the two methods. The first method is inadequate: even when using high-precision quartz oscillator, the oscillation circuit of the load capacitance according to the presence of differences, so this is actually impossible to obtain the same high-precision crystal oscillator, and therefore regardless of 11 more expensive components, it is impossible to obtain a highly accurate time. Deficiencies of the second method comprising: using a general quartz oscillator although cost is not too high, but requires a frequency adjustment means, such as a trimmer capacitor, causing an increase in component cost and make the process more complicated frequency adjusting defects, particularly is an increase in the number of components will result in miniaturization of mobile phones interfere.

In view of this, there is a need to provide both a mobile phone without increasing the cost, and does not affect the time the mobile phone automatic calibration method for a mobile phone volume.

SUMMARY OF THE INVENTION The present invention aims to provide a mobile phone without increasing either the cost, and does not affect the time the mobile phone automatic calibration method for a mobile phone volume.

CLAIMS (10) translated from Chinese

A mobile phone automatic time correction method, the mobile phone includes a signal receiving / transmitting unit receives the signal and the transmitted signal, the received signal samples from the time information in the time signal sampling unit that stores the time information and the setting information memory, the central processor and display unit, characterized in that the automatic time correction method comprising the steps of: setting an initial time a mobile phone, the correction time period, and the contacts for the source of the standard time and time request, and such data is stored in memory of the mobile phone; mobile phone to determine whether the need for a central processor time correction, otherwise continue as judge; For the time correction, the mobile phone automatically transmit a request signal to the standard time source; transmission time information source standard time upon request to the mobile phone; mobile phone time signal sampling means sampling and storing the time signal into the memory; central processing time is set to the system time of the mobile phone.

The mobile phone automatic time correction method according to claim 1, characterized in that: the method further comprises the mobile telephone system time is displayed on the display unit in step.

Automatic time correction method for a mobile phone according to claim 1 or claim 2, wherein: the standard time for the sound source exercise station.

The mobile phone automatic time correction method according to claim 3, characterized in that: the mobile phone equipped with a voice generating unit and a voice recognition unit, the mobile phone has to call a pre-request signal into sound inquiry time.

The mobile phone automatic time correction method according to claim 4, wherein: when the mobile telephone calling sound exercise station, mobile phone unit made by voice time inquiry request is generated.

Identification of the mobile phone and the speech sound exercise station by a time request signal to the mobile phone, the mobile phone voice signal through generating unit issued. The mobile phone automatic time correction method according to claim 5, characterized in that means sampling and storing the time signal into the memory.

To achieve the above object, a mobile phone embodiment of the present invention includes a signal receiving / transmitting unit receives the signal and the transmitted signal, a time signal sampling unit from the received signal, the memory storing the time information and setting information, Automatic time correction method for a mobile phone central processor and a display unit, the present invention comprises the steps of: setting the mobile phone of the initial time, the correction time period, and the contacts for the source of the standard time and time request, and such data stored in the mobile phone memory; the central processor determines whether the mobile phone need to be time correction, otherwise continue as judge;

For a time correction, the mobile phone automatically transmit a request signal to the standard time source; Standard Time time information sources according to the request of the mobile phone; mobile phone signal sampling unit time sampling the time signal and storage to memory; a central processing The time is set to a mobile telephone system time.

Preferably, the standard time for the sound source exercise station, mobile telephone inquiry station calling sound made by the time the request, and the time the signal transmitted by the acoustic exercise station to the mobile phone, the signal through the mobile phone voice generating unit is issued, and the mobile phone sampling the speech recognition unit time signal and stores into the memory.

Preferably, the standard time source for mobile phone service provider networks, mobile phone by sending an SMS to a mobile phone service network in time to make the request, and the mobile phone service provider network in standard time sent to the mobile phone, mobile phone time signal sampling means sampling the time signal and stores into the memory.

Compared with the prior art, the present invention is the use of a mobile phone outside the regular standard time source mobile phone system time is corrected, thereby periodically time error promptly eliminated so that even if the mobile phone is generally of a clock circuit using a quartz oscillator nor will cause inconvenience to the user, so the need to adopt a more expensive quartz oscillator or other fine-tuning capacitor, etc., it will not increase the cost of mobile phones, and nor will it interfere with the formation of the miniaturization of mobile phones.

For the purposes of this invention, the structural features and functions have a better understanding, with a detailed description of the drawings hereby follows: BRIEF DESCRIPTION Figure 1 is a block diagram of the invention of mobile phones.

Figure 2 is a schematic flow chart of a mobile phone automatic time correction method.

[DETAILED DESCRIPTION] Hereinafter, in conjunction with Figure 1 and Figure 2 the present invention will be described in detail, based on the mobile phone as an example in the following description, one of ordinary skill in the art will appreciate, electronic embodiment of the electronic apparatus of the present invention is not limited to a mobile phone, having a wireless communication function such as smart phones and personal digital assistants (PDA) can be applied to the present invention.

See Figure 1, the embodiment of the present invention, a mobile phone 1 includes: a signal receiving / transmitting unit 10 for transmitting and receiving wireless communication signals; time signal sampling unit 11, and the signal receiving / transmitting unit 10 is coupled to the received signal in the time signal samples; a memory 12 for storing a system program of the mobile telephone, the time correction period, the standard time source contacts and the mobile phone 1 of the first setting time; a display unit 14 for displaying the system time of the mobile phone 1; central processor 13, and each of the unit is coupled to the control over the operation of the different units.

See Figure 2, the mobile phone 1 of the present invention, the automatic time correction method comprising the steps of:

Setting the mobile phone of the initial time, the time correction cycle, and the standard time source contact and time of the request, and such data is stored in a memory of the mobile phone 12, wherein the time correction period can be set to one week or one month, The standard time for the sound source can exercise stations, a query such as 114 Chinese mainland China Taiwan 104 repeater stations or station (step 100); mobile phone a central processor 13 determines whether the need for time correction, that is, from the initial set time Since, if after a set time correction cycle time, as otherwise continue to determine (step 101); For the time correction, that is, from the initial set time has been set time correction cycle time, the move The central processor 13 performs an automatic telephone contact function, reads the standard time source contacts from the memory 12, and automatically links, signal receiving / transmitting unit 10 transmit a request to the time the standard time source (step 102); standard time sent by the source of the mobile phone 1 requests the time information to the mobile phone 1 (step 103); time signal sampling unit 11 of the mobile phone 1 and the sampling time for

The mobile phone automatic time correction method according to claim 1 or claim 2, wherein: the standard time source for cellular phone service network.

Mobile phone time automatic calibration method according to claim 7, characterized in that: the mobile phone in advance of the time provided for the inquiry message query request time.

The mobile phone automatic time correction method according to claim 8, wherein: the mobile phone reads from the memory the standard time source contact, and automatic contact, signal receiving / transmitting unit transmitting the inquiry message time Mobile phone service providers to network in.

Mobile phone time automatic calibration method as claimed in claim 9, wherein: the mobile phone service provider network in order to send a message in the form of standard time to the mobile phone, mobile phone signal sampling unit time sampling the time signal and stores to memory.

=====

the signal stored to the memory 12 (step 104); a central processor 13 This time is set to the system time of the mobile phone 1 and displayed on (step 105) the display unit 14.

Preferably, when the standard time for the sound source exercise station, and the mobile phone 1 is equipped with a voice generating unit and a voice recognition unit, step 100 includes a pre-set time in the mobile phone 1 inquiry request, such as may be inquired time sound signal, step 102 includes the following steps: When a mobile phone call sound exercise stations, a mobile phone made by voice generating unit time inquiry request, and the corresponding step 103 includes the following steps: Time sound exercise station in turn request sent signal to the mobile telephone 1, the signal through the mobile phone voice generating unit 1 to issue, and the speech recognition unit of the mobile phone 1 and the sampling time for the signal stored to the memory 12.

Preferably, the standard time when the source is a mobile telephone service provider network, step 100 comprises a pre-set time in the mobile phone 1 inquiry request, such as SMS for inquiry time, step 102 includes the following steps: the mobile phone 1 read from the memory 12 times the standard source of contact information, and automatically links the signal receiver / transmitter unit 10 will ask for time to transmit messages to the mobile phone service provider network in, while the corresponding step 103 includes the following steps: mobile phone service providers network in order to send a text message to the mobile phone standard time a mobile phone signal sampling unit 11 hours a time signal sampling and storage to memory 12.

Compared with the prior art, the present invention is the use of a mobile phone outside the regular standard time source mobile phone system time is corrected, thereby periodically time error promptly eliminated so that even if the mobile phone is generally of a clock circuit using a quartz oscillator nor will cause inconvenience to the user, so the need to adopt a more expensive quartz oscillator or other fine-tuning capacitor, etc., it will not increase the cost of mobile phones, and nor will it interfere with the formation of the miniaturization of mobile phones.

CLASSIFICATIONS

International Classification G04R20/00, H04M1/21, H04M1/00

LEGAL EVENTS

Date	Code	Event	Description
Nov 26, 2008	C02	Deemed withdrawal of patent application after publication (patent law 2001)	
Sep 6, 2006	C10	Request of examination as to substance	
Jul 12, 2006	C06	Publication	

[Google Home](#) - [Sitemap](#) - [USPTO Bulk Downloads](#) - [Privacy Policy](#) - [Terms of Service](#) - [About Google Patents](#) - [Send Feedback](#)

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.

H04M 17/00 (2006.01)

H04Q 7/22 (2006.01)

H04L 12/14 (2006.01)



[12] 发明专利申请公开说明书

[21] 申请号 200510070958.9

[43] 公开日 2006 年 11 月 22 日

[11] 公开号 CN 1867024A

[22] 申请日 2005.5.19

[21] 申请号 200510070958.9

[71] 申请人 华为技术有限公司

地址 518129 广东省深圳市龙岗区坂田华为
总部办公楼

[72] 发明人 申海 孙谦

[74] 专利代理机构 北京同达信恒知识产权代理有限公司

代理人 郭润湘

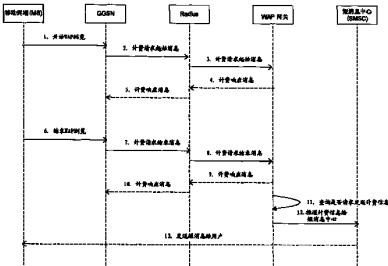
权利要求书 3 页 说明书 9 页 附图 2 页

[54] 发明名称

一种计费信息发送方法

[57] 摘要

本发明公开了一种计费信息发送方法，应用于无线应用协议(WAP)业务，该方法包括：移动终端经 WAP 网关使用 WAP 业务，WAP 网关对移动终端进行计费，WAP 网关发送计费信息给移动终端。本发明方法能实现由 WAP 网关将用户使用 WAP 业务的计费信息即时发送给用户终端，方便用户控制和使用 WAP 业务。



1、一种计费信息发送方法，应用于无线应用协议（WAP）业务，该方法包括：移动终端经 WAP 网关使用 WAP 业务，WAP 网关对移动终端进行计费，WAP 网关发送计费信息给移动终端。

2、如权利要求 1 所述的方法，其特征在于，在 WAP 网关中预先设置计费信息发送方式，在移动终端使用 WAP 业务过程中或使用 WAP 业务结束后 WAP 网关根据设置的计费信息发送方式发送计费信息给移动终端。

3、如权利要求 2 所述的方法，其特征在于，所述 WAP 网关中预先设置的计费信息发送方式与移动终端对应，在移动终端使用 WAP 业务过程中或使用 WAP 业务完成后 WAP 网关采用移动终端对应的计费信息发送方式发送计费信息给该移动终端。

4、如权利要求 2 或 3 所述的方法，其特征在于，所述计费信息发送方式为短消息发送；WAP 网关通过 WAP 推送方式发送移动终端使用 WAP 业务的计费信息给短消息中心；短消息中心以短消息方式将所述计费信息下发给移动终端。

5、如权利要求 4 所述的方法，其特征在于，所述计费信息发送方式中还包括设定的时间间隔，在移动终端使用 WAP 业务过程中，WAP 网关按所述设定的时间间隔发送所述计费信息给短消息中心。

6、如权利要求 4 所述的方法，其特征在于，所述计费信息发送方式中还包括设定的余额阈值、流量阈值或费用阈值，在移动终端使用 WAP 业务过程中，当 WAP 网关检测到预付费移动终端的余额小于设定的余额阈值、移动终端使用 WAP 业务流量超过设定的流量阈值或移动终端使用 WAP 业务费用超过设定的费用阈值时，WAP 网关发送计费信息给短消息中心。

7、如权利要求 2 或 3 所述的方法，其特征在于，所述计费信息发送方式为 WAP 网页；具体包括：在移动终端使用 WAP 业务过程中，WAP 网关为该

移动终端产生一个包含计费信息的临时 WAP 网页，并将该临时 WAP 网页的超链接地址以及超链接的显示文字插入到移动终端当前请求浏览的网页中，移动终端通过访问所述超链接地址获取计费信息；并在 WAP 业务结束后，删除所述临时 WAP 网页。

8、如权利要求 2 或 3 所述的方法，其特征在于，所述计费信息发送方式为 WAP 网页；具体包括：在移动终端使用 WAP 业务过程中，WAP 网关将指向一个即时计费单元的超链接插入到移动终端当前请求浏览的网页中，移动终端访问所述超链接时，即时计费单元从 WAP 网关中获取该移动终端的计费信息，并生成 WAP 网页返回给移动终端。

9、如权利要求 2 或 3 所述的方法，其特征在于，所述计费信息发送方式为 WAP 网页；具体包括：设定一个用于发送计费信息的固定超链接地址，当 WAP 网关检测到移动终端请求该固定超链接地址时将该移动终端的计费信息以 WAP 网页方式发送给移动终端。

10、如权利要求 9 所述的方法，其特征在于，所述固定超链接地址预置在所述移动终端中。

11、如权利要求 2 或 3 所述的方法，其特征在于，所述计费信息发送方式为 IP 数据包发送，WAP 网关接收到移动终端的计费信息请求或根据设定的时间间隔将包含计费信息的数据包按照 IP 协议格式发送给移动终端对应的 IP 地址，由移动终端显示出计费信息。

12、如权利要求 11 所述的方法，其特征在于，在移动终端 WAP 浏览器界面的固定位置显示所述计费信息。

13、如权利要求 1 所述的方法，其特征在于，当移动终端为预付费终端，还包括 WAP 网关在该移动终端请求 WAP 业务时，查询其预付费余额的步骤；若预付费余额不足，则 WAP 网关通知该移动终端，并拒绝其使用请求的 WAP 业务，否则移动终端正常使用 WAP 业务。

14、如权利要求 1 所述的方法，其特征在于，所述 WAP 业务为 WAP 浏览

类业务或 WAP 流媒体业务。

15、如权利要求 1 所述的方法，其特征在于，所述计费信息为移动终端本次使用 WAP 业务流量、累计使用 WAP 业务流量、本次使用 WAP 业务费用、累计使用 WAP 业务费用、本次业务使用时长、本次业务费率和预付费余额其中之一或任意多个的组合信息。

16、如权利要求 15 所述的方法，其特征在于，若 WAP 网关发送的计费信息包括累计使用 WAP 业务流量、累计使用 WAP 业务费用、本次业务费率或预付费余额中至少其中之一时，还包括 WAP 网关向数据业务管理平台发送请求消息，获取上述计费信息的步骤。

17、如权利要求 16 所述的方法，其特征在于，若数据业务管理平台没有保存相应请求的计费信息，则由数据业务管理平台到智能网的业务控制点（SCP）上获取。

一种计费信息发送方法

技术领域

本发明涉及无线通信领域，尤其涉及无线应用协议（Wireless Application Protocol，WAP）业务的计费信息发送方法。

背景技术

WAP技术目前已成为移动通信网络中终端访问无线信息服务的全球主要标准，也是实现现有移动数据及增值业务的技术基础。WAP浏览类业务是最普通和常用的移动数据业务，用户通过终端的浏览器查看从服务器收到的WAP网页信息，作为移动数据业务的一种基础业务，WAP浏览类业务正被越来越多的移动用户所使用并接受。另外基于WAP的移动流媒体业务，也将成为3G通信网络中的主流应用。开放移动联盟（Open Mobile Alliance，OMA）在WAP业务具体计费实现上并没有做出限定，而现有技术中也还没有一种将WAP业务计费信息即时传送给移动终端的方法。移动终端的计费信息只能在话费月结时由计费系统如BOSS对从WAP网关采集来的话单进行统计批价，然后打印出来提供给用户，而且通常还没有费用的明细记录。由于WAP网关很多情况都是按流量进行计费，这样对于预付费和后付费用户，都存在一个同样的问题：用户在使用WAP业务中或进行一次WAP业务后，不知道产生了多少流量，也不知道本月累计使用了多少流量，使得用户无法及时掌握或控制WAP业务的使用情况；特别是对于预付费用户，当预付费用完时，在用户无法事先获知的情况下WAP网关会强行中断业务，给用户使用WAP业务造成困扰。

发明内容

本发明提供一种计费信息发送方法，用以解决现有技术中存在的 WAP 业

务不能即时提供计费信息的问题。

本发明方法包括：移动终端经 WAP 网关使用 WAP 业务，WAP 网关对移动终端进行计费，WAP 网关发送计费信息给移动终端。

根据本发明的上述方法，在 WAP 网关中预先设置计费信息发送方式，在移动终端使用 WAP 业务过程中或使用 WAP 业务结束后 WAP 网关根据设置的计费信息发送方式发送计费信息给移动终端。

所述 WAP 网关中预先设置的计费信息发送方式与移动终端对应，在移动终端使用 WAP 业务过程中或使用 WAP 业务完成后 WAP 网关采用移动终端对应的计费信息发送方式发送计费信息给该移动终端。

所述计费信息发送方式为短消息发送；WAP 网关通过 WAP 推送方式发送移动终端使用 WAP 业务的计费信息给短消息中心；短消息中心以短消息方式将所述计费信息下发给移动终端。

所述计费信息发送方式中还包括设定的时间间隔，在移动终端使用 WAP 业务过程中，WAP 网关按所述设定的时间间隔发送所述计费信息给短消息中心。

所述计费信息发送方式中还包括设定的余额阈值、流量阈值或费用阈值，在移动终端使用 WAP 业务过程中，当 WAP 网关检测到预付费移动终端的余额小于设定的余额阈值、移动终端使用 WAP 业务流量超过设定的流量阈值或移动终端使用 WAP 业务费用超过设定的费用阈值时，WAP 网关发送计费信息给短消息中心。

所述计费信息发送方式为 WAP 网页；具体包括：在移动终端使用 WAP 业务过程中，WAP 网关为该移动终端产生一个包含计费信息的临时 WAP 网页，并将该临时 WAP 网页的超链接地址以及超链接的显示文字插入到移动终端当前请求浏览的网页中，移动终端通过访问所述超链接地址获取计费信息；并在 WAP 业务结束后，删除所述临时 WAP 网页。

所述计费信息发送方式为 WAP 网页；具体包括：在移动终端使用 WAP

业务过程中，WAP 网关将指向一个即时计费单元的超链接插入到移动终端当前请求浏览的网页中，移动终端访问所述超链接时，即时计费单元从 WAP 网关中获取该移动终端的计费信息，并生成 WAP 网页返回给移动终端。

所述计费信息发送方式为 WAP 网页；具体包括：设定一个用于发送计费信息的固定超链接地址，当 WAP 网关检测到移动终端请求该固定超链接地址时将该移动终端的计费信息以 WAP 网页方式发送给移动终端。

所述固定超链接地址预置在所述移动终端中。

所述计费信息发送方式为 IP 数据包发送，WAP 网关接收到移动终端的计费信息请求或根据设定的时间间隔将包含计费信息的数据包按照 IP 协议格式发送给移动终端对应的 IP 地址，由移动终端显示出计费信息。

在移动终端 WAP 浏览器界面的固定位置显示所述计费信息。

当移动终端为预付费终端，还包括 WAP 网关在该移动终端请求 WAP 业务时，查询其预付费余额的步骤；若预付费余额不足，则 WAP 网关通知该移动终端，并拒绝其使用请求的 WAP 业务，否则移动终端正常使用 WAP 业务。

所述 WAP 业务为 WAP 浏览类业务或 WAP 流媒体业务。

所述计费信息为移动终端本次使用 WAP 业务流量、累计使用 WAP 业务流量、本次使用 WAP 业务费用、累计使用 WAP 业务费用、本次业务使用时长、本次业务费率和预付费余额其中之一或任意多个的组合信息。

若 WAP 网关发送的计费信息包括累计使用 WAP 业务流量、累计使用 WAP 业务费用、本次业务费率或预付费余额中至少其中之一时，还包括 WAP 网关向数据业务管理平台发送请求消息，获取上述计费信息的步骤。

若数据业务管理平台没有保存相应请求的计费信息，则由数据业务管理平台到智能网的业务控制点（SCP）上获取。

本发明有益效果如下：

（1）本发明通过利用 WAP 网关向终端发送计费信息，实现了用户在使用 WAP 业务过程中或刚刚使用 WAP 业务完成后的时间内能够即时获取计费信

息，方便用户控制和使用 WAP 业务。

(2) 本发明提供了多种计费信息发送方式的实现方案，包括：短消息方式、WAP 网页方式和 IP 数据包方式，WAP 网关可以根据网络状况和能力选择其中至少一种计费信息发送的实现方案将计费信息即时发送给用户终端；而对于同时提供了多种计费信息发送方式的 WAP 网关，用户也可以灵活设置计费信息发送方式，充分满足用户的个性化需求和使用习惯。

(3) 本发明可以对需要 WAP 业务计费信息即时发送的用户预先进行登记，系统只对登记的用户按默认或设置的计费信息发送方式发送计费信息，在充分满足用户需求的同时，减少系统负荷。

附图说明

图 1 为计费信息下发所涉及的系统结构示意图；

图 2 为本发明实施例中 WAP 浏览业务计费过程及通过短消息下发计费信息的信令流程图；

图 3 为本发明实施例中 WAP 流媒体业务计费过程及通过短消息下发计费信息的信令流程图。

具体实施方式

本发明方法是由 WAP 网关在移动终端使用 WAP 业务过程中或使用 WAP 业务结束后发送计费信息给移动终端。而 WAP 网关发送计费信息的方式可以是短消息，WAP 网页等，具体实施中可以在 WAP 网关中实现一种或同时实现多种计费信息发送方式。

对于不同的移动终端，通过预先在 WAP 网关存储对应的计费信息发送方式，在移动终端使用 WAP 业务过程中或使用 WAP 业务完成后 WAP 网关采用移动终端对应的计费信息发送方式发送计费信息给该移动终端。

在实际应用中，可以将计费信息发送作为一个新的 WAP 业务功能，由用

户进行登记。对于登记使用该业务功能的用户，在使用 WAP 业务过程中或业务结束后，WAP 网关采用该移动终端对应的计费信息发送方式发送计费信息给该移动终端，如果 WAP 网关不允许用户设置自己的计费信息发送方式或者用户没有设置自己的计费信息发送方式则 WAP 网关采用系统默认的计费信息发送方式发送计费信息给移动终端；对于没有登记该业务功能的用户，则可以不发送计费信息。

具体实施方法包括：在 WAP 网关的用户信息数据库中添加表明用户希望使用 WAP 计费信息即时发送标识（为描述方便，称之为第一标识），当用户申请 WAP 计费信息即时发送这项业务功能时，给该移动用户的第一标识赋值为“1”；否则，赋值为“0”表示该用户不使用 WAP 业务计费信息即时发送业务功能。同时，需要添加计费信息发送方式标识（为描述方便，称之为第二标识）；在第二标识中可以用不同的值代表不同的发送方式，如：“0”表示以短消息方式发送，“1”表示以 WAP 网页方式发送，“2”表示以 IP 数据包方式发送等；同种方式还可以衍生出多种子类型，如按时间间隔周期性发送，超过设定的流量阈值或费用阈值时发送等。还可以将其中一种发送方式作为系统默认的发送方式，如第二标识为“0”的短消息方式发送方式。

当移动用户请求 WAP 业务时，WAP 网关查询存储的用户信息数据库，若检测到该移动用户已申请 WAP 计费信息即时发送业务功能，则将其计费信息按照设置的发送方式发送给移动终端。

发送的计费信息包括至少下列之一：本次或累计流量，本次或累计费用，业务使用时长，业务费率，预付费余额等。WAP 网关一般只有当前流量信息，累计流量以及费率等需要从数据业务管理平台（DSMP）和业务控制点（SCP）上获取，如图 1 所示，WAP 网关向 DSMP 发送请求，如果 DSMP 上没有相应信息，则 DSMP 向 SCP 请求信息，获取业务相关的费率、预付费余额以及终端累计费用信息等，然后发送给移动终端。一般情况下，WAP 网关不直接与 SCP 相连，而是通过 DSMP 连接 SCP 获取计费信息。

若移动终端对应的计费信息发送方式为短消息发送，则 WAP 网关通过 WAP 推送方式发送计费信息给短消息中心；短消息中心以短消息方式将计费信息下发给移动终端。

如图 2 所示，为 WAP 浏览业务计费过程及通过短消息下发计费信息的信令流程图，包括如下流程：

- 1、移动用户通过移动终端发起 WAP 浏览；
- 2、网关 GPRS 支持节点（GGSN）为移动终端（MS）分配了 IP 地址后向远程身份验证拨入用户服务（RADIUS）服务器发送计费请求起始消息，在该消息中包含分配给 MS 的 IP 地址和手机号码；
- 3、RADIUS 服务器向 WAP 网关转发计费请求起始消息；
- 4、WAP 网关收到计费请求起始消息后，向 RADIUS 服务器发送计费响应消息；
- 5、RADIUS 服务器收到计费响应消息后转发给 GGSN，若 GGSN 未收到计费响应消息，应向 RADIUS 服务器重新发送计费请求起始消息；
- 6、移动用户结束此次 WAP 浏览；
- 7、GGSN 向 RADIUS 服务器发送计费请求结束消息；
- 8、RADIUS 服务器向 WAP 网关转发计费请求结束消息；
- 9、WAP 网关收到计费请求结束消息后，向 RADIUS 服务器发送计费响应消息；
- 10、RADIUS 服务器收到计费响应消息后转发给 GGSN，若 GGSN 未收到计费响应消息，应重新发送计费请求结束消息；
- 11、WAP 网关发送计费响应后，判断该移动用户的第一标识，如果第一标识为“0”，则结束；如果第一标识为“1”，且第二标识为通过短消息方式发送计费信息，则执行步骤 12；
- 12、WAP 网关通过推送代理网关（Push Proxy GateWay，PPG）向短消息中心（SMSC）推送用户本次使用流量（费用）以及累计流量（费用）等信息；

13、SMSC 以短消息方式将接收的计费信息发送到移动终端上。

图 3 为 WAP 流媒体业务计费过程及通过短消息下发计费信息的信令流程图。WAP 网关收到 MS 发出的访问请求后,对访问请求的统一定位资源 (URL) 进行解析,判断为流媒体业务后将相关业务的提供商标识信息 (SPID)、业务标识信息 (ServiceID) 以及用户的 IP 地址等与计费相关的信息上报给 DSMP 进行业务鉴权批价。流媒体业务计费同时支持预付费用户和后付费用户。对于预付费用户,DSMP 通过与 SCP 的交互完成实时扣费。具体信令交互流程如图 3 所示,包括:

1、MS 向 WAP 网关发起流媒体业务访问请求。

2、WAP 网关收到访问请求后,判断是否对用户请求进行转发,如果满足转发条件,则继续处理;否则,拒绝此次访问请求。

在该步骤中,是否对用户的业务请求进行前转或拒绝,是根据系统数据库中的一个“转发控制表”来执行的,该表存储有不可访问某项业务的 MS 的 IP 地址或终端号码,比如,在用户欠费或余额不足的情况下,将对其禁用某些类型的业务请求;当 MS 请求业务时,WAP 网关将查找“转发控制表”,如果发送业务请求的 MS 包含在“转发控制表”中,则确定所请求此项业务是否为不可访问业务,如果是,则对此 MS 禁用该项业务,并将用户的欠费信息发送给 MS;如果发送业务请求的 MS 不在转发控制表中,则说明此 MS 是合法的,WAP 网关则将该请求透传给业务提供商 (SP),并进行内容计费或流量计费,在业务使用过程中或使用后将计费信息发给 MS。为了防止用户在已经充值的情况下,仍然无法使用某项业务,转发控制表中的用户信息是实时更新的。

3、WAP 网关将业务请求转发给相应的业务提供商或内容提供商 (SP/CP)。

4、SP/CP 返回访问请求应答消息给 WAP 网关。

5、WAP 网关把请求应答消息下发给终端 MS。

6、WAP 网关记录或查询用户在线信息,并判断用户类型 (根据 MSISDN 号段或 IMSI 号段区分用户类型,如预付费用户、后付费用户),如果是后付费

用户，业务使用结束后直接跳转到第 11 步；如果是预付费用户，根据请求的 URL 采集 SPID、ServiceID 以及用户 IP 地址等计费相关信息。

7、WAP 网关将采集到的计费相关信息上报 DSMP，进行鉴权批价。

8、DSMP 到 SCP 申请费用预扣。

9、SCP 向 DSMP 返回费用预扣应答消息。

10、DSMP 向 WAP 网关返回鉴权批价应答消息。

11、MS 向 WAP 网关发出断连请求。

12、WAP 网关把断连请求转发给 SP/CP。

13、SP/CP 向 WAP 网关返回断连请求应答消息。

14、WAP 网关把断连请求应答消息下发给终端 MS。

15、WAP 网关生成话单记录（Call Detail Record，CDR），包括业务开始时间，结束时间，终端号码，业务类型等。

16、WAP 网关将 CDR 话单中的计费信息通过 WAP PUSH 短消息发给 MS。

以上用 WAP 浏览业务和流媒体业务的计费过程为例，对本发明采用短消息方式发送 WAP 业务计费信息进行了详细描述。其中，短消息发送方式可以是在移动终端使用 WAP 业务过程中，由 WAP 网关按设定的时间间隔发送；或在移动终端使用 WAP 业务过程中，当预付费移动终端的余额小于设定的余额阈值、移动终端使用 WAP 业务流量超过设定的流量阈值或移动终端使用 WAP 业务费用超过设定的费用阈值时，在 WAP 浏览业务的第 5 步与第 6 步之间或在 WAP 流媒体业务的第 10 步与第 11 步之间，由 WAP 网关发送计费信息给短消息中心。另外对于流媒体业务与浏览业务同时使用的情形，如 WAP 浏览时打开了一个流媒体，这样 WAP 网关同时将两个业务的计费信息分别或合并在一起发送给 MS。

对于计费信息的发送，除了采用短消息方式发送外，还可以采用 WAP 网页方式发送，包括下列具体方法：

方法一：在移动终端使用 WAP 业务过程中，WAP 网关为该移动终端产生

一个包含计费信息的临时 WAP 网页,并将该临时 WAP 网页的超链接地址插入到移动终端当前浏览的网页中,移动终端通过访问所述超链接地址获取计费信息;并在 WAP 业务结束后,删除产生的临时 WAP 网页。

方法二:在移动终端使用 WAP 业务过程中,WAP 网关将指向一个即时计费单元的超链接插入到移动终端当前请求浏览的网页中,移动终端访问所述超链接时,即时计费单元从 WAP 网关中获取该移动终端的计费信息,并生成包含计费信息的 WAP 网页由 WAP 网关返回给移动终端。

方法三:将移动终端使用 WAP 业务的计费信息存储到一个固定超链接地址的 WAP 网页中,当移动终端访问该固定超链接地址时,WAP 网关获取相应的计费信息并更新到上述 WAP 网页然后返回给移动终端。为用户使用方便,可以将上述固定超链接地址预先存储到移动终端中,用户可以随时通过访问该超链接地址获取计费信息。

计费信息发送方式还可以为 IP 数据包发送,可以设置为当 WAP 网关接收到移动终端的计费信息请求时,将包含计费信息的数据包按照 IP 协议格式发送给移动终端对应的 IP 地址,或 WAP 网关按照设定的时间间隔将包含计费信息的数据包按照 IP 协议格式发送给移动终端对应的 IP 地址,由移动终端显示出计费信息。同时改进 WAP 浏览器,使之在终端浏览器界面的固定位置显示 WAP 网关发送的计费信息(流量或费用信息)。

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

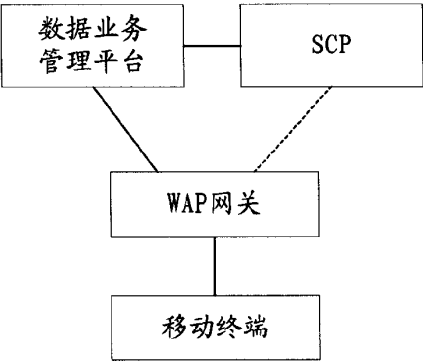


图 1

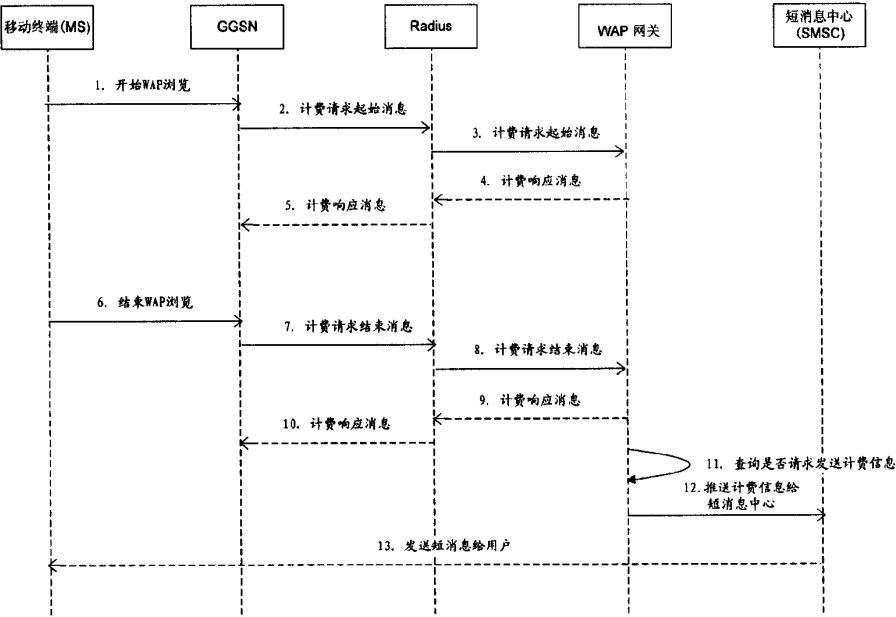


图 2

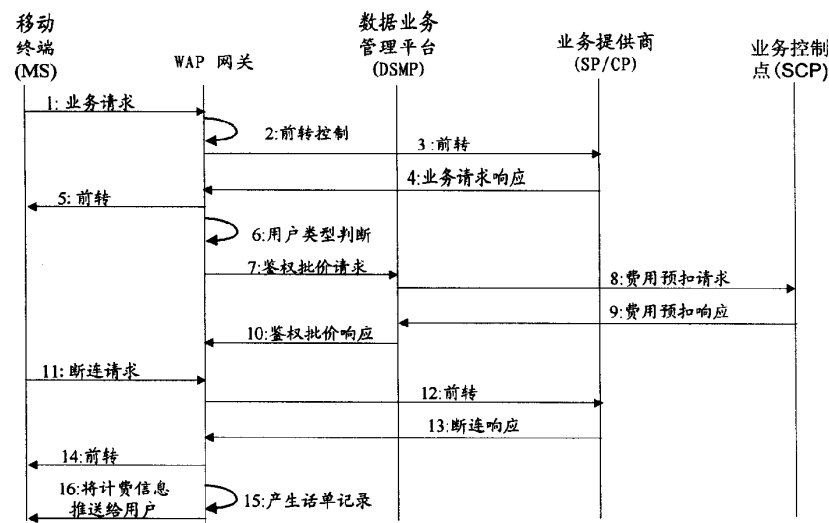


图 3

Sign in

Patents

Application

Grant

English

Chinese

Find prior art

Discuss this application

View PDF

Download PDF



Charging information transmitting method

CN 1867024 A

ABSTRACT

The invention relates to a charge information sending method, used in wireless application protocol (WAP) service, which comprises: the mobile terminal via WAP gateway uses WAP service; the WAP gateway charges the mobile terminal and sends the charge information to the mobile terminal. The invention can make the WAP gateway instantly send the charge information of consumed WAP service to the user terminal, to support the control and application of WAP service.

Publication number	CN1867024 A
Publication type	Application
Application number	CN 200510070958
Publication date	22 Nov 2006
Filing date	19 May 2005
Priority date	19 May 2005
Also published as	CN1867024B
Inventors	申海, 孙谦
Applicant	华为技术有限公司
Export Citation	BiBTeX, EndNote, RefMan
Referenced by (6), Classifications (3), Legal Events (3)	
External Links: SIPO, Espacenet	

DESCRIPTION translated from Chinese

An information transmission method accounting

FIELD

The present invention relates to the field of wireless communications, and more particularly to a wireless application protocol (Wireless Application Protocol, WAP) service charging information transmission method.

BACKGROUND

WAP technology has become a major global standard for mobile communications network terminal access wireless information services, as well as the technical foundation of existing mobile data and value-added services. WAP browser is the most common class of business and popular mobile data services, the user terminal via a browser to view WAP pages of information received from the server, as a basis for business mobile data services, WAP browsing class of business is being more and more Mobile users are using and accepted. Also WAP-based mobile streaming media business, will become the mainstream of 3G communication network applications. Open Mobile Alliance (Open Mobile Alliance, OMA) on WAP service specific implementation does not make a limited charging, while the prior art has not yet a WAP service billing information to a method for real time transmission to the mobile terminal. Billing information of the mobile terminal only when such calls monthly billing system by BOSS collected from the WAP gateway to the words of a single statistical rating, then print it out to users, but usually no expense detail records. Many cases are due to a WAP gateway billing by traffic, so for prepaid and postpaid users, there is a similar problem: the user in the use of WAP services, or conduct a WAP service, I do not know how much traffic generated, but also I do not know how much traffic this month cumulative use, so users can not grasp or control the use of WAP services; especially for prepaid subscribers, prepaid expenses when exhausted, in case the user can not be informed in advance of the WAP gateway will be forced to interrupt business users to use WAP services to cause trouble.

SUMMARY

The present invention provides a method for transmitting charging information to solve the prior art are not readily available WAP service charging information problems.

CLAIMS (17) translated from Chinese

A charging information transmission method, applied to a wireless application protocol (WAP) service, the method comprising: a mobile terminal using WAP services via the WAP gateway, WAP gateway of the mobile terminal for billing, WAP gateway sends accounting information to the mobile terminal.

- The method according to claim 1, characterized in that the WAP gateway is preset in the charging information transmission method, in a mobile terminal using the WAP services used during or after the WAP gateway WAP service charging information according to the transmission setting Billing information is sent to the mobile terminal.
- The method according to claim 2, characterized in that the charging information transmission method with the mobile terminal of the WAP gateway preset correspondence, using WAP service in a mobile terminal during or after completion of the WAP gateway WAP services using accounting information corresponding to the mobile terminal sending to send accounting information to the mobile terminal.
- A method as claimed in claim 2 or claim 3, characterized in that the charging information transmission method for transmitting a short message, WAP gateway sends the mobile terminal using the WAP service charging information via WAP push mode to the short message center; SMS short message center to the next billing information to the mobile terminal.
- The method according to claim 4, characterized in that the charging information transmission mode further includes setting the time interval, the mobile terminal using WAP in the course of business, WAP gateway according to the set time intervals sending the accounting information to the short message center.
- The method of claim 4 when the WAP gateway detection claim, characterized in that the charging information transmission mode further includes setting a threshold value of the balance, the flow rate threshold or cost threshold, the mobile terminal using WAP in the course of business, When the prepaid balance of the mobile terminal is less than a set threshold balance value, the mobile terminal uses the mobile terminal traffic threshold or WAP traffic exceeds the costs of the use of WAP services cost more than the set threshold value, WAP

The method of the present invention includes: a mobile terminal via WAP gateway using WAP services, WAP gateway for mobile terminals for billing, WAP gateway sends billing information to the mobile terminal.

The above-described method according to the invention, the WAP gateway preset charging information transmission method, the business process using WAP or WAP gateway used to send accounting information to the accounting information based on the transmission method set by the mobile terminal after the WAP service in a mobile terminal.

Billing information transmitting manner with the WAP gateway of the mobile terminal set in advance corresponding to, in a mobile terminal using the WAP services used during or after completion of WAP gateway WAP services using the mobile terminal corresponding to the charging information sending to send accounting information to the mobile terminal.

The charging information transmission method for sending short messages; WAP gateway sends the mobile terminal using the WAP service billing information via WAP push mode to the short message center; short message center to a mobile short message will be sent to the billing information under terminal.

Information transmission mode further includes setting the charging time interval, using the WAP service in a mobile terminal during, WAP gateway according to the preset time interval to transmit the accounting information to the short message center.

The billing information transmitting mode further includes setting a threshold value of the balance, the flow rate threshold or cost threshold, the mobile terminal using WAP in the course of business, when the WAP gateway detects that the mobile terminal prepaid balance is less than the set threshold balance, moving When the end-use flow threshold or WAP mobile terminal traffic exceeds the cost of using WAP services exceeds the cost threshold, WAP gateway sends billing information to the short message center.

The charging information transmission method for WAP pages; including: the mobile terminal business processes using WAP, WAP gateway WAP page that contains the provisional billing information for the mobile terminal, and the temporary WAP page hyperlink address and display text hyperlinks inserted in the mobile terminal is currently viewed page request, the mobile terminal acquires the billing information by accessing the hyperlink address; and after the WAP service, deleting the temporary WAP page.

The charging information transmission method as WAP pages; specifically include: the mobile terminal using the WAP business process, WAP gateway will point to an immediate hyperlink accounting unit is inserted into the mobile terminal is currently viewed page request, the mobile terminal accesses when said hyperlink, immediate accounting unit receives charging information of the mobile terminal from the WAP gateway, and generates WAP pages returned to the mobile terminal.

The charging information transmission method as WAP pages; specifically includes: setting a fixed address hyperlink for transmitting the charging information, when the WAP gateway detects that the mobile terminal requests the fixed address of the mobile terminal hyperlink billing information sent to the WAP pages to the mobile terminal.

Said fixed hyperlink address preset in the mobile terminal.

The charging information transmission method for transmitting IP packets, WAP gateway receives the charging information to the mobile terminal or a request intervals containing charging information according to the set time of the data packet transmitted to the mobile terminal corresponding to the IP protocol in accordance with the format of IP address, the mobile terminal displays the charging information.

gateway sends accounting information to the short message center.

7. The method according to claim 2 or claim 3, characterized in that the charging information transmission method as WAP pages; specifically include: the mobile terminal using the WAP business process, WAP gateway generates a count for the mobile terminal comprising Temporary fee WAP pages of information, and the temporary WAP page hyperlink address and hyperlink display text is inserted into the mobile terminal is currently viewed page request, the mobile terminal to obtain billing information by accessing the hyperlink address; and After the WAP service, delete the temporary WAP pages.

8. The method according to claim 2 or claim 3, characterized in that the charging information transmission method as WAP pages; specifically include: the mobile terminal using the WAP service process, WAP gateway will point to a real-time accounting unit hyperlink into the mobile terminal is currently viewed web page request, the mobile terminal to access the hyperlink, the accounting unit immediately obtain charge information of the mobile terminal from the WAP gateway, and generates WAP pages returned to the mobile terminal.

When the WAP gateway detection setting a fixed hyperlink address for sending billing information: Including: 9. The method of claim 2 or claim 3, wherein the charging information transmission method for WAP pages to the mobile terminal requests the address of the hyperlink fixed charge information to the mobile terminal WAP page sent to the mobile terminal.

10. The method according to claim 9, characterized in that the fixed hyperlink address preset in the mobile terminal.

11. The method according to claim 2 or claim 3, characterized in that the charging information transmission method for transmitting IP packets, WAP gateway receives the charging information to the mobile terminal according to a request or set time interval will contain packet transmission according to the charging information to the mobile terminal IP protocol format corresponding to the IP address, the mobile terminal displays the charging information.

12. The method according to claim 11, characterized in that the charging information is displayed in a fixed position of the mobile terminal WAP browser interface.

13. The method of claim 1, wherein, when the mobile terminal is a prepaid terminal, further comprising the WAP gateway when the mobile terminal requests the WAP service, its pre-paid balance inquiry step; if insufficient pre-paid balance, the WAP gateway informs the mobile terminal, and reject the use of WAP service request, otherwise normal use of WAP mobile terminal business.

14. A method as claimed in claim 1, characterized in that the WAP service for WAP browsing WAP class of business or streaming media services.

15. A method as claimed in claim 1, characterized in that the billing information for mobile terminal using WAP traffic in this, the cumulative use of WAP traffic, this time using WAP operating expenses, total operating expenses using WAP, this When using a long time business, this business combination and prepaid tariff information which one or any number of balance.

16. The right to at least one of the times when business rates or prepaid balance method of claim 15, wherein if the WAP gateway sends billing information, including cumulative use WAP traffic, total

in the fixed position of the mobile terminal WAP browser interface displays the charging information.

When the mobile terminal for prepaid terminals, including WAP gateway when the mobile terminal requests WAP services, check their prepaid balance steps; pre-paid balance if less, the WAP gateway informs the mobile terminal, and reject the use of the requested WAP business, otherwise normal use of WAP mobile terminal business.

The WAP service for WAP Browser WAP class of business or streaming media services.

The charging information for the mobile terminal using WAP traffic in this, the cumulative use of WAP traffic, this time using WAP operating expenses, total operating expenses using WAP, use a long time in this business, this business rates and pre-paid balance among One or a combination of any number of information.

If the WAP gateway sends billing information, including cumulative use WAP traffic, the cumulative cost of using WAP services, at least one of the times when business rates or pre-paid balance, which also includes a WAP gateway to the data service management platform sends a request message to get said step of charging information.

If the data is not saved billing service management platform information corresponding request by the data service management platform to the service control point (SCP) on the acquisition of the intelligent network.

Beneficial effects of the present invention is as follows: (1) The present invention utilizing WAP gateway sends billing information to the terminals, the user in the course of business using WAP or just use the time after the completion of WAP services can instantly obtain billing information, user-friendly control and use WAP services.

(2) The present invention provides a variety of billing information transmission method implementations, including: short message, WAP page mode and IP packet mode, WAP gateway can select at least one of the charging information is sent according to the network status and the ability realization of the program will immediately send the charging information to the user terminal; and for a variety of billing information while providing a way to send a WAP gateway, users can flexibly set billing information transmission mode, fully meet the user's individual needs and habits .

(3) The present invention may require the user to send instant WAP service billing information pre-registration, the system only to registered users by default or set of accounting information send send billing information, while fully meet user demand, reduce system load.

Brief Description

Figure 1 is a schematic structural view of the system under the charging information issued involved; Fig. 2 embodiment of the present invention, WAP browse service billing process and the short message sent by a flowchart of charging information at a signaling; Figure 3 embodiment of the present invention example WAP streaming service billing process and issued the flow chart via SMS billing information signaling.

DETAILED DESCRIPTION

The method of the present invention is a mobile terminal using the WAP gateway WAP in the course of business or accounting information sent to the mobile terminal after the end of the use of WAP services. The WAP gateway sends billing information can be a way SMS, WAP pages, the specific implementation can be achieved in a WAP gateway or billing information is sent simultaneously to achieve a variety of ways.

For different mobile terminal via the WAP gateway is stored in advance in the charging information corresponding to the transmission method, in a mobile terminal during use or after use WAP services complete WAP gateway WAP services using the mobile terminal corresponding to the charging information sending to send accounting information to the mobile terminal.

In practice, the charging information may be sent as a new WAP service function registration by the user. For registered users to use the business functions, after or during the use of the WAP service end of the business, WAP gateway uses the mobile terminal corresponding billing information send billing information is sent to the mobile terminal, if the WAP gateway does not allow users to set their own billing information is sent way or you do not set your own way billing information is sent using the default WAP gateway sends billing information send billing information to the mobile terminal; for there is no registration of the business functions of the user, you can not send billing information.

DETAILED DESCRIPTION The method comprises: a WAP gateway in the user information database indicates that the user wishes to add in a WAP charging information sent immediately identified (for convenience of description, referred to the first identification), when the user applies the charging information immediately send the WAP service When the function assigned to the first identification of the mobile subscriber is "1"; otherwise, the value "0" indicates that the user

operating expenses using WAP, further comprising a WAP gateway to the data service management platform sends a request message, the charge information acquisition step.

17. The method of claim 16, wherein, if the data service management platform does not save the corresponding charging information requested by the data service management platform to a service control point (SCP) of the intelligent network on the acquisition.

does not immediately send a service function using the WAP service billing information. Meanwhile, the need to add the accounting information identifies the transmission mode (for convenience of description, referred to the second identification); in the second identification can be different values represent different transmission methods, such as: "0" indicates that a short message sent "1" means to send WAP pages, "2" to send IP packets, etc; the same way many seeds can also be derived types, such as by sending periodic intervals, the flow exceeds the set threshold value or cost of When the threshold is sent and the like. Wherein a further short message transmission mode as the default transmission mode, such as the second identifier is "0" may be input mode.

When the mobile user requests a WAP service, the WAP gateway queries the user information database stored, if it is detected that the mobile user has applied charging information sent immediately WAP service function, it is the accounting information sent to the mobile terminal according to the transmission mode set.

Billing information sent includes at least one of the following: The total flow or that this or cumulative cost, long-time business use, business rates, and other pre-paid balance. WAP gateway generally only current traffic information, as well as cumulative flow rate, etc. need to obtain from the data service management platform (DSMP) and a service control point (SCP), as shown in Figure 1, WAP gateway sends a request to DSMP, if on no DSMP appropriate information, then DSMP to SCP request information, access to business-related rates, pre-paid balance and terminal cumulative cost information, and then sent to the mobile terminal. Generally, WAP gateway not directly connected with the SCP, but is connected SCP receives charging information DSMP.

If the mobile terminal corresponding to the charging information transmission method for sending short messages, the WAP gateway sends billing information via WAP push mode to the short message center; short message center to short message will be sent to the mobile terminal next billing information.

2, the billing process for the WAP browsing service by sending the next charging information and a signaling message flow diagram, comprises the following processes: 1, the mobile terminal through the mobile user initiates a WAP browser; 2, Gateway GPRS Support Node (After GGSN) for the mobile terminal (MS) is assigned an IP address to the Remote Authentication Dial-In User Service (RADIUS) server sends an accounting request start message containing the IP address assigned to the MS, and phone number in the message; 3, RADIUS server forwards the request to start charging WAP gateway message; 4, WAP gateway billing request after receiving the initial message, send a response message to the RADIUS accounting server; 5, RADIUS server receives the forwarded after charging response message to the GGSN If the GGSN charging response message is not received, the RADIUS server should start charging request to resend the message; 6, the end of the WAP mobile users browse; 7, GGSN sends an accounting request to the RADIUS server end of the message; 8, RADIUS WAP billing gateway server forwards the request to the end of the message; 9, WAP gateway charging request received after the end of the message, send a response message to the RADIUS accounting server; 10, RADIUS server receives forwarded to the GGSN after charging response message, if the GGSN charging response message is not received, the end should resend the charging request message; 11, WAP gateway after sending charging response, determines the first identification of the mobile user, if the first identifier is "0", the end; if the first one identified as "1", and the second is identified as sending billing information via short message, proceed to Step 12; 12, WAP Push Proxy Gateway gateway (Push Proxy GateWay, PPG) to the Short Message Service Center (SMSC) to push users The use of flow (expense) and total flow (expense) and other information;

13, SMSC to send billing information received short message to the mobile terminal.

Figure 3 WAP streaming service billing process and issued the flow chart via SMS billing information signaling. After the WAP gateway receives an access request issued by MS, unified resource location (URL) access request is parsed to determine the identification information for the provider of streaming media services-related business will (SPID), business identification information (ServiceID) and user The IP address and billing-related information reported to the grant price DSMP authorization to conduct business. Streaming service billing support prepaid and postpaid users users. For prepaid subscribers, DSMP through real-time interaction with the completion of the SCP deductions. Specific signaling interaction process shown in Figure 3, including: 1, MS initiates streaming service access request to the WAP gateway.

2, after the WAP gateway receives an access request to determine whether the request is forwarded to the user, if the forwarding condition, then continue processing; otherwise, reject the access request.

In this step, the front of the user's service request is transposed or rejected based on the system database in a "forwarding control table" to be executed, the table stores a business of MS is not accessible IP address or a station number, for example, in the user arrears or insufficient balance situation, which will be disable certain types of service requests; "Forward Control Table" When MS requests a service, WAP gateway will find, MS If you send a service request is contained in " forwarding control table ", it is determined whether the requested service is inaccessible to this service, if yes, the service is disabled for this MS, and the information is sent to the user arrears MS; if the MS is not transmitting a service request forwarding control table, the description for this MS is legitimate, WAP gateway through the request is passed to the service provider (SP), and content-based billing or traffic accounting, business use during or after the use of accounting information sent to MS. To prevent the user has to recharge the case is still unable to use certain services,

forwarding control table user information is updated in real time.

3, WAP gateway service request will be forwarded to the appropriate service provider or content provider (SP / CP).

4, SP / CP returns an access request response message to the WAP gateway.

5, WAP gateway to request a response message to the terminal MS under.

6, WAP gateway records or query the user online information, and determine the type of user (based on MSISDN or IMSI number section number section all types of users, such as pre-paid subscribers, post-paid subscribers), if it is post-paid users to jump directly after the end of the business use Go to Step 11; if it is a pre-paid subscribers, collecting SPID, ServiceID as well as the user's IP address and other billing related information according to the requested URL.

7, WAP gateway will be collected charging related information reporting DSMP, authenticate the grant price.

8, DSMP to SCP application fee withholding.

9, SCP DSMP return costs to withhold a response message.

10, DSMP grant price return authorization response message to the WAP gateway.

11, MS issued a disconnection request to the WAP gateway.

12, WAP gateway forwards the request to put off even the SP / CP.

13, SP / CP returns to the WAP gateway disconnection request response message.

14, WAP gateway to the disconnection request response message to the terminal under MS.

15, WAP gateway CDR record generation (Call Detail Record, CDR), including business start time, end time, terminal number, type of service.

16, WAP gateway bill in the CDR billing information to the MS via WAP PUSH short message.

WAP browser with more services and streaming services billing process, for example, the present invention uses the short message sent WAP service billing information described in detail. Wherein, the short message transmission mode in the mobile terminal may be a business process using the WAP, the WAP gateway send at set time intervals; or in the mobile terminal using the WAP service process, when the prepaid balance of the mobile terminal is less than the set balance threshold, the mobile terminal using flow threshold or mobile terminal WAP traffic exceeds the use of WAP service fee exceeds the cost threshold between Step 5 WAP browsing services with step 6 or WAP streaming media business section 10 steps between step 11 and sent by the WAP gateway billing information to the short message center. In addition to the case of streaming services and browse business use, such as the WAP browser to open a streaming media, such WAP gateway billing information while the two businesses separately or combined to the MS.

For sending billing information, in addition to the short message sent, but also can be sent using WAP pages, including the following specific methods: Method One: In the mobile terminal business process using WAP, WAP gateway generates a count for the mobile terminal contains Temporary fee WAP pages of information, and the temporary WAP page hyperlink address into the mobile terminal while browsing the mobile terminal to obtain billing information by accessing the hyperlink address; and after the WAP service, delete produce Temporary WAP pages.

Method 2: In the mobile terminal business process using WAP, WAP gateway will instantly hyperlink pointing to a billing unit is inserted into the mobile terminal is currently viewed web page request, the mobile terminal to access the hyperlink, instant charging unit from WAP gateway acquires accounting information of the mobile terminal, and generates charging information WAP page containing the return by the WAP gateway to the mobile terminal.

Method three: the mobile terminal using the WAP service billing information is stored to a fixed address hyperlink WAP pages, when the mobile terminal to access the fixed hyperlink addresses, WAP gateway obtains the corresponding charging information and updates to said WAP page then returned to the mobile terminal. The user easy to use, can be a hyperlink to the fixed address previously stored in the mobile terminal, the user can obtain billing information at any time by visiting the hyperlink address.

Accounting information packet transmission method can also transmit IP packets, may be provided to the WAP gateway when the mobile terminal receives the request for charging information, the charging information contains the mobile terminal transmits the corresponding IP address according to the IP protocol format, or a WAP gateway according to the set time interval will contain data packets transmitted to the accounting information corresponding to the IP address of the mobile terminal according to IP protocol format, the mobile terminal displays the charging information. While improving the WAP browser that displays the charging information (traffic or cost information) WAP gateway sends the location of the terminal in a fixed browser interface.

Obviously, those skilled in the art may make various modifications of the present invention and modifications without departing from the spirit and scope of the invention. Thus, if such modifications and variations of the present invention and the claims of the invention belongs to the technical scope of equivalents, the present invention is also intended to include these changes and modifications included.

REFERENCED BY

Citing Patent	Filing date	Publication date	Applicant	Title
CN100450130C	21 Dec 2005	7 Jan 2009	中兴通讯股份有限公司	System and method for realizing intermediately informing user telephone fee
CN101286858B	12 Apr 2007	8 Dec 2010	中兴通讯股份有限公司	Method and system for charging of WAP gateway for mobile terminal
CN101287161B	14 May 2008	20 Apr 2011	华为软件技术有限公司	Service request forwarding method, gateway for wireless application protocol and communication system
CN101583095B	3 Jun 2009	8 May 2013	中兴通讯股份有限公司	Telephone charge prewarning method and prewarning system
CN101674561B	15 Jan 2009	4 Jul 2012	华为技术有限公司	Subscriber arrearage treatment method, device and system
WO2010028556A1 *	10 Jul 2009	18 Mar 2010	Huawei Technologies Co., Ltd.	Method for processing user debt, mobile management entity and network system

* Cited by examiner

CLASSIFICATIONS

International Classification	H04Q7/22, H04L12/14, H04M17/00
------------------------------	--------------------------------

LEGAL EVENTS

Date	Code	Event	Description
6 Oct 2010	C14	Granted	
17 Jan 2007	C10	Request of examination as to substance	
22 Nov 2006	C06	Publication	



(12) 发明专利申请

(10) 申请公布号 CN 101815275 A

(43) 申请公布日 2010.08.25

(21) 申请号 201010143134.0

(22) 申请日 2010.04.09

(71) 申请人 刘泱

地址 100190 北京市海淀区知春路 63 号卫
星大厦 6 层 604 单元

(72) 发明人 梁秋实 袁彬

(74) 专利代理机构 北京联创佳为专利事务所
(普通合伙) 11362

代理人 郭防

(51) Int. Cl.

H04W 4/24 (2009.01)

H04W 88/02 (2009.01)

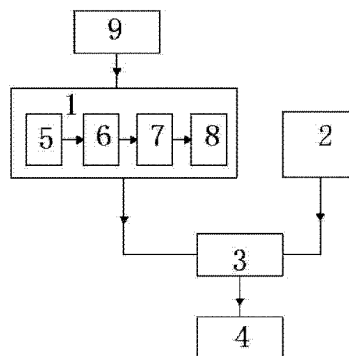
权利要求书 1 页 说明书 4 页 附图 2 页

(54) 发明名称

一种手机话费计算装置

(57) 摘要

本发明公开了一种手机话费计算装置,其特征在于:包括无线网络、业务支撑服务器(9)和手机;还包括设置在手机上的同步用户的话费计费规则到手机的网络同步模块(1),记录用户通话详情的监控模块(2),使用网络同步模块(1)上的话费计费规则对监控模块(2)记录的用户通话详情进行批价的批价模块(3)和将批价后的账单存储在手机上的存储模块(4)。本发明计算话费时的实时性和准确性高,并且可直接在手机上查询,话费详单数据量小,无需密码,更加方便快捷,同时存储的账单也便于用户对话费的核对。



1. 一种手机话费计算装置,其特征在于:包括无线网络、业务支撑服务器(9)和手机;还包括设置在手机上的

网络同步模块(1),用于同步用户的话费计费规则到手机上,通过无线网络与业务支撑服务器(9)相连;

监控模块(2),用于记录用户通话详情;

批价模块(3),用于将网络同步模块(1)上的话费计费规则对监控模块(2)记录的用户通话详情进行批价;

存储模块(4),用于将批价后的账单存储在手机上,并与手机的显示设备相连;

监控模块(2)和网络同步模块(1)与批价模块(3)相连,批价模块(3)与存储模块(4)相连。

2. 根据权利要求1所述的手机话费计算装置,其特征在于:所述网络同步模块(1)包括获取手机的运营商、归属地和品牌信息的用户信息模块(5),根据获取的用户信息从业务支撑服务器(9)下载运营商该品牌下所有的套餐列表的列表下载模块(6)、用于用户选择所用套餐的选择模块(7)和根据用户所选套餐从业务支撑服务器(9)获取该套餐计费规则的规则下载模块(8)。

3. 根据权利要求2所述的手机话费计算装置,其特征在于:所述用户信息模块(5)为人工输入或选择运营商、手机卡归属地、手机卡品牌和用户所在地信息的模块。

4. 根据权利要求2所述的手机话费计算装置,其特征在于:所述用户信息模块(5)为通过手机的短信中心号来判断用户的运营商和归属省份,通过手机当前的基站信息来辅助确定用户所在地的模块。

5. 根据权利要求4所述的手机话费计算装置,其特征在于:所述短信中心号与运营商、省份的对应关系从业务支撑服务器(9)下载,或预先存储在手机上。

6. 根据权利要求2所述的手机话费计算装置,其特征在于:所述规则下载模块(8)下载的套餐计费规则包括通话话费计费规则、短信计费规则、短信增值业务号码、GPRS上网费用计费规则、月租费、套餐费和手机号段。

7. 根据权利要求1所述的手机话费计算装置,其特征在于:所述监控模块(2)在手机端监控用户的通话、发送短信、通过GPRS联网的行为作为通话详情,并将此行为存为详细日志,或直接调用手机通话记录作为通话详情。

8. 根据权利要求7所述的手机话费计算装置,其特征在于:所述通话详情包括用户的通话、发送短信和通过GPRS联网行为的发话时间、结束时间、被叫方、主叫方、发话地点和流量。

9. 根据权利要求1、2或5所述的手机话费计算装置,其特征在于:所述业务支撑服务器(9)是储存套餐列表、套餐计费规则和短信中心号与运营商、省份的对应关系的服务器。

一种手机话费计算装置

技术领域

[0001] 本发明涉及一种手机话费计算装置,特别是一种手机上使用的手机话费计算装置。

背景技术

[0002] 一个典型的电信运营商所使用的计费系统中,业务网元是电信运营商提供基础服务的系统,电信的核心服务包括通话、短信、GPRS (General Packet Radio Service) 等,每个服务对应一组业务网元。CDR (call detail record) 是业务详情记录,记录业务网元向用户提供的每次服务的详情。CDR40 不仅仅指通话详情记录,也包括短信或 GPRS 的使用详情记录。每条 CDR 中包含发话时间、结束时间、主叫、被叫、发话地点等信息。系统向业务网元查询 CDR40,然后对 CDR40 批价,得到账单详情,并将账单详情存入账单数据库。

[0003] 而现有的话费计算系统存在下述问题:

首先,现有的话费计算系统是在各电信运营商内部运作,且因为一些技术原因容易出现话费错算、误算的情况,手机用户很难清楚的了解自己每笔话费的产生原因,进而无法确定自己话费的准确性、正确性。

[0004] 其次,因为话单的数量巨大,一些电信运营商并不对全部用户提供话费详单查询服务。即便某些电信运营商对于部分用户开放了详单查询的业务,也存在使用不便(比如要输入服务密码、或者到移动营业厅现场办理)、实时性不强(比如只能查上月的话费详单、或几天前的话费详单)等问题。

[0005] 再次,即便用户拿到了话费详单,也会因为各运营商、各种套餐的计算规则各异,如存在优惠时段、赠送通话分钟数等特殊规则,导致用户对话费的核对非常困难。

发明内容

[0006] 本发明的目的在于,提供一种手机话费计算装置。它是一种便于用户查看和理解,具有高实时性、准确性的手机话费计算装置。

[0007] 本发明的技术方案:一种手机话费计算装置,其特征在于:包括无线网络、业务支撑服务器和手机;还包括设置在手机上的

网络同步模块,用于同步用户的话费计费规则到手机上,通过无线网络与业务支撑服务器相连;

监控模块,用于记录用户通话详情;

批价模块,用于将网络同步模块上的话费计费规则对监控模块记录的用户通话详情进行批价;

存储模块,用于将批价后的账单存储在手机上,并与手机的显示设备相连;

监控模块和网络同步模块与批价模块相连,批价模块与存储模块相连。

[0008] 上述的手机话费计算装置中,所述网络同步模块包括获取手机的运营商、归属地

和品牌信息的用户信息模块,根据获取的用户信息从业务支撑服务器下载运营商该品牌下所有的套餐列表的列表下载模块、用于用户选择所用套餐的选择模块和根据用户所选套餐从业务支撑服务器获取该套餐计费规则的规则下载模块。

[0009] 前述的手机话费计算装置中,所述用户信息模块为人工输入或选择运营商、手机卡归属地、手机卡品牌和用户所在地信息的模块。

[0010] 前述的手机话费计算装置中,所述用户信息模块为通过手机的短信中心号来判断用户的运营商和归属省份,通过手机当前的基站信息来辅助确定用户所在地的模块。

[0011] 前述的手机话费计算装置中,所述短信中心号与运营商、省份的对应关系从业务支撑服务器下载,或预先存储在手机上。

[0012] 前述的手机话费计算装置中,所述规则下载模块下载的套餐计费规则包括通话话费计费规则、短信计费规则、短信增值业务号码、GPRS 上网费用计费规则、月租费、套餐费和手机号段。

[0013] 前述的手机话费计算装置中,所述监控模块在手机端监控用户的通话、发送短信、通过 GPRS 联网的行为作为通话详情,并将此行为存为详细日志,或直接调用手机通话记录作为通话详情。

[0014] 前述的手机话费计算装置中,所述通话详情包括用户的通话、发送短信和通过 GPRS 联网行为的发话时间、结束时间、被叫方、主叫方、发话地点和流量。

[0015] 前述的手机话费计算装置中,所述业务支撑服务器是储存套餐列表、套餐计费规则和短信中心号与运营商、省份的对应关系的服务器。

[0016] 与现有技术相比,本发明由于使用了无线网络、业务支撑服务器和手机组成的基本构架,并在手机上结合了用于同步用户的话费计费规则到手机上的网络同步模块、用于记录用户通话详情的监控模块和用于将网络同步模块上的话费计费规则对监控模块记录的用户通话详情进行批价的批价模块。这种结合方式可以使计算话费时的实时性和准确性高,并且可直接在手机上查询,无需密码,更加方便快捷,同时存储的账单也便于用户对话费的核对。本发明所提供的手机话费计算装置,针对特定用户计算他自身的手机话费,话费详单数据量小,使用户可以很方便、快捷的查看、汇总自己以往的话费使用情况,并且可以在通话结束后立刻看到通话费用的变化。同时利用了电信运营商的话费计算规则,保证了话费计算的准确性,透明性。又因为计费规则存储在手机上,所以无需等待一次通话、联网结束即可实时计算当前通话、联网所产生的费用,更可以在拨出、接听一个电话之前预估本次通话每分钟的费用。现有的计费装置是在电信端计算,这套装置要对于一个地市或一省的所有用户提供计费服务,其计算、存储的数据量相当庞大,因此也造成了计算的实时性较差,准确度不高,查询不便的问题。而本装置只针对特定用户计算,数据量、运算量只有电信计费装置的数百万至数千万分之一。对于正常使用的用户,每个月的数据存储只消耗数百 K,每天需要计费的电话、短信、上网等次数也只有数百次以内,完全可以做到实时准确的计算。

附图说明

[0017] 图 1 是本发明的结构示意图;

图 2 是本发明实施例的工作流程图;

图 3 是图 2 中步骤 S10 的工作流程图。

[0018] 附图中的标记:1- 网络同步模块,2- 监控模块,3- 批价模块,4- 存储模块,5- 用户信息模块,6- 列表下载模块,7- 选择模块,8- 规则下载模块,9- 业务支撑服务器。

具体实施方式

[0019] 下面结合附图和实施例对本发明作进一步的说明,但并不作为对本发明限制的依据。

实施例

[0020] 一种手机话费计算装置,结构如图 1 所示,包括无线网络、业务支撑服务器 3 和手机;还包括设置在手机上的

网络同步模块 1,用于同步用户的话费计费规则到手机上,通过无线网络与业务支撑服务器 9 相连;

监控模块 2,用于记录用户通话详情;

批价模块 3,用于将网络同步模块 1 上的话费计费规则对监控模块 2 记录的用户通话详情进行批价;

存储模块 4,用于将批价后的账单存储在手机上,并与手机的显示设备相连;

监控模块 2 和网络同步模块 1 与批价模块 3 相连,批价模块 3 与存储模块 4 相连。

[0021] 网络同步模块 1 包括获取手机的运营商、归属地和品牌信息的用户信息模块 5,根据获取的用户信息从业务支撑服务器 9 下载运营商该品牌下所有的套餐列表的列表下载模块 6、用于用户选择所用套餐的选择模块 7 和根据用户所选套餐从业务支撑服务器 9 获取该套餐计费规则的规则下载模块 8。

[0022] 用户信息模块 5 为人工输入或选择运营商、手机卡归属地、手机卡品牌和用户所在地信息的模块。

[0023] 用户信息模块 5 也为通过手机的短信中心号来判断用户的运营商和归属省份,通过手机当前的基站信息来辅助确定用户所在地的模块。

[0024] 短信中心号与运营商、省份的对应关系从业务支撑服务器 9 下载,或预先存储在手机上。

[0025] 规则下载模块 8 下载的套餐计费规则包括通话话费计费规则、短信计费规则、短信增值业务号码、GPRS 上网费用计费规则、月租费、套餐费和手机号段。

[0026] 监控模块 2 在手机端监控用户的通话、发送短信、通过 GPRS 联网的行为作为通话详情,并将此行为存为详细日志,或直接调用手机通话记录作为通话详情。

[0027] 通话详情包括用户的通话、发送短信和通过 GPRS 联网行为的发话时间、结束时间、被叫方、主叫方、发话地点和流量。

[0028] 业务支撑服务器 9 是储存套餐列表、套餐计费规则和短信中心号与运营商、省份的对应关系的服务器。

[0029] 本发明的工作流程(如图 2):

步骤 S10,通过网络同步模块 1 同步该用户的话费计费规则到手机;

步骤 S20,在手机端通过监控模块 2 监控用户的通话、发送短信、通过 GPRS 联网的行为,

并将此行为存为详细日志；

步骤 S30, 在批价模块 3 上, 使用该用户的话费计费规则对详细日志进行批价；

步骤 S50, 用存储模块 4 将批价后的账单存储在手机上。并通过手机显示设备(可为手机显示屏)展现给用户。

[0030] 其中步骤 S10 还包括以下步骤(如图 3)：

步骤 S101, 通过用户信息模块 5, 用户选择所用手机的运营商、归属地和品牌；

步骤 S102, 通过列表下载模块 6, 手机从支撑服务器获取该运营商该品牌下所有的套餐列表；

步骤 S103, 通过选择模块 7, 用户从列表中选择自己采用的套餐；

步骤 S104, 通过规则下载模块 8, 手机从支撑服务器获取该套餐的计费规则。

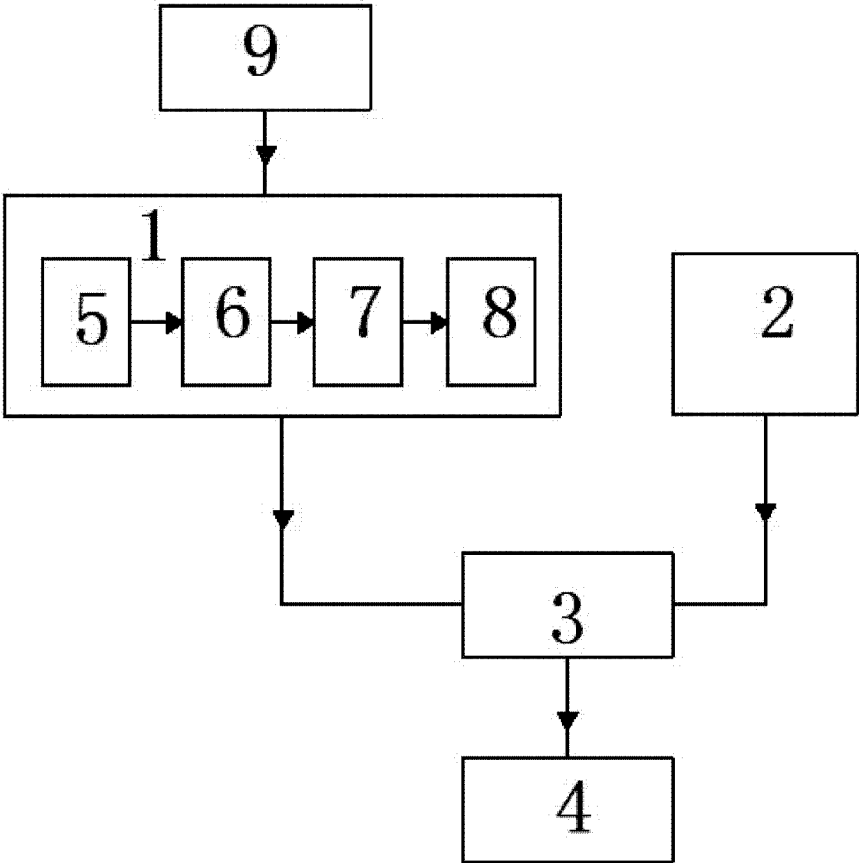


图 1

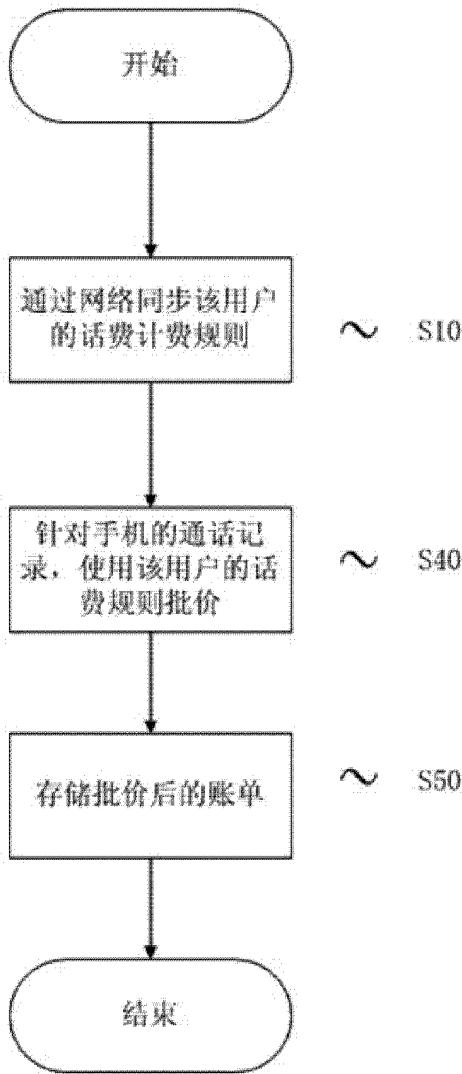


图 2

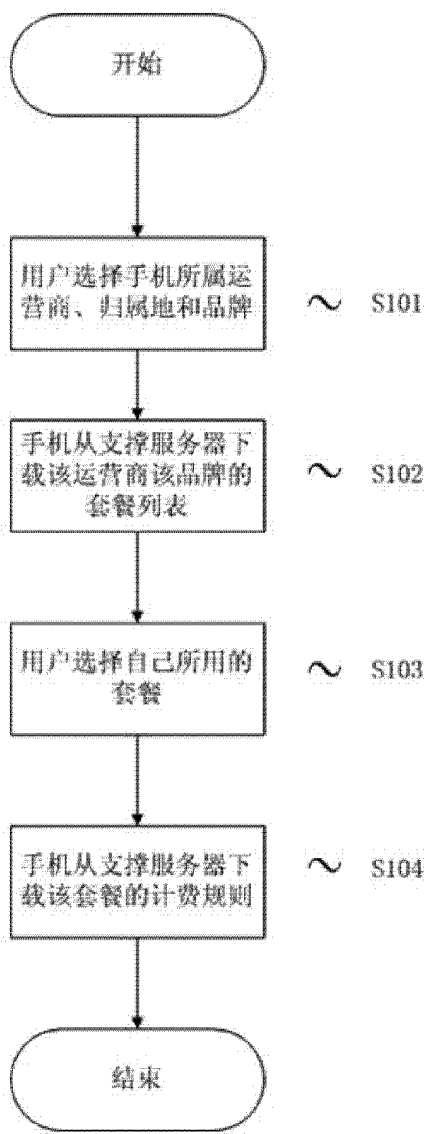


图 3

[Sign in](#)

Patents

[English](#)[Chinese](#)[Find prior art](#)[Discuss this application](#)[View PDF](#)[Download PDF](#)

Mobile phone charge calculating device

CN 101815275 A

ABSTRACT

The invention discloses a mobile phone charge calculating device, which is characterized by comprising a wireless network, a service support server (9), a mobile phone, a network synchronization module (1), a monitoring module (2), a pricing module (3) and a storage module (4), wherein the network synchronization module (1) is arranged on the mobile phone and is used for synchronizing a charge billing rule of a user to the mobile phone; the monitoring module (2) is used for recording user conversation details; the pricing module (3) is used for pricing the user conversation details recorded by the monitoring module (2) by using the charge billing rule on the network synchronization module (1); and the storage module (4) is used for storing a bill after pricing in the mobile phone. The calculating device has high real-time performance and accuracy during charge calculation, can query the charge on the mobile phone directly, has a small charge detail record data volume, needs no password and is more convenient and efficient, and simultaneously the stored bill is convenient for a user to check the charge.

Publication number	CN101815275 A
Publication type	Application
Application number	CN 201010143134
Publication date	Aug 25, 2010
Filing date	Apr 9, 2010
Priority date	Apr 9, 2010
Inventors	梁秋实, 袁彬
Applicant	刘沙
Export Citation	BiBTeX, EndNotes, RefMan
Referenced by (2), Classifications (2), Legal Events (5)	
External Links: SIPO, Espacenet	

DESCRIPTION translated from Chinese

One kind of phone calls computing device

Art

[0001] The present invention relates to a phone bill computing devices, especially cell phone calls on a computing device to use the phone.

BACKGROUND

[0002] A typical billing system used by telecom operators, the business NE telecommunications operators to provide basic services systems, telecommunications core services include calls, SMS, GPRS (GeneralPacketRadioService), etc., each service corresponds to a Group business NE. (3)R (calldetailrecord) is the business details of the recording, the details of each service provided to the user NE business records. CDR40 not only refers to the call detail records, including SMS or GPRS usage detail records. Each CDR contains the utterance time, end time, caller, callee, caller location and other information. Systems to business NE query CDR40, then CDR40 grant price, get bill details and billing details stored in the billing database.

[0003] and the existing computing system calls the following problems:

First, the existing computing system calls in the inner workings of the telecom operators, and prone to technical reasons because some calls wrong calculation, miscalculation of the situation, the mobile phone user is difficult to clearly understand the causes of their own each bill, and thus can not be determine their own phone bill accuracy, correctness.

[0004] Second, because of the huge number of single words, some carriers do not bill for all users with details of a single query service. Even some telecom operators for some users open the details of a single query of business, there are also inconvenient to use (for example, to enter the service password, or to apply for Business Hall site), real-time is not strong (such as last month's bill can only check single detail, or details of a single bill a few days ago) and other

CLAIMS (9) translated from Chinese

1. A phone bill computing device, comprising: a wireless network, business support server (9) and mobile phones; also includes network settings on the phone synchronization module (1), is used to synchronize the user's calls to a cell phone charging rules connected through a wireless network and business support server (9); monitoring module (2) for recording call details of the user; grant price module (3) for network synchronization module calls accounting rules (1), for monitoring Module User Call Details (2) batch record price; memory module (4) for the phone, and connected storage bills after the grant price and the phone's display equipment; monitoring module (2) and network synchronization module (1) the approved price module (3) is connected, (4) is connected to the grant price module (3) and memory modules.
2. The phone calls computing device of claim 1, wherein, wherein: said network synchronization module (1) including access to mobile phone operators, attribution and brand information subscriber information module (5), according to the obtained user information from the business support server (9) Downloads operators under the brand list download module lists all the packages (6) for the user to select the choice with our subscription module (7) and based on user selected business support package from the server (9) to get the package charging rules rules download module (8).
3. Phone calls computing device according to claim 2, wherein, wherein: said subscriber information module (5) for manual input or select the module carrier, phone cards attribution, phone card brand and user location information.
4. The phone calls computing device according to claim 2, wherein, wherein: said subscriber information module (5) through the phone's SMS center number to determine the user's operators and the home provinces, through the mobile phone base station information to the current assist in determining the

issues.

[0005] Once again, even if the user got the details of a single bill, also because the calculation rules for each operator, a variety of different packages, such as the existence of preferential period, giving the number of calls and other special rules minute, causing the user to check the phone bill is very difficult .

SUMMARY

The purpose of [0006] The present invention is to provide a phone bill computing device. It is a user-friendly viewing and understanding, with a high real-time accuracy of phone calls computing device.

[0007] aspect of the present invention: a phone bill computing device, comprising: a wireless network, business support servers and mobile phones; also includes setting on the phone

Network synchronization module for synchronizing user charging rules to the phone calls connected through a wireless network and business support server;

Monitoring module for recording user call details;

Grant price module for network synchronization module calls on the accounting rules for the monitoring module records the user calls the details were approved price;

Storage module for on the phone, and connected storage bills after the grant price and the phone's display device; connected monitoring module and network synchronization module and the grant price of the module, the module is connected to the grant price and the storage module.

[0008] The computing device of phone calls, the network synchronization module includes access to mobile phone operators, attribution and subscriber information module brand of information, access to information based on user downloads carriers under the brand all the support from the business server Package list List Download module for the user to select the package selection module and access rules of the charging rules package package downloaded from the service module supporting server based on user-selected packages.

[0009] The aforementioned phone bill computing device, wherein the user information module for manual input or select the module carrier, phone cards attribution, phone card brand and user location information.

[0010] The foregoing phone calls computing device, the mobile phone subscriber information module for SMS center number to determine the user's operators and the home provinces, the current through the mobile phone base station information to assist in determining the location of the user module.

[0011] The foregoing phone calls computing device, the message center number correspondence between operators, provinces and downloaded from the service support server or stored on the phone.

[0012] The foregoing phone calls computing device, the rules of the download module download package billing rules include rules call toll billing, SMS billing rules, SMS value-added service numbers, costs GRPS Internet billing rules, monthly fees, Package fee and phone number section.

[0013] The aforementioned phone bill computing device, wherein the monitoring module to monitor the end user in the mobile phone calls, send text messages through GPRS network acts as the call details, and this behavior is saved as a detailed log, or directly call phone call records As the call details.

[0014] The foregoing calculation means phone calls, the call details including the user's calls, send text messages and through the GPRS network behavior utterance time, end time, the called party, the caller, the caller location and traffic.

[0015] The foregoing phone calls computing device, the storage server is a business support package lists, correspondence between server packages billing rules and message center number with operators, provinces.

[0016] Compared with the prior art, the basic framework of the present invention is the use of a wireless network, composed of business support servers and mobile phones, combined with a bill charging rules for synchronizing user on the phone to the network synchronization module on your phone record the call details of the user for the monitoring module and charging rules calls for network synchronization module for monitoring module records the user's call details were awarded the grant price price module. This combination can make calls when calculating real-time and high

location of the user module.

5. 5. phone calls computing device according to claim 4, wherein, characterized in that: the SMS center number correspondence between operators, provinces and from business support server (5) download, or stored on the phone.
6. 6. phone calls computing device according to claim 2, wherein, wherein: said rules download module (8) Download the package billing rules include rules call toll billing, SMS billing rules, SMS value-added service numbers, GRPS Charging Rules Internet access charges, monthly fees, course fees and phone number section.
7. 7. The phone calls computing device according to claim 1, characterized in that: the monitoring module (2) monitor the user's end of the phone call, send SMS, via GPRS network acts as the call details, and keep this behavior for detailed logging, or directly call phone call records as a call for more information.
8. 8. phone calls computing device according to claim 7, wherein, wherein: said call details including the user's calls, send SMS and GPRS network behavior by utterance time, ending time, the called party, the caller, the caller Location and traffic.
9. 9. phone calls, 2 or computing device according to claim 5, characterized in that: the business support server (9) is a storage package list, the corresponding charging rule packages and SMS center number and operators, provinces server relationship.

=====

accuracy, and can query directly on the phone without a password, faster and more convenient, but also easy for users to store bills for calls reconciliation. Phone calls computing device of the present invention provides, calculated for a particular user's phone bill of his own, a small amount of data calls single detail, so that users can easily and quickly view, summarizing his past calls usage, and can end in a call After seeing changes in the cost of calls immediately. While taking advantage of the service provider's bill calculation rules to ensure that the bill calculation accuracy, transparency. And because the accounting rules are stored on the phone, so no need to wait for a call, the networking end the current call to real-time computing, networking costs arising, more can be set aside, before answering a phone call estimate this cost per minute. Existing billing system is to calculate the telecommunications side, this device is to provide billing services for all users by one city or a province, which is calculated, the amount of data storage is quite large, and therefore resulted in the more real-time computing poor accuracy is not high, the query inconvenient questions. And this is only for a specific user computing device, the amount of data, computation device only telecommunications billing millions to thousands of parts per million. For normal use, the monthly data storage consumes only several hundred K, daily need billing telephone, text messaging, Internet and other times only within hundreds of times, can be done in real-time and accurate count Da Bian.

Brief Description

[0017] Figure 1 is a schematic structural view of the present invention; FIG. 2 is a flowchart of an embodiment of the present invention; FIG. 3 is a flowchart of step S10 of Figure 2.

[0018] The drawings mark: 1- network synchronization module, 2-monitoring module, 3 grant price module, 4 storage modules, user information module 5-, 6- List Download module, 7-selection module, 8 Rules download module, 9-business support server.

Specific embodiments

[0019] accompanying drawings and the following embodiment of the present invention will be further illustrated by, but not as a basis for limiting the present invention.

Example

[0020] A computing device phone calls, the structure shown in Figure 1, including Wi-Fi, business support server 3 and mobile phones; also includes setting on the phone

Network synchronization module 1, calls for synchronizing user charging rules to the phone, connected through a wireless network and business support server 9;

Monitoring Module 2, is used to record the call details of the user;

Module 3 approved price for network synchronization module Call Details user charging rule calls for a monitoring module 2 on the batch record price;

Storage Module 4 for the bill after the grant price of storage on the phone, and the phone is connected to a display device; monitoring module 2 and network synchronization module 1 module 3 is connected with the grant price, grant price of module 3 is connected with the storage module 4.

[0021] network synchronization module 1 includes access to mobile phone operators, attribution and brand information user information module 5, download carriers under the brand list all the packages to download the module from the list of six business support server 9 based on user access to information for the user to select the package selection module download module with 7 and rules based on user-selected packages to get the package from the service support server charging rules 9 8.

[0022] The user information module 5 for manual input or select the module carrier, phone cards attribution, phone card brand and user location information.

[0023] The user information module 5 also via mobile phone SMS center number to determine the user's operators and the home provinces, the current through the mobile phone base station information to assist in determining the location of the user module.

[0024] SMS center number corresponds to the relationship operators, provinces and downloaded from the service support server 9, or stored on the phone.

[0025] Rule 8 download download module packages billing rules include rules call toll billing, SMS billing rules, SMS value-added service numbers, costs GRPS Internet billing rules, monthly fees, package costs and phone number section.

[0026] 2 at the end of the phone monitoring module to monitor the user's call, send SMS, via GPRS network acts as the call details, and keep a detailed log of this behavior, or directly call phone call records as a call for more information.

[0027] Call details include the user's calls, send text messages and through the GPRS network behavior utterance time,

end time, the called party, the caller, the caller location and traffic.

[0028] 9 is a storage server business support package lists, correspondence between server packages billing rules and message center number with operators, provinces.

[0029] The workflow of the invention (Figure 2):

Step S10, the synchronous network synchronization module 1 through the user's calls to the phone charging rules; step S20, the mobile terminal 2 through the monitoring module to monitor users' calls, send text messages through GPRS network behavior, and this behavior is saved for details logs;

Step S30, the grant price Module 3, using the user's calls for a detailed log accounting rules grant price; step S50, with a storage module 4 will grant price after the bill is stored on the phone. And through mobile display devices (for mobile phone display) presented to the user.

[0030] wherein step further comprises the step S10 (Figure 3):

Step S101, the user information module 5, the user selects the mobile phone operators, attribution and brand; step S102, 6, cell phones get packages list of all under the carrier of the brand from the supporting server list download module; step S103, 7, users choose their own package by selecting the modules used from the list; step S104, the adoption of the rules download module 8, cell phone charging rules to get the package from the support server.

REFERENCED BY

Citing Patent	Filing date	Publication date	Applicant	Title
CN102711076B *	May 24, 2012	Feb 11, 2015	武汉诚迈科技有限公司	一种实时预测手机通话余额的方法
WO2012171369A1 *	Mar 15, 2012	Dec 20, 2012	Zte Corporation	Method and system for calculating call charge of terminal

* Cited by examiner

CLASSIFICATIONS

International Classification	H04W4/24, H04W38/02
------------------------------	---------------------

LEGAL EVENTS

Date	Code	Event	Description
Oct 30, 2013	C12	Rejection of an application for a patent	
Jun 1, 2011	C41	Transfer of the right of patent application or the patent right	
Jun 1, 2011	ASS	Succession or assignment of patent right	Effective date: 20110421 Free format text: FORMER OWNER: LIU YANG Owner name: BEIJING WALI NETWORK TECHNOLOGY CO., LTD.
Jun 1, 2011	COR	Bibliographic change or correction in the description	Free format text: CORRECT: ADDRESS; FROM: 100190 UNIT 604, 6/F, SATELLITE BUILDING, NO. 63, ZHICHUN ROAD, HAIDIAN DISTRICT, BEIJING TO: 100114 ROOM 2533, BUILDING 3, NO. 3, XIJING ROAD, BADACHU HIGH-TECH. PARK, SHIJINGSHAN DISTRICT, BEIJING
Aug 25, 2010	C06	Publication	

Electronic Acknowledgement Receipt	
EFS ID:	22209236
Application Number:	14673625
International Application Number:	
Confirmation Number:	9085
Title of Invention:	Wireless end-user device with differentiated network access status for different device applications
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	James E. Harris/Ann Taylor
Filer Authorized By:	James E. Harris
Attorney Docket Number:	RALEP032C1C2
Receipt Date:	29-APR-2015
Filing Date:	30-MAR-2015
Time Stamp:	17:41:37
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Assignee showing of ownership per 37 CFR 3.73	P032C1C2_Statement.pdf	118446 dfe4d3a8c38e842757e5e929d6f2c72ba5c14976	no	3

Warnings:

Information:

2	Transmittal Letter	P032C1C2_IDSTransmittalLetter.pdf	59018	no	2
			ffe614be82ab4126ee6ca74db4adc9d53958b91d		
Warnings:					
Information:					
3	Information Disclosure Statement (IDS) Form (SB08)	IDS1.pdf	623001	no	37
			8b935d291e404ac3c56f4686a9ae919aadd439a0		
Warnings:					
Information:					
4	Information Disclosure Statement (IDS) Form (SB08)	IDS2.pdf	620743	no	31
			02039517801336442bc3bb708a5461c3edb5d61b		
Warnings:					
Information:					
5	Information Disclosure Statement (IDS) Form (SB08)	IDS3.pdf	619009	no	31
			d704eb13cd20eaf9541d6ccde80269e6c215d341		
Warnings:					
Information:					
6	Information Disclosure Statement (IDS) Form (SB08)	IDS4.pdf	614233	no	10
			0fb12b56dc9d9181c253756527b74b70d94666e0		
Warnings:					
Information:					
7	Foreign Reference	2060.pdf	1082588	no	10
			d731de97188a46d46fa00f136f87db05a28d9044		
Warnings:					
Information:					
8	Foreign Reference	2061.pdf	2061940	no	21
			86232d632925d26176ca285a7928e3c5a3f21baa		
Warnings:					
Information:					
9	Foreign Reference	2062.pdf	907410	no	12
			8e1e1537e7aa0c658cd339f06c2b1b63ab448ad0		
Warnings:					
Information:					
10	Non Patent Literature	3039.pdf	1271520	no	12
			5ff7631e8a8dfa2c00f75e44b77d86a2e9719407		
Warnings:					
Information:					

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

New Applications Under 35 U.S.C. 111

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

National Stage of an International Application under 35 U.S.C. 371

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

New International Application Filed with the USPTO as a Receiving Office

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

STATEMENT UNDER 37 CFR 3.73(c)

Applicant/Patent Owner: Gregory G. Raleigh

Application No./Patent No.: 14/673,625 Filed/Issue Date: March 30, 2015

Titled: Wireless End-User Device With Differentiated Network Access Status for Different Device Applications
Headwater Partners I LLC, a Limited Liability Company

(Name of Assignee)

(Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that, for the patent application/patent identified above, it is (choose **one** of options 1, 2, 3 or 4 below):

1. ☒ The assignee of the entire right, title, and interest.
2. ☐ An assignee of less than the entire right, title, and interest (check applicable box):
- ☐ The extent (by percentage) of its ownership interest is ____%. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.
- ☐ There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

3. ☐ The assignee of an undivided interest in the entirety (a complete assignment from one of the joint inventors was made). The other parties, including inventors, who together own the entire right, title, and interest are:

Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

4. ☐ The recipient, via a court proceeding or the like (e.g., bankruptcy, probate), of an undivided interest in the entirety (a complete transfer of ownership interest was made). The certified document(s) showing the transfer is attached.

The interest identified in option 1, 2 or 3 above (not option 4) is evidenced by either (choose **one** of options A or B below):

- A. ☒ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel 035292, Frame 0649, or for which a copy thereof is attached.
- B. ☐ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

2. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

[Page 1 of 2]

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450**

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

STATEMENT UNDER 37 CFR 3.73(c)

3. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

4. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

5. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

6. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

☐ As required by 37 CFR 3.73(c)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/James E. Harris/

Signature

James E. Harris

Printed or Typed Name

April 29, 2015

Date

40013

Title or Registration Number

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Raleigh et al.	Examiner: not yet assigned
Serial No.: 14/673,625	Art Unit: 2642
Filed: March 30, 2015	Conf. No.: 9085
Title: Wireless End-User Device With Differentiated Network Access Status for Different Device Applications	

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

INFORMATION DISCLOSURE STATEMENT

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

In accordance with 37 CFR §1.98(d), copies of the references can be found in related U.S. Patent Application No. 14/082,040 filed November 15, 2013, of which the instant application is a continuation, or in related U.S. Patent Application No. 13/134,028 filed May 25, 2011, of which 14/082,040 is a divisional.

It is respectfully requested that the cited references be expressly considered during the prosecution of this application, and the references be made of record therein and appear among the “references cited” on any patent to issue therefrom.

As provided for by 37 CFR § 1.97(g) and (h), no inference should be made that the information and references cited are prior art merely because they are in this statement and no

representation is being made that a search has been conducted or that this statement encompasses all the possible relevant information.

Applicant believes that no fee is required for submission of this statement, but if for any reason an insufficient fee has been paid, please charge the insufficiency to Deposit Account No. **50-5876**.

Respectfully submitted,

Date: April 29, 2015

By: /James E. Harris/
James E. Harris
Reg. No. 40,013
Headwater Partners I LLC
555 Twin Dolphin Dr., Suite 310
Redwood City, CA 94065
(650) 517-2798

CERTIFICATE OF ELECTRONIC TRANSMISSION

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

Date: April 29, 2015 By: /Ann Taylor/
Ann Taylor

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625
	Filing Date		2015-03-30
	First Named Inventor	Raleigh	
	Art Unit	2642	
	Examiner Name	not yet assigned	
	Attorney Docket Number	RALEP032C1C2	

U.S. PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1	8174970		2012-05-08	Adamczyk, Maria et al.	
	2	8165576		2012-04-24	Raju, Vishwanath et al.	
	3	8073721		2011-12-06	Lewis, Lundy	
	4	8032899		2011-10-04	Archer, Charles J. et al.	
	5	7974624		2011-07-05	Gallagher, Michael D. et al.	
	6	7907970		2011-03-15	Park, Vincent D. et al.	
	7	7778176		2010-08-17	Morford, Michael Robert	
	8	7725570		2010-05-25	Lewis, Lundy	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	14673625
	Filing Date	2015-03-30
	First Named Inventor	Raleigh
	Art Unit	2642
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1C2

	9	7634388		2009-12-15	Archer, Charles J. et al.	
	10	7633438		2009-12-15	Tysowski, Piotr Konrad	
	11	7593417		2009-09-22	Wang, James et al.	
	12	7551922		2009-06-23	Roskowski, Steve et al.	
	13	7545782		2009-06-09	Rayment, Stephen G. et al.	
	14	7039037		2006-05-02	Wang, Jiwei R. et al.	
	15	6928280		2005-08-09	Xanthos, James et al.	
	16	6765925		2004-07-20	Sawyer, Wilson et al.	
	17	5889477		1999-03-30	Fastenrath, Ulrich	
	18	8332517		2012-12-11	Russell, Jesse E.	
	19	8315718		2012-11-20	Caffrey, Paul Oliver et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	14673625
	Filing Date	2015-03-30
	First Named Inventor	Raleigh
	Art Unit	2642
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1C2

	20	8447980		2013-05-21	Godfrey, James A. et al.	
	21	8429403		2013-04-23	Moret, Eric et al.	
	22	8411587		2013-04-02	Curtis, William et al.	
	23	8396929		2013-03-12	Helfman, Nadav et al.	
	24	8363658		2013-01-29	Delker, Jason R. et al.	
	25	8265004		2012-09-11	Toutonghi, Michael J.	
	26	8233895		2012-07-31	Tysowski, Piotr Konrad	
	27	7685254		2010-03-23	Pandya, Ashish A.	
	28	7181017		2007-02-20	Nagel, Robert H. et al.	
	29	6965872		2005-11-15	Grdina, Jerome M.	
	30	8406427		2013-03-26	Chand, Naresh et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	14673625
	Filing Date	2015-03-30
	First Named Inventor	Raleigh
	Art Unit	2642
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1C2

	31	8429409		2013-04-23	Wall, Jonathan et al.	
	32	8402540		2013-03-19	Kapoor, Harsh et al.	
	33	8135657		2012-03-13	Kapoor, Harsh et al.	
	34	8271992		2012-09-18	Chatley, Scott P. et al.	
	35	8315999		2012-11-20	Chatley, Scott P. et al.	
	36	8332375		2012-12-11	Chatley, Scott P. et al.	
	37	8468337		2013-06-18	Gaur, Santosh P. et al.	
	38	8477778		2013-07-02	Lehmann Jr., L. Curtis et al.	
	39	8352630		2013-01-08	Hart, Justin Scott	
	40	6640097		2003-10-28	Corrigan, Louis et al.	
	41	7039713		2006-05-02	Van Gunter, David et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	14673625
	Filing Date	2015-03-30
	First Named Inventor	Raleigh
	Art Unit	2642
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1C2

	42	5915008		1999-06-22	Dulman, Scott	
	43	8126476		2012-02-28	Vardi, Yosef et al.	
	44	8000276		2011-08-16	Scherzer, Shimon et al.	
	45	8358638		2013-01-22	Scherzer, Tamir et al.	
	46	8356336		2013-01-15	Johnston, Keith et al.	
	47	8307067		2012-11-06	Ryan, Nicholas M.	
	48	7286848		2007-10-23	Vireday, Richard P. et al.	
	49	7313237		2007-12-25	Bahl, Paramvir et al.	
	50	7444669		2008-10-28	Bahl, Paramvir et al.	
	51	7548976		2009-06-16	Bahl, Paramvir et al.	
	52	8027339		2011-09-27	Short, Joel E. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625
	Filing Date		2015-03-30
	First Named Inventor	Raleigh	
	Art Unit	2642	
	Examiner Name	not yet assigned	
	Attorney Docket Number	RALEP032C1C2	

	53	8095112		2012-01-10	Chow, Richard et al.	
	54	8369274		2013-02-05	Sawai, Ryo	
	55	7881697		2011-02-01	Baker, Matthew Donald et al.	
	56	7899438		2011-03-01	Baker, Matthew Donald et al.	
	57	7945238		2011-05-17	Baker, Matthew Donald et al.	
	58	8078140		2011-12-13	Baker, Matthew Donald et al.	
	59	8285249		2012-10-09	Baker, Matthew Donald et al.	
	60	7493659		2009-02-17	Wu, Handong et al.	
	61	7801985		2010-09-21	Pitkow, Jim et al.	
	62	8242959		2012-08-14	Mia, Rashidus S. et al.	
	63	8326319		2012-12-04	Davis, Richard W.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625
	Filing Date		2015-03-30
	First Named Inventor	Raleigh	
	Art Unit	2642	
	Examiner Name	not yet assigned	
	Attorney Docket Number	RALEP032C1C2	

	64	8019886		2011-09-13	Harrang, Jeffrey Paul et al.	
	65	7102620		2006-09-05	Harries, Andrew Stanely Guy et al.	
	66	7139569		2006-11-21	Kato, Akira	
	67	7529204		2009-05-05	Bourlas, Yair et al.	
	68	7720960		2010-05-18	Pruss, Richard Manfred et al.	
	69	7969950		2011-06-28	Iyer, Pradeep J. et al.	
	70	8032409		2011-10-04	Mikurak, Michael G.	
	71	8045973		2011-10-25	Chambers, Michael D.	
	72	8116781		2012-02-14	Chen, Xixian et al.	
	73	8126396		2012-02-28	Bennett, James D.	
	74	8351898		2013-01-08	Raleigh, Gregory G.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625
	Filing Date		2015-03-30
	First Named Inventor	Raleigh	
	Art Unit	2642	
	Examiner Name	not yet assigned	
	Attorney Docket Number	RALEP032C1C2	

	75	5630159		1997-05-13	Zancho, William F.	
	76	5633484		1997-05-27	Zancho, William F. et al.	
	77	5814798		1998-09-29	Zancho, William F.	
	78	7039403		2006-05-02	Wong, Gregory A.	
	79	7583964		2009-09-01	Wong, Gregory A.	
	80	7593730		2009-09-22	Khandelwal, Deepak et al.	
	81	7948953		2011-05-24	Melkote, Keerti G. et al.	
	82	8200509		2012-06-12	Kenedy, Andrew Alexander et al.	
	83	8270972		2012-09-18	Otting, Marcia J. et al.	
	84	7929959		2011-04-19	DeAtley, Dallas et al.	
	85	7478420		2009-01-13	Wright, Michael et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625
	Filing Date		2015-03-30
	First Named Inventor	Raleigh	
	Art Unit	2642	
	Examiner Name	not yet assigned	
	Attorney Docket Number	RALEP032C1C2	

	86	7502672		2009-03-10	Kolls, H. Brock	
	87	7756757		2010-07-13	Oakes III, Charles Lee	
	88	7930446		2011-04-19	Kesselman, Alex et al.	
	89	8078163		2011-12-13	Lemond, Eric et al.	
	90	8068829		2011-11-29	Lemond, Eric et al.	
	91	8086497		2011-12-27	Oakes III, Charles Lee	
	92	8166040		2012-04-24	Brindisi, Richard G. et al.	
	93	6934249		2005-08-23	Bertin, Olivier et al.	
	94	7774456		2010-08-10	Lownsborough, Derek Leigh et al.	
	95	8447607		2013-05-21	Weider, Chris et al.	
	96	8504729		2013-08-06	Pezzutti, David A.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	14673625
	Filing Date	2015-03-30
	First Named Inventor	Raleigh
	Art Unit	2642
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1C2

	97	8495227		2013-07-23	Kaminsky, David L. et al.	
	98	8472371		2013-06-25	Bari, Farooq et al.	
	99	8134954		2012-03-13	Godfrey, James A. et al.	
	100	7535880		2009-05-19	Hinman, Brian L. et al.	
	101	7499438		2009-03-03	Hinman, Brian L. et al.	
	102	7496652		2009-02-24	Pezzutti, David	
	103	6957067		2005-10-18	Iyer, Pradeep J. et al.	
	104	6654814		2003-11-25	Britton, Kathryn H. et al.	
	105	8374592		2013-02-12	Proctor, Jr. James A. et al.	
	106	8325638		2012-12-04	Jin, Haipeng et al.	
	107	8116749		2012-02-14	Proctor Jr., James Arthur et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	14673625
	Filing Date	2015-03-30
	First Named Inventor	Raleigh
	Art Unit	2642
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1C2

	108	8090616		2012-01-03	Proctor Jr., James Arthur et al.	
	109	8090359		2012-01-03	Proctor Jr., James Arthur et al.	
	110	8150431		2012-04-03	Wolovitz, Lionel et al.	
	111	8483135		2013-07-09	Cai, Yigang et al.	
	112	6104700		2000-08-15	Haddock, Stephen R. et al.	
	113	8185127		2012-05-22	Cai, Zheng et al.	
	114	8521110		2013-08-27	Rofougaran, Ahmadreza	
	115	7310424		2007-12-18	Gehring, Stephan Walter et al.	
	116	7356011		2008-04-08	Waters, Christopher J.F. et al.	
	117	7546460		2009-06-09	Maes, Stephane H.	
	118	7921463		2011-04-05	Sood, Kapil et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	14673625
	Filing Date	2015-03-30
	First Named Inventor	Raleigh
	Art Unit	2642
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1C2

	119	7940751		2011-05-10	Hansen, Christopher J.	
	120	8122249		2012-02-21	Falk, Rainer et al.	
	121	8495360		2013-07-23	Falk, Rainer et al.	
	122	8520589		2013-08-27	Bhatt, Yogesh et al.	
	123	6542992		2003-04-01	Peirce, Kenneth L. et al.	
	124	8379847		2013-02-19	Bell, Robert H. et al.	
	125	8185093		2012-05-22	Jheng, Yu-Syuan et al.	
	126	8296404		2012-10-23	McDysan, Dave et al.	
	127	8195163		2012-06-05	Gisby, Doug et al.	
	128	8437734		2013-05-07	Ray, Amar N. et al.	
	129	8280351		2012-10-02	Ahmed, Shahid et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	14673625
	Filing Date	2015-03-30
	First Named Inventor	Raleigh
	Art Unit	2642
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1C2

	130	7460837		2008-12-02	Diener, Neil R.	
	131	7653394		2010-01-26	McMillin, Brian K.	
	132	8130793		2012-03-06	Edwards, Stephen K. et al.	
	133	8509082		2013-08-13	Heinz, John M. et al.	
	134	8526329		2013-09-03	Mahany, Ronald L. et al.	
	135	5983270		1999-11-09	Abraham, Dalen M. et al.	
	136	6598034		2003-07-22	Kloth, Axel K.	
	137	7032072		2006-04-18	Quinn, Michael J. et al.	
	138	7580356		2009-08-25	Mishra, Sanjeev K. et al.	
	139	7742406		2010-06-22	Muppala, Suresh	
	140	7953877		2011-05-31	Vemula, Narendra et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625
	Filing Date		2015-03-30
	First Named Inventor	Raleigh	
	Art Unit	2642	
	Examiner Name	not yet assigned	
	Attorney Docket Number	RALEP032C1C2	

	141	7957381		2011-06-07	Clermidy, Fabien et al.	
	142	8031601		2011-10-04	Feroz, Azeem et al.	
	143	8255534		2012-08-28	Assadzadeh, Alireza	
	144	8489720		2013-07-16	Morford, Michael Robert et al.	
	145	7774323		2010-08-10	Helfman, Nadav	
	146	7043268		2006-05-09	Yukie, Satoru et al.	
	147	8391262		2013-03-05	Maki, Lasse et al.	
	148	7113780		2006-09-26	McKenna, Daniel Bernard et al.	
	149	8166554		2012-04-24	John, Pramod	
	150	7697540		2010-04-13	Haddad, Reda et al.	
	151	6748195		2004-06-08	Phillips, W. Garland	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	14673625
	Filing Date	2015-03-30
	First Named Inventor	Raleigh
	Art Unit	2642
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1C2

	152	8583499		2013-11-12	De Judicibus, Dario et al.	
	153	8352360		2013-01-08	De Judicibus, Dario et al.	
	154	8463232		2013-06-11	Tuli, Amol et al.	
	155	7958029		2011-06-07	Bobich, Thomas et al.	
	156	7540408		2009-06-02	Levine, Judah Joseph et al.	
	157	7826427		2010-11-02	Sood, Kapil et al.	
	158	8185088		2012-05-22	Klein, Robert S. et al.	
	159	8548428		2013-10-01	Raleigh, Gregory G.	
	160	8483694		2013-07-09	Lewis, Allan D. et al.	
	161	8351592		2013-01-08	Freeny, Jr., Charles C. et al.	
	162	8452858		2013-05-28	Wu, John et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	14673625
	Filing Date	2015-03-30
	First Named Inventor	Raleigh
	Art Unit	2642
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1C2

	163	7610396		2009-10-27	Taglienti, Claudio et al.	
	164	7984511		2011-07-19	Kocher, Paul Carl et al.	
	165	7987510		2011-07-26	Kocher, Paul C. et al.	
	166	8571993		2013-10-29	Kocher, Paul C. et al.	
	167	8543265		2013-09-24	Ekhuagere, David E. et al.	
	168	8385975		2013-02-26	Forutanpour, Babak	
	169	6873988		2005-03-29	Hermann, Conrad K. et al.	
	170	7013469		2006-03-14	Smith, Adam W. et al.	
	171	7203169		2007-04-10	Okholm, Jon Eric et al.	
	172	7286834		2007-10-23	Walter, Edward	
	173	7555757		2009-06-30	Smith, Adam W. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	14673625
	Filing Date	2015-03-30
	First Named Inventor	Raleigh
	Art Unit	2642
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1C2

	174	7574509		2009-08-11	Nixon, Mark J. et al.	
	175	7826607		2010-11-02	de Carvalho Resende, Mauricio Guilherme et al.	
	176	7940685		2011-05-10	Breslau, Lee Michel et al.	
	177	8196199		2012-06-05	Hrastar, Scott E. et al.	
	178	8204505		2012-06-19	Jin, Haipeng et al.	
	179	8228818		2012-07-24	Chase, Christopher J. et al.	
	180	8320244		2012-11-27	Muqattash, Alaa et al.	
	181	8411691		2013-04-02	Aggarwal, Rahul	
	182	8461958		2013-06-11	Saenz, Jorge E. et al.	
	183	8484327		2013-07-09	Werner, Eran et al.	
	184	8522039		2013-08-27	Hyndman, Arn et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625
	Filing Date		2015-03-30
	First Named Inventor	Raleigh	
	Art Unit	2642	
	Examiner Name	not yet assigned	
	Attorney Docket Number	RALEP032C1C2	

	185	8544105		2013-09-24	McClean, Ivan H. et al.	
	186	8571474		2013-10-29	Chavez, Timothy R. et al.	
	187	8194572		2012-06-05	Horvath, Robert et al.	
	188	8516552		2013-08-20	Raleigh, Gregory G.	
	189	8441955		2013-05-14	Wilkinson, Robert Todd et al.	
	190	5774532		1998-06-30	Gottlieb, Louis G. et al.	
	191	8095124		2012-01-10	Balia, Hinal K.	
	192	7797060		2010-09-14	Grgic, Richard J. et al.	
	193	7930327		2011-04-19	Craft, David Jones et al.	
	194	8264965		2012-09-11	Dolganow, Andrew et a.	
	195	8626115		2014-01-07	Raleigh, Gregory G. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625
	Filing Date		2015-03-30
	First Named Inventor	Raleigh	
	Art Unit	2642	
	Examiner Name	not yet assigned	
	Attorney Docket Number	RALEP032C1C2	

	196	6885997		2005-04-26	Roberts, David T.	
	197	8229394		2012-07-24	Karlberg, Johan	
	198	8495700		2013-07-23	Shahbazi, Majid	
	199	8548427		2013-10-01	Chow, Paulo S.T. et al.	
	200	8572117		2013-10-29	Rappaport, Theodore S.	
	201	8589955		2013-11-19	Roundtree, Brian et al.	
	202	8660853		2014-02-25	Robb, Terence A. et al.	
	203	8601125		2013-12-03	Huang, Shibi et al	
	204	8046449		2011-10-25	Yoshiuchi, Hideya	
	205	8635164		2014-01-21	Rosenhaft, Matthew et al.	
	206	8566236		2013-10-22	Busch, James David	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625
	Filing Date		2015-03-30
	First Named Inventor	Raleigh	
	Art Unit	2642	
	Examiner Name	not yet assigned	
	Attorney Docket Number	RALEP032C1C2	

	207	8528068		2013-09-03	Weglein, Joseph et al.	
	208	8442015		2013-05-14	Behzad, Arya et al	
	209	7853255		2010-12-14	Karaoguz, Jeyhan et al	
	210	7720464		2010-05-18	Batta, Puneet	
	211	8300575		2012-10-30	Willars, Per	
	212	8666395		2014-03-04	Silver, Andrew	
	213	8315593		2012-11-20	Gallant, John K. et al.	
	214	8180881		2012-05-15	Seo, Kyoung-II et al.	
	215	7539132		2009-05-26	Werner, Carl E. et al.	
	216	8589541		2013-11-19	Raleigh, Gregory G. et al.	
	217	7805606		2010-09-28	Birger, Chet et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625
	Filing Date		2015-03-30
	First Named Inventor	Raleigh	
	Art Unit	2642	
	Examiner Name	not yet assigned	
	Attorney Docket Number	RALEP032C1C2	

	218	8347378		2013-01-01	Merkin, Aaron E. et al.	
	219	8391834		2013-03-05	Raleigh, Gregory G.	
	220	6185576		2001-02-06	McIntosh, Lowrie	
	221	8175574		2012-05-08	Panda, Biswaranjan et al.	
	222	8375128		2013-02-12	Tofighbakhsh, Mostafa et al.	
	223	8527410		2013-09-03	Markki, Outi et al.	
	224	7320029		2008-01-15	Rinne, Janne Petri et al.	
	225	8275415		2012-09-25	Huslak, Nicholas S.	
	226	8539561		2013-09-17	Gupta, Akhilesh et al.	
	227	8554876		2013-10-08	Winsor, Gerald W.	
	228	8191124		2012-05-29	Wynn, Simon et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	14673625
	Filing Date	2015-03-30
	First Named Inventor	Raleigh
	Art Unit	2642
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1C2

	229	7805140		2010-09-28	Friday, Robert J. et al.	
	230	8605691		2013-12-10	Soomro, Amjad et al.	
	231	8655357		2014-02-18	Gazzard, Daryl Robert et al.	
	232	8706863		2014-04-22	Fadell, Anthony	
	233	6640334		2003-10-28	Rasmussen, John H.	
	234	7668612		2010-02-23	Okkonen, Harri	
	235	5325532		1994-06-28	Crosswy, Wm. Caldwell et al.	
	236	7614051		2009-11-03	Glaum, Jeffrey D. et al.	
	237	5131020		1992-07-14	Liebesny, John P. et al.	
	238	8223741		2012-07-17	Bartlett, Roger Danforth et al.	
	239	8396458		2013-03-12	Raleigh, Gregory G.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	14673625
	Filing Date	2015-03-30
	First Named Inventor	Raleigh
	Art Unit	2642
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1C2

	240	8370483		2013-02-05	Choong et al.	
	241	8670334		2014-03-11	Keohane et al.	
	242	8693323		2014-04-08	McDysan, David E.	
	243	7409447		2008-08-05	Assadzadeh, Alireza	
	244	8725899		2014-05-13	Short, Joel et al.	
	245	8676925		2014-03-18	Liu, Jiawei et al.	
	246	8645518		2014-02-04	David, Scott L.	
	247	7756056		2010-07-13	Kim et al	
	248	8131281		2012-03-06	Hildner et al.	
	249	8160598		2012-04-17	Savoor, Raghvendra	
	250	8375136		2013-02-12	Roman et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625
	Filing Date		2015-03-30
	First Named Inventor	Raleigh	
	Art Unit	2642	
	Examiner Name	not yet assigned	
	Attorney Docket Number	RALEP032C1C2	

	251	6119933		2000-09-19	Wong et al.	
	252	8694772		2014-04-08	Kao et al.	
	253	8719423		2014-05-06	Wyld, Jeremy	
	254	8347104		2013-01-01	Pathiyal, Krishna K.	
	255	7149229		2006-12-12	Leung, Kent K.	
	256	7242668		2007-07-10	Kan, Chao et al.	
	257	8095640		2012-01-10	Guingo, Pierrick et al.	
	258	8705361		2014-04-22	Venkataraman, Ramesh et al.	
	259	8780857		2014-07-15	Balasubramanian, Srinivasan et al.	
	260	8811991		2014-08-19	Jain, Nikhil et al.	
	261	7809351		2010-10-05	Panda et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	14673625
	Filing Date	2015-03-30
	First Named Inventor	Raleigh
	Art Unit	2642
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1C2

	262	8346210		2013-01-01	Balsan, Damien et al.	
	263	8355696		2013-01-15	Olding et al.	
	264	8488597		2013-07-16	Nie et al.	
	265	6438575		2002-08-20	Khan et al.	
	266	7222304		2007-05-22	Beaton et al.	
	267	7561899		2009-07-14	Lee, Changseok	
	268	8200200		2012-06-12	Belser et al.	
	269	8229914		2012-07-24	Ramer et al.	
	270	8522249		2013-08-27	Beaule, Stephane	
	271	8701015		2014-04-15	Bonnat, Pierre	
	272	6697821		2004-02-24	Ziff et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625	
	Filing Date		2015-03-30	
	First Named Inventor	Raleigh		
	Art Unit	2642		
	Examiner Name	not yet assigned		
	Attorney Docket Number	RALEP032C1C2		

	273	6763226		2004-07-13	McZeal Jr., Alfred	
	274	6982733		2006-01-03	McNally et al.	
	275	6983370		2006-01-03	Eaton, et al.	
	276	7318111		2008-01-08	Zhao, Wen	
	277	8064418		2011-11-22	Maki, Lasse	
	278	8249601		2012-08-21	Emberson et al.	
	279	8514927		2013-08-20	Sundararajan et al.	

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

Add

U.S.PATENT APPLICATION PUBLICATIONS

Remove

Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

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

Add

FOREIGN PATENT DOCUMENTS

Remove

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	14673625
	Filing Date	2015-03-30
	First Named Inventor	Raleigh
	Art Unit	2642
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1C2

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ² j	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1	1538730A	CN		2004-10-20	Zhongxing Communication Co., Ltd.		☐
	2	101115248A	CN		2008-01-30	Lenovo Beijing Ltd.		☐
	3	101341764A	CN		2009-01-07	Telefonaktiebolaget LM Ericsson		☐
	4	2007068288A1	WO		2007-06-21	Telefonaktiebolaget LM Ericsson		☐
	5	1802839A	CN		2006-07-12	Motorola Inc.		☐
	6	2004064306A2	WO		2004-07-29	Motorola Inc.		☐
	7	101123553A	CN		2007-09-11	SouTheast University		☐
	8	1937511A	CN		2007-03-28	ZTE		☐
	9	2466831A1	EP		2012-06-20	Openet Telecom Ltd./ McNamee et al.		☐
	10	1999027723 A1	WO		1999-06-03	Telefonaktiebolaget LM Ericsson		☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625	
	Filing Date		2015-03-30	
	First Named Inventor	Raleigh		
	Art Unit	2642		
	Examiner Name	not yet assigned		
	Attorney Docket Number	RALEP032C1C2		

	11	2007133844	WO		2007-11-22	Camiant, Inc.		☐
	12	2011149532 A1	WO		2011-12-01	Raleigh, Gregory G. et al.		☐
	13	101183958A	CN		2008-05-21	Huawei Tech. Co. Ltd.		☐
	14	1801829A	CN		2006-07-12	Kunda Computer Technology (Kunshan) Co., Ltd.		☐
	15	1867024A	CN		2006-11-22	Huawei Technologies Co., Ltd.		☐
	16	101815275A	CN		2010-08-25	Yang, Liu		☐

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

NON-PATENT LITERATURE DOCUMENTS

Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1	VerizonWireless.com news, "Verizon Wireless Adds to Portfolio of Cosumer-Friendly Tools With Introduction of Usage Controls, Usage Controls and Chaperone 2.0 Offer Parents Full Family Security Solution," August 18, 2008	☐
	2	"The Construction of Intelligent Residential District in Use of Cable Television Network," Shandong Science, Vol. 13, No. 2, June 2000	☐
	3	"Communication Concepts for Mobile Agent Systems," by Joachim Baumann et al.; Inst. Of Parallel and Distributed High-Performance Systems, Univ. of Stuttgart, Germany, pp. 123-135, 1997	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625
	Filing Date		2015-03-30
	First Named Inventor	Raleigh	
	Art Unit	2642	
	Examiner Name	not yet assigned	
	Attorney Docket Number	RALEP032C1C2	

	4	"Prevent iCloud Documents & Data from using your data plan," October 26, 2011; CNET webarchive, by Jason Cipriani	☐
	5	"3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Policy and charging control architecture (Release 11)," 3GPP Standard; 3GPP TS 23.203 v11.6.0; Sophia Antipolis, France; pp. 1-177; June 2012	☐
	6	"End to End QoS Solution for Real-time Multimedia Application;" Computer Engineering and Applications, 2007, 43 (4): 155-159, by Tan Zu-guo, Wang Wen-juan; Information and Science School, Zhanjian Normal College, Zhan jiang, Guangdong 524048, China	☐
	7	"ASA/PIX: Allow Split Tunneling for VPN Clients on the ASA Configuration Example," Document ID 70917, January 10, 2008	☐

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

EXAMINER SIGNATURE

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	14673625
	Filing Date	2015-03-30
	First Named Inventor	Raleigh
	Art Unit	2642
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1C2

CERTIFICATION STATEMENT

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

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

OR

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

☐ See attached certification statement.

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

☒ None

SIGNATURE

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

Signature	/James E. Harris/	Date (YYYY-MM-DD)	2015-04-29
Name/Print	James E. Harris	Registration Number	40013

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

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625
	Filing Date		2015-03-30
	First Named Inventor	Raleigh	
	Art Unit	2642	
	Examiner Name	not yet assigned	
	Attorney Docket Number	RALEP032C1C2	

U.S. PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1	5577100		1996-11-19	McGREGOR et al.	
	2	5794142		1998-08-11	VANTTILA et al.	
	3	5892900		1999-04-06	GINTER et al.	
	4	5903845		1999-05-11	BUHRMANN et al.	
	5	5933778		1999-08-03	BUHRMANN et al.	
	6	5940472		1999-08-17	NEWMAN et al.	
	7	6047268		2000-04-04	BARTOLI et al.	
	8	6078953		2000-06-20	VAID et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625
	Filing Date		2015-03-30
	First Named Inventor	Raleigh	
	Art Unit	2642	
	Examiner Name	not yet assigned	
	Attorney Docket Number	RALEP032C1C2	

	9	6098878		2000-08-08	DENT et al.	
	10	6141686		2000-10-31	JACKOWSKI et al.	
	11	6148336		2000-11-14	THOMAS et al.	
	12	6198915		2001-03-06	McGREGOR et al.	
	13	6263055		2001-07-17	GARLAND et al.	
	14	6317584		2001-11-13	ABU-AMARA et al.	
	15	6418147		2002-07-09	WIEDEMAN, Robert A.	
	16	6449479		2002-09-10	SANCHEZ, Eduardo	
	17	6532235		2003-03-11	BENSON et al.	
	18	6532579		2003-03-11	SATO et al.	
	19	6539082		2003-03-25	LOWE et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625
	Filing Date		2015-03-30
	First Named Inventor	Raleigh	
	Art Unit	2642	
	Examiner Name	not yet assigned	
	Attorney Docket Number	RALEP032C1C2	

	20	6563806		2003-05-13	YANO et al.	
	21	6574321		2003-06-03	COX et al.	
	22	6574465		2003-06-03	MARSH et al.	
	23	6603969		2003-08-05	VUORISTO et al.	
	24	6639975		2003-10-28	O'NEAL et al.	
	25	6650887		2003-11-18	McGREGOR et al.	
	26	6651101		2003-11-18	GAI et al.	
	27	6658254		2003-12-02	PURDY et al.	
	28	6684244		2004-01-27	GOLDMAN et al.	
	29	6725031		2004-04-20	WATLER et al.	
	30	6765864		2004-07-20	NATARAJAN et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	14673625
	Filing Date	2015-03-30
	First Named Inventor	Raleigh
	Art Unit	2642
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1C2

	31	6785889		2004-08-31	WILLIAMS, Peter	
	32	6829596		2004-12-07	FRAZEE, Steve	
	33	6829696		2004-12-07	BALMER et al.	
	34	6920455		2005-07-19	WESCHLER, Paul	
	35	6952428		2005-10-04	NECKA et al.	
	36	6965667		2005-11-15	TRABANDT et al.	
	37	6996076		2006-02-07	FORBES et al.	
	38	6998985		2006-02-14	REISMAN et al.	
	39	7024200		2006-04-04	McKENNA et al.	
	40	7027408		2006-04-11	NABKEL et al.	
	41	7042988		2006-05-09	JUITT et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	14673625
	Filing Date	2015-03-30
	First Named Inventor	Raleigh
	Art Unit	2642
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1C2

	42	7058968		2006-06-06	ROWLAND et al.	
	43	7069248		2006-06-27	HUBER, Adriano	
	44	7092696		2006-08-15	HOSAIN et al.	
	45	7142876		2006-11-28	TROSSEN et al.	
	46	7158792		2007-01-02	COOK et al.	
	47	7174174		2007-02-06	BORIS et al.	
	48	7180855		2007-02-20	LIN , Wei	
	49	7197321		2007-03-27	ERSKINE et al.	
	50	7242920		2007-07-10	MORRIS, Robert P.	
	51	7245901		2007-07-17	McGREGOR et al.	
	52	7280816		2007-10-09	FRATTI et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625
	Filing Date		2015-03-30
	First Named Inventor	Raleigh	
	Art Unit	2642	
	Examiner Name	not yet assigned	
	Attorney Docket Number	RALEP032C1C2	

	53	7280818		2007-10-09	CLAYTON, Steve	
	54	7289489		2007-10-30	KUNG et al.	
	55	7290283		2007-10-30	COPELAND III, John A.	
	56	7317699		2008-01-08	GODFREY et al.	
	57	7322044		2008-01-22	HRASTAR, Scott E.	
	58	7324447		2008-01-29	MORFORD, Michael Robert	
	59	7325037		2008-01-29	LAWSON, Karen L.	
	60	7349695		2008-03-25	OOMMEN et al.	
	61	7353533		2008-04-01	WRIGHT et al.	
	62	7356337		2008-04-08	FLORENCE, Shahar	
	63	7366497		2008-04-29	NAGATA, Hideaki	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625
	Filing Date		2015-03-30
	First Named Inventor	Raleigh	
	Art Unit	2642	
	Examiner Name	not yet assigned	
	Attorney Docket Number	RALEP032C1C2	

	64	7373136		2008-05-13	WATLER et al.	
	65	7388950		2008-06-17	ELSEY et al.	
	66	7401338		2008-07-15	BOWEN et al.	
	67	7403763		2008-07-22	MAES, Stephane H.	
	68	7418253		2008-08-26	KAVANAHA, Alan	
	69	7421004		2008-09-02	FEHER, Kamilo	
	70	7450591		2008-11-11	KORLING et al.	
	71	7450927		2008-11-11	CRESWELL et al.	
	72	7486185		2009-02-03	CULPEPPER et al.	
	73	7499537		2009-03-03	ELSEY et al.	
	74	7516219		2009-04-07	MOGHADDAM et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	14673625
	Filing Date	2015-03-30
	First Named Inventor	Raleigh
	Art Unit	2642
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1C2

	75	7574731		2009-08-11	FASCENDA, Anthony C.	
	76	7580857		2009-08-25	VanFLEET et al.	
	77	7610328		2009-10-27	HAASE et al.	
	78	7617516		2009-11-10	HUSLAK et al.	
	79	7620065		2009-11-17	FALARDEAU, Eric	
	80	7620162		2009-11-17	AARON et al.	
	81	7647047		2010-01-12	MOGHADDAM et al.	
	82	7650137		2010-01-19	JOBS et al.	
	83	7668903		2010-02-23	EDWARDS et al.	
	84	7693720		2010-04-06	KENNEWICK et al.	
	85	7720505		2010-05-18	GOPI et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	14673625
	Filing Date	2015-03-30
	First Named Inventor	Raleigh
	Art Unit	2642
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1C2

	86	7734784		2010-06-08	ARAUJO et al.	
	87	7747240		2010-06-29	BRISCOE et al.	
	88	7747699		2010-06-29	PRUEITT et al.	
	89	7792708		2010-09-07	ALVA, Jessi	
	90	7797204		2010-09-14	BALENT, Bruce F.	
	91	7797401		2010-09-14	STEWART et al.	
	92	7822837		2010-10-26	URBAN et al.	
	93	7848768		2010-12-07	OMORI et al.	
	94	7868778		2011-01-11	KENWRIGHT, David Norris	
	95	7873705		2011-01-18	KALISH, Dan	
	96	7882029		2011-02-01	WHITE, Craig R.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	14673625
	Filing Date	2015-03-30
	First Named Inventor	Raleigh
	Art Unit	2642
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1C2

	97	7929960		2011-04-19	MARTIN et al.	
	98	7937069		2011-05-03	RASSAM, Frederic	
	99	7941184		2011-05-10	PRENDERGAST et al.	
	100	7949529		2011-05-24	WEIDER et al.	
	101	7957511		2011-06-07	DRUDIS et al.	
	102	7975184		2011-07-05	GOFF et al.	
	103	7984130		2011-07-19	BOGINENI et al.	
	104	7986935		2011-07-26	D'SOUZA et al.	
	105	8005459		2011-08-23	BALSILLIE, Jim	
	106	8010080		2011-08-30	THENTHIRUPERAI et al.	
	107	8010081		2011-08-30	ROSKOWSKI, Steve	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625
	Filing Date		2015-03-30
	First Named Inventor	Raleigh	
	Art Unit	2642	
	Examiner Name	not yet assigned	
	Attorney Docket Number	RALEP032C1C2	

	108	8015133		2011-09-06	WU et al.	
	109	8015234		2011-09-06	LUM et al.	
	110	8019687		2011-09-13	WANG et al.	
	111	8023425		2011-09-20	RALEIGH, Gregory G.	
	112	8095666		2012-01-10	SCHMIDT et al.	
	113	8099077		2012-01-17	CHOWDHURY et al.	
	114	8099517		2012-01-17	JIA et al.	
	115	8144591		2012-03-27	GHAJ et al.	
	116	8170553		2012-05-01	BENNETT, James D.	
	117	6606744		2003-08-12	MIKURAK, Michael G.	
	118	7336960		2008-02-26	ZAVALKOVSKY et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625
	Filing Date		2015-03-30
	First Named Inventor	Raleigh	
	Art Unit	2642	
	Examiner Name	not yet assigned	
	Attorney Docket Number	RALEP032C1C2	

	119	8190675		2012-05-29	TRIBBETT, David	
	120	8194549		2012-06-05	HUBER et al.	
	121	8200775		2012-06-12	MOORE, James F.	
	122	8135392		2012-03-13	MARCELLINO et al.	
	123	7953808		2011-05-31	SHARP et al.	
	124	6502131		2002-12-31	VAID, Aseem et al.	
	125	6505114		2003-01-07	LUCIANI, Sergio	
	126	6763000		2004-07-13	WALSH, Peter J.	
	127	6967958		2005-11-22	ONO, Yoshiyuki et al.	
	128	7644267		2010-01-05	YLIKOSKI, Martti et al.	
	129	7710932		2010-05-04	MUTHUSWAMY, Sivakumar et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	14673625
	Filing Date	2015-03-30
	First Named Inventor	Raleigh
	Art Unit	2642
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1C2

	130	7881199		2011-02-01	KRSTULICH, Zlatko	
	131	7886047		2011-02-08	POTLURI, Dora	
	132	7911975		2011-03-22	DROZ, Patrick et al.	
	133	8050275		2011-11-01	IYER, Jayaraman R.	
	134	8194553		2012-06-05	LIANG, Zhi Yong et al.	
	135	8239520		2012-08-07	GRAH, Adrian	
	136	7890084		2011-02-15	Dudziak, Thaddeus Jude et al.	
	137	7890111		2011-02-15	Bugenhagen, Michael K.	
	138	6226277		2001-05-01	Chuah, Mooi Choo	
	139	6839340		2005-01-04	Voit, Eric A. et al.	
	140	6922562		2005-07-26	Ward, Stephen L. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	14673625
	Filing Date	2015-03-30
	First Named Inventor	Raleigh
	Art Unit	2642
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1C2

	141	7620041		2009-11-17	Dunn, Jeffrey H. et al.	
	142	7627314		2009-12-01	Carlson, Steven I. et al.	
	143	7792538		2010-09-07	Kozisek, Steven E.	
	144	7801523		2010-09-21	Kenderov, Stoyan	
	145	7877090		2011-01-25	Maes, Stephane H.	
	146	7912025		2011-03-22	Pattenden, Christopher E. S. et al.	
	147	7948968		2011-05-24	Voit, Eric A. et al.	
	148	7970426		2011-06-28	Poe, Brian R. et al.	
	149	8185158		2012-05-22	Tamura, Motoshi et al.	
	150	8254915		2012-08-28	Kozisek, Steven E.	
	151	7418257		2008-08-26	Kim, Myong-Ju	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	14673625
	Filing Date	2015-03-30
	First Named Inventor	Raleigh
	Art Unit	2642
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1C2

	152	8126123		2012-02-28	Cai, Yigang et al.	
	153	7903553		2011-03-08	Liu, Enhui	
	154	8155620		2012-04-10	Wang, Jun et al.	
	155	8238287		2012-08-07	Gopi, Paramesh et al.	
	156	7113997		2006-09-26	Jayapalan, Jay et al.	
	157	5594777		1997-01-14	Makkonen, Matti et al.	
	158	8244241		2012-08-14	Montemurro, Michael	
	159	7756534		2010-07-13	Anupam, Vinod et al.	
	160	7636574		2009-12-22	Poosala, Viswanath	
	161	6678516		2004-01-13	Nordman, Ian et al.	
	162	6477670		2002-11-05	Ahmadvand, Nima	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625
	Filing Date		2015-03-30
	First Named Inventor	Raleigh	
	Art Unit	2642	
	Examiner Name	not yet assigned	
	Attorney Docket Number	RALEP032C1C2	

	163	6038452		2000-03-14	Strawczynski, Leo et al.	
	164	8108520		2012-01-31	Ruutu, Jussi et al.	
	165	7778643		2010-08-17	Laroia, Rajiv et al.	
	166	7668176		2010-02-23	Chuah, Mooi Choo	
	167	7515608		2009-04-07	Yuan, Yuan et al.	
	168	7251218		2007-07-31	Jorgensen, Jacob W.	
	169	7002920		2006-02-21	Ayyagari, Deepak et al.	
	170	7685131		2010-03-23	Batra, Vishal Singh et al.	
	171	7283561		2007-10-16	Picher-Dempsey, Heidi	
	172	7212491		2007-05-01	Koga, Takahiro	
	173	6683853		2004-01-27	Kannas, Chris et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625
	Filing Date		2015-03-30
	First Named Inventor	Raleigh	
	Art Unit	2642	
	Examiner Name	not yet assigned	
	Attorney Docket Number	RALEP032C1C2	

	174	8064896		2011-11-22	BELL, Kris M. et al.	
	175	8160015		2012-04-17	RASHID, Mohammed H. et al.	
	176	8275830		2012-09-25	Raleigh, Gregory G.	
	177	7609700		2009-10-27	Ying, Wen-Ping et al.	
	178	8255515		2012-08-28	MELMAN, David et al.	
	179	7945240		2011-05-17	KLOCK, Jacqueline et al.	
	180	7912056		2011-03-22	BRASSEM, Wayne	
	181	7920529		2011-04-05	MAHLER, Roger et al.	
	182	8184530		2012-05-22	SWAN, Tim L. et al.	
	183	8214536		2012-07-03	ZHAO, Wen	
	184	8213363		2012-07-03	Ying, Wen-Ping et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625
	Filing Date		2015-03-30
	First Named Inventor	Raleigh	
	Art Unit	2642	
	Examiner Name	not yet assigned	
	Attorney Docket Number	RALEP032C1C2	

	185	8255689		2012-08-28	KIM, Eun Ah et al.	
	186	7746854		2010-06-29	AMBE, Shekhar et al.	
	187	7068600		2006-06-27	CAIN, Joseph Bibb	
	188	6876653		2005-04-05	AMBE, Shekhar et al.	
	189	6631122		2003-10-07	ARUNACHALAM, Vaidhyanathan et al.	
	190	7599288		2009-10-06	COLE, Raymond E. et al.	
	191	7546629		2009-06-09	ALBERT, Anthony et al.	
	192	7747730		2010-06-29	HARLOW, James D.	
	193	7609650		2009-10-27	ROSKOWSKI, Steve et al.	
	194	6581092		2003-06-17	MOTOYAMA, Tetsuro	
	195	7283963		2007-10-16	FITZPATRICK, John E. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	14673625
	Filing Date	2015-03-30
	First Named Inventor	Raleigh
	Art Unit	2642
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1C2

	196	8271049		2012-09-18	SILVER, Andrew et al.	
	197	7644151		2010-01-05	JERRIM, John et al.	
	198	8291238		2012-10-16	GINTER, Karl L. et al.	
	199	8068824		2011-11-29	SHAN, Xueshan et al.	
	200	7228354		2007-06-05	CHAMBLISS, David Darden et al.	
	201	5283904		1994-02-01	CARSON, David G. et al.	
	202	8208919		2012-06-26	KOTECHA, Lalit Ratilal	
	203	8185152		2012-05-22	GOLDNER, Alla	
	204	7844728		2010-11-30	ANDERSON, Thomas W. et al.	
	205	7873344		2011-01-18	BOWSER, Robert et al.	
	206	7856226		2010-12-21	WONG, Ellis L. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	14673625
	Filing Date	2015-03-30
	First Named Inventor	Raleigh
	Art Unit	2642
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1C2

	207	7948952		2011-05-24	HURTTA, Tuija et al.	
	208	7957020		2011-06-07	MINE, Ryuta et al.	
	209	7346410		2008-03-18	UCHIYAMA, Kenji	
	210	7167078		2007-01-23	POURCHOT, Shawn C.	
	211	8102814		2012-01-24	RAHMAN, Shahriar I. et al.	
	212	7970350		2011-06-28	SHEYNMAN, Arnold	
	213	8094551		2012-01-10	HUBER, Kurt Donald et al.	
	214	8335161		2012-12-18	Foottit, Tom et al.	
	215	8315594		2012-11-20	Mauser, Edward Ronald et al.	
	216	8135388		2012-03-13	Gailloux, Michael A. et al.	
	217	6947723		2005-09-20	Gurnani, Roger et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625
	Filing Date		2015-03-30
	First Named Inventor	Raleigh	
	Art Unit	2642	
	Examiner Name	not yet assigned	
	Attorney Docket Number	RALEP032C1C2	

	218	8353001		2013-01-08	Herrod, Allan	
	219	8195093		2013-06-05	Garrett, Darrin et al.	
	220	8036600		2011-10-11	Garrett, Darrin et al.	
	221	8301513		2012-10-30	Peng, Shih-Ta et al.	
	222	8230061		2012-07-24	Hassan, Amer A. et al.	
	223	8204794		2012-06-19	Peng, Shih-Ta et al.	
	224	8350700		2013-01-08	Fast, Raymond D. et al.	
	225	8204190		2012-06-19	Bang, Jung-Hee et al.	
	226	7865182		2011-01-04	Macaluso, Anthony G.	
	227	7962622		2011-06-14	Friend, John et al.	
	228	7583964		2009-09-01	Wong, Gregory A.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625
	Filing Date		2015-03-30
	First Named Inventor	Raleigh	
	Art Unit	2642	
	Examiner Name	not yet assigned	
	Attorney Docket Number	RALEP032C1C2	

	229	7565141		2009-07-21	Macaluso, Anthony G.	
	230	7373179		2008-05-13	Stine, Ted et al.	
	231	7236780		2007-06-26	Benco, David S.	
	232	7039403		2006-05-02	Wong, Gregory A.	
	233	8370477		2013-02-05	Short, Joel E. et al.	
	234	8364806		2013-01-29	Short, Joel E. et al.	
	235	8279067		2012-10-02	BERGER, Thomas R. et al.	
	236	8213296		2012-07-03	SHANNON, Frank M. et al.	
	237	8019868		2011-09-13	RAO, Goutham et al.	
	238	8005988		2011-08-23	MAES, Stephane H.	
	239	7978627		2011-07-12	TAYLOR, William Scott et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625
	Filing Date		2015-03-30
	First Named Inventor	Raleigh	
	Art Unit	2642	
	Examiner Name	not yet assigned	
	Attorney Docket Number	RALEP032C1C2	

	240	7711848		2010-05-04	MAES, Stephane H.	
	241	6782412		2004-08-24	BROPHY, Kevin et al.	
	242	6081591		2000-06-27	SKOOG, Frederick H.	
	243	6064878		2000-05-16	DENKER, John Stewart et al.	
	244	7730123		2010-06-01	ERICKSON, Richard R. et al.	
	245	8024397		2011-09-20	ERICKSON, Richard R. et al.	
	246	8156206		2012-04-10	KILEY, Kevin J. et al.	
	247	8126722		2012-02-28	ROBB, Terence Alan et al.	
	248	8364089		2013-01-29	PHILLIPS, Derek	
	249	6754470		2004-06-22	Hendrickson, Keith et al.	
	250	8122128		2012-02-21	Burke, II, Robert M. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625
	Filing Date		2015-03-30
	First Named Inventor	Raleigh	
	Art Unit	2642	
	Examiner Name	not yet assigned	
	Attorney Docket Number	RALEP032C1C2	

	251	8149823		2012-04-03	Turcan, Diane Brown et al.	
	252	8326359		2012-12-04	Kauffman, Donald C.	
	253	8131256		2012-03-06	MARTTI, Jyrki et al.	
	254	6381316		2002-04-30	JOYCE, Simon James et al.	
	255	7965983		2011-06-21	SWAN, Tim et al.	
	256	8284740		2012-10-09	O'CONNOR, Dennis M.	
	257	8116223		2012-02-14	TIAN, Dan et al.	
	258	6154738		2000-11-28	CALL, Charles Gainor	
	259	8423016		2013-04-16	BUCKLEY, Adrian et al.	
	260	8306518		2012-11-06	GAILLOUX, Michael A.	
	261	8422988		2013-04-16	KESHAV, Srinivasan	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	14673625
	Filing Date	2015-03-30
	First Named Inventor	Raleigh
	Art Unit	2642
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1C2

	262	6035281		2000-03-07	Crosskey, James P. et al.	
	263	6996393		2006-02-07	Pyhalammi, Seppo et al.	
	264	7760711		2010-07-20	Kung, Fen-Chung et al.	
	265	8000318		2011-08-16	Wiley, William L. et al.	
	266	8098579		2012-01-17	Ray, Amar N. et al.	
	267	8155670		2012-04-10	Fullam, Scott et al.	
	268	8374090		2013-02-12	Morrill, Robert J. et al.	
	269	7457265		2008-11-25	Julka, Vibhor et al.	
	270	7729326		2010-06-01	Sekhar, Ramesh	
	271	7929973		2011-04-19	Zavalkovsky, Arthur et al.	
	272	7945945		2011-05-17	Graham, Richard et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625	
	Filing Date		2015-03-30	
	First Named Inventor	Raleigh		
	Art Unit	2642		
	Examiner Name	not yet assigned		
	Attorney Docket Number	RALEP032C1C2		

	273	8059530		2011-11-15	Cole, Terry L.	
	274	8266681		2012-09-11	Deshpande, Sumit B. et al.	
	275	8280354		2012-10-02	Smith, Christopher et al.	
	276	8331293		2012-12-11	Sood, Kapil	
	277	8019820		2011-09-13	Son, Giyeong et al.	
	278	8191116		2012-05-29	Gazzard, Daryl	
	279	6292828		2001-09-18	Williams, David L.	
	280	7043226		2006-05-09	Yamauchi, Toshiaki	
	281	7472189		2008-12-30	Mallya, Arvind R. et al.	
	282	7944948		2011-05-17	Chow, Albert T. et al.	
	283	7802724		2010-09-28	Nohr, Steven Paul	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	14673625
	Filing Date	2015-03-30
	First Named Inventor	Raleigh
	Art Unit	2642
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1C2

	284	8155155		2012-04-10	Chow, Albert T. et al.	
	285	8447324		2013-05-21	Shuman, Mohammed Ataur et al.	
	286	8005009		2011-08-23	McKee, Neil et al.	
	287	7760861		2010-07-20	Croak, Marian et al.	
	288	8060463		2011-11-15	Spiegel, Joel R.	
	289	8224773		2012-07-17	Spiegel, Joel R.	
	290	8352980		2013-01-08	Howcroft, Jerald Robert	
	291	8386386		2013-02-26	Zhu, Kevin	
	292	8347362		2013-01-01	Cai, Yigang et al.	
	293	8340718		2012-12-25	Colonna, Massimo et al.	
	294	8385896		2013-02-26	Proctor Jr., James A. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625	
	Filing Date		2015-03-30	
	First Named Inventor	Raleigh		
	Art Unit	2642		
	Examiner Name	not yet assigned		
	Attorney Docket Number	RALEP032C1C2		

	295	8320949		2012-11-27	Matta, Sudheer Poorna Chandra	
	296	8279864		2012-10-02	Wood, Daniel M.	
	297	8271045		2012-09-18	Parolkar, Satish et al.	
	298	8233883		2012-07-31	De Froment, Eric	
	299	8224382		2012-07-17	Bultman, Michael J.	
	300	8184590		2012-05-22	Rosenblatt, Ariel	

If you wish to add additional U.S. Patent citation information please click the Add button. [Add](#)

U.S.PATENT APPLICATION PUBLICATIONS

[Remove](#)

Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. [Add](#)

FOREIGN PATENT DOCUMENTS

[Remove](#)

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625	
	Filing Date		2015-03-30	
	First Named Inventor	Raleigh		
	Art Unit	2642		
	Examiner Name	not yet assigned		
	Attorney Docket Number	RALEP032C1C2		

	1	1463238	EP		2004-09-29	Alcatel		☐
	2	1739518	EP		2007-01-03	Research In Motion Limited		☐
	3	1772988	EP		2007-04-11	Huawei Technologies Co., Ltd.		☐
	4	1978772	EP		2008-10-08	British Telecommunications Public Limited Company		☐
	5	1999065185	WO		1999-12-16	British Telecommunications Public Limited Company		☐
	6	2003014891	WO		2003-02-20	The Boeing Company		☐
	7	2003058880	WO		2003-07-17	Telia AB		☐
	8	2004028070	WO		2004-04-01	Credant Technologies, Inc.		☐
	9	2004077797	WO		2004-09-10	Boston Communications Group, Inc. (Erskine)		☐
	10	2004095753	WO		2004-11-04	Motorola Inc.		☐
	11	2006004467	WO		2006-01-12	Telefonaktiebolaget LM Ericsson		☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	14673625
	Filing Date	2015-03-30
	First Named Inventor	Raleigh
	Art Unit	2642
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1C2

	12	2006050758	WO		2006-05-18	Telefonaktiebolaget LM Ericsson		☐
	13	2006073837	WO		2006-07-13	Symbol Technologies, Inc.		☐
	14	2006077481	WO		2006-07-27	TrueContext Corporation		☐
	15	2006130960	WO		2006-12-14	Mobidia, Inc.		☐
	16	2007001833	WO		2007-01-04	Symbol Technologies, Inc.		☐
	17	2007014630	WO		2007-02-08	Telefonaktiebolaget LM Ericsson		☐
	18	2007018363	WO		2007-02-15	Upresto, Inc.		☐
	19	2007053848	WO		2007-05-10	Mobile Armor, LLC		☐
	20	2007069245	WO		2007-06-21	Yoggie Security Systems, Inc.		☐
	21	2007107701	WO		2007-09-27	British Telecommunications Public Limited Company		☐
	22	2008017837	WO		2008-02-14	Symbian Software Limited		☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625	
	Filing Date		2015-03-30	
	First Named Inventor	Raleigh		
	Art Unit	2642		
	Examiner Name	not yet assigned		
	Attorney Docket Number	RALEP032C1C2		

	23	2008051379	WO		2008-05-02	Verizon Services Corp.		☐
	24	2008066419	WO		2008-06-05	Telefonaktiebolaget LM Ericsson		☐
	25	2008080139	WO		2008-07-03	Integrated Mobile, Inc.		☐
	26	2008080430	WO		2008-07-10	Telecom Italia S.P.A.		☐
	27	2008099802	WO		2008-08-21	NEC Corporation		☐
	28	2010088413	WO		2010-08-05	Headwater Partners I LLC		☐
	29	2006120558	WO		2006-11-16	Nokia Corp.		☐
	30	1889777A	CN		2006-07-19	Huawei Tech. Co. Ltd.		☐
	31	101155343A	CN		2006-09-29	Huawei Tech. Co. Ltd.		☐
	32	101035308A	CN		2006-03-09	Huawei Tech. Co. Ltd.		☐
	33	2007124279	WO		2007-11-01	Cisco Technology, Inc., et al.		☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625	
	Filing Date		2015-03-30	
	First Named Inventor	Raleigh		
	Art Unit	2642		
	Examiner Name	not yet assigned		
	Attorney Docket Number	RALEP032C1C2		

	34	2005008995	WO		2005-01-27	Starhub Ltd.		☐
	35	1998058505	WO		1998-12-23	Sonera Oy		☐
	36	2007097786	WO		2007-08-30	Sony Ericsson Mobile Communications AB		☐

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

NON-PATENT LITERATURE DOCUMENTS

Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5
	1	3rd Generation Partnership Project, "Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) Enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) Access," Release 8, Document No. 3GPP TS 23.401, V8.4.0, December 2008	☐
	2	3rd Generation Partnership Project, "Technical Specification Group Services and System Aspects; Policy and Charging Control Architecture," Release 8, Document No. 3GPP TS 23.203, V8.4.0, December 2008	☐
	3	ALONISTIOTI et al., "Intelligent Architectures Enabling Flexible Service Provision and Adaptability," 2002	☐
	4	Amazon Technologies, Inc., "Kindle™ User's Guide," 3rd Edition, Copyright 2004-2009	☐
	5	CHANDRASEKHAR et al., "Femtocell Networks: A Survey," June 28, 2008	☐
	6	CHAOUCHI et al., "Policy Based Networking in the Integration Effort of 4G Networks and Services," 2004 IEEE	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625
	Filing Date		2015-03-30
	First Named Inventor	Raleigh	
	Art Unit	2642	
	Examiner Name	not yet assigned	
	Attorney Docket Number	RALEP032C1C2	

7	Cisco Systems, Inc., "Cisco Mobile Exchange (CMX) Solution Guide: Chapter 2 - Overview of GSM, GPRS, and UMTS," November 4, 2008	☐
8	DIKAIKOS et al., "A Distributed Middleware Infrastructure for Personalized Services," November 24, 2003	☐
9	European Commission, "Data Roaming Tariffs - Transparency Measures," [online] retrieved from http://web.archive.org/web/20081220232754/http://ec.europa.eu/information_society/activities/roaming/data/measures/index_en.htm , December 20, 2008 [retrieved May 16, 2012]	☐
10	FAROOQ et al., "An IEEE 802.16 WiMax Module for the NS-3 Simulator," March 2-6, 2009	☐
11	HAN et al., "Information Collection Services for Qos-Aware Mobile Applications," 2005	☐
12	HARTMANN et al., "Agent-Based Banking Transactions & Information Retrieval - What About Performance Issues?" 1999	☐
13	Hewlett-Packard Development Company, LP, "IP Multimedia Services Charging," white paper, January 2006	☐
14	HOSSAIN et al., "Gain-Based Selection of Ambient Media Services in Pervasive Environments," Mobile Networks and Applications. 03 October 2008	☐
15	KNIGHT et al., "Layer 2 and 3 Virtual Private Networks: Taxonomy, Technology, and Standardization Efforts," IEEE Communications Magazine, June 2004	☐
16	KOUTSOPOULOU et al., "Middleware Platform for the Support of Charging Reconfiguration Actions," 2005	☐
17	KYRIAKAKOS et al., "Ubiquitous Service Provision in Next Generation Mobile Networks," Proceedings of the 13th IST Mobile and Wireless Communications Summit, Lyon, France, June 2004	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625
	Filing Date		2015-03-30
	First Named Inventor	Raleigh	
	Art Unit	2642	
	Examiner Name	not yet assigned	
	Attorney Docket Number	RALEP032C1C2	

	18	LI, Yu, "Dedicated E-Reading Device: The State of the Art and The Challenges," Scroll, Vol. 1, No. 1, 2008	☐
	19	NILSSON et al., "A Novel MAC Scheme for Solving the QoS Parameter Adjustment Problem in IEEE802.11e EDCA," February 2006	☐
	20	OPPLIGER, Rolf, "Internet Security: Firewalls and Bey," Communications of the ACM, May 1997, Vol. 40. No. 5	☐
	21	RAO et al., "Evolution of Mobile Location-Based Services," Communication of the ACM, December 2003	☐
	22	STEGLICH, Stephan, "I-Centric User Interaction," November 21, 2003	☐
	23	VAN EIJK, et al., "GigaMobile, Agent Technology for Designing Personalized Mobile Service Brokerage," July 1, 2002	☐
	24	ZHU et al., "A Survey of Quality of Service in IEEE 802.11 Networks," IEEE Wireless Communications, August 2004	☐
	25	ANTON, B. et al., "Best Current Practices for Wireless Internet Service Provider (WISP) Roaming"; Release Date February 2003, Version 1.0; Wi-Fi Alliance – Wireless ISP Roaming (WISPr)	☐
	26	Ruckus Wireless – White Paper; "Smarter Wi-Fi for Mobile Operator Infrastructures" 2010	☐
	27	Accuris Networks, "The Business Value of Mobile Data Offload – a White Paper", 2010	☐
	28	Wireless Broadband Alliance, "WISPr 2.0, 08 April, 2010"; Doc. Ref. No.: WBA/RM/WISPr, Version 01.00	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625
	Filing Date		2015-03-30
	First Named Inventor	Raleigh	
	Art Unit	2642	
	Examiner Name	not yet assigned	
	Attorney Docket Number	RALEP032C1C2	

	29	THURSTON, Richard, "WISPr 2.0 Boosts Roaming Between 3G and Wi-Fi"; June 23, 2010; Web page from zdnet.com; Zdnet.com/wispr-2-0-boosts-roaming-between-3g-and-wi-fi-3040089325/	☐
	30	Wi-Fi Alliance Technical Committee Hotspot 2.0 Technical Task Group, "Hotspot 2.0 (Release 1) Technical Specification – Version 1.0.0"; 2012	☐
	31	Wi-Fi Alliance Hotspot 2.0 Technical Task Group, "Wi-Fi Certified Passpoint™ (Release 1) Deployment Guidelines – Version 1.0 – October 2012"	☐

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

EXAMINER SIGNATURE

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		14673625
	Filing Date		2015-03-30
	First Named Inventor	Raleigh	
	Art Unit	2642	
	Examiner Name	not yet assigned	
	Attorney Docket Number	RALEP032C1C2	

CERTIFICATION STATEMENT

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

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

OR

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

☐ See attached certification statement.

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

☒ None

SIGNATURE

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

Signature	/James E. Harris/	Date (YYYY-MM-DD)	2015-04-29
Name/Print	James E. Harris	Registration Number	40013

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

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875						Application or Docket Number 14/673,625				
APPLICATION AS FILED - PART I										
(Column 1)		(Column 2)		SMALL ENTITY		OTHER THAN SMALL ENTITY				
FOR	NUMBER FILED	NUMBER EXTRA	RATE(\$)	FEE(\$)		RATE(\$)	FEE(\$)			
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	70		N/A				
SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A	300		N/A				
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	360		N/A				
TOTAL CLAIMS (37 CFR 1.16(j))	29	minus 20 = *	9	x 40 =	360					
INDEPENDENT CLAIMS (37 CFR 1.16(h))	1	minus 3 = *		x 210 =	0.00					
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			200						
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00						
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL	1290	TOTAL				
APPLICATION AS AMENDED - PART II										
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		OTHER THAN SMALL ENTITY		
AMENDMENT A		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x	=		x	=
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x	=		x	=
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))									
						TOTAL ADD'L FEE			TOTAL ADD'L FEE	
AMENDMENT B		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x	=		x	=
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x	=		x	=
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))									
						TOTAL ADD'L FEE			TOTAL ADD'L FEE	
<p style="font-size: x-small;">* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.</p> <p style="font-size: x-small;">** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".</p> <p style="font-size: x-small;">*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".</p> <p style="font-size: x-small;">The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.</p>										



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY. DOCKET NO	TOT CLAIMS	IND CLAIMS
14/673,625	03/30/2015	2642	1290	RALEP032C1C2	29	1

CONFIRMATION NO. 9085

106963

Headwater Partners I LLC
555 Twin Dolphin Drive, Suite 310
Redwood Shores, CA 94065

FILING RECEIPT



OC000000074549465

Date Mailed: 04/14/2015

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

Inventor(s)

Gregory G. Raleigh, Woodside, CA;
James Lavine, Corte Madera, CA;
Alireza Raissinia, Monte Sereno, CA;

Applicant(s)

Headwater Partners I LLC, Redwood City, CA

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

Domestic Priority data as claimed by applicant

This application is a CON of 14/082,040 11/15/2013
which is a DIV of 13/134,028 05/25/2011 PAT 8589541
which is a CIP of 13/134,005 05/25/2011 PAT 8635335
and is a CIP of 12/695,021 01/27/2010 PAT 8346225
and claims benefit of 61/348,022 05/25/2010
and claims benefit of 61/381,159 09/09/2010
and claims benefit of 61/381,162 09/09/2010
and claims benefit of 61/384,456 09/20/2010
and claims benefit of 61/389,547 10/04/2010
and claims benefit of 61/385,020 09/21/2010
and claims benefit of 61/387,243 09/28/2010
and claims benefit of 61/387,247 09/28/2010
and claims benefit of 61/407,358 10/27/2010
and claims benefit of 61/418,507 12/01/2010
and claims benefit of 61/418,509 12/01/2010
and claims benefit of 61/420,727 12/07/2010
and claims benefit of 61/422,565 12/13/2010

page 1 of 4

and claims benefit of 61/422,572 12/13/2010
 and claims benefit of 61/422,574 12/13/2010
 and claims benefit of 61/435,564 01/24/2011
 and claims benefit of 61/472,606 04/06/2011
 and said 12/695,021 01/27/2010
 is a CIP of 12/380,780 03/02/2009 PAT 8839388
 and claims benefit of 61/252,153 10/15/2009
 and claims benefit of 61/252,151 10/15/2009
 and said 13/134,005 05/25/2011
 is a CIP of 12/380,780 03/02/2009 PAT 8839388
 and is a CIP of 12/380,778 03/02/2009 PAT 8321526
 and said 12/380,780 03/02/2009
 claims benefit of 61/206,354 01/28/2009
 and claims benefit of 61/206,944 02/04/2009
 and claims benefit of 61/207,393 02/10/2009
 and claims benefit of 61/207,739 02/13/2009
 and said 12/380,778 03/02/2009
 claims benefit of 61/206,354 01/28/2009
 and claims benefit of 61/206,944 02/04/2009
 and claims benefit of 61/207,393 02/10/2009
 and claims benefit of 61/207,739 02/13/2009
 and said 13/134,028 05/25/2011
 is a CIP of 12/695,019 01/27/2010 PAT 8275830
 and is a CIP of 12/695,020 01/27/2010 PAT 8406748
 and is a CIP of 12/694,445 01/27/2010 PAT 8391834
 and is a CIP of 12/694,451 01/27/2010 PAT 8548428
 and is a CIP of 12/694,455 01/27/2010 PAT 8402111
 and is a CIP of 12/695,980 01/28/2010 PAT 8340634
 and said 12/695,019 01/27/2010
 claims benefit of 61/270,353 07/06/2009
 and claims benefit of 61/264,126 11/24/2009
 and said 12/695,020 01/27/2010
 claims benefit of 61/275,208 08/25/2009
 and claims benefit of 61/237,753 08/28/2009
 and said 12/694,455 01/27/2010
 claims benefit of 61/264,120 11/24/2009

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

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

If Required, Foreign Filing License Granted: 04/10/2015

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 14/673,625**

Projected Publication Date: 07/23/2015

Non-Publication Request: No

page 2 of 4

Early Publication Request: Yes

**** SMALL ENTITY ****

Title

Wireless end-user device with differentiated network access status for different device applications

Preliminary Class

455

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

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

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

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

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

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER
Title 35, United States Code, Section 184
Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

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

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

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

NOT GRANTED

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

SelectUSA

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Raleigh	Examiner: not yet assigned
Serial No.: 14/673,625	Art Unit: 2642
Filed: March 30, 2015	Conf. No.: 9085
Title: Wireless End-User Device With Differentiated Network Access Status for Different Device Applications	

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

SECOND PRELIMINARY AMENDMENT

Prior to examination on the merits, please amend the above-identified application as follows:

Amendments to the Claims begin on page 2.

Remarks begin on page 7.

AMENDMENTS TO THE CLAIMS

Please amend the claims as follows:

1. (Canceled).
2. (Previously Presented) A wireless end-user device, comprising:
 - a wireless wide area network (WWAN) modem to receive and transmit Internet data between the device and at least one WWAN when configured for and connected to the at least one WWAN;
 - a wireless local area network (WLAN) modem to receive and transmit Internet data between the device and at least one WLAN when configured for and connected to the at least one WLAN; and
 - one or more processors configured to
 - apply a stored WWAN differential traffic control policy to Internet data service provided using the WWAN modem and the at least one WWAN, and
 - indicate to a particular application, via an application program interface (API), one or more network access conditions based on the applied WWAN differential traffic control policy, wherein the one or more network access conditions includes a network access condition that indicates the unavailability to the particular application of an Internet data service that is currently available via the WWAN modem to a different application, but that is indicated as unavailable to the particular application.
3. (Previously Presented) The wireless end-user device of claim 2, wherein the one or more processors are further configured to apply the differential traffic control policy to the particular application when a user of the device is not directly interacting with the particular application or perceiving any benefit from the particular application.
4. (Previously Presented) The wireless end-user device of claim 2, further comprising a user interface to provide a user of the device with information regarding why the differential traffic control policy is applied to the particular application.
5. (Previously Presented) The wireless end-user device of claim 2, further comprising a user interface to inform a user of the device when there are options to set, control,

override, or modify service usage controls that affect the differential traffic control policy.

6. (Previously Presented) The wireless end-user device of claim 2, wherein the differential traffic control policy is part of a multimode profile having different policies for different networks.
7. (Previously Presented) The wireless end-user device of claim 6, wherein the one or more processors are further configured to select a traffic control policy from the multimode profile based at least in part on the type of network connection currently in use by the device.
8. (Previously Presented) The wireless end-user device of claim 7, wherein the one or more processors are further configured to, when the type of network connection is at least one type of WLAN connection, select a traffic control policy from the multimode profile based at least in part on a type of network connection from the WLAN to the Internet.
9. (Previously Presented) The wireless end-user device of claim 2, further comprising a network stack interface integrated with the API.
10. (Previously Presented) The wireless end-user device of claim 2, further comprising a networking stack, wherein the one or more processors are further configured to, at an application service interface layer, identify application traffic flows prior to the flows entering the networking stack.
11. (Previously Presented) The wireless end-user device of claim 2, wherein the API comprises a network access API.
12. (Previously Presented) The wireless end-user device of claim 2, wherein the one or more network access conditions indicated via the API to the particular application comprises information on whether a current connected WWAN is a roaming network or a non-roaming network.

13. (Previously Presented) The wireless end-user device of claim 2, wherein the API informs the particular application when it is allowed to access Internet data service that is currently available via the WWAN modem.
14. (Previously Presented) The wireless end-user device of claim 2, wherein the API informs the particular application of one or more network traffic controls that the application is expected to implement.
15. (Previously Presented) The wireless end-user device of claim 2, wherein the API instructs the particular application to transition to a different state.
16. (Previously Presented) The wireless end-user device of claim 2, wherein the API instructs the device to transition to a power save state.
17. (Previously Presented) The wireless end-user device of claim 2, wherein the one or more processors are further configured to dynamically change the application of the stored WWAN differential traffic control policy based on a power state of the device.
18. (Previously Presented) The wireless end-user device of claim 2, wherein the one or more processors are further configured to dynamically change the application of the stored WWAN differential traffic control policy based on a device usage state.
19. (Previously Presented) The wireless end-user device of claim 2, wherein the one or more processors are further configured to dynamically change the application of the stored WWAN differential traffic control policy based on monitoring of user interaction with the device.
20. (Previously Presented) The wireless end-user device of claim 2, wherein the one or more processors are further configured to dynamically change the application of the stored WWAN differential traffic control policy based on power control state changes for one or more of the modems.
21. (Previously Presented) The wireless end-user device of claim 2, wherein the one or more processors are configured to associate the particular application with the differential traffic control policy based on an application behavior.

22. (Previously Presented) The wireless end-user device of claim 2, wherein the differential traffic control policy defines that applications to which the policy applies can only have WWAN network access events during particular time windows.
23. (Previously Presented) The wireless end-user device of claim 2, further comprising a network stack interface that intercepts network socket interface messages for applications and OS functions, the one or more processors configured to apply the stored WWAN differential traffic control policy to at least some of the intercepted network socket interface messages.
24. (Previously Presented) The wireless end-user device of claim 2, wherein the one or more processors are further configured to update the stored WWAN differential traffic control policy based on information received from a network element.
25. (New) The wireless end-user device of claim 2, the WWAN differential traffic control policy comprising first and second differential traffic control policies applicable respectively to Internet data service provided using the WWAN modem to connect to a home WWAN and a roaming WWAN, wherein the one or more processors are further configured to apply the first differential traffic control policy when Internet data service is provided through a home WWAN and to apply the second differential traffic control policy when Internet data service is provided through a roaming WWAN.
26. (Previously Presented) The wireless end-user device of claim 2, wherein the one or more processors are further configured to determine that the different application is an active application based on a user interaction with the different application.
27. (Previously Presented) The wireless end-user device of claim 2, further comprising an agent to block, modify, remove, or replace user interface messages generated by the particular application based on the applied WWAN differential traffic control policy.
28. (Previously Presented) The wireless end-user device of claim 2, wherein the one or more processors are configured to apply the stored WWAN differential traffic

control policy to selectively block network access by the particular application by intercepting open, connect, and/or write requests by the particular application to a network stack.

29. (Previously Presented) The wireless end-user device of claim 2, wherein the API indicates the unavailability to the particular application of an Internet data service that is currently available by emulating network messaging.
30. (Previously Presented) The wireless end-user device of claim 29, wherein emulating network messaging comprises responding to a network request from the particular application by blocking the request from passing to a network stack and returning to the particular application a message indicating the network request was not successful.
31. (Canceled).

REMARKS

Claims 2-31, now pending, were presented for the first time in a preliminary amendment filed March 31, 2015. Upon further review, Applicant has discovered that no claim was numbered as Claim 25. Accordingly, Applicant is now canceling Claim 31, and adding it as new Claim 25. No new matter has been added.

The Commissioner is authorized to charge any fee deficiency or credit any overpayment to Deposit Account 50-5876.

Respectfully submitted,

Date: April 8, 2015

By: /James E. Harris/

James E. Harris
Reg. No. 40,013
Patent Counsel
Headwater Partners I LLC
555 Twin Dolphin Dr., Suite 310
Redwood Shores, CA 94065
(650) 517-2798

CERTIFICATE OF ELECTRONIC TRANSMISSION

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

Date: April 8, 2015

By: /Ann Taylor/
Ann Taylor

Electronic Acknowledgement Receipt	
EFS ID:	22007401
Application Number:	14673625
International Application Number:	
Confirmation Number:	9085
Title of Invention:	Device-Assisted Services for Protecting Network Capacity
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	James E. Harris/Ann Taylor
Filer Authorized By:	James E. Harris
Attorney Docket Number:	RALEP032C1C2
Receipt Date:	08-APR-2015
Filing Date:	
Time Stamp:	16:57:57
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		P032C1C2_SecondPreliminary Amendment.pdf	79387 a453c3ba70790c6917964da30bc6a6cd075e9d34	yes	7

	Multipart Description/PDF files in .zip description		
	Document Description	Start	End
	Preliminary Amendment	1	1
	Claims	2	6
	Applicant Arguments/Remarks Made in an Amendment	7	7
Warnings:			
Information:			
Total Files Size (in bytes):		79387	
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>			

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Raleigh	Examiner: not yet assigned
Serial No.: 14/673,625	Art Unit: 2642
Filed: March 30, 2015	Conf. No.: 9085
Title: Device-Assisted Services for Protecting Network Capacity	

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

PRELIMINARY AMENDMENT

Prior to examination on the merits, please amend the above-identified application as follows:

Amendments to the Specification begin on page 2.

Amendments to the Claims begin on page 3.

Remarks begin on page 8.

AMENDMENTS TO THE SPECIFICATION

Please amend the **Application Title** as follows:

Wireless End-User Device With Differentiated Network Access Status for
Different Device Applications

Please replace the **Abstract** with the following:

A wireless end-user device has wireless wide-area network (WWAN) and wireless local-area network (WLAN) modems. One or more processors apply a WWAN-specific differential traffic control policy to Internet data service provided using the WWAN modem. Based on the applied policy, an application program interface (API) can indicate to particular applications that Internet data service available via the WWAN modem to other applications is not available to those particular applications.

AMENDMENTS TO THE CLAIMS

Please amend the claims as follows:

1. (Canceled).
2. (New) A wireless end-user device, comprising:
 - a wireless wide area network (WWAN) modem to receive and transmit Internet data between the device and at least one WWAN when configured for and connected to the at least one WWAN;
 - a wireless local area network (WLAN) modem to receive and transmit Internet data between the device and at least one WLAN when configured for and connected to the at least one WLAN; and
 - one or more processors configured to
 - apply a stored WWAN differential traffic control policy to Internet data service provided using the WWAN modem and the at least one WWAN, and
 - indicate to a particular application, via an application program interface (API), one or more network access conditions based on the applied WWAN differential traffic control policy, wherein the one or more network access conditions includes a network access condition that indicates the unavailability to the particular application of an Internet data service that is currently available via the WWAN modem to a different application, but that is indicated as unavailable to the particular application.
3. (New) The wireless end-user device of claim 2, wherein the one or more processors are further configured to apply the differential traffic control policy to the particular application when a user of the device is not directly interacting with the particular application or perceiving any benefit from the particular application.
4. (New) The wireless end-user device of claim 2, further comprising a user interface to provide a user of the device with information regarding why the differential traffic control policy is applied to the particular application.
5. (New) The wireless end-user device of claim 2, further comprising a user interface to inform a user of the device when there are options to set, control, override, or modify service usage controls that affect the differential traffic control policy.

6. (New) The wireless end-user device of claim 2, wherein the differential traffic control policy is part of a multimode profile having different policies for different networks.
7. (New) The wireless end-user device of claim 6, wherein the one or more processors are further configured to select a traffic control policy from the multimode profile based at least in part on the type of network connection currently in use by the device.
8. (New) The wireless end-user device of claim 7, wherein the one or more processors are further configured to, when the type of network connection is at least one type of WLAN connection, select a traffic control policy from the multimode profile based at least in part on a type of network connection from the WLAN to the Internet.
9. (New) The wireless end-user device of claim 2, further comprising a network stack interface integrated with the API.
10. (New) The wireless end-user device of claim 2, further comprising a networking stack, wherein the one or more processors are further configured to, at an application service interface layer, identify application traffic flows prior to the flows entering the networking stack.
11. (New) The wireless end-user device of claim 2, wherein the API comprises a network access API.
12. (New) The wireless end-user device of claim 2, wherein the one or more network access conditions indicated via the API to the particular application comprises information on whether a current connected WWAN is a roaming network or a non-roaming network.
13. (New) The wireless end-user device of claim 2, wherein the API informs the particular application when it is allowed to access Internet data service that is currently available via the WWAN modem.

14. (New) The wireless end-user device of claim 2, wherein the API informs the particular application of one or more network traffic controls that the application is expected to implement.
15. (New) The wireless end-user device of claim 2, wherein the API instructs the particular application to transition to a different state.
16. (New) The wireless end-user device of claim 2, wherein the API instructs the device to transition to a power save state.
17. (New) The wireless end-user device of claim 2, wherein the one or more processors are further configured to dynamically change the application of the stored WWAN differential traffic control policy based on a power state of the device.
18. (New) The wireless end-user device of claim 2, wherein the one or more processors are further configured to dynamically change the application of the stored WWAN differential traffic control policy based on a device usage state.
19. (New) The wireless end-user device of claim 2, wherein the one or more processors are further configured to dynamically change the application of the stored WWAN differential traffic control policy based on monitoring of user interaction with the device.
20. (New) The wireless end-user device of claim 2, wherein the one or more processors are further configured to dynamically change the application of the stored WWAN differential traffic control policy based on power control state changes for one or more of the modems.
21. (New) The wireless end-user device of claim 2, wherein the one or more processors are configured to associate the particular application with the differential traffic control policy based on an application behavior.
22. (New) The wireless end-user device of claim 2, wherein the differential traffic control policy defines that applications to which the policy applies can only have WWAN network access events during particular time windows.

23. (New) The wireless end-user device of claim 2, further comprising a network stack interface that intercepts network socket interface messages for applications and OS functions, the one or more processors configured to apply the stored WWAN differential traffic control policy to at least some of the intercepted network socket interface messages.
24. (New) The wireless end-user device of claim 2, wherein the one or more processors are further configured to update the stored WWAN differential traffic control policy based on information received from a network element.
26. (New) The wireless end-user device of claim 2, wherein the one or more processors are further configured to determine that the different application is an active application based on a user interaction with the different application.
27. (New) The wireless end-user device of claim 2, further comprising an agent to block, modify, remove, or replace user interface messages generated by the particular application based on the applied WWAN differential traffic control policy.
28. (New) The wireless end-user device of claim 2, wherein the one or more processors are configured to apply the stored WWAN differential traffic control policy to selectively block network access by the particular application by intercepting open, connect, and/or write requests by the particular application to a network stack.
29. (New) The wireless end-user device of claim 2, wherein the API indicates the unavailability to the particular application of an Internet data service that is currently available by emulating network messaging.
30. (New) The wireless end-user device of claim 29, wherein emulating network messaging comprises responding to a network request from the particular application by blocking the request from passing to a network stack and returning to the particular application a message indicating the network request was not successful.
31. (New) The wireless end-user device of claim 2, the WWAN differential traffic control policy comprising first and second differential traffic control policies

applicable respectively to Internet data service provided using the WWAN modem to connect to a home WWAN and a roaming WWAN, wherein the one or more processors are further configured to apply the first differential traffic control policy when Internet data service is provided through a home WWAN and to apply the second differential traffic control policy when Internet data service is provided through a roaming WWAN.

REMARKS

Applicant respectfully requests entry of the amendments provided herein. This preliminary amendment is presented before any office action. Claim 1 has been canceled, and new claims 2-31 have been added. No new matter has been added. If the Examiner has any questions or needs any additional information, the Examiner is invited to contact the undersigned.

The Commissioner is authorized to charge any fee deficiency or credit any overpayment to Deposit Account 50-5876.

Respectfully submitted,

Date: March 31, 2015

By: /James E. Harris/

James E. Harris
Reg. No. 40,013
Patent Counsel
Headwater Partners I LLC
555 Twin Dolphin Dr., Suite 310
Redwood Shores, CA 94065
(650) 517-2798

CERTIFICATE OF ELECTRONIC TRANSMISSION

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

Date: March 31, 2015

By: /Ann Taylor/

Ann Taylor

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(c).

I hereby appoint:



Practitioners associated with Customer Number:

106963

OR



Practitioner(s) named below (if more than ten patent practitioners are to be named, then a customer number must be used):

Name	Registration Number

Name	Registration Number

As attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignments documents attached to this form in accordance with 37 CFR 3.73(c).

Please change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(c) to:



The address associated with Customer Number:

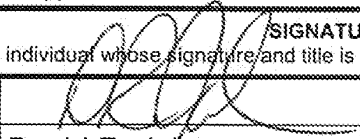
106963

OR

☐	Firm or Individual Name			
	Address			
	City	State	Zip	
	Country			
	Telephone	Email		

Assignee Name and Address: Headwater Partners I LLC
555 Twin Dolphin Drive, Suite 310
Redwood City, CA 94065 U.S.A.

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

SIGNATURE of Assignee of Record	
The individual whose signature and title is supplied below is authorized to act on behalf of the assignee	
Signature	 Date 25 June 2014
Name	David R. Johnson Telephone 650-517-2782
Title	Chief Financial Officer

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

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

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal				
Application Number:		14673625		
Filing Date:				
Title of Invention:		Device-Assisted Services for Protecting Network Capacity		
First Named Inventor/Applicant Name:		Gregory G. Raleigh		
Filer:		James E. Harris/Ann Taylor		
Attorney Docket Number:		RALEP032C1C2		
Filed as Small Entity				
Filing Fees for Utility under 35 USC 111(a)				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Claims in excess of 20	2202	10	40	400
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				400

Electronic Acknowledgement Receipt	
EFS ID:	21931960
Application Number:	14673625
International Application Number:	
Confirmation Number:	9085
Title of Invention:	Device-Assisted Services for Protecting Network Capacity
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	James E. Harris/Ann Taylor
Filer Authorized By:	James E. Harris
Attorney Docket Number:	RALEP032C1C2
Receipt Date:	31-MAR-2015
Filing Date:	
Time Stamp:	16:34:58
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$400
RAM confirmation Number	3367
Deposit Account	505876
Authorized User	
<p>The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:</p> <p>Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)</p> <p>Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)</p>	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)					
Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)					
Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)					
File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		P032C1C2_PreliminaryAmendment.pdf	85698	yes	8
			7aa5979b35587e00cd8e74e3629f69dd6828553		
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Preliminary Amendment		1	1	
	Specification		2	2	
	Claims		3	7	
	Applicant Arguments/Remarks Made in an Amendment		8	8	
Warnings:					
Information:					
2	Power of Attorney	POA.pdf	645382	no	2
			515a132f61663477437881ed77cd308133200ab1		
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30096	no	2
			b1089b3422e792ea57f8a6bfe0c4f2bcade8baa2		
Warnings:					
Information:					
Total Files Size (in bytes):			761176		

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

New Applications Under 35 U.S.C. 111

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

National Stage of an International Application under 35 U.S.C. 371

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

New International Application Filed with the USPTO as a Receiving Office

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

Document code: WFEE

United States Patent and Trademark Office
Sales Receipt for Accounting Date: 04/10/2015

VVAN11	SALE	#00000002	Mailroom Dt: 03/31/2015	505876	14673625
		01	FC : 2202	360.00	DA

Document code: WFEE

United States Patent and Trademark Office
Sales Receipt for Accounting Date: 04/10/2015

VVAN11	ADJ #00000002	Mailroom Dt: 03/31/2015		
	Seq No: 3367	Sales Acctg Dt: 04/01/2015	505876	14673625
	01 FC : 2202	400.00 CR		

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

First Named Inventor:	Raleigh	Nonprovisional Application Number (if known):	RALEP032C1C2
Title of Invention:	Device-Assisted Services for Protecting Network Capacity		

APPLICANT HEREBY CERTIFIES THE FOLLOWING AND REQUESTS PRIORITIZED EXAMINATION FOR THE ABOVE-IDENTIFIED APPLICATION.

1. The processing fee set forth in 37 CFR 1.17(i)(1) and the prioritized examination fee set forth in 37 CFR 1.17(c) have been filed with the request. The publication fee requirement is met because that fee, set forth in 37 CFR 1.18(d), is currently \$0. The basic filing fee, search fee, and examination fee are filed with the request or have been already been paid. I understand that any required excess claims fees or application size fee must be paid for the application.
2. I understand that the application may not contain, or be amended to contain, more than four independent claims, more than thirty total claims, or any multiple dependent claims, and that any request for an extension of time will cause an outstanding Track I request to be dismissed.
3. The applicable box is checked below:

I. ☒ Original Application (Track One) - Prioritized Examination under § 1.102(e)(1)

- i. (a) The application is an original nonprovisional utility application filed under 35 U.S.C. 111(a). This certification and request is being filed with the utility application via EFS-Web.
---OR---
(b) The application is an original nonprovisional plant application filed under 35 U.S.C. 111(a). This certification and request is being filed with the plant application in paper.
- ii. An executed inventor's oath or declaration under 37 CFR 1.63 or 37 CFR 1.64 for each inventor, or the application data sheet meeting the conditions specified in 37 CFR 1.53(f)(3)(i) is filed with the application.

II. ☐ Request for Continued Examination - Prioritized Examination under § 1.102(e)(2)

- i. A request for continued examination has been filed with, or prior to, this form.
- ii. If the application is a utility application, this certification and request is being filed via EFS-Web.
- iii. The application is an original nonprovisional utility application filed under 35 U.S.C. 111(a), or is a national stage entry under 35 U.S.C. 371.
- iv. This certification and request is being filed prior to the mailing of a first Office action responsive to the request for continued examination.
- v. No prior request for continued examination has been granted prioritized examination status under 37 CFR 1.102(e)(2).

Signature <u>/James E. Harris/</u>	Date <u>2015-03-30</u>
Name (Print/Typed) <u>James E. Harris</u>	Practitioner Registration Number <u>40013</u>
Note: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. Submit multiple forms if more than one signature is required.*	
☐ *Total of _____ forms are submitted.	

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

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

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	RALEP032C1C2
		Application Number	
Title of Invention	Device-Assisted Services for Protecting Network Capacity		
<p>The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.</p> <p>This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.</p>			

Secrecy Order 37 CFR 5.2

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

Inventor Information:

Inventor 1					Remove
Legal Name					
Prefix	Given Name	Middle Name	Family Name	Suffix	
	Gregory	G.	Raleigh		
Residence Information (Select One) ☒ US Residency ☐ Non US Residency ☐ Active US Military Service					
City	Woodside	State/Province	CA	Country of Residence i	US
Mailing Address of Inventor:					
Address 1		555 Twin Dolphin Dr., Suite 310			
Address 2					
City	Redwood City	State/Province	CA		
Postal Code	94065	Country i	US		
Inventor 2					Remove
Legal Name					
Prefix	Given Name	Middle Name	Family Name	Suffix	
	James		Lavine		
Residence Information (Select One) ☒ US Residency ☐ Non US Residency ☐ Active US Military Service					
City	Corte Madera	State/Province	CA	Country of Residence i	US
Mailing Address of Inventor:					
Address 1		555 Twin Dolphin Dr., Suite 310			
Address 2					
City	Redwood City	State/Province	CA		
Postal Code	94065	Country i	US		
Inventor 3					Remove
Legal Name					
Prefix	Given Name	Middle Name	Family Name	Suffix	
	Alireza		Raissinia		
Residence Information (Select One) ☒ US Residency ☐ Non US Residency ☐ Active US Military Service					

Application Data Sheet 37 CFR 1.76		Attorney Docket Number		RALEP032C1C2	
		Application Number			
Title of Invention		Device-Assisted Services for Protecting Network Capacity			
City	Monte Sereno	State/Province	CA	Country of Residence i	US
Mailing Address of Inventor:					
Address 1		555 Twin Dolphin Dr., Suite 310			
Address 2					
City	Redwood City	State/Province	CA		
Postal Code	94065	Country i	US		
All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the Add button.					Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below. For further information see 37 CFR 1.33(a).		
☐ An Address is being provided for the correspondence information of this application.		
Customer Number	106963	
Email Address	patent@headwaterllc.com	<input type="button" value="Add Email"/> <input type="button" value="Remove Email"/>

Application Information:

Title of the Invention	Device-Assisted Services for Protecting Network Capacity		
Attorney Docket Number	RALEP032C1C2	Small Entity Status Claimed	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	29	Suggested Figure for Publication (if any)	

Filing By Reference :

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country i

Publication Information:

☒ Request Early Publication (Fee required at time of Request 37 CFR 1.219)
☐ Request Not to Publish. I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application has not and will not be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	RALEP032C1C2
		Application Number	
Title of Invention	Device-Assisted Services for Protecting Network Capacity		

Representative Information:

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

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

Domestic Benefit/National Stage Information:

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

When referring to the current application, please leave the application number blank.

Prior Application Status	Pending		Remove		
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)		
notyetassigned	Continuation of	14082040	2013-11-15		
Prior Application Status	Patented		Remove		
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
14082040	Division of	13134028	2011-05-25	8589541	2013-11-19
Prior Application Status	Patented		Remove		
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13134028	Continuation in part of	13134005	2011-05-25	8635335	2014-01-21
Prior Application Status	Patented		Remove		
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13134028	Continuation in part of	12695021	2010-01-27	8346225	2013-01-01
Prior Application Status	Expired		Remove		
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)		
13134028	Claims benefit of provisional	61348022	2010-05-25		
Prior Application Status	Expired		Remove		
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)		
13134028	Claims benefit of provisional	61381159	2010-09-09		
Prior Application Status	Expired		Remove		

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	RALEP032C1C2
		Application Number	
Title of Invention	Device-Assisted Services for Protecting Network Capacity		

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
13134028	Claims benefit of provisional	61381162	2010-09-09
Prior Application Status	Expired	Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
13134028	Claims benefit of provisional	61384456	2010-09-20
Prior Application Status	Expired	Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
13134028	Claims benefit of provisional	61389547	2010-10-04
Prior Application Status	Expired	Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
13134028	Claims benefit of provisional	61385020	2010-09-21
Prior Application Status	Expired	Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
13134028	Claims benefit of provisional	61387243	2010-09-28
Prior Application Status	Expired	Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
13134028	Claims benefit of provisional	61387247	2010-09-28
Prior Application Status	Expired	Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
13134028	Claims benefit of provisional	61407358	2010-10-27
Prior Application Status	Expired	Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
13134028	Claims benefit of provisional	61418507	2010-12-01
Prior Application Status	Expired	Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
13134028	Claims benefit of provisional	61418509	2010-12-01
Prior Application Status	Expired	Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
13134028	Claims benefit of provisional	61420727	2010-12-07
Prior Application Status	Expired	Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
13134028	Claims benefit of provisional	61422565	2010-12-13
Prior Application Status	Expired	Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
13134028	Claims benefit of provisional	61422572	2010-12-13
Prior Application Status	Expired	Remove	

Application Data Sheet 37 CFR 1.76		Attorney Docket Number		RALEP032C1C2	
		Application Number			
Title of Invention		Device-Assisted Services for Protecting Network Capacity			

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)		
13134028	Claims benefit of provisional	61422574	2010-12-13		
Prior Application Status	Expired	Remove			
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)		
13134028	Claims benefit of provisional	61435564	2011-01-24		
Prior Application Status	Expired	Remove			
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)		
13134028	Claims benefit of provisional	61472606	2011-04-06		
Prior Application Status	Expired	Remove			
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)		
12695021	Claims benefit of provisional	61252151	2009-10-15		
Prior Application Status	Expired	Remove			
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)		
12695021	Claims benefit of provisional	61252153	2009-10-15		
Prior Application Status	Patented	Remove			
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
12695021	Continuation in part of	12380780	2009-03-02	8839388	2014-09-16
Prior Application Status	Patented	Remove			
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13134005	Continuation in part of	12380780	2009-03-02	8839388	2014-09-16
Prior Application Status	Patented	Remove			
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13134005	Continuation in part of	12380778	2009-03-02	8321526	2012-11-27
Prior Application Status	Expired	Remove			
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)		
12380780	Claims benefit of provisional	61206354	2009-01-28		
Prior Application Status	Expired	Remove			
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)		
12380780	Claims benefit of provisional	61206944	2009-02-04		
Prior Application Status	Expired	Remove			
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)		
12380780	Claims benefit of provisional	61207393	2009-02-10		
Prior Application Status	Expired	Remove			

Application Data Sheet 37 CFR 1.76		Attorney Docket Number		RALEP032C1C2	
		Application Number			
Title of Invention		Device-Assisted Services for Protecting Network Capacity			

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)		
12380780	Claims benefit of provisional	61207739	2009-02-13		
Prior Application Status	Expired	Remove			
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)		
12380778	Claims benefit of provisional	61206354	2009-01-28		
Prior Application Status	Expired	Remove			
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)		
12380778	Claims benefit of provisional	61206944	2009-02-04		
Prior Application Status	Expired	Remove			
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)		
12380778	Claims benefit of provisional	61207393	2009-02-10		
Prior Application Status	Expired	Remove			
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)		
12380778	Claims benefit of provisional	61207739	2009-02-13		
Prior Application Status	Patented	Remove			
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13134028	Continuation in part of	12695019	2010-01-27	8275830	2012-09-25
Prior Application Status	Patented	Remove			
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13134028	Continuation in part of	12695020	2010-01-27	8406748	2013-03-26
Prior Application Status	Patented	Remove			
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13134028	Continuation in part of	12694445	2010-01-27	8391834	2013-03-05
Prior Application Status	Patented	Remove			
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13134028	Continuation in part of	12694451	2010-01-27	8548428	2013-10-01
Prior Application Status	Patented	Remove			
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13134028	Continuation in part of	12694455	2010-01-27	8402111	2013-03-19
Prior Application Status	Patented	Remove			
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13134028	Continuation in part of	12695980	2010-01-28	8340634	2012-12-25
Prior Application Status	Expired	Remove			

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	RALEP032C1C2
		Application Number	
Title of Invention	Device-Assisted Services for Protecting Network Capacity		

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
12695019	Claims benefit of provisional	61270353	2009-07-06
Prior Application Status	Expired	Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
12695019	Claims benefit of provisional	61264126	2009-11-24
Prior Application Status	Expired	Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
12695020	Claims benefit of provisional	61275208	2009-08-25
Prior Application Status	Expired	Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
12695020	Claims benefit of provisional	61237753	2009-08-28
Prior Application Status	Expired	Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
12694455	Claims benefit of provisional	61264120	2009-11-24

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

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(d). When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX) ¹the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(h)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

[Remove](#)

Application Number	Country ⁱ	Filing Date (YYYY-MM-DD)	Access Code ^j (if applicable)

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button. [Add](#)

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	RALEP032C1C2
		Application Number	
Title of Invention	Device-Assisted Services for Protecting Network Capacity		

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

<p>This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.</p> <p>☐ NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.</p>
--

Authorization to Permit Access:

<p>☒ Authorization to Permit Access to the Instant Application by the Participating Offices</p> <p>If checked, the undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the instant patent application is filed access to the instant patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the instant patent application is filed to have access to the instant patent application.</p> <p>In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the instant patent application with respect to: 1) the instant patent application-as-filed; 2) any foreign application to which the instant patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the instant patent application; and 3) any U.S. application-as-filed from which benefit is sought in the instant patent application.</p> <p>In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date of filing this Authorization.</p>
--

Applicant Information:

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

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	RALEP032C1C2
		Application Number	
Title of Invention	Device-Assisted Services for Protecting Network Capacity		

Applicant 1				Remove
<p>If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.</p>				
Clear				
☒ Assignee		☐ Legal Representative under 35 U.S.C. 117		☐ Joint Inventor
☐ Person to whom the inventor is obligated to assign.		☐ Person who shows sufficient proprietary interest		
If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:				
Name of the Deceased or Legally Incapacitated Inventor : <input type="text"/>				
If the Applicant is an Organization check here. ☒				
Organization Name	Headwater Partners I LLC			
Mailing Address Information:				
Address 1	555 Twin Dolphin Dr., Suite 310			
Address 2				
City	Redwood City	State/Province	CA	
Country ⁱ	US	Postal Code	94065	
Phone Number	650-517-2798	Fax Number		
Email Address	patent@headwaterllc.com			
Additional Applicant Data may be generated within this form by selecting the Add button.				
Add				

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.	
Assignee 1	
<p>Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication. An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.</p>	
Remove	
If the Assignee or Non-Applicant Assignee is an Organization check here. ☐	

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

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	RALEP032C1C2
		Application Number	
Title of Invention	Device-Assisted Services for Protecting Network Capacity		

Prefix	Given Name	Middle Name	Family Name	Suffix

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1			
Address 2			
City		State/Province	
Country i		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button.

Add

Signature:

Remove

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

Signature	/James E. Harris/		Date (YYYY-MM-DD)	2015-03-30
First Name	James E.	Last Name	Harris	Registration Number
				40013

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

Add

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

UNITED STATES PATENT APPLICATION

FOR

**DEVICE-ASSISTED SERVICES FOR PROTECTING
NETWORK CAPACITY**

INVENTORS:

GREGORY G. RALEIGH

ALI RAISSINIA

JAMES LAVINE

PREPARED BY:

**HEADWATER PARTNERS I LLC
555 TWIN DOLPHIN DRIVE, SUITE 310
REDWOOD SHORES, CA 94065
650-517-2798**

ATTORNEY DOCKET NO.: RALEP032C1C2

DEVICE-ASSISTED SERVICES FOR PROTECTING NETWORK CAPACITY

BACKGROUND

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

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

[0003] The foregoing example of trends and issues is intended to be illustrative and not exclusive. Other limitations of the art will become apparent to those of skill in the relevant art upon a reading of the specification and a study of the drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] FIG. 1 illustrates a functional diagram of a network architecture for providing quality of service (QoS) for device assisted services (DAS) and/or for providing DAS for protecting network capacity in accordance with some embodiments.

[0005] FIG. 2 illustrates another functional diagram of another network architecture for providing quality of service (QoS) for device assisted services (DAS) and/or for providing DAS for protecting network capacity in accordance with some embodiments.

[0006] FIG. 3 illustrates a functional diagram of an architecture including a device based service processor and a service controller for providing quality of service (QoS) for device assisted services (DAS) and/or for providing DAS for protecting network capacity in accordance with some embodiments.

[0007] FIGS. 4A through 4C illustrates a functional diagram for providing quality of service (QoS) for device assisted services (DAS) in accordance with some embodiments.

[0008] FIG. 5 illustrates a functional diagram for generating a QoS activity map for quality of service (QoS) for device assisted services (DAS) in accordance with some embodiments.

[0009] FIG. 6 illustrates a functional diagram for quality of service (QoS) for device assisted services (DAS) for an end to end coordinated QoS service channel control in accordance with some embodiments.

[0010] FIG. 7 illustrates a flow diagram for quality of service (QoS) for device assisted services (DAS) in accordance with some embodiments.

[0011] FIGS. 8A through 8C each illustrate another flow diagram for quality of service (QoS) for device assisted services (DAS) in accordance with some embodiments.

[0012] FIG. 9 illustrates another flow diagram for quality of service (QoS) for device assisted services (DAS) in accordance with some embodiments.

[0013] FIG. 10 illustrates another flow diagram for quality of service (QoS) for device assisted services (DAS) in accordance with some embodiments.

[0014] FIG. 11 illustrates another flow diagram for quality of service (QoS) for device assisted services (DAS) in accordance with some embodiments.

[0015] FIG. 12 illustrates a device stack for providing various service usage measurement techniques in accordance with some embodiments.

[0016] FIG. 13 illustrates another device stack for providing various service usage measurement techniques in accordance with some embodiments.

[0017] FIG. 14 illustrates a flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments.

[0018] FIG. 15 illustrates another flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments.

[0019] FIG. 16 illustrates another flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments.

[0020] FIG. 17 illustrates another flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments.

[0021] FIG. 18 illustrates another flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments.

[0022] FIG. 19 illustrates another flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments.

[0023] FIG. 20 illustrates another flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments.

[0024] FIG. 21 illustrates another flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments.

[0025] FIG. 22 illustrates another flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments.

[0026] FIG. 23 illustrates a network capacity controlled services priority level chart for device assisted services (DAS) for protecting network capacity in accordance with some embodiments.

[0027] FIG. 24 depicts a diagram of a network capacity protection system utilizing device-assisted services (DAS).

[0028] FIG. 25 depicts a diagram an example of a differential access control notification system.

[0029] FIG. 26 depicts an example of a computer system on which techniques described in this paper can be implemented.

[0030] FIG. 27 depicts a diagram of an example of a system for application-specific differential network access control.

DETAILED DESCRIPTION

[0031] 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.

[0032] 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.

[0033] As the network capacity gains are less than what is required to meet growing digital networking demand, a network capacity crunch is developing due to increasing network congestion on various wireless networks, such as mobile networks. The increasing popularity of various smart phone devices, net book devices, tablet computing devices, and various other wireless mobile computing devices, which are becoming increasingly popular on 3G, 4G, and other advanced wireless networks, is contributing to the network capacity crunch. Some network carriers have indicated that a relatively small number of users on such devices demand a

disproportionately significant amount of their network capacity. For example, AT&T has recently indicated that about 3 percent of its smart phone device users (e.g., Apple iPhone® users) are generating approximately 40 percent of the operator's data traffic.

[0034] For example, in wireless networks, managing the wireless access connection capacity and network access connection resources is important to maintain network performance as network resources/capacity demand increases. Many network performance measures can be advantageously maintained or improved as network loading increases if capacity management and/or network resource management is employed. For example, these performance measures include network availability; the ability to deliver connections to all devices, users and/or applications seeking connections and enabled for service on the network; network access attempt success rate; the transmission speed experienced by one or more devices, users or applications; the average transmission speed experienced by all devices, users and/or applications; network bit error rate or packet error rate; the time delay from network access request to delivered access connection; the one-way delay or round-trip delay for a transmission; the delay timing jitter for a transmission; the time variation in transmission speed for one or more connections; the ability of the network to deliver various requested/needed levels of Quality of Service (QoS) to devices, users or applications that require differentiated connection QoS classes; the ability of the network to maintain efficiency (e.g., aggregated service throughput measured across all devices, users, and/or applications); the ability of the network to share or distribute a performance measure (e.g., the performance measures listed above) uniformly or fairly across multiple devices, users, and/or applications that all have the same service quality class or the same service plan performance parameters.

[0035] For example, if there is a limited amount of shared bandwidth for a set of user devices (e.g., a set of devices on a wireless network, such as a given base station or base station controller or femto cell or pico cell; or a set of devices on a cable modem networks, etc.), and if multiple and/or all devices allow all applications to indiscriminately access or attempt to access network resources or transmit/receive traffic, then the network can generally become overloaded. As a result, a subset of users/devices or in some cases most or all users/devices obtain poor network performance. As another example, if one or more devices forming a subset of devices on the network allow multiple and/or all applications to indiscriminately access or attempt to access network resources or transmit/receive traffic, then the network can become overloaded.

As a result, a subset of users/devices or in some cases most or all users/devices obtain poor network performance.

[0036] Traditionally, mobile devices typically have specialized designs that are optimized to preserve network capacity and protect network resources from being over taxed. For example, wireless devices that browse the Internet often use specialized protocols such as WAP and data traffic compression or low resolution techniques rather than standard HTTP protocols and traffic used in wired Internet devices.

[0037] However, the wireless devices that implement specialized methods for accessing the Internet and/or other networks often implement complex specifications provided by one or more wireless carriers that own the networks that the device is designed to connect to. Such complex specifications often require time consuming design, testing, and certification processes. These processes in part have the effect of narrowing the base of device suppliers to those qualified and willing to perform the specialized design work required, slowing time to market for new devices, increasing the expense to develop new devices and reducing the types of applications that are supported.

[0038] Device OEMs have recently created wireless devices that are designed more like standard Internet devices and not fully optimized to preserve network capacity and resources. Many wireless service customers desire this type of device, and the OEMs generally want to reduce the complexity and time to market to deliver such devices. In addition, new market needs and new government requirements sometimes require that carriers offer a more open process for bringing new devices onto their network, in which the process does not require all of the specialized design and certification described above. These and various other factors are driving a growing need and trend for less complex and time consuming wireless device design and certification processes.

[0039] This trend has led many carriers to begin selling devices that are designed more as standard Internet service devices that connect to the Internet and other data networks through carrier wireless networks. As the cellular network is opened up to more and more new devices, applications and markets, there is a growing demand to allow general purpose Internet devices and applications to gain access to wireless networks without necessarily going through

specialized design and certification process requirements to make the devices and applications efficient and authorized for access to such wireless networks.

[0040] However, general purpose Internet devices are not as frugal or sparing with wireless network access bandwidth. Moreover, with the advent of always on wide area network connections to the Internet has led to popular Internet services and applications that typically assume very inexpensive access and generally heed no attention to, for example, network busy state. As more general purpose Internet devices are provided for us on various wireless networks (e.g., mobile wireless networks), a high frequency of inefficient wireless network accesses continue to rise, which can reduce network capacity sometimes to levels that hinder access to service for that device (e.g., user, device, software demand) and/or other devices on that wireless network and/or that wireless network segment. As discussed above, judicious use of wireless network bandwidth, capacity, and resources generally results in better service for all users, but at present, device manufacturers and wireless network providers (e.g., wireless network carriers or carriers) have not provided or implemented more intelligent bandwidth usage techniques. These factors generally result in less carrier control of device design, which poses a threat to longer term network capacity and performance preservation as the volume of devices with less optimized wireless designs continues to grow.

[0041] There are many network performance and user performance factors that are impacted by the efficiency of the network, including, for example, overall network congestion; the access network performance experienced by one or more groups of users, devices, applications, network service sources, communication protocols, and/or operating system functions; and/or the performance experienced by a given user, device, application, network service source, communication protocol, and/or operating system function. Under a relatively low capacity demand of a wireless network, network performance as experienced by a group of devices, applications, network service sources, communication protocols, operating system functions, and/or users or by a single device, application, network service source, communication protocol, operating system function, and/or user can degrade somewhat proportionally (e.g., aggregate traffic delivered by the network may be roughly proportional to the peak available network traffic) with incremental increases in network access and/or traffic demand from one or more groups of users, devices, applications, network service sources, communication protocols and/or operating system functions. However, as network resources/network capacity demand

increases (e.g., more wireless network data traffic is demanded in aggregate; more devices are serviced by the network; more users are serviced by the network; more applications are serviced by the network; more network service sources are serviced by the network; more operating system functions are serviced by the network; and/or more differentiated QoS sessions are serviced by the network), network availability/performance can decrease and/or the network may not adequately service one or more users, devices, applications, network service sources, communication protocols, and/or operating system functions, or may not service one or more groups of users, devices, applications, network service sources, communication protocols, and/or operating system functions.

[0042] There are many examples of how increasing network capacity demand can decrease network performance, including for example, to a decrease in average bandwidth offered per device (e.g., one or more users on a device, application, network service source, communication protocol, and/or operating system function executed/implemented on the device); an increase in traffic delivery latency; an increase in traffic delivery latency jitter; insufficient guaranteed or differentiated bandwidth for one or more differentiated QoS and/or dynamic QoS services (e.g., as described herein) to one or more devices, users, applications, network service sources, communication protocols, and/or operating system functions; increased latency for bandwidth reservation services; increased latency for QoS reservation services; performance problems with one or more communication protocols; unacceptable delays in user experience, and/or various other or similar consequences and device or user impacts resulting from reduced network availability and/or reduced network capacity. Examples of network communication protocols that can have degraded performance with excessive network loading or degraded network performance include, for example, Internet protocol (IP), HTML protocols, voice communication protocols including VOIP protocols, real-time video communication protocols, streaming media protocols (e.g., audio, video, etc), gaming protocols, VPN protocols, file download protocols, background service protocols, software update protocols, and/or various other network communication protocols. Thus, is it important to preserve/protect network capacity.

[0043] It is also important to control the number of transactions demanded from a given network resource (e.g., edge network segment, base station, base station controller, MAC resources, pico cell, femto cell, etc.) in a given period of time so that demand does not overcome

the transaction servicing ability of that network resource. For example, network resources that should not be subjected to excess transaction demand can include base station or base station controller resources, media access control (MAC) resources, traffic transport resources, AAA resources, security or authentication resources, home agent (HA) resources, DNS resources, resources that play a part in network discovery, gateway or router resources, data session reservation or establishment resources (e.g., network resources required to manage, set up, conduct, and/or close service sessions, PPP sessions, communication flows, communication streams, QoS flows, radio access bearer reservation resources, tunnels, VPNs, APNs, special service routing, etc.), bandwidth reservation resources, QoS reservation or coordination resources, QoS transport resources, service charging resources, traffic analysis resources, network security resources, and/or various other or similar network resources. In some networks, the network performance degradation due to a given measure of incremental increase in network resource/capacity demand can become relatively large as various network resources become increasingly taxed due to either limited transaction processing capability or limited traffic bandwidth for one or more of the network resources that participate in establishing, servicing, conducting, maintaining, and/or closing the necessary network service connections and/or information exchanges required to conduct a service activity. For example, if the equipment required to establish a PPP session can only handle a certain number of new PPP session openings and/or closings per given period of time, and if device behavior is such that PPP sessions are often opened and/or closed, then the rate of PPP session transactions (e.g., openings and/or closings) can exceed the transaction capacity of the PPP session management resources. This is sometimes referred to as “flooding” or “overloading” a network resource with excess demand or excess connections, and, in such cases, the network resource may begin falling behind in servicing transaction demand in a well controlled manner (e.g., the network resource may continue processing transactions at or near a maximum rate for that network resource), or in some cases, the resource may fall behind transaction demand in a less well controlled manner (e.g., the network resource may become overwhelmed such that its processing rate not only falls below aggregate transaction demand, but the transaction rate processing capability decreases under overload as well). In the PPP session establishment resource example, once the rate of requested transactions exceeds the resource maximum transaction rate, then unmet device

demand can grow to a point where one or more devices experiences delays in connecting to and/or communicating (e.g., sending/receiving data) with the network.

[0044] As another example, in any type of random access bandwidth reservation protocol, MAC protocol, or bandwidth delivery protocol, in a network without proper management and/or control of traffic access reservations and/or transmissions, as the network demand increases there may be more collisions between reservation requests, traffic transmissions, application demands, network service source demands, communication protocol demands, and/or operating system function demands causing a decreasing network efficiency that can degrade user, device, application and/or network service performance so that performance falls below acceptable levels. As another example, in systems in which there is a QoS service session reservation system, uncontrolled and/or unmanaged QoS reservation requests and/or reservation grants can lead to a situation where the QoS reservation resources and/or QoS service delivery resources are over taxed to the point where QoS service performance falls below desired levels. As another example, in networks that require some form of minimum resource allocation for transmissions, reservations, or network resource transactions, the network can become inefficient if one or more devices, applications, network service sources, operating system functions, and/or communication protocols have a relatively high rate of network resource access attempts, network accesses or data transmissions for small transmission payloads (e.g., minimum MAC reservation factors, minimum security overhead factors, minimum QoS reservation factors, minimum time responses for establishing a base station connection, minimum time responses for establishing or closing/being released from a session, etc). Even if the data packet comprising the access event is small, the network resources required to complete the access event are often busy servicing the access event for much longer periods of time than are required for the actual data transmission.

[0045] Another example of device service activity behavior that can have an impact on network performance is the way the device, device subsystem, and/or modem subsystem power cycling or transitions from one power save state to another. For example, establishing a basic connection from a device to a wireless base station consumes base station resources for a period of time and in some cases can also consume other network resources such as AAA, HLR, HA, gateway, billing, and/or charging gateway resources. If a device terminates the connection to the base station when the modem subsystem (e.g., or some other portion of the device) goes from

active connection state to a power save state, then each time the device enters power save state and then exits power save state network resources are consumed, sometimes for time periods measured on the order of seconds or in extreme cases even minutes. If such a device has an aggressive power save algorithm that enters power save state after a short idle period, then the device behavior can consume a proportionally large amount of resources such that the network ability to support multiple devices is diminished, or such that the network cannot support very many similar devices on the network. Another similar example is the establishment of network sessions once the base station connection is established (e.g., establishing a PPP session between the device and a home agent (HA) or other gateway), in which network resources required to open and/or close the network session are ignorantly consumed if a device exhibits aggressive power save state cycling or frequently terminates the data session for other reasons.

[0046] Another example of device service activity behavior that can impact network performance is applications that maintain persistent network communication that generates a relatively high frequency of network data packets. Some applications have persistent signaling that falls into this category. Specific examples include frequent device signaling sequences to update widgets on a desktop; synchronize user data such as calendars, contacts, email, and/or other information/content; check or update email or RSS feeds; access social networking websites or tools; online text, voice or video chat tools; update real-time information; and conduct other repetitive actions. Additional application behavior that can significantly tie up network resources and capacity include, for example, conference meeting services, video streaming, content update, software update, and/or other or similar application behavior. For example, even when the user is not directly interacting with or benefiting from this type of application, the application can be running in the background and continuing to consume potentially significant network resources.

[0047] For example, the types of service activities and/or device behavior that can reduce network capacity and/or network resource availability include software updates for OS and applications, frequent OS and application background network accesses and signaling, frequent network discovery and/or signaling (e.g., EtherType messages, ARP messages, and/or other messaging related to network access), cloud synchronization services, RSS feeds and/or other background information feeds, application (e.g., web browser) or device behavior reporting, background email downloads, content subscription service updates and downloads (e.g.,

music/video downloads, news feeds, etc.), text/voice/video chat clients, virus updates, peer to peer networking applications, inefficient network access sequences during frequent power cycling or power save state cycling, large downloads or other high bandwidth accesses, and/or greedy application programs that continually and/or frequently access the network with small transmissions or requests for information. Various other examples will now be apparent to one of ordinary skill in the art.

[0048] Thus, not only can network capacity, network performance, and/or network resource availability be degraded by high device transmission bandwidth demand, but other types of persistent or frequent traffic resulting from network resource requests, network data accesses or other network interaction can also degrade network capacity, network performance, and/or network resource whether or not the aggregate bandwidth demand as measured by the total data throughput is high or not. Thus, techniques are needed to preserve network capacity by, for example, differentially controlling these types of network service usage activities in various ways depending on the type of service activity requesting network access and/or requesting transactions with network resources.

[0049] Smart phones and similar devices are exacerbating the problem by making frequent queries of the wireless network as such devices move among cell sites to, while in transit, for example, push email, access social networking tools, and/or conduct other repetitive actions. While data traffic is also growing, signaling traffic is outpacing actual mobile data traffic by 30 percent to 50 percent by some estimates. For example, a Yahoo IM user may send a message but then wait a couple of seconds between messages. To preserve battery life, the smart phone typically moves into an idle mode. When the user pushes another message seconds later, the device has to set up a signaling path again, and even when the signaling resource is released by the smart phone, the network typically does not react fast enough to allow for the next station to use resources until several seconds and sometimes minutes. As a result, the base station controller in this example is spending a lot of its resources trying to process the signaling so it cannot perform other tasks, such as allocate additional resources for data network usage, and such inefficiencies exacerbate the data network capacity crunch and dropped calls on such wireless networks.

[0050] One approach used by smart phone vendors to address this problem and save battery life on their devices is to implement a fast dormancy feature, which allows the mobile device to quickly make a query to the radio network controller to release the connection so that it can return to the idle state faster. In other words, the device is relaying the fact that the phone is going dormant saving device resources (e.g., signaling channel) rather than network resources. However, the fast dormancy feature can exacerbate this problem by prematurely requesting a network release only to follow on with a request to connect back to the network or by a request to re-establish a connection with the network.

[0051] Network carriers have typically attempted to manage network capacity using various purely central/core network based approaches. For example, some carriers have indicated a robust capacity planning process and sufficient investment is needed to alleviate this growing capacity crunch. Purely centralized network solutions with no assistance from a device based software agent (or service processor) can have several limitations. For example, for some device applications, OS functions or other service usage activities, if the activity is blocked somewhere in the network behind the base station after over the air (OTA) spectrum bandwidth is consumed to open or begin to open a communication socket, then there can still be an appreciable amount of network capacity or resources consumed even though the data transfer is not allowed to complete. In addition, if the service usage activity is aggressive in re-attempting to establish the network connection to transfer the data, and the network continues to allow the OTA portion of the connection establishment but blocks the connection somewhere in the network, then a large amount of capacity can be consumed by many devices exhibiting such behavior even though no useful service is being allowed. Accordingly, some embodiments for protecting network capacity include controlling network service usage activities at the source of the demand – the device. Furthermore, in some embodiments, service usage is controlled in a manner that delays, prevents, or reduces the frequency of service usage activity re-try attempts to connect to the network.

[0052] In some cases, an additional drawback of purely centralized network solutions to protect network capacity arises when service usage activities are controlled, blocked, throttled, and/or delayed by central network equipment with no mechanisms or support to link to a device user interface (UI) to inform the user what is happening and why it is happening. This can lead to a frustrating user experience and reduced carrier customer satisfaction. Accordingly, in some

embodiments, a device based UI is provided to provide the user with real time or near real time information regarding why a service usage activity is being controlled, blocked, throttled, and/or otherwise controlled in order to protect network capacity. In some embodiments, a UI is provided that also informs the user when there are options to set, control, override, or modify service usage controls for the purpose of protecting network capacity. In some embodiments, such user preference inputs also correspond to a change in service usage billing. In some embodiments, such changes in service usage billing due to capacity sparing service control changes by the user are communicated to the user via a UI notification sequence. In some embodiments, techniques for protecting network capacity employ user warnings when a service usage activity classified for differential user notification policies is likely to cause the user to go over service plan caps (e.g., total data byte count usage caps).

[0053] What is needed is intelligent network monitoring to provide real-time traffic monitoring network service usage (e.g., at the packet level/layer, network stack application interface level/layer, and/or application level/layer) of the wireless network (e.g., radio access networks and/or core networks) and to effectively manage the network service usage for protecting network capacity (e.g., while still maintaining an acceptable user experience). Using Device Assisted Services (DAS) techniques, and in some cases, network assisted/based techniques, to provide for network service usage monitoring of devices, network carriers/operators would be provided greater insight into what devices, which users and what applications, and when and where network congestion problems occur, enabling operators to intelligently add additional resources to certain areas when necessary (e.g., offloading data traffic onto femto cells or WiFi hotspots and adding more network resources), to differentially control network service usage, and/or to differentially charge for network service usage based on, for example, a network busy state, for protecting network capacity.

[0054] Intelligent network monitoring of the wireless network to effectively manage network service usage for protecting network capacity can include providing Device Assisted Services (DAS) for protecting network capacity in accordance with various embodiments described herein. For example, intelligent network monitoring of the wireless network to effectively manage network service usage for protecting network capacity can include differentially controlling over the air software updates and/or performing software updates via wired connections only. As another example, intelligent network monitoring of the wireless

network to effectively manage network service usage for protecting network capacity can include differentially controlling various applications that demand significant network resources or network capacity. As another example, intelligent network monitoring of the wireless network to effectively manage network service usage for protecting network capacity can include managing network access connection requests resulting from repeated power down modes in the modem, which can cause resource intensive re-connection and/or re-authentication processes. As another example, intelligent network monitoring of the wireless network to effectively manage network service usage for protecting network capacity can include techniques for keeping PPP sessions alive to avoid the need to consume network resources to re-establish PPP sessions (e.g., unless the application behavior analysis predicts that a mean access time is long enough for the PPP session to be dropped off and yet not causing overall network resource limitations).

[0055] Unlike traditional QoS techniques, which are used to establish a single end or end to end guaranteed service level(s) on a network, techniques disclosed herein for protecting network capacity facilitate implementation of services on a network to facilitate differential control of certain services to protect network capacity (e.g., to reduce network congestion, network capacity demand, network resource demand; and/or to increase network availability). As also disclosed herein, techniques disclosed herein for protecting network capacity facilitate implementation of services on a network to facilitate differential control of certain services to protect network capacity can also facilitate QoS implementations by maintaining needed levels of network capacity/availability to facilitate delivery of certain QoS levels/classes. For example, techniques disclosed herein for protecting network capacity can aggregate across multiple services and/or devices to facilitate differential control of certain services to protect network capacity. As another example, techniques disclosed herein for protecting network capacity can be used to provide for dynamic QoS classifications (e.g., dynamically assigning/classifying and reassigning/reclassifying (based on various criteria, events, and/or measures) network service usage activities to various QoS levels/classes, such as described herein) to facilitate differential control of certain services to protect network capacity.

[0056] Accordingly, Device Assisted Services (DAS) for protecting network capacity is provided. In some embodiments, DAS for protecting network capacity provides for protection of network capacity (e.g., network congestion and/or network access/resource demand and/or

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

[0057] In some embodiments, techniques are provided for assigning a priority to a network service usage activity and controlling traffic associated with the network services usage activity based on the assigned priority. In some embodiments, techniques are provided for implementing a differentiated and dynamic background services classification, for example, as a function of network availability state and/or network busy state.

[0058] In some embodiments, a service usage control policy is used for assisting in network access control of network service usage activities (e.g., deferring some or all of the network capacity demand from these source activities). In some embodiments, some or all of the network capacity demand is satisfied at a point where the network resources or capacity are more available or less busy. In some embodiments, techniques are provided for classifying network service activities associated with one or more applications or OS functions to a background service class and differentially controlling the background service class traffic. In some embodiments, techniques are provided for classifying one or more network service activities associated with an application or OS function to a background service class, while other network service activities associated with that application or OS function are classified to other service classes (e.g., or to different background service class priority levels).

[0059] In some embodiments, techniques are provided for determining a network busy state (e.g., for a network edge element connection to a device, such as for a RAN for the device's current wireless network access and/or to the current base station/base station controller in wireless communication with the device). In some embodiments, techniques are provided for implementing a service usage control policy to differentially control network services traffic based on a network busy state for an activity, a group of activities, or for a service class.

[0060] In some embodiments, DAS for protecting network capacity includes monitoring a network service usage activity of the communications device in network communication; classifying the network service usage activity for differential network access control for protecting network capacity; and associating the network service usage activity with a network service usage control policy based on a classification of the network service usage activity to facilitate differential network access control for protecting network capacity.

[0061] In some embodiments, a network service usage activity is any activity by the device that includes wireless network communication. In some embodiments, an application, an

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

[0062] In some embodiments, a network service usage activity is classified, associated with, and/or assigned to a background class (e.g., a background service or QoS class) to facilitate differential network service usage control to protect network capacity. In some embodiments, differential network service usage control includes one or more of the following: monitoring network service usage activity; accounting for network service usage activity; reporting network service usage activity; generating a user notification for a network service usage activity; requesting a user preference for control of network service usage activity; accepting a user preference for network service usage activity; implementation of a network service usage activity policy (e.g., block/allow; traffic control techniques, such as throttle, delay, priority queue, time window, suspend, quarantine, kill, remove, and other well known traffic control techniques); implementing UI intercept procedures; generating a network busy state notification; generating a background class notification; generating a user notification for differential network service

usage control of a network service usage activity; and various other techniques as described herein.

[0063] In some embodiments, a network availability state includes a state or measure of availability/capacity of a segment of a network (e.g., a last edge element of a wireless network). In some embodiments, a network busy state includes a state or measure of the network usage level or network congestion of a segment of a network (e.g., a last edge element of a wireless network). In some embodiments, network availability state and network busy state are inverse measures. As used herein with respect to certain embodiments, network availability state and network busy state can be used interchangeably based on, for example, a design choice (e.g., designing to assign background policies based on a network busy state or a network availability state yields similar results, but they are different ways to characterize the network performance and/or capacity and/or congestion). In some embodiments, network availability state and network busy state are dynamic measures as such states change based on network usage activities (e.g., based on a time of day, availability/capacity level, congestion level, and/or performance level). In some embodiments, differential network service usage control of a network service usage activity is based on a network busy state or network availability state.

[0064] In some embodiments, certain network service usage activities are classified as background services. In some embodiments, lower priority and/or less critical (and/or based on various other criteria/measures) network service usage activities are classified as background services based on a network busy state and differentially controlled based on a network busy state to protect network capacity. In some embodiments, differential network service usage control policies are based on a time of day, a network busy state, background services and/or QoS class changes based on a time of day and/or a network busy state, a random back-off for access for certain network service usage activities, a deterministic schedule for certain network service usage activities, a time windowing in which network service usage control policies for one or more service activities or background/QoS classes changes based on time of day, network busy state, a service plan, and various other criteria, measures, and/or techniques as described herein.

[0065] In some embodiments, a network capacity controlled service or network capacity controlled services class includes one or more network services (e.g., background download

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

[0066] For example, differentially controlling network service usage activities based on network capacity controlled services or dynamic QoS or QoS classifications can protect network capacity by, for example, improving network performance, increasing network availability, reducing network resources demand, and/or reducing network capacity demand (e.g., based on an individual device, aggregate devices connected to an edge element, and/or aggregate devices connected to many edge elements). In some embodiments, differentially controlling network service usage activities based on network capacity controlled services or dynamic QoS or QoS classifications can protect network capacity while maintaining proper device operation. In some embodiments, differentially controlling network service usage activities based on network capacity controlled services or dynamic QoS or QoS classifications can protect network capacity while maintaining an acceptable user experience (e.g., proper and/or expected device operation, proper and/or software/application/OS/function operation, avoiding (whenever possible) significant adverse impact on device functions, and/or user notifications to keep the user informed of various differential control implemented on the device).

[0067] In some embodiments, dynamic QoS classifications include QoS classifications that can be dynamically modified (e.g., reclassified, reprioritized, upgraded, and/or downgraded) based on various criteria, measures, settings, and/or user input as described herein (e.g., based on a time of day and/or day of week, based on a network busy state, based on a user preference, and/or based on a service plan). In some embodiments, the various techniques described herein

related to DAS for providing network capacity and/or QoS for DAS are applied to dynamic QoS related techniques.

[0068] As wireless networks, such as mobile networks, evolve towards higher bandwidth services, which can include or require, for example, various levels of Quality of Service (QoS) (e.g., conversational, interactive data, streaming data, and/or various (end-to-end) real-time services that may benefit from QoS), demands will increase for converged network services to facilitate such services for end-to-end services between networks (e.g., to allow for control and/or support for such services, for example, QoS support, across network boundaries, such as between wireless networks (such as various service provider networks) and IP networks (such as the Internet), and/or other networks). While various efforts have attempted to address such QoS needs, such as policy management frameworks for facilitating QoS end-to end solutions, there exists a need to facilitate various QoS requirements using Device Assisted Services (DAS).

[0069] Accordingly, Quality of Service (QoS) for Device Assisted Services (DAS) is provided. In some embodiments, QoS for DAS is provided.

[0070] To establish a QoS channel, differentiated services are typically available, in which one class/level of service has a higher priority than another to provide for differentiated services on a network, such as a wireless network. For example, in a wireless network, various network elements/functions can be provisioned and controlled to establish a single end to end QoS channel. In some embodiments, a centralized QoS policy coordination and decision function using DAS techniques to assist in coordinating the QoS channel setup and control among the various elements of a wireless network is provided.

[0071] In some embodiments, QoS channel refers to the logical communication channel connected to a device that provides a desired level of QoS service level. For example, the QoS channel can be created with one or more QoS links, in which each link represents a QoS enabled connection that spans a portion of the total end to end network communication path from a near end device to a far end device. For example, the far end device can be on the same network or on a different network, potentially with different access technology and/or a different access network carrier. In some embodiments, the QoS channel includes one or more QoS links in which each link in the channel is QoS enabled, or one or more of the links in the channel is QoS enabled and others are not. As an example, a QoS channel can include the following links: a

first device traffic path link, a first device to access network equipment element link (e.g., 2G/3G/4G wireless base station, WiFi access point, cable network head end, DSLAM, fiber aggregation node, satellite aggregation node, or other network access point/node), a first carrier core network, a long haul IPX network, a second carrier core network, a second device to access network equipment element link, and a second device traffic path link as similarly described herein with respect to various embodiments.

[0072] In some embodiments, each of the links described above has the ability to provide QoS services for that segment of an overall QoS channel. In some embodiments, the device traffic path link and/or the device to access network equipment element link are QoS enabled, but the carrier core network and/or IPX network links are not QoS enabled. In some embodiments, the core network and/or IPX network have sufficient over-provisioning of bandwidth that QoS is not limited by these network elements and, for example, can be limited by the device traffic link and/or the device to access network equipment element link do not have sufficient excess bandwidth making it desirable to QoS enable these QoS channel links. A common example is a 2G/3G/4G wireless network in which a device traffic path link and the device to access network element link (e.g., Radio Access Bearer (RAB)) are QoS enabled while the carrier core network and IPX network links are not (e.g., are provided at a best effort service level or other service levels).

[0073] In some embodiments, a QoS session refers to the QoS enabled traffic for a given device that flows over a QoS channel or QoS link. This QoS traffic supports a QoS service activity. In some embodiments, a QoS service activity includes a device service usage that is requested, configured, or preferably serviced with a given level of QoS. In some embodiments, a device QoS activity is a combination of one or more of the following: application, destination, source, socket (e.g., IP address, protocol, and/or port), socket address (e.g., port number), URL or other similar service identifier, service provider, network type, traffic type, content type, network protocol, session type, QoS identifier, time of day, network capacity (e.g., network busy state), user service plan authorization or standing, roaming/home network status, and/or other criteria/measures as similarly described herein. For example, QoS service activities that are supported by QoS sessions can include VOIP traffic, streaming video traffic, differentiated access bandwidth during busy network periods, real-time interactive traffic, such as network connected multimedia meetings (e.g., shared presentations, picture, video, voice, and/or other

such applications/services), best effort interactive, such as Internet browsing, time sensitive services, such as email message body delivery, near real-time interactive services, such as SMS or push to talk, background download services, such as email downloads and other file transfers (e.g., FTP), and/or truly background download services, such as software updates (e.g., OS or application software updates and/or antimalware updates including content/signature updates).

[0074] In some embodiments, various QoS levels or classes are supported. For example a conversation class can provide for real-time traffic, which is typically very delay sensitive but can tolerate bit errors and packet losses. The conversational class is typically used for Voice Over IP (VOIP) and video telephony, in which users of such services benefit from the short delay features of the conversational class. A streaming class is similar to the conversational class except that the streaming class typically can tolerate more delay than the conversational class. The streaming class is generally used for when one end of the connection is a user (e.g., human user) and the other end is a machine/computer (e.g., for streaming content applications, such as streaming of video, such as movies or other video content). An interactive class is generally intended for traffic that allows delay variation while requiring reasonably low response time (e.g., web browsing or other applications in which the channel can be unused for long periods of time but when a user makes a request for a new page/data, the response time should be reasonably low). A background class is generally used for lowest priority service usages (e.g., typically used for e-mail with and without downloads/attachments, application software updates, OS software updates, and/or other similar applications/functions). In some embodiments, various QoS classes or services are applicable to the conversational class. In some embodiments, various QoS classes or services are also applicable to the streaming class. In some embodiments, various QoS classes or services are also applicable to the interactive class but typically not applicable to the background class. As will now be apparent to one of ordinary skill in the art, various other classes can be provided with lower or higher granularity based on service usage/channel requirements and/or network architectures.

[0075] In some embodiments, a QoS link or a QoS channel supports one QoS session. In some embodiments, a QoS link or a QoS channel supports multiple QoS sessions. In some embodiments, QoS link provisioning is provided to setup the QoS traffic level for a given QoS session or group of QoS sessions.

[0076] In some embodiments, a QoS channel is a single ended QoS channel or an end to end QoS channel. For example, if a QoS channel is end to end, then the QoS channel provisioning is accomplished in a coordinated manner for each QoS enabled link in the QoS channel. If a QoS channel is single ended, then the network elements and/or device participate in provisioning as much of one end of the QoS channel as possible, leaving provisioning of the QoS for the other end of the channel as the responsibility of the device and/or network elements that handle the traffic at the other end of the QoS channel. In some embodiments, a single ended QoS channel includes another single ended QoS channel at the other end. In some embodiments, only one end has single ended QoS channel enablement while the other end of the channel is a best effort service level, which, for example, can be used where one end of the QoS channel has tighter constraints on traffic capacity or quality than the other end (e.g., a VOIP call with one end that is QoS enabled on a 3G wireless network that has relatively tight bandwidth compared to a lightly loaded cable modem network device on the other end which may not need to be QoS enabled in order to achieve adequate voice quality).

[0077] In some embodiments, a QoS request (e.g., a QoS channel request or QoS service request) is a request for a QoS provisioning event to enable a QoS channel for one or more QoS service activities. In some embodiments, QoS availability assessment includes determining whether one or more of the links in a possible QoS channel are available (e.g., based on network capacity and transmission quality) to provision the necessary level of QoS for a requested QoS channel. In some embodiments, a QoS request is initiated by a device, a user, an application, and/or a network element/function as similarly described herein.

[0078] In some embodiments, a service plan refers to the collection of access service capabilities, QoS capabilities, and/or network capacity controlled services that are associated with a communications device. In some embodiments, the access service capabilities, QoS capabilities, and/or network capacity controlled services are determined by the collection of access service control policies for the device. In some embodiments, these service control policies are implemented in the network equipment. In some embodiments, these access service control policies are implemented both in the device and in the network equipment. In some embodiments, these access service control policies are implemented in the device. In some embodiments, there are different levels of service control capabilities (e.g., policies) based on different levels of service plan payments or device standing or user standing. In some

embodiments, there are different levels of service control policies based on network type, time of day, network busy status, and/or other criteria/measures as similarly described herein with respect to various embodiments. In some embodiments, the access control and QoS control policies are based on the type of service activity being sought. In some embodiments, the QoS level and access level available for a given service activity for a given device or user is determined by the policies associated with the service plan. In some embodiments, a QoS authorization assessment is performed to determine whether a device or user has sufficient service plan standing to allow the requested level of QoS.

[0079] In some embodiments, before a QoS channel or link is provisioned (or before a QoS request is responded to or filled), a QoS availability assessment is performed to determine whether sufficient communication channel resources are available to provision the necessary level of QoS for the QoS channel or link. In some embodiments, this QoS availability assessment is determined by assessing the available QoS capacity for one or more necessary QoS links in the channel. For example, the available QoS link capacity can be assessed for one or more of a device traffic path, a device to access network equipment element link, a core network link, and/or an IPX network link. If the QoS assessment shows that the necessary channel capacity and quality are available for the desired QoS level for one or more desired QoS service activities, then a QoS channel request or QoS service request can be granted. In some embodiments, a QoS link or QoS channel reservation process is provided to reserve QoS capacity and quality in advance of link or channel provisioning to ensure that the available QoS resources are not assigned between the time of QoS availability assessment and QoS channel provisioning.

[0080] In some embodiments, the QoS availability assessment is performed after QoS authorization assessment. This prevents the unnecessary exercising of network elements when the device or user does not have sufficient service plan standing to receive the desired level of QoS even if it is available. This can be an important screening function performed on the device in the service processor, or by a centralized network function such as the service controller (e.g., or interchangeably, the home agent; Home Location Register (HLR); Authentication, Authorization, and Accounting (AAA) server/gateway/function; base station; one of the gateways, policy and charging rules function (PCRF), or other network element/function). In

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

[0081] In some embodiments, a QoS channel is provisioned to create the QoS channel to support a QoS session (e.g., a QoS service activity). In some embodiments, QoS channel provision includes assigning, routing, and/or otherwise causing the QoS session traffic to flow over one or more QoS links in the assigned QoS channel.

[0082] In some embodiments, device assisted service traffic control and QoS apply readily and directly to the problems of managing a QoS device link for QoS channel provisioning. Accordingly, in some embodiments, a service processor is provided to assist in provisioning the device portion of the QoS channel. In some embodiments, the service processor provisions the device link portion of the QoS channel by placing a higher priority on higher QoS level traffic. In some embodiments, this QoS priority is implemented in a number of ways, including routing the higher priority QoS traffic into first priority in the downstream and/or upstream traffic queues. Upstream traffic queuing is performed directly in some embodiments by transmitting guaranteed bit rate traffic first at higher available throttling rates, differentiated QoS traffic second with a controlled throttling rate, best effort traffic third with possibly lower controlled throttled rates, and/or background traffic fourth when/if bandwidth not needed by the higher levels of QoS traffic and at lower controlled throttling rates. For example, downstream traffic can be handled by queuing traffic and delaying or preventing TCP acknowledgements to be returned for the lower levels of QoS priority, while immediately passing the traffic and TCP acknowledgements for higher levels of QoS priority. The device link portion of the QoS channel is thus provisioned by assigning policies for the queuing priority, delay, throttle rate, and TCP acknowledgement return rate for device traffic in accordance with the bandwidth that is available at any point in time for the device. In some embodiments, various device service processor traffic control capabilities regulate or partially regulate QoS in accordance with a set of network policy instructions, including, in some embodiments, a service plan policy set.

[0083] In some embodiments the device service processor establishes multiple QoS channels through the device traffic path with each QoS channel having traffic control policies as described herein, with each QoS channel policy set creating a different class of QoS. In some embodiments, employing this multiple QoS channel approach, QoS for a given service activity is

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

[0084] Based on the aggregate demand for each traffic QoS class, and the traffic capacity and quality level available to the device, the service processor can adjust the total available bit rate or percentage of available traffic capacity for each QoS class. For example, in some embodiments, the aggregate demand for the real-time interactive traffic control class (e.g., services, such as VOIP, emergency communication services or high performance real-time competitive gaming) can be determined, and the QoS routing function on the device (e.g., a QoS router agent/function) can first allocate enough constant bit rate traffic capacity from the available traffic capacity to satisfy these services, with each QoS service activity that requires this QoS class being assigned to this QoS channel. As more QoS service activities require this traffic class, the capacity allocated to the QoS channel out of the available device capacity is increased, and when fewer QoS service activities require this traffic class the capacity for this QoS channel is released. In the event that the device does not have any more available capacity with a guaranteed bit rate QoS level, then additional QoS service activities that desire, require or request this QoS level will not be provided this QoS level, and instead will either be provided with a lower QoS level or will not be allowed to connect to the access network. In some embodiments, there can be a hierarchy among the possible QoS service activities so that if there

is no more capacity available at a given service QoS level, then the available capacity for that QoS class is provided to the service activities requiring that QoS from highest priority to lowest, until the available QoS class capacity is consumed, and then one or more QoS service activities that are too low on the priority list to obtain service with that QoS class are either bumped to a lower QoS class or are denied access. In some embodiments, once the required capacity to satisfy the real-time constant rate traffic needs is satisfied, the remaining capacity available to the device is then divided among the other QoS channel classes in accordance with a priority policy, with the priority policy being based on the relative priority of each service class, the relative priority of each QoS service activity, or a combination of the relative priority of each QoS service class and each QoS service activity. For example, these relative priority policies can vary from device to device based on service plan selection, device type, user standing, user group, device location, device network connection, type of network, time of day, network busy state, and/or other criteria/measures.

[0085] In some embodiments, a QoS link is established between the device and an access network equipment element. For example, such equipment element embodiments can include a 2G/3G/4G wireless base station, a wireless access point, a cable network head end, a DSL network DSLAM, a fiber network device traffic aggregator, a satellite network device traffic aggregator, a frame relay aggregation node, an ATM aggregation node, and/or other network equipment. In some embodiments, a logical communication channel is created between the device and the network equipment element, with the logical communication channel supporting a given level of QoS or QoS class traffic policy set. For example, the logical channel can include a RAB formed between a 2G/3G/4G base station and a wireless end point device. The RAB can be formed by controlling the media access control (MAC) parameters of the base station radio channel so that a given level of QoS class policies can be implemented. For example, the RAB can support constant bit rate, low latency communication traffic for guaranteed bit rate real-time traffic, or a differentiated high priority access channel for streaming traffic, or a best effort random access channel for best effort traffic, or an available unused capacity traffic for background traffic. The QoS channel link created in this manner can be dedicated to a single device, or shared with a subset of devices, or available to all devices. The QoS channel link created in this manner can be used by the device to support a single QoS activity as described herein, or a group of QoS activities as described herein. It will now be apparent to one of

ordinary skill in the art that similar settings for cable head end and cable modem MAC can yield similar QoS classes for QoS links for the cable modem case and that similar techniques can be applied for a wireless access point or a satellite system MAC to achieve similar QoS classes for QoS links. It will also now be apparent to one of ordinary skill in the art that by creating multiple logical channels in the device link, and/or adjusting the available access network capacity and quality for each logical device communication channel in the DSLAM or fiber aggregator, similar QoS class QoS links can be established for the DSL and fiber distribution network cases.

[0086] In some embodiments the device service processor serves to route QoS service activities to the appropriate logical communication channel established for the desired QoS class supported by a QoS link between the device and the access network equipment element. In some embodiments, the device service processor elements (e.g., the policy implementation agent and/or the policy control agent) can be used in some embodiments to assign the same QoS traffic control policies to one or more QoS service activities that require the same QoS level. In a similar manner, in some embodiments, the device service processor elements can be used to assign or route service activity traffic for a given QoS class to the correct logical communication channel between the device and the access network element (e.g., a 2G/3G/4G base station) that supports the traffic control policies for the desired QoS class. For example, a QoS service link that supports guaranteed bit rate and latency can be established with one or more RABs from a base station to the device, and a second QoS service link can be established that supports differentiated preferred access for streaming content using one or more differentiated access RABs, and a third best effort RAB can be used to support best effort traffic. Each of the required RABs is first requested and then provisioned as described herein based on the aggregate required capacity and quality for one or more QoS service activities that require or desire the specific QoS service class associated with the RAB logical channel policy parameters. Once the set of logical QoS channels is thus established, the service processor (e.g., QoS router agent/function) routes the traffic associated with each QoS service activity to the appropriate RAB. In some embodiments, the service processor can detect increases or decreases in aggregate QoS class demand for each QoS class as QoS activities are initiated or terminated for that QoS class, and the service processor can communicate the required increases or decreases in the RAB assignments required to support that logical QoS channel.

[0087] In some embodiments, the access QoS link is established by direct communication from the device in which the device requests the QoS channel or link from the access network equipment element, or the device requests the QoS channel or link from an intermediate networking device, such as a service controller (e.g., or a readily substituted device with similar features, such as a home agent, an HLR, a mobile switching center, a base station, an access gateway, a AAA system, PCRF, or a billing system). In some embodiments, the device service processor bases the QoS channel or link request on an association the device performs to match a QoS service activity with a desired or required QoS class or QoS traffic control policy set. For example, this association of QoS class or QoS traffic control policy set with QoS service activity can be determined by a predefined policy mapping that is stored on the device and used by the service processor. In some embodiments, this policy mapping store is populated and/or updated by a service controller (e.g., or similar function as described herein). In some embodiments, the mapping is determined by a service controller (e.g., or similar function as described herein) based on a report from the device of the QoS service activity that needs the QoS channel or link.

[0088] In some embodiments, the required or desired QoS level for one or more QoS service activities is determined by a set of QoS service traffic control policies that are pre-assigned to various QoS service activities. For example, a given application can be pre-assigned a QoS class. As another example, a web service destination such as a VOIP service site can be assigned a QoS class. As another example, a given application can have one QoS assignment level for general Internet traffic but have a QoS assignment for real-time gaming traffic. As another example, a real-time broadcasting website can have a best effort QoS level assigned to programming information and general browsing and have a differentiated streaming QoS level for broadcast traffic content. In some embodiments, detection of QoS need or QoS assignment request for a given activity can be assigned by a device service processor according to a pre-defined QoS policy rules table (e.g., QoS activity table), or can be determined by a service controller based on information reported by the device, or can be requested by an application through a QoS application interface (e.g., QoS API), or can be determined by the nature of incoming traffic.

[0089] In embodiments, in which both end points in the QoS channel participate in establishing an end to end QoS channel, the required QoS level is determined and/or

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

[0090] In some embodiments, the near end or originating end device service processor contacts the far end or terminating device service processor to initiate a QoS channel. In some embodiments, the initiation of the QoS channel from the near end or originating device is performed automatically by the far end device when its service processor detects that a given level of QoS is needed for the communication between the two devices. In some embodiments, the near end or originating device service processor detects the need for a QoS channel to the far end or terminating device and contacts a central network resources, such as the service controller (e.g., or other equipment element with similar function for this purpose), and the service controller provisions the far end of the QoS channel, either by communicating directly with the far end device or by communicating with the far end device's service controller (e.g., or other equipment element with similar function for this purpose). In some embodiments, in which the far end device service controller is contacted to assist in provisioning the QoS channel, there is a look up function to determine the address of the far end service controller based on a look up index formed from some aspect of the far end device credentials (e.g., phone number, SIM ID, MEID, IMSI, IP address, user name, and/or other device credentials).

[0091] In some embodiments, the mapping of QoS service activity to the desired level of QoS class or QoS traffic control policies is determined by providing a QoS API in the device service processor that applications use to request a QoS class or QoS channel connection. In

some embodiments, an API is provided so that application developers can create application software that uses the standard interface commands to request and set up QoS channels. In some embodiments, the API does one or more of the following: accepts QoS requests from an application, formats the QoS channel request into a protocol appropriate for transmission to network equipment responsible for assessing QoS channel availability (e.g., including possibly the device traffic control system), coordinates with other network elements (e.g., including possibly the device traffic control system) to reserve a QoS channel, coordinates with other network elements (e.g., including possibly the device traffic control system) to provision a QoS channel, informs the application that the desired QoS channel can be created or not, and/or coordinates with other network elements (e.g., including possibly the device traffic control system) to connect the application with the desired QoS channel class. In some embodiments, the QoS API accepts the application QoS request and communicates and possibly coordinates with one or more QoS network equipment elements, such as a base station, cable head end or access point. In some embodiments, the QoS API accepts the QoS request from the application and communicates and possibly coordinates with an intermediate network element, such as a service processor (e.g., or other similar function as described herein). In some embodiments the QoS API assesses the QoS service plan standing for the device or user before sending QoS channel requests to other network elements, and only initiates the QoS request sequence if required service plan authorization is in place. In this manner, the potentially complex process of establishing a QoS channel with all the specific equipment communication protocols that typically need to be supported to assess QoS channel availability and provision the QoS channel are simplified into a limited set of API commands that are easy for an application development community to learn about and use for QoS differentiated services and applications.

[0092] In some embodiments, local traffic control on the device service processor is combined with traffic control in the link between the device and the access network equipment element. In this manner, both the device traffic control path QoS link and the device to access network element QoS link can be coordinated for best device QoS performance results given the available capacity and quality of the access network traffic for the device. In some embodiments, the policies for how the device manages local traffic control, establishes access network element logical channels (e.g., RABs) and routes traffic to and from the access network element logical channels is all determined by predefined policy rules loaded onto the device by

the service controller (or other equivalent network element). In some embodiments, these policies are determined in the service controller itself.

[0093] In some embodiments, a QoS user interface (e.g., QoS UI) is presented to the device user. In some embodiments, the QoS UI notifies the user what level of QoS services the device is authorized to receive based on the service plan selection. In some embodiments, the QoS UI notifies the user what level of QoS services are available on the present network the device is connected to at the present time. In some embodiments, the QoS UI notifies the user when a level of QoS service that is higher than that authorized by the user service plan is required or desirable for a given service activity that the device has initiated. In some embodiments, the QoS UI provides the user with a set of one or more upgrade options to upgrade the service plan to include a higher level of QoS for one or more service activities. In some embodiments, the QoS UI provides the user with an opportunity to specify what level of QoS the user would like to employ for one or more service usage activities. In some embodiments, the QoS UI allows the user to specify a service plan setting that provides differentiated QoS during times when the network is busy. In some embodiments, the QoS UI allows the user to purchase one or more grades of service QoS with either a post-pay for a pre-defined service period and one or more pre-defined service usage limits by QoS class, a pre-pay for one or more pre-defined service usage limits by QoS class, or another payment system for differentiated QoS services. In some embodiments, the QoS UI provides the user with an opportunity to QoS enable or pay for QoS services for a connection that is initiated by an incoming connection to the device.

[0094] In some embodiments, QoS for DAS techniques include verifying that the device is properly implementing the QoS traffic control policies, for example, in accordance with a service plan. This ensures that errors, hacking, user device software settings manipulations, or other malware events do not result in inappropriate levels of QoS for a given device or group of devices. Accordingly, in some embodiments, the traffic control and QoS verification techniques described herein are employed to verify that the proper level of QoS is applied for a given service usage activity in accordance with a QoS priority policy. For example, verification of QoS channel request policy rules behavior can be implemented in a variety of ways including, as an example, monitoring device QoS channel requests and comparing the level of QoS requested with the level of QoS the device is authorized to receive in the service plan in effect for the device. Verification of proper QoS channel usage behavior by a device can be implemented in a

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

[0095] In some embodiments, the QoS router prioritizes traffic on the device. In some embodiments, the QoS router connects the QoS enabled session to the RAB that has the proper QoS level. In some embodiments, one session is routed to the RAB. In some embodiments, more than one session can be routed to an RAB. In some embodiments, multiple RABs providing multiple QoS levels are created to the device, and the QoS router routes each service activity to the RAB dictated by the QoS policy rules in effect on the device.

[0096] In some embodiments, the network collects service usage charges for different QoS classes. In some embodiments, there is differentiated service charging for the different classes of QoS service usage. As an example, since guaranteed bit rate traffic consumes network resources whether the traffic capacity is used or not, there can be a time element involved in the charging calculations. As a more detailed example, guaranteed bit rate services can be charged by the total bandwidth provisioned to the device at a given time multiplied by the amount of time that that bandwidth is made available. In some embodiments, differentiated access traffic that has higher QoS than best effort traffic but is not guaranteed bit rate can be charged at a higher rate than best effort traffic but lower than guaranteed bit rate. In some embodiments, such traffic can be charged based on the time the QoS channel is made available and the total amount of data transmitted over the channel, or can only be based on the total amount of data transmitted over the channel. Best effort traffic is charged in some embodiments based only on the total amount of data used, with the data charges being less than differentiated streaming access services. Background data services in some embodiments are charged at the lowest rate, possibly with only certain times of the day or periods of low network traffic demand being available for such services, and with the service being based on total data transmitted. In some embodiments, all QoS service levels can be charged based on a fixed price for a fixed charging period, possibly

with a service usage cap with additional charges if the service cap is exceeded. In such fixed price scenario embodiments, the price charged is again higher for higher levels of QoS. In some embodiments, the network collects service usage charges for different network capacity controlled service classes. In some embodiments, there is differentiated service charging for the different classes of network capacity controlled service usage, as described herein.

[0097] In some embodiments, the network equipment (e.g., access network element, gateways, AAA, service usage storage systems, home agent, HLR, mobile data center, and/or billing systems) record and report service usage for one or more of the QoS service classes used by the device. In some embodiments, the device service processor records and reports service usage for one or more of the QoS service classes used by the device and reports the QoS service class usage to the service controller (e.g., or another substitute network element). In some embodiments, in which the device is recording reporting usage for one or more QoS service classes, it is important to verify the device service usage reports to ensure that the device usage reports are not distorted, tampered with, and/or otherwise in error. In some embodiments, verifying service usage reports against service usage that should be occurring given the service control policies in place on the device, service processor agent functional operation verification, test service usage events, agent query response sequences, device service processor software protection techniques, device service processor software environment checks, and several other techniques are provides as described herein. For example, using one or more of these verification techniques can provide a verifiable device assisted QoS service usage charging system. As another example, using one or more of these verification techniques can provide a verifiable network capacity controlled service usage charging system. In some embodiments, the network equipment (e.g., access network element, gateways, AAA, service usage storage systems, home agent, HLR, mobile data center, and/or billing systems) record and report service usage for one or more of the network capacity controlled service classes used by the device, as described herein.

[0098] In some embodiments, device assisted traffic control is provided for managing network congestion as follows. For example, when a given base station or group of base stations experience traffic demand that is high relative to the available capacity and/or service quality that can be provided, and such a condition is determined (e.g., detected or reported) based on a network busy state assessment as described below and further herein, then a service controller

(e.g., or another network function) can issue, send, and/or implement traffic control throttling policies to/for the devices in accordance with a measure of the excess traffic demand the one or more base stations is experiencing. For example, the device service processors connected to an overly busy base station can be instructed to reduce the traffic control priority for one or more classes of QoS traffic, reducing the queuing priority, throttling rate, delay and/or access allowance for some or all of one or more classes of traffic. As another example, the device service processors connected to an overly busy base station can be instructed to reduce the traffic control priority for one or more classes of network capacity controlled services traffic, reducing the queuing priority, throttling rate, delay and/or access allowance for some or all of one or more classes of such traffic. As another example, one or more classes of network capacity controlled services traffic, such as background download processes, which can include, for example, software updates can be turned off completely or throttled back significantly. As another example, best effort traffic such as Internet browsing can be throttled or reduced for a group of devices connected to base stations experiencing excess traffic demand. As another example, a policy can be implemented on the devices connected to busy base stations in which the device is allowed to browse or conduct other best effort service activities at a relatively high throttling rate for a period of time, but if the device uses more than a certain amount of service (e.g., total data downloaded and/or uploaded) in a certain period of time then the device may be traffic controlled according to an adaptive throttling policy as described herein. In some embodiments, higher QoS level traffic cannot be throttled in such circumstances, such as VOIP traffic where real-time guaranteed bit rate is important to meet user service needs or expectations, while lower priority traffic such as interactive browsing and/or background download are throttled and/or blocked. In some embodiments, the QoS availability assessment processes described herein are adjusted so that higher QoS channels are not provided and provisioned in times or locations in which a given base station or group of base stations experience excess demand or demand above a given threshold.

[0099] In some embodiments, users or devices that have service plans with higher QoS levels, or service plans with higher priority during busy network periods have different traffic control policies (e.g., for QoS services and/or network capacity controlled services) applied to them that result in a higher level of traffic performance and/or a higher level of QoS service availability. For example, emergency service workers can be given higher traffic control access

policies that result in differentiated services during peak busy times on the network or a portion of the network. In some embodiments, users can obtain a premium service plan for differentiated access during peak busy time periods or may use higher levels of QoS service settings and/or service plans to achieve differentiated service during peak busy periods. As another example, services that demand high levels of QoS classes, such as real-time voice services, instant messaging, push to talk, differentiated video streaming, and/or interactive gaming, are not traffic controlled to the same extent that other lower priority services or lower class service plans are traffic controlled during peak busy times. For example, this type of service differentiation can also be applied based on device type, user group, user standing, user reward zone points, and/or other criteria/measures as similarly described herein.

[00100] In some embodiments, the decision to control (e.g., reduce, increase, and/or otherwise control in some manner) the access traffic control settings as described above is made by the device service processor based on the device's assessment of the network capacity, which can be determined using various techniques as described herein. In some embodiments, the decision to control the access traffic control settings as described above is made by a service controller (e.g., or other interchangeable network equipment element or elements as described herein) connected to the device that provides instructions to the device to adjust the access policy settings. For example, the service controller can obtain the network capacity information from access equipment elements, from device reports of traffic capacity and/or quality as described herein, or from reports on traffic capacity and/or quality obtained from dedicated devices used for the purpose of assessing network capacity. In some embodiments, the decision to control the access traffic control settings as described above is based on the time of day, the day of week, or both to accommodate cyclical patterns in network capacity and traffic demand.

[00101] In some embodiments, a service controller (e.g., or another network equipment element or elements, as described herein) assesses network busy state and then controls device traffic demand by reducing the offered capacity for one or more service classes (e.g., for QoS services and/or network capacity controlled services) supported by the access network equipment elements, such as a wireless base station. In such embodiments, the service controller (e.g., or similar function) gathers the network capacity information with one of the techniques described herein and instructs one or more of the access network equipment elements to reduce the offered capacity for one or more levels of QoS classes and/or network capacity controlled service

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

[00102] In some embodiments, the device is enabled with ambient services that have differentiated QoS services and/or network capacity controlled services as part of the ambient service offering. For example, ambient QoS techniques can be provided using the pre-assigned QoS policies for a given service activity set within the ambient service, or using an ambient service application that requests QoS through the QoS API. Other embodiments for providing QoS differentiated service activities within ambient service offerings will now be apparent to one of ordinary skill in the art. As another example, ambient network capacity controlled service techniques can be provided using the pre-assigned network capacity controlled policies for a given service activity set within the ambient service, monitoring and dynamically assigned techniques, and/or using an ambient service application that uses API or emulated API techniques, and/or other techniques as described herein.

[00103] In some embodiments, a QoS service control policy is adapted as a function of the type of network the device is connected to. For example, the QoS traffic control policies and/or the QoS service charging policies can be different when the device is connected to a wireless network (e.g., a 3G/4G network where there is in general less available QoS enabled traffic capacity) than when the device is connected to a wired network (e.g., a cable or DSL network where there is in general a higher level of QoS capacity available). In such embodiments, the device service processor and the service controller can coordinate to adapt the QoS service control policies and/or the QoS service charging policies to be different depending on which network the device is connected to. Similarly, the device QoS service control policy and/or QoS service charging policy can also be adapted based on whether the device is connected to a home wireless network or a roaming wireless network. In some embodiments, a network capacity controlled service control policy and/or a network capacity controlled charging policy is adapted as a function of the type of network the device is connected to, as similarly described herein.

[00104] In some embodiments, various of the QoS related techniques and/or network capacity controlled services techniques described herein are performed on the device using DAS techniques and/or on the service controller in secure communication with a verified service processor executed on the device using DAS techniques. In some embodiments, various of the QoS related techniques and/or network capacity controlled services techniques described herein are performed by/in coordination/communication with one or more intermediate network elements/functions for assisting in various techniques (e.g., functions) for QoS techniques and/or network capacity controlled services techniques as described herein.

[00105] FIG. 1 illustrates a functional diagram of a network architecture for providing quality of service (QoS) for device assisted services (DAS) and/or for providing DAS for protecting network capacity in accordance with some embodiments. In some embodiments, QoS for DAS techniques described herein are implemented using the network architecture shown in FIG. 1. In some embodiments, DAS for protecting network capacity techniques described herein are implemented using the network architecture shown in FIG. 1.

[00106] As shown, FIG. 1 includes a 4G/3G/2G wireless network operated by, for example, a central provider. As shown, various wireless devices 100 are in communication with base stations 125 for wireless network communication with the wireless network (e.g., via a firewall 124), and other devices 100 are in communication with Wi-Fi Access Points (APs) or Mesh 702 for wireless communication to Wi-Fi Access CPE 704 in communication with central provider access network 109. In some embodiments, one or more of the devices 100 are in communication with other network element(s)/equipment that provides an access point, such as a cable network head end, a DSL network DSLAM, a fiber network aggregation node, and/or a satellite network aggregation node. In some embodiments, each of the wireless devices 100 includes a service processor 115 (as shown) (e.g., executed on a processor of the wireless device 100), and each service processor connects through a secure control plane link to a service controller 122 (e.g., using encrypted communications).

[00107] In some embodiments, service usage information includes network based service usage information (e.g., network based service usage measures or charging data records (CDRs), which can, for example, be generated by service usage measurement apparatus in the network equipment), which is obtained from one or more network elements (e.g., BTS/BSCs 125, RAN

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

[00108] In some embodiments, CDR mediation is used to account for the micro-CDR service usage information by depositing it into an appropriate service usage account and deducting it from the user device bulk service usage account. For example, this technique provides for a flexible service usage billing solution that uses pre-existing solutions, infrastructures, and/or techniques for CDR mediation and billing. For example, the billing system (e.g., billing system 123 or billing interface 127) processes the mediated CDR feed from CDR mediation, applies the appropriate account billing codes to the aggregated micro-CDR information that was generated by the device, and then generates billing events in a manner that does not require changes to the existing billing systems (e.g., using new transaction codes to label the new device assisted billing capabilities). In some embodiments, network provisioning system 160 provisions various network elements/functions for authorization in the network, such as to authorize certain network elements/functions (e.g., CDR storage, aggregation, mediation, feed 118 or other network elements/functions) for providing micro-CDRs, reformatted micro-CDRs, and/or aggregated or reconciled CDRs.

[00109] As shown in FIG. 1, a CDR storage, aggregation, mediation, feed 118 is provided. In some embodiments, the CDR storage, aggregation, mediation, feed 118 receives, stores,

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

[00110] In some embodiments, various techniques for partitioning of device groups are used for partitioning the mobile devices 100 (e.g., allocating a subset of mobile devices 100 for a distributor, an OEM, a MVNO, and/or another partner or entity). As shown in FIG. 1, a MVNO core network 210 includes a MVNO CDR storage, aggregation, mediation, feed 118, a MVNO billing interface 122, and a MVNO billing system 123 (and other network elements as shown in FIG. 1). In some embodiments, the MVNO CDR storage, aggregation, mediation, feed 118 receives, stores, aggregates and mediates micro-CDRs received from mobile devices 100 (e.g., MVNO group partitioned devices).

[00111] Those of ordinary skill in the art will appreciate that various other network architectures can be used for providing device group partitions and a settlement platform, and FIG. 1 is illustrative of just one such example network architecture for which device group partitions and settlement platform techniques described herein can be provided.

[00112] In some embodiments, CDR storage, aggregation, mediation, feed 118 (e.g., service usage 118, including a billing aggregation data store and rules engine) is a functional descriptor for, in some embodiments, a device/network level service usage information collection, aggregation, mediation, and reporting function located in one or more of the networking equipment apparatus/systems attached to one or more of the sub-networks shown in FIG. 1 (e.g., central provider access network 109 and/or central provider core network 110), which is in communication with the service controller 122 and a central billing interface 127. As shown in FIG. 1, service usage 118 provides a function in communication with the central provider core network 110. In some embodiments, the CDR storage, aggregation, mediation, feed 118 function is located elsewhere in the network or partially located in elsewhere or integrated with/as part of other network elements. In some embodiments, CDR storage, aggregation, mediation, feed 118 functionality is located or partially located in the AAA server 121 and/or the mobile wireless center/Home Location Register(HLR) 132 (as shown, in

communication with a DNS/DHCP server 126). In some embodiments, service usage 118 functionality is located or partially located in the base station, base station controller and/or base station aggregator, collectively referred to as base station 125 in FIG. 1. In some embodiments, CDR storage, aggregation, mediation, feed 118 functionality is located or partially located in a networking component in the central provider access network 109, a networking component in the core network 110, the central billing system 123, the central billing interface 127, and/or in another network component or function. This discussion on the possible locations for the network based and device based service usage information collection, aggregation, mediation, and reporting function (e.g., CDR storage, aggregation, mediation, feed 118) can be easily generalized as described herein and as shown in the other figures and embodiments described herein by one of ordinary skill in the art. Also, as shown in FIG. 1, the service controller 122 is in communication with the central billing interface 127 (e.g., sometimes referred to as the external billing management interface or billing communication interface), which is in communication with the central billing system 123. As shown in FIG. 1, an order management 180 and subscriber management 182 are also in communication with the central provider core network 110 for facilitating order and subscriber management of services for the devices 100 in accordance with some embodiments.

[00113] In some embodiments, a service processor download 170 is provided, which provides for periodical downloads/updates of service processors (e.g., service processor 115). In some embodiments, verification techniques include periodically updating, replacing, and/or updating an obfuscated version of the service processor, or performing any of these techniques in response to an indication of a potential compromise or tampering of any service processor functionality (e.g., QoS functionality and/or network capacity controlled services functionality) executed on or implemented on the device 100.

[00114] In some embodiments, the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements) provides a device/network level service usage information collection, aggregation, mediation, and reporting function. In some embodiments, the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements) collects device generated/assisted service usage information (e.g., micro-CDRs) for one or more devices on the wireless network (e.g., devices 100); and provides the device generated service usage information in a syntax and a

communication protocol that can be used by the wireless network to augment or replace network generated usage information for the one or more devices on the wireless network. In some embodiments, the syntax is a charging data record (CDR), and the communication protocol is selected from one or more of the following: 3GPP, 3GPP2, or other communication protocols. In some embodiments, as described herein, the CDR storage, aggregation, mediation, feed 118 collects/receives micro-CDRs for one or more devices on the wireless network (e.g., devices 100). In some embodiments, the CDR storage, aggregation, mediation, feed 118 (e.g., or other network elements and/or various combinations of network elements) includes a service usage data store (e.g., a billing aggregator) and a rules engine for aggregating the collected device generated service usage information. In some embodiments, the network device is a CDR feed aggregator, and the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements) also aggregates (network based) CDRs and/or micro-CDRs for the one or more devices on the wireless network; applies a set of rules to the aggregated CDRs and/or micro-CDRs using a rules engine (e.g., bill by account, transactional billing, revenue sharing model, and/or any other billing or other rules for service usage information collection, aggregation, mediation, and reporting), and communicates a new set of CDRs for the one or more devices on the wireless network to a billing interface or a billing system (e.g., providing a CDR with a billing offset by account/service). In some embodiments, a revenue sharing platform is provided using various techniques described herein. In some embodiments, QoS usage accounting/charging and/or network capacity controlled services usage accounting/charging is provided using various techniques described herein.

[00115] In some embodiments, the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements) communicates a new set of CDRs (e.g., aggregated and mediated CDRs and/or micro-CDRs that are then translated into standard CDRs for a given wireless network) for the one or more devices on the wireless network to a billing interface (e.g., central billing interface 127) or a billing system (e.g., central billing system 123). In some embodiments, the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements) communicates with a service controller (e.g., service controller 122) to collect the device generated service usage information (e.g., micro-CDRs) for the one or more devices on the wireless network. In some embodiments, the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or

combinations of network elements) communicates with a service controller, in which the service controller is in communication with a billing interface or a billing system. In some embodiments, the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements) communicates the device generated service usage information to a billing interface or a billing system. In some embodiments, the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements) communicates with a transport gateway and/or a Radio Access Network (RAN) gateway to collect the network generated/based service usage information for the one or more devices on the wireless network. In some embodiments, the service controller 122 communicates the device assisted service usage information (e.g., micro-CDRs) to the CDR storage, aggregation, mediation, feed 118 (e.g., or other network elements and/or various combinations of network elements).

[00116] In some embodiments, the CDR storage, aggregation, mediation, feed 118 (e.g., or other network elements and/or various combinations of network elements) performs rules for performing a bill by account aggregation and mediation function. In some embodiments, the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements) performs rules for performing a service billing function, as described herein, and/or for performing a service/transactional revenue sharing function, as described herein. In some embodiments, the service controller 122 in communication with the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements) performs a rules engine for aggregating and mediating the device assisted service usage information (e.g., micro-CDRs). In some embodiments, a rules engine device in communication with the CDR storage, aggregation, mediation, feed 118 (e.g., or other network elements and/or various combinations of network elements) performs a rules engine for aggregating and mediating the device assisted service usage information (e.g., QOS service usage information and/or network capacity controlled services usage information).

[00117] In some embodiments, the rules engine is included in (e.g., integrated with/part of) the CDR storage, aggregation, mediation, feed 118. In some embodiments, the rules engine and associated functions, as described herein, is a separate function/device. In some embodiments, the service controller 122 performs some or all of these rules engine based functions, as described herein, and communicates with the central billing interface 127. In some

embodiments, the service controller 122 performs some or all of these rules engine based functions, as described herein, and communicates with the central billing system 123.

[00118] In some embodiments, a settlement platform service is provided. For example, micro-CDRs can be aggregated and mediated to associate service usage for one or more services used by a communications device (e.g., a user of the communications device). A rules engine or another function can determine a revenue share allocation for the service usage for a particular service to determine the settlement for such service usage for the revenue sharing allocation/model and to distribute accounting and settlement information to one or more of carriers, distribution partners, MVNOs, wholesale partners, and/or other partners or entities. In some embodiments, the service is a transactional service.

[00119] In some embodiments, duplicate CDRs are sent from the network equipment to the billing system 123 that is used for generating service billing. In some embodiments, duplicate CDRs are filtered to send only those CDRs/records for devices controlled by the service controller and/or service processor (e.g., managed devices). For example, this approach can provide for the same level of reporting, lower level of reporting, and/or higher level of reporting as compared to the reporting required by the central billing system 123.

[00120] In some embodiments, a bill-by-account billing offset is provided. For example, bill-by-account billing offset information can be informed to the central billing system 123 by providing a CDR aggregator feed that aggregates the device assisted service usage data feed to provide a new set of CDRs for the managed devices to the central billing interface 127 and/or the central billing system 123. In some embodiments, transaction billing is provided using similar techniques. For example, transaction billing log information can be provided to the central billing interface 127 and/or the central billing system 123.

[00121] In some embodiments, the rules engine (e.g., performed by the service usage 118 or another network element, as described herein) provides a bill-by-account billing offset. For example, device assisted service usage information (e.g., micro-CDRs) includes a transaction type field or transaction code (e.g., indicating a type of service for the associated service usage information). For example, the rules engine can apply a rule or a set of rules based on the identified service associated with the device generated service usage information to determine a bill-by-account billing offset (e.g., a new CDR can be generated to provide the determined bill-

by-account billing offset). In some examples, the determined bill-by-account billing offset can be provided as a credit to the user's service usage account (e.g., a new CDR can be generated with a negative offset for the user's service usage account, such as for network chatter service usage, or transactional service usage, or for any other purposes based on one or more rules performed by the rules engine).

[00122] As another example, for a transactional service, a first new CDR can be generated with a negative offset for the user's service usage account for that transactional service related usage, and a second new CDR can be generated with a positive service usage value to charge that same service usage to the transactional service provider (e.g., Amazon, eBay, or another transactional service provider). In some embodiments, the service controller 122 generates these two new CDRs, and the service usage 118 stores, aggregates, and communicates these two new CDRs to the central billing interface 127. In some embodiments, the service controller 122 generates these two new CDRs, and the service usage 118 stores, aggregates, and communicates these two new CDRs to the central billing interface 127, in which the central billing interface 127 applies rules (e.g., performs the rules engine for determining the bill-by-account billing offset).

[00123] In some embodiments, the service controller 122 sends the device generated CDRs to the rules engine (e.g., a service usage data store and rules engine, such as CDR storage, aggregation, mediation, feed 118), and the rules engine applies one or more rules, such as those described herein and/or any other billing/service usage related rules as would be apparent to one of ordinary skill in the art. In some embodiments, the service controller 122 generates CDRs similar to other network elements, and the rules (e.g., bill-by-account) are performed in the central billing interface 127. For example, for the service controller 122 to generate CDRs similar to other network elements, in some embodiments, the service controller 122 is provisioned on the wireless network (e.g., by network provision system 160) and behaves substantially similar to other CDR generators on the network).

[00124] In some embodiments, the service controller 122 is provisioned as a new type of networking function that is recognized as a valid, authorized, and secure source for CDRs by the other necessary elements in the network (e.g., CDR storage, aggregation, mediation, feed 118). In some embodiments, if the necessary network apparatus only recognize CDRs from certain

types of networking equipment (e.g., a RAN gateway or transport gateway), then the service controller 122 provides authentication credentials to the other networking equipment that indicate that it is one of the approved types of equipment for providing CDRs. In some embodiments, the link between the service controller 122 and the necessary CDR aggregation and mediation equipment is secured, authenticated, encrypted, and/or signed.

[00125] In some embodiments, the CDR storage, aggregation, mediation, feed 118 discards the network based service usage information (e.g., network based CDRs) received from one or more network elements. In these embodiments, the service controller 122 provides the device assisted service usage information (e.g., device based CDRs or micro-CDRs) to the CDR storage, aggregation, mediation, feed 118 (e.g., the CDR storage, aggregation, mediation, feed 118 can just provide a store, aggregate, and communication function(s), as it is not required to mediate network based CDRs and device assisted CDRs), and the device based service usage information is provided to the central billing interface 127 or the central billing system 123.

[00126] In some embodiments, the device based CDRs (e.g., micro-CDRs) and/or new CDRs generated based on execution of a rules engine as described herein are provided only for devices that are managed and/or based on device group, service plan, or any other criteria, categorization, and/or grouping, such as based on ambient service or ambient service provider or transactional service or transactional service provider.

[00127] In some embodiments, QoS for DAS includes a service processor (e.g., any device assisted element/function) that facilitates coordination for and/or provisions wireless access/radio access bearers (e.g., RABs). In some embodiments, the service processor determines whether a request for QoS is authorized (e.g., according to QoS service level, user standing, available local network capacity (e.g., as reported by other device(s) and/or network)). In some embodiments, device QoS capacity demand reports provide and/or augment network capacity demand reports.

[00128] In some embodiments, QoS for DAS includes a service controller (e.g., any network device based service control element/function) that facilitates coordination for and/or provisions wireless access/radio access bearers (e.g., RABs) on a device (e.g., a communications device, such as a mobile wireless communications device and/or an intermediate networking device), on network, and/or on device plus network. In some embodiments, the service

controller provides device QoS capacity demand reports to other network equipment/elements/functions, and then also provisions the RAB channel based on various criteria and determinations.

[00129] In some embodiments, QoS for DAS provides for device assisted monitoring, information, and/or functionality to facilitate QoS without and/or to assist network based monitoring, information, and/or functionality (e.g., Deep Packet Inspection (DPI) and/or provides such monitoring, information, and/or functionality that may not be available via network based monitoring, information, and/or functionality (e.g., encrypted activities on the device may not be accessible by DPI or other network based techniques). For example, QoS for DAS can assist in the QoS setup to facilitate the QoS setup and provide such information that may not otherwise be available using network based only techniques. For example, device assisted activity and/or service monitoring techniques can assist in classifying the QoS for the monitored activity and/or service using, for example, a QoS activity map (e.g., as described herein or other similar techniques). For example, using such device assisted techniques eliminates and/or minimizes DPI or other network based techniques that can give rise to privacy concerns/issues, network neutrality concerns/issues, and/or otherwise may not be able to provide similar or equivalent granular service/activity monitoring, as discussed above, and/or also off loads such processing from the network (e.g., network elements/devices/functionality) to the communications devices (e.g., at least for such communications devices that can perform such functions, based on their processing and/or memory capabilities, as would be apparent to one of ordinary skill in the art). In some embodiments, QoS for DAS includes the service provider for providing an initial authorization/clearance for a QoS request (e.g., using various techniques described herein), and the service controller determines if the QoS request should be authorized (e.g., based on various QoS authorization/clearance/approval criteria (e.g., QoS activity maps and/or QoS request rule) and/or network capacity, as described herein). In some embodiments, QoS for DAS includes the service provider for providing a QoS request including a QoS class to the service controller, and the service controller determines if the QoS request should be authorized, as described herein. In some embodiments, DAS for protecting network capacity provides for device assisted monitoring, information, and/or functionality to facilitate protecting network capacity without and/or to assist network based monitoring, information, and/or functionality (e.g., Deep Packet Inspection (DPI) and/or provides such monitoring, information,

and/or functionality that may not be available via network based monitoring, information, and/or functionality (e.g., encrypted activities on the device may not be accessible by DPI or other network based techniques). In some embodiments, DAS for protecting network capacity provides for device assisted monitoring, information, and/or functionality to facilitate protecting network capacity without solely relying upon DPI and/or without any use or any significant use of DPI wireless network, which conserves network resources and network capacity by controlling device network access behavior at the device instead of deep in the core network at a DPI gateway (e.g., DPI based techniques consume over the air wireless network capacity even if chatty device behavior is blocked at a DPI gateway; in contrast, DAS for protecting network capacity techniques that do not use DPI based techniques for controlling device service usage can, for example, provide a device based usage notification and service selection UI that does not consume over the air wireless network capacity).

[00130] In some embodiments, QoS for DAS and/or DAS for protecting network capacity includes providing or facilitating reports for base station (BTS) for network capacity (e.g., sector, channel, busy state information or network capacity usage/availability, and/or network capacity expected demand) based on, for example, one or more of the following: monitored application usage on the communications device, monitored user activity on the communications device, location of the communications, other available networks, and/or other monitored or determined activity, service usage measure, and/or metric. In some embodiments, at or after execution of an application that is determined to require network service usage (e.g., may require increased wireless network bandwidth, such as based on a service usage activity map), QoS for DAS sends information to the network (e.g., a network controller or other network device element/function) that capacity demand is forthcoming for the communications device (e.g., potentially initiating a provisioning of a QoS radio access bearer (RAB) or other type of RAB).

[00131] In some embodiments, network capacity (e.g., busy state information) is collected from one or more communications devices in communication with a wireless network (e.g., network capacity/usage information measured from each respective communications device's perspective is determined and stored by the service processor on each respective communications device) and reported to the service controller, and the service controller (e.g., or another network element/function) uses this information to determine what resources are available for allocation to various levels of QoS (e.g., to respond to/facilitate various QoS requests) and/or to workload

balance across multiple base stations and/or networks (e.g., wired networks, cellular, Wi-Fi, and/or other wireless networks).

[00132] In some embodiments, the service processor executed on the communications device sends a QoS request (e.g., a wireless network bearer channel reservation request or Radio Access Bearer (RAB) request) to the service controller. The service controller verifies the request using various verification techniques as described herein. In some embodiments, the service controller facilitates coordination of various device QoS requests with one or more base stations (BTSs) in communication with the communications device to provide for the requested QoS reservation to facilitate the new QoS session. In some embodiments, the service controller provides a QoS routing function by, for example, providing various QoS routing instructions to a device service processor (e.g., aggregating, prioritizing, queuing, authorizing, allocating reservations/RABs, denying, re-routing (such as to other BTSs and/or other networks) and/or otherwise managing QoS requests), in which the BTS may or may not be QoS aware. For example, QoS priority can be based on activity (e.g., service usage and/or application), service level, user standing, network capacity, time of day, and/or QoS priority can be purchased on a transaction basis, a session basis, a pre-pay basis or a plan basis. As another example, QoS priority can also vary by device type, user within a group, group, application type, content type, or any other criteria or measure and/or any combination thereof. In some embodiments, the service controller also facilitates coordination of various device QoS requests with other network elements/functions for QoS implementation and management to provide for an end to end QoS solution.

[00133] In some embodiments, QoS can be symmetric for two mobile devices or asymmetric. In some embodiments, QoS resource availability can be from communications devices, BTS(s), other network functions (e.g., service control, service controller and/or any other network elements/functions) or any combination thereof. In some embodiments, the service controller provides QoS demand information to another network element/function. In some embodiments, the service controller provides the central aggregator and policy decision point (PDP). In some embodiments, the service controller controls (e.g., at least in part) QoS related functions for communications devices, BTS(s), and/or a combination of both.

[00134] In some embodiments, charging (e.g., monitoring and/or determining associating charging or billing) for QoS service usage/transactions and/or network capacity controlled services usage/transactions is determined using various techniques described herein. For example, the service processor can assist in charging for QoS and/or network capacity controlled activities. In some embodiments, the service processor uses device assisted Charging Data Records (CDRs) or micro-CDRs to assist in charging for QoS and/or network capacity controlled activities (e.g., using QoS class related transaction codes and/or network capacity controlled related transaction codes), as described herein with respect to various embodiments. In some embodiments, charging for QoS and/or network capacity controlled services is performed in whole or in part by one or more network elements/functions (e.g., service controller, SGSN/GGSN/other gateways, and/or billing interfaces/servers).

[00135] In some embodiments, service usage information includes network based service usage information. In some embodiments, the network based service usage information includes network based CDRs. In some embodiments, service usage information includes device based service usage information. In some embodiments, device based service usage information includes device assisted CDRs, also referred to herein as micro-CDRs, as described herein. In some embodiments, micro-CDRs are used for CDR mediation or reconciliation that provides for service usage accounting on any device activity that is desired (e.g., providing granular service usage information, such as based on application layer service usage monitoring, transaction service usage monitoring, QoS activities/sessions/transactions, network capacity controlled activities/sessions/transactions, and/or other types of service usage information). In some embodiments, each device includes a service processor (e.g., a service processor executed on a processor of a communications device, such as a mobile device or an intermediate networking device that can communicate with a wireless network).

[00136] In some embodiments, each device activity that is desired to be associated with a billing event (e.g., for a QoS related billing event) is assigned a micro-CDR transaction code, and the service processor is programmed to account for that activity associated with that transaction code (e.g., various transaction codes can be associated with service usage associated with certain services, applications, and/or based on QoS classes or priorities, respectively, which can be used for providing granular service usage for these various Internet/network based services/sites/transactions and/or any other Internet/network based services/sites, which can

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

[00137] In some embodiments, CDR mediation is used to properly account for the micro-CDR service usage information by depositing it into an appropriate service usage account and deducting it from the user device bulk service usage account. For example, this technique provides for a flexible service usage billing solution that uses pre-existing solutions for CDR mediation and billing. For example, the billing system can process the mediated CDR feed from CDR mediation, apply the appropriate account billing codes to the aggregated micro-CDR information that was generated by the device, and then generate billing events in a manner that does not require changes to existing billing systems, infrastructures, and techniques (e.g., using new transaction codes to label the new device assisted billing capabilities).

[00138] In some embodiments, the various QoS techniques performed on or by the communications device (e.g., using a service processor to provide or assist in providing QoS session provisioning, QoS policy management, QoS policy enforcement, and/or QoS accounting/charging, such as QoS charging records and reports) are verified (e.g., using various verification techniques described herein). In some embodiments, the various network capacity controlled services techniques performed on or by the communications device (e.g., using a service processor to provide or assist in providing network capacity controlled services policy management, network capacity controlled services policy enforcement, and/or network capacity controlled services charging, such as network capacity controlled services charging records and reports) are verified (e.g., using various verification techniques described herein).

[00139] For example, a QoS request, QoS related policy rules (e.g., QoS activity map, QoS related service plan and/or service policy settings) and implementation, QoS policy enforcement, and QoS charging are verified (e.g., periodically, per transaction, and/or based on some other criteria/metric). In some embodiments, verification techniques include one or more of the following: compare a network based service usage measure with a first service policy associated with the communications device, compare a device assisted service usage measure with the first service policy, compare the network based service usage measure to the device assisted service usage measure, perform a test and confirm a device assisted service usage measure based on the test, perform a User Interface (UI) notification (e.g., which can include a user authentication, password, question/answer challenge, and/or other authentication technique), and/or other similar verification techniques as will now be apparent to one of ordinary skill in the art. Accordingly, in some embodiments, QoS for DAS “closes the loop” for verification of various QoS related techniques, such as QoS requests, QoS grants, QoS usage, and/or QoS charging. In some embodiments, the service processor and the service controller serve as a verifiable QoS management/coordination system for other QoS elements/functions in network. In some embodiments, if such or other verification techniques determine or assist in determining that a QoS request, QoS report, and/or QoS policy behavior (e.g., or similarly, network capacity controlled services monitoring, reporting, and/or policy behavior) does not match expected requests, reports, and/or policy, then responsive actions can be performed, for example, the communications device (e.g., and/or suspect services) can be suspended, quarantined, killed/terminated, and/or flagged for further analysis/scrutiny to determine whether the device is malfunctioning, needs updating, has been tampered with or compromised, is infected with malware, and/or if any other problem exists.

[00140] In some embodiments, the communications device (e.g., the service processor) maintains a QoS flow table that associates or maps device activity to QoS level/class to RAB/QoS channel, and in some embodiments, the communications device also informs a QoS management network function/element of the relative priority of the QoS flows for the communications device (e.g., based on or using the QoS flow table). In some embodiments, the service controller receives or collects information from the communications device and maintains such a QoS flow table for the communications device and, in some embodiments, the service controller also informs a QoS management network function/element of the relative

priority of the QoS flows for the communications device (e.g., based on or using the QoS flow table). In some embodiments, flows can be assigned to activities originating at the communications device in a transparent way, or simply by activity class or user preference, or using other techniques.

[00141] In some embodiments, the communications device maintains a table of QoS billing rates, scheduled transmission times, and/or other QoS related information to implement an overlay MAC at the data networking level to manage QoS on legacy networks that are not QoS MAC enabled and/or do not have the various functionality to support QoS controls (e.g., and such techniques can also be used to provide for QoS functionality across different networks). In some embodiments, QoS related policies are exchanged between roaming and home service controllers to facilitate QoS support while roaming on a non-home network(s).

[00142] In some embodiments, the communications device serves as a network capacity indicator (e.g., collecting network capacity information for a local cell and communicating or reporting that network capacity information to the service controller). For example, permanent local cell communications devices can be placed in local cell areas to augment legacy equipment for such network capacity indicator/reporting functions. Various other techniques for determining network capacity and/or network availability are described herein.

[00143] In some embodiments, service partners and/or service providers can subsidize in whole or in part to upgrade a given user or group of users to better QoS related service level agreement (SLA)/class for a preferred destination. In some embodiments, based on monitored service usage and/or other monitored behavior of the communications device, such subsidized QoS upgrade/offers can be presented to a user of the communications device (e.g., as an incentive/reward for desired or preferred user behavior or for other reasons). Similarly, in some embodiments, these techniques are also applied to network capacity controlled services.

[00144] In some embodiments, QoS charging is based on QoS channel/reservation, service flow, or RAB charging (e.g., single flow per RAB, multi-flow per RAB, multi-RAB per flow). In some embodiments, charging (e.g., for QoS and/or for network capacity controlled services) is based on one or more of the following: network busy state, time criteria, user service class request, traffic volume and class, time and class, network capacity (e.g., network busy state) and class, time of day and class, location, traffic type, application type, application class, destination,

destination type, partner service, and/or other criteria/measures. In some embodiments, QoS charging is verified using the various verification techniques described herein (e.g., test charging events). In some embodiments, network capacity controlled services charging is verified using the various verification techniques described herein (e.g., test charging events). In some embodiments, QoS charging is by data usage (e.g., by Megabyte (MB)), service flow by time by QoS class, speed by time, network busy state, time of day/day of week, service plan, current network, and/or other criteria/measures. In some embodiments, network capacity controlled services charging is by data usage (e.g., by Megabyte (MB)), service flow by time by network capacity controlled services class, speed by time, network busy state, time of day/day of week, service plan, current network, and/or other criteria/measures.

[00145] In some embodiments, QoS for DAS includes coordinating functions with one or more of the following: DAS elements/functions, Radio Access Network (RAN), Transport network, Core network, GRX network, IPX network, and/or other networks/elements/functions.

[00146] FIG. 2 illustrates another functional diagram of another network architecture for providing quality of service (QoS) for device assisted services (DAS) and/or for providing DAS for protecting network capacity in accordance with some embodiments. In some embodiments, QoS for DAS techniques described herein are implemented using the network architecture shown in FIG. 2. In some embodiments, DAS for protecting network capacity techniques described herein are implemented using the network architecture shown in FIG. 2.

[00147] As shown, FIG. 2 includes various devices 100 including service processors 115. For example, devices 100 can include various types of mobile devices, such as phones, PDAs, computing devices, laptops, net books, tablets, cameras, music/media players, GPS devices, networked appliances, and any other networked device; and/or devices 100 can include various types of intermediate networking devices, as described herein. The devices 100 are in communication with service control 210 and central provider access and core networks 220. Service policies and accounting functions 230 are also provided in communication with the central provider access and core networks 220. For example, devices 100 can communicate via the central provider access and core networks 220 to the Internet 120 for access to various Internet sites/services 240 (e.g., Google sites/services, Yahoo sites/services, Blackberry services,

Apple iTunes and AppStore, Amazon.com, FaceBook, and/or any other Internet service or other network facilitated service).

[00148] In some embodiments, FIG. 2 provides a wireless network architecture that supports various DAS for protecting network capacity techniques as described herein. Those of ordinary skill in the art will appreciate that various other network architectures can be used for providing various DAS for protecting network capacity techniques as described herein, and FIG. 2 is illustrative of just another such example network architecture for which DAS for protecting network capacity techniques as described herein can be provided.

[00149] FIG. 3 illustrates another functional diagram of an architecture 300 including a device based service processor 115 and a service controller 122 for providing quality of service (QoS) for device assisted services (DAS) and/or for providing DAS for protecting network capacity in accordance with some embodiments. In some embodiments, QoS for DAS techniques described herein are implemented using the functions/elements shown in FIG. 3. In some embodiments, DAS for protecting network capacity techniques described herein are implemented using the functions/elements shown in FIG. 3.

[00150] For example, the architecture 300 provides a relatively full featured device based service processor implementation and service controller implementation. As shown, this corresponds to a networking configuration in which the service controller 122 is connected to the Internet 120 and not directly to the access network 1610. As shown, a data plane (e.g., service traffic plane) communication path is shown in solid line connections and control plane (e.g., service control plane) communication path is shown in dashed line connections. As will be apparent to one of ordinary skill in the art, the division in functionality between one device agent and another is based on, for example, design choices, networking environments, devices and/or services/applications, and various different combinations can be used in various different implementations. For example, the functional lines can be re-drawn in any way that the product designers see fit. As shown, this includes certain divisions and functional breakouts for device agents as an illustrative implementation, although other, potentially more complex, embodiments can include different divisions and functional breakouts for device agent functionality specifications, for example, in order to manage development specification and testing complexity and workflow. In addition, the placement of the agents that operate, interact with or monitor the

data path can be moved or re-ordered in various embodiments. For example, the functional elements shown in FIG. 3 are described below with respect to, for example, FIGS. 4, 12, and 13 as well as FIGS. 5 through 11 (e.g., QoS for DAS related embodiments) and FIGS. 14 through 23 (e.g., DAS for protecting network capacity related embodiments).

[00151] As shown in FIG. 3, service processor 115 includes a service control device link 1691. For example, as device based service control techniques involving supervision across a network become more sophisticated, it becomes increasingly important to have an efficient and flexible control plane communication link between the device agents and the network elements communicating with, controlling, monitoring, or verifying service policy. In some embodiments, the service control device link 1691 provides the device side of a system for transmission and reception of service agent to/from network element functions. In some embodiments, the traffic efficiency of this link is enhanced by buffering and framing multiple agent messages in the transmissions. In some embodiments, the traffic efficiency is further improved by controlling the transmission frequency or linking the transmission frequency to the rate of service usage or traffic usage. In some embodiments, one or more levels of security or encryption are used to make the link robust to discovery, eavesdropping or compromise. In some embodiments, the service control device link 1691 also provides the communications link and heartbeat timing for the agent heartbeat function. As discussed below, various embodiments disclosed herein for the service control device link 1691 provide an efficient and secure solution for transmitting and receiving service policy implementation, control, monitoring and verification information with other network elements.

[00152] As shown in FIG. 3, the service controller 122 includes a service control server link 1638. In some embodiments, device based service control techniques involving supervision across a network (e.g., on the control plane) are more sophisticated, and for such it is increasingly important to have an efficient and flexible control plane communication link between the device agents (e.g., of the service processor 115) and the network elements (e.g., of the service controller 122) communicating with, controlling, monitoring, or verifying service policy. For example, the communication link between the service control server link 1638 of service controller 122 and the service control device link 1691 of the service processor 115 can provide an efficient and flexible control plane communication link, a service control link 1653 as shown in FIG. 3, and, in some embodiments, this control plane communication link provides for

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

[00153] In some embodiments, the service control server link 1638 provides for securing, signing, encrypting and/or otherwise protecting the communications before sending such communications over the service control link 1653. For example, the service control server link 1638 can send to the transport layer or directly to the link layer for transmission. In another example, the service control server link 1638 further secures the communications with transport layer encryption, such as TCP TLS or another secure transport layer protocol. As another example, the service control server link 1638 can encrypt at the link layer, such as using IPSEC, various possible VPN services, other forms of IP layer encryption and/or another link layer encryption technique.

[00154] As shown in FIG. 3, the service controller 122 includes an access control integrity server 1654 (e.g., service policy security server). In some embodiments, the access control integrity server 1654 collects device information on service policy, service usage, agent configuration, and/or agent behavior. For example, the access control integrity server 1654 can cross check this information to identify integrity breaches in the service policy implementation and control system. In another example, the access control integrity server 1654 can initiate action when a service policy violation (e.g., QoS policy violation and/or a network capacity controlled services policy violation) or a system integrity breach is suspected.

[00155] In some embodiments, the access control integrity server 1654 (and/or some other agent of service controller 122) acts on access control integrity agent 1694 (e.g., service policy security agent) reports and error conditions. Many of the access control integrity agent 1654 checks can be accomplished by the server. For example, the access control integrity agent 1654 checks include one or more of the following: service usage measure against usage range consistent with policies (e.g., usage measure from the network and/or from the device); configuration of agents; operation of the agents; and/or dynamic agent download.

[00156] In some embodiments, the access control integrity server 1654 (and/or some other agent of service controller 122) verifies device service policy implementations by comparing various service usage measures (e.g., based on network monitored information, such as by using IPDRs or CDRs, and/or local service usage monitoring information) against expected service usage behavior given the policies that are intended to be in place (e.g., a QoS policy and/or a network capacity controlled services policy). For example, device service policy implementations can include measuring total QoS data passed, QoS data passed in a period of time, IP addresses, data per IP address, and/or other measures such as location, downloads, email accessed, URLs, and comparing such measures expected service usage behavior given the policies that are intended to be in place.

[00157] In some embodiments, the access control integrity server 1654 (e.g., and/or some other agent of service controller 122) verifies device service policy, and the verification error conditions that can indicate a mismatch in QoS service measure and QoS service policy include one or more of the following: unauthorized network access (e.g., access beyond ambient service policy limits); unauthorized network speed (e.g., average speed beyond service policy limit); network data amount does not match QoS policy limit (e.g., device not stop at limit without re-up/revising service policy); unauthorized network address; unauthorized service usage (e.g., VOIP, email, and/or web browsing); unauthorized application usage (e.g., email, VOIP, email, and/or web); service usage rate too high for plan, and policy controller not controlling/throttling it down; and/or any other mismatch in service measure and service policy. Accordingly, in some embodiments, the access control integrity server 1654 (and/or some other agent of service controller 122) provides a policy/service control integrity service to continually (e.g., periodically and/or based on trigger events) verify that the service control of the device has not

been compromised and/or is not behaving out of policy (e.g., a QoS policy and/or a network capacity controlled services policy).

[00158] As shown in FIG. 3, service controller 122 includes a service history server 1650 (e.g., charging server). In some embodiments, the service history server 1650 collects and records service usage or service activity reports from the Access Network AAA Server 1621 and the Service Monitor Agent 1696. For example, although service usage history from the network elements can in certain embodiments be less detailed than service history from the device, the service history from the network can provide a valuable source for verification of device service policy implementation, because, for example, it is extremely difficult for a device error or compromise event on the device to compromise the network based equipment and software. For example, service history reports from the device can include various service tracking information, as similarly described above. In some embodiments, the service history server 1650 provides the service history on request to other servers and/or one or more agents. In some embodiments, the service history server 1650 provides the service usage history to the device service history 1618 (e.g., CDR feed and CDR mediation). In some embodiments, for purposes of facilitating the activation tracking service functions (described below), the service history server 1650 maintains a history of which networks the device has connected to. For example, this network activity summary can include a summary of the networks accessed, activity versus time per connection, and/or traffic versus time per connection. As another example, this activity summary can further be analyzed or reported to estimate the type of service plan associated with the traffic activity for the purpose of bill sharing reconciliation.

[00159] As shown in FIG. 3, service controller 122 includes a policy management server 1652 (e.g., policy decision point (PDP) server) for managing service usage policies, such as QoS policies and/or a network capacity controlled services policies. In some embodiments, the policy management server 1652 transmits policies to the service processor 115 via the service control link 1653. In some embodiments, the policy management server 1652 manages policy settings on the device (e.g., various policy settings as described herein with respect to various embodiments) in accordance with a device service profile. In some embodiments, the policy management server 1652 sets instantaneous policies on policy implementation agents (e.g., policy implementation agent 1690). For example, the policy management server 1652 can issue policy settings, monitor service usage and, if necessary, modify policy settings. For example, in

the case of a user who prefers for the network to manage their service usage costs, or in the case of any adaptive policy management needs, the policy management server 1652 can maintain a relatively high frequency of communication with the device to collect traffic and/or service measures and issue new policy settings. In this example, device monitored service measures and any user service policy preference changes are reported, periodically and/or based on various triggers/events/requests, to the policy management server 1652. In this example, user privacy settings generally require secure communication with the network (e.g., a secure service control link 1653), such as with the policy management server 1652, to ensure that various aspects of user privacy are properly maintained during such configuration requests/policy settings transmitted over the network. For example, information can be compartmentalized to service policy management and not communicated to other databases used for CRM for maintaining user privacy.

[00160] In some embodiments, the policy management server 1652 provides adaptive policy management on the device. For example, the policy management server 1652 can issue policy settings and objectives and rely on the device based policy management (e.g., service processor 115) for some or all of the policy adaptation. This approach can require less interaction with the device thereby reducing network chatter on the service control link 1653 for purposes of device policy management (e.g., network chatter is reduced relative to various server/network based policy management approaches described above). This approach can also provide robust user privacy embodiments by allowing the user to configure the device policy for user privacy preferences/settings so that, for example, sensitive information (e.g., geo-location data, website history, and/or other sensitive information) is not communicated to the network without the user's approval. In some embodiments, the policy management server 1652 adjusts service policy based on time of day. In some embodiments, the policy management server 1652 receives, requests, and/or otherwise obtains a measure of network availability/capacity and adjusts traffic shaping policy and/or other policy settings based on available network availability/capacity (e.g., a network busy state).

[00161] As shown in FIG. 3, service controller 122 includes a network traffic analysis server 1656. In some embodiments, the network traffic analysis server 1656 collects/receives service usage history for devices and/or groups of devices and analyzes the service usage. In some embodiments, the network traffic analysis server 1656 presents service usage statistics in

various formats to identify improvements in network service quality and/or service profitability. In some embodiments, the network traffic analysis server 1656 estimates the service quality and/or service usage for the network under variable settings on potential service policies. In some embodiments, the network traffic analysis server 1656 identifies actual or potential service behaviors by one or more devices that are causing problems for overall network service quality or service cost. In some embodiments, the network traffic analysis server 1656 estimates the network availability/capacity for the network under variable settings on potential service policies. In some embodiments, the network traffic analysis server 1656 identifies actual or potential service behaviors by one or more devices that are impacting and/or causing problems for overall network availability/capacity.

[00162] As shown in FIG. 3, Service Analysis, Test & Download 122B includes a beta test server 1658 (e.g., policy creation point and beta test server). In some embodiments, the beta test server 1658 publishes candidate service plan policy settings to one or more devices. In some embodiments, the beta test server 1658 provides summary reports of network service usage or user feedback information for one or more candidate service plan policy settings. In some embodiments, the beta test server 1658 provides a mechanism to compare the beta test results for different candidate service plan policy settings or select the optimum candidates for further policy settings optimization, such as for protecting network capacity.

[00163] As shown in FIG. 3, service controller 122 includes a service download control server 1660 (e.g., a service software download control server). In some embodiments, the service download control server 1660 provides a download function to install and/or update service software elements (e.g., the service processor 115 and/or agents/components of the service processor 115) on the device, as described herein.

[00164] As shown in FIG. 3 service controller 122 includes a billing event server 1662 (e.g., micro-CDR server). In some embodiments, the billing event server 1662 collects billing events, provides service plan information to the service processor 115, provides service usage updates to the service processor 115, serves as interface between device and central billing server 1619, and/or provides trusted third party function for certain ecommerce billing transactions.

[00165] As shown in FIG. 3, the Access Network HLR AAA server 1621 is in network communication with the access network 1610. In some embodiments, the Access Network AAA

server 1621 provides the necessary access network AAA services (e.g., access control and authorization functions for the device access layer) to allow the devices onto the central provider access network and the service provider network. In some embodiments, another layer of access control is required for the device to gain access to other networks, such as the Internet, a corporate network and/or a machine to machine network. This additional layer of access control can be implemented, for example, by the service processor 115 on the device. In some embodiments, the Access Network AAA server 1621 also provides the ability to suspend service for a device and resume service for a device based on communications received from the service controller 122. In some embodiments, the Access Network AAA server 1621 also provides the ability to direct routing for device traffic to a quarantine network or to restrict or limit network access when a device quarantine condition is invoked. In some embodiments, the Access Network AAA server 1621 also records and reports device network service usage (e.g., device network service usage can be reported to the device service history 1618).

[00166] As shown in FIG. 3, the device service history 1618 is in network communication with the access network 1610. In some embodiments, the device service history 1618 provides service usage data records used for various purposes in various embodiments. In some embodiments, the device service history 1618 is used to assist in verifying service policy implementation. In some embodiments, the device service history 1618 is used to verify service monitoring. In some embodiments, the device service history 1618 is used to verify billing records and/or billing policy implementation (e.g., to verify service usage charging). In some embodiments, the device service history 1618 is used to synchronize and/or verify the local service usage counter (e.g., to verify service usage accounting).

[00167] As shown in FIG. 3, the central billing 1619 (e.g., central provider billing server) is in network communication with the access network 1610. In some embodiments, the central provider billing server 1619 provides a mediation function for central provider billing events. For example, the central provider billing server 1619 can accept service plan changes. In some embodiments, the central provider billing server 1619 provides updates on device service usage, service plan limits and/or service policies. In some embodiments, the central provider billing server 1619 collects billing events, formulates bills, bills service users, provides certain billing event data and service plan information to the service controller 122 and/or device 100.

[00168] As shown in FIG. 3, in some embodiments, modem selection and control 1811 (e.g., in communication with connection manager 1804 as shown) selects the access network connection and is in communication with the modem firewall 1655, and modem drivers 1831, 1815, 1814, 1813, 1812 convert data traffic into modem bus traffic for one or more modems and are in communication with the modem selection and control 1811. In some embodiments, different profiles are selected based on the selected network connection (e.g., different service profiles/policies for WWAN, WLAN, WPAN, Ethernet and/or DSL network connections), which is also referred to herein as multimode profile setting. For example, service profile settings can be based on the actual access network (e.g., home DSL/cable or work network) behind the Wi-Fi not the fact that it is Wi-Fi (e.g., or any other network, such as DSL/cable, satellite, or T-1), which is viewed as different than accessing a Wi-Fi network at the coffee shop. For example, in a Wi-Fi hotspot situation in which there are a significant number of users on a DSL or T-1 backhaul, the service controller can sit in a service provider cloud or an MVNO cloud, the service controls can be provided by a VSP capability offered by the service provider or the service controller can be owned by the hotspot service provider that uses the service controller on their own without any association with an access network service provider. For example, the service processors can be controlled by the service controller to divide up the available bandwidth at the hotspot according to QoS or user sharing rules (e.g., with some users having higher differentiated priority (e.g., potentially for higher service payments) than other users). As another example, ambient services (e.g., as similarly described herein) can be provided for the hotspot for verified service processors.

[00169] In some embodiments, the service processor 115 and service controller 122 are capable of assigning multiple service profiles associated with multiple service plans that the user chooses individually or in combination as a package. For example, a device 100 starts with ambient services that include free transaction services wherein the user pays for transactions or events rather than the basic service (e.g., a news service, eReader, PND service, pay as you go session Internet) in which each service is supported with a bill by account capability to correctly account for any subsidized partner billing to provide the transaction services (e.g., Barnes and Noble may pay for the eReader service and offer a revenue share to the service provider for any book or magazine transactions purchased from the device 100). In some embodiments, the bill by account service can also track the transactions and, in some embodiments, advertisements for

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

[00170] As shown in FIG. 3, an agent communication bus 1630 represents a functional description for providing communication for the various service processor 115 agents and functions. In some embodiments, as represented in the functional diagram illustrated in FIG. 3, the architecture of the bus is generally multipoint to multipoint so that any agent can communicate with any other agent, the service controller or in some cases other components of the device, such user interface 1697 and/or modem components. As described below, the architecture can also be point to point for certain agents or communication transactions, or point to multipoint within the agent framework so that all agent communication can be concentrated, or secured, or controlled, or restricted, or logged or reported. In some embodiments, the agent communication bus is secured, signed, encrypted, hidden, partitioned, and/or otherwise protected from unauthorized monitoring or usage. In some embodiments, an application interface agent (not shown) is used to literally tag or virtually tag application layer traffic so that the policy

implementation agent(s) 1690 has the necessary information to implement selected traffic shaping solutions. In some embodiments, an application interface agent (not shown) is in communication with various applications, including a TCP application 1604, an IP application 1605, and a voice application 1602.

[00171] As shown in FIG. 3, service processor 115 includes an API and OS stack interface 1693. In some embodiments, the API and OS stack interface 1693 provides the QoS API functionality as similarly described herein with respect to various embodiments. In some embodiments, a QoS API is used to report back QoS availability to applications. In some embodiments, the API and OS stack interface 1693 provides the network capacity controlled API and/or emulated API functionality as similarly described herein with respect to various embodiments. As shown, service processor 115 also includes a router 1698 (e.g., a QoS router agent/function and/or a network capacity controlled services router agent/function) and a policy decision point (PDP) agent 1692. In some embodiments, the router 1698 provides QoS router functionality as similarly described herein with respect to various embodiments. In some embodiments, the router 1698 provides network capacity controlled services router functionality as similarly described herein with respect to various embodiments. In some embodiments, the QoS router supports multiple QoS channels (e.g., one or more provisioned/allocated QoS links forming a QoS channel between the device and the desired end point, such as an access point/BTS/gateway/network for a single ended QoS channel or other communication device for an end to end QoS channel, depending on the QoS connection/network support/availability/etc.). In some embodiments, the QoS router supports multiple QoS channels, which can each have different QoS classes/levels. In some embodiments, the QoS router routes application/service usage traffic to an appropriate QoS channel. In some embodiments, the QoS router determines the routing/mapping based on, for example, one or more of the following: a QoS API request, a QoS activity map, a user request, a service plan, a service profile, service policy settings, network capacity, service controller or other intermediate QoS network element/function/device, and/or any other criteria/measure, as similarly described herein with respect to various embodiments. In some embodiments, multiple different applications/services are routed to a particular QoS channel using various techniques described herein. In some embodiments, different applications/services are routed to different QoS channels using various techniques described herein. In some embodiments, the QoS router assists in managing and/or optimizing

QoS usage for the communications device. In some embodiments, the QoS router assists in managing and/or optimizing QoS usage across multiple communications devices (e.g., based on network capacity for a given cell area/base station or other access point). In some embodiments, PDP agent 1692 provides the PDP agent functionality as similarly described herein with respect to various embodiments. As shown, architecture 300 also includes a suspend resume interface 320, network QoS provisioning interfaces 330 (e.g., for providing the various QoS techniques described herein), and an activation/suspend resume server 340 and billing interface server 350 in the service controller 122A.

[00172] In some embodiments, device assisted services (DAS) techniques for providing an activity map for classifying or categorizing service usage activities to associate various monitored activities (e.g., by URL, by network domain, by website, by network traffic type, by application or application type, and/or any other service usage activity categorization/classification) with associated IP addresses are provided. In some embodiments, a policy control agent (not shown), service monitor agent 1696 (e.g., charging agent), or another agent or function (or combinations thereof) of the service processor 115 provides a DAS activity map. In some embodiments, a policy control agent (not shown), service monitor agent, or another agent or function (or combinations thereof) of the service processor provides an activity map for classifying or categorizing service usage activities to associate various monitored activities (e.g., by Uniform Resource Locator (URL), by network domain, by website, by network traffic type, by socket (such as by IP address, protocol, and/or port), by socket id (such as port address/number), by port number, by content type, by application or application type, and/or any other service usage activity classification/categorization) with associated IP addresses and/or other criteria/measures. In some embodiments, a policy control agent, service monitor agent, or another agent or function (or combinations thereof) of the service processor determines the associated IP addresses for monitored service usage activities using various techniques to snoop the DNS request(s) (e.g., by performing such snooping techniques on the device 100 the associated IP addresses can be determined without the need for a network request for a reverse DNS lookup). In some embodiments, a policy control agent, service monitor agent, or another agent or function (or combinations thereof) of the service processor records and reports IP addresses or includes a DNS lookup function to report IP addresses or IP addresses and associated URLs for monitored service usage activities. For example, a policy control agent,

service monitor agent, or another agent or function (or combinations thereof) of the service processor can determine the associated IP addresses for monitored service usage activities using various techniques to perform a DNS lookup function (e.g., using a local DNS cache on the monitored device 100). In some embodiments, one or more of these techniques are used to dynamically build and maintain a DAS activity map that maps, for example, URLs to IP addresses, applications to IP addresses, content types to IP addresses, and/or any other categorization/classification to IP addresses as applicable. In some embodiments, the DAS activity map is used for various DAS traffic control and/or throttling techniques as described herein with respect to various embodiments for providing QoS for DAS and/or for providing DAS for protecting network capacity. In some embodiments, the DAS activity map is used to provide the user various UI related information and notification techniques related to service usage as described herein with respect to various embodiments. In some embodiments, the DAS activity map is used to provide service usage monitoring, prediction/estimation of future service usage, service usage billing (e.g., bill by account and/or any other service usage/billing categorization techniques), DAS techniques for ambient services usage monitoring, DAS techniques for generating micro-CDRs, and/or any of the various other DAS related techniques as described herein with respect to various embodiments.

[00173] In some embodiments, all or a portion of the service processor 115 functions disclosed herein are implemented in software. In some embodiments, all or a portion of the service processor 115 functions are implemented in hardware. In some embodiments, all or substantially all of the service processor 115 functionality (e.g., as discussed herein) is implemented and stored in software that can be performed on (e.g., executed by) various components in device 100. In some embodiments, it is advantageous to store or implement certain portions or all of service processor 115 in protected or secure memory so that other undesired programs (e.g., and/or unauthorized users) have difficulty accessing the functions or software in service processor 115. In some embodiments, service processor 115, at least in part, is implemented in and/or stored on secure non-volatile memory (e.g., non volatile memory can be secure non-volatile memory) that is not accessible without pass keys and/or other security mechanisms (e.g., security credentials). In some embodiments, the ability to load at least a portion of service processor 115 software into protected non-volatile memory also requires a secure key and/or signature and/or requires that the service processor 115 software components

being loaded into non-volatile memory are also securely encrypted and appropriately signed by an authority that is trusted by a secure software downloader function, such as service downloader 1663 as shown in FIG. 3. In some embodiments, a secure software download embodiment also uses a secure non-volatile memory. Those of ordinary skill in the art will also appreciate that all memory can be on-chip, off-chip, on-board, and/or off-board.

[00174] FIGS. 4A through 4C illustrates a functional diagram for providing quality of service (QoS) for device assisted services (DAS) in accordance with some embodiments. In some embodiments, QoS for DAS techniques described herein are implemented using the network architecture shown in FIGS. 4A through 4C.

[00175] Referring to FIG. 4A, in some embodiments, QoS functionality is performed at the communications device 100 using service processor 115 as similarly described herein. For example, the service processor 115 determines whether or not a QoS request is authorized (e.g., based on the associated service plan and/or other criteria/measures). If the QoS request is authorized, then the service processor 115 communicates with the base station (BTS) 125 to send the QoS request (e.g., a RAB or multi-RAB reservation request) to the local BTS. The BTS determines whether to accept or deny the QoS request (e.g., based on network capacity, such as using a first come first service QoS/network bandwidth or best effort access policy or other techniques, and/or other criteria/measures). The BTS responds to the QoS request accordingly. If the QoS request is granted, the QoS session can be initiated as similarly described herein. In some embodiments, the service processor 115 also performs various QoS charging functions using various techniques described herein, and the service processor 115 periodically sends QoS charging records or reports to the service controller 122 (e.g., and/or another network element/function). In some embodiments, the service processor 115 and the QoS related functions performed by the service processor 115 are periodically verified using the various techniques described herein.

[00176] Referring to FIG. 4B, FIG. 4B is similar to FIG. 4A except that the service controller 122 is also shown to be in communication with the service processor 115 of the communications device 100, which can provide for the download and periodically updating of the QoS rules and/or other service plan/profile/policy information that can include QoS related information. In some embodiments, the service processor 115 also performs various QoS

charging functions using various techniques described herein, and the service processor 115 periodically sends QoS charging records or reports to the service controller 122 (e.g., and/or another network element/function). In some embodiments, the service processor 115 and the QoS related functions performed by the service processor 115 are periodically verified using the various techniques described herein.

[00177] Referring to FIG. 4C, at 410, the service processor 115 sends a QoS request to the service controller 122 (e.g., the service processor can also (at least in part) determine whether the QoS request is authorized as similarly described with respect to FIG. 4A). At 420, the service controller 122 sends the QoS request to the BTS 125 if it is determined that the QoS request is authorized using various techniques described herein and/or whether the BTS 125 has network capacity for the QoS request. For example, the service controller can provide a central policy decision point function for QoS related activities (e.g., based on QoS prioritization, network capacity, and/or other criteria/measures/policies). At 430, the service controller 122 communicates the response to the QoS request accordingly. At 440, if the QoS request was approved, the device 100 initiates the QoS session (e.g., using a RAB or multi-RAB reservation) via the BTS 125. In some embodiments, the service processor 115 also performs various QoS charging functions using various techniques described herein, and the service processor 115 periodically sends QoS charging records or reports to the service controller 122 (e.g., and/or another network element/function). In some embodiments, the service processor 115 and the QoS related functions performed by the service processor 115 are periodically verified using the various techniques described herein.

[00178] In some embodiments, QoS techniques as described herein are implemented in the device (e.g., using the service processor 115) and one or more other network elements/functions, such as the BTS 125, service controller 125, RAN, SGSN/GGSN/other gateways and/or other network elements/functions, in which various of the QoS related functions can be distributed or allocated to such network elements/functions based on various design/network architecture approaches as will now be apparent to one of ordinary skill in the art, in which QoS related activities and/or functions at the device 100 are verified using various verification techniques described herein.

[00179] In some embodiments, the device determines QoS availability by directly querying QoS link reservation equipment in the network (e.g., an access point, such as the BTS 125). In some embodiments, the device determines QoS availability based on an intermediate network function that coordinates QoS requests with one or more network QoS link resources. In some embodiments, the device requests a QoS reservation in advance of QoS link establishment with one or more QoS network link resources. In some embodiments, in response to a QoS request, a QoS channel is reported as available only if/after it is determined that the necessary one or more QoS links required to create the QoS channel are available, and, for example, the QoS channel can then be reserved based on a confirmation or automatically be reserved in response to the QoS request.

[00180] FIG. 5 illustrates a functional diagram for generating a QoS activity map for quality of service (QoS) for device assisted services (DAS) in accordance with some embodiments. In particular, FIG. 5 illustrates techniques for mapping a service plan or a set of service plan policies/rules for QoS 510 to a set of QoS activity rules 530. As shown, a set of QoS rules/QoS related device state information 510 (e.g., a set of associated service plan, service plan usage, other state such as network capacity or forecasted demand or time of day/day of week, activity usage, QoS level, and/or user preferences) is mapped using a QoS mapping function to a set of QoS activity rules 530 using various techniques described herein. At 530, activity rules (e.g., activity policy rules instructions) 530 are determined using the mapping function 520. In some embodiments, DAS for network capacity controlled services techniques can similarly be implemented using the techniques described with respect to FIG. 5 (e.g., for generating and implementing a network capacity controlled services activity map).

[00181] In some embodiments, the service plan includes a list of activity policies, and each activity policy in the service plan specifies how the activity policy is modified by rules state information. In some embodiments, each activity policy then becomes the instruction for the engine (e.g., QoS mapping function 520) that maps the activity policy to QoS activity rules 530. In some embodiments, service controller 122 downloads QoS mapping function 520, which is implemented by service processor 115.

[00182] In some embodiments, the service processor determines (e.g., and classifies) application/service usage activity demand with or without granular application/service usage

activity (e.g., depending on various user/service plan/service provider/network/legal and/or other privacy restrictions and/or any other related requirements or settings). For example, policies (e.g., service policy settings and/or service profile settings) can be downloaded to provide such application/service usage activity monitoring rules and a QoS activity map for assigning such monitored activities to various QoS classes or priorities, and, in some embodiments, such monitoring and the QoS activity map can also be implemented using various verification techniques described herein (e.g., periodically audited, tested, compared with network service usage information). In some embodiments, the QoS activity map is based on a service plan, service profile, and/or service policy settings associated with the communications device. In some embodiments, the QoS activity map is based on a device group and/or user group. In some embodiments, the QoS activity map is based on user input (e.g., a user of the communications device can identify QoS classes/service levels for various applications and/or service activities, in response to requests for user input, based on user configurations, user defined rules (e.g., to eliminate or mitigate privacy and/or net neutrality concerns/issues), and/or confirmed monitored user behavior QoS related patterns or preferences). In some embodiments, the QoS activity map includes mappings/associations based on one or more of the following: a user preference for a given destination, destination class, application, application class (e.g., by application class instead of with respect to a specific application can also eliminate or mitigate privacy and/or net neutrality concerns/issues), flow, traffic or flow class, time period, time of day, location, network busy state (e.g., provide QoS when you can, then charge more when busy, notify user of busy state), device type, user type, user plan, user group, user standing, partner service, tokens, service type, and/or other criteria or measures.

[00183] In some embodiments, various techniques described herein are managed for device 100 for incoming and/or outgoing QoS requests. In some embodiments, as shown in FIG. 6, QoS for DAS includes establishing an end to end coordinated QoS service channel control.

[00184] FIG. 6 illustrates a functional diagram for quality of service (QoS) for device assisted services for an end to end coordinated QoS service channel control in accordance with some embodiments. As shown in FIG. 6, a wireless communications device 100A includes a service processor 115A in secure communication with service controller 122A. A wireless communications device 100B includes a service processor 115B in secure communication with service controller 122B. In some embodiments, when, for example, device 100A initiates a QoS

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

[00185] FIG. 7 illustrates a flow diagram for quality of service (QoS) for device assisted services (DAS) in accordance with some embodiments. At 702, the process begins. At 704, QoS rules are received or determined (e.g., a service processor receives or requests the QoS

rules, which may be included in service plan, service profile, and/or service policy settings associated with the communications device). In some embodiments, the QoS rules are verified using various techniques as described herein (e.g., periodically updated, replaced, downloaded, obfuscated, and/or tested using by a service controller and/or using other verification techniques). In some embodiments, a QoS API is also used by various applications to initiate a QoS request, as described herein with respect to various embodiments. In some embodiments, the QoS rules are implemented in the form of a QoS activity map in accordance with various embodiments described herein. At 706, the communications device's standing for QoS is determined using various techniques described herein (e.g., based on the service plan, service profile, service policy settings, QoS rules, based on QoS class, current service usage, current billing standing, and/or any other criteria/measure). In some embodiments, in addition to verifying the device/user standing for the QoS request, whether the device is following or in compliance with an assigned QoS reservation request policy is also verified using various techniques described herein. If the device is determined to not be eligible for QoS, then at 708, the device User Interface (UI) provides information concerning the denial/ineligibility for QoS session(s) (e.g., denial/ineligibility explanation and/or options for providing for one or more QoS options, such as a service plan upgrade or payment for a certain/set of/period of time for QoS session(s) access). If the device is determined to be eligible for QoS, then at 710, QoS availability is determined (e.g., based on network capacity, which may be determined at the device, via communication with the service controller, via communication with the BTS, and/or any combination thereof, using the various techniques described herein). If QoS is determined to not be available, then at 712, the UI provides information and/or options concerning the QoS availability (e.g., unavailability explanation and/or options for providing for one or more QoS options, such as a service plan upgrade or payment for a certain/set of/period of time for QoS session(s) access). If QoS is determined to be available, then at 714, a request for network resources for the QoS session is sent to one or more network resources (e.g., service controller, BTS, gateway, core/transport network, IPX/GRX networks, and/or other network elements/functions/resources). At 716, a confirmation of the approved QoS session is received to close the loop for the QoS for DAS (e.g., a QoS schedule is received that provides the QoS session confirmation information, such as a scheduled RAB/multi-RAB and/or other reserved network resource(s) by schedule/other criteria). At 718, one or more verification techniques are

performed to verify the QoS for DAS implementation on the device using various verification techniques described herein (e.g., comparing QoS service usage reports from a network source with the associated device policy; comparing QoS service usage reports from a network source with the QoS service usage reports from the device, and/or using other verification techniques as similarly described herein). At 720, the process is completed.

[00186] FIGS. 8A through 8C each illustrate another flow diagram for quality of service (QoS) for device assisted services (DAS) in accordance with some embodiments. FIG. 8A illustrates another flow diagram for quality of service (QoS) for device assisted services (DAS) in accordance with some embodiments. At 802, the process begins. In some embodiments, the QoS policies are implemented on the device (e.g., service processor collects/receives an associated service plan that defines/specifies basic policies for QoS, which can include a QoS activity map, which, for example, maps QoS classes based on application, service usage, flow type, destination, time of day, network capacity, and/or other criteria/measures, as similarly described herein). In some embodiments, a QoS API is also used by various applications to initiate a QoS request, as described herein with respect to various embodiments. In some embodiments, the QoS rules are implemented in the form of a verified QoS activity map in accordance with various embodiments described herein. At 804, a QoS request is determined (e.g., by QoS class for a particular associated service/application). In some embodiments, the QoS request is determined at least in part by using the QoS activity map using various techniques described herein, for example, based on service/application usage monitoring on the device (e.g., by the service processor service usage monitoring agent). In some embodiments, the QoS request is determined based on the QoS API. In some embodiments, the QoS request is determined to be associated with an outgoing connection or an incoming connection. At 806, whether the QoS request is authorized is determined (e.g., whether the QoS request supported by the service plan, sufficient charging credit exists for this QoS request, and/or other criteria/measures). If not, then at 808, the UI provides a responsive notification and/or option as similarly described herein. If the QoS request is approved, then at 810, a request for network resources for the QoS session is sent to one or more network resources (e.g., service controller, BTS, gateway, core/transport network, IPX/GRX networks, a/another service controller in communication with another communications device such as for setting up a conversational class QoS connection with the other communications device, and/or other network

elements/functions/resources). If the device is determined to be eligible for QoS, then at 810, QoS availability is determined (e.g., based on network capacity, which may be determined at the device, via communication with the service controller, via communication with the BTS or another network element/function, and/or any combination thereof, using the various techniques described herein). If QoS is determined to not be available, then at 812, the UI provides information and/or options concerning the QoS availability (e.g., unavailability explanation and/or options for providing for one or more QoS options, such as a service plan upgrade or payment for a certain/set of/period of time for QoS session(s) access). If QoS is determined to be available, then at 814, a request for network resources for the QoS session is sent to one or more network resources (e.g., service controller, BTS, gateway, core/transport network, IPX/GRX networks, and/or other network elements/functions/resources, to setup, for example, a QoS end to end connection – coordinate all resources end to end for the approved and verified QoS flow). At 816, a confirmation of the approved QoS session is received to close the loop for the QoS for DAS (e.g., a QoS schedule is received that provides the QoS session confirmation information, such as a scheduled RAB/multi-RAB and/or other reserved network resource(s) by schedule/other criteria). At 818, a QoS router is executed/performed on the communications device to assist in implementing QoS for DAS using various verification techniques described herein (e.g., to perform QoS queuing, throttling, and/or other QoS router related functions as described herein). At 820, verified QoS charging is performed (e.g., at least in part) on the device using various techniques described herein (e.g., using the service processor, such as the charging/service usage monitoring and/or other agents as described herein). In some embodiments, QoS charging records and/or reports are provided to one or more network elements for managing QoS billing and/or other QoS management/billing related service control functions (e.g., to the service controller and/or the billing interface or billing server). In some embodiments, QoS for DAS also facilitates reestablishing the QoS session/connection/channel/stream if the QoS session/connection/channel/stream is lost or goes down, using similar techniques to those described herein as would be apparent to one of ordinary skill in the art. At 822, the process is completed. In some embodiments, the QoS provisioning channel is closed when the device session is over to, for example, free up various resources.

[00187] FIG. 8B illustrates another flow diagram for quality of service (QoS) for device assisted services (DAS) in accordance with some embodiments. In some embodiments, QoS for

DAS includes identifying the QoS requirements (e.g., QoS level or QoS class) for a service activity. At 824, the process begins. In some embodiments, the QoS policies are implemented on the device (e.g., service processor collects/receives an associated service plan that defines/specifies basic policies for QoS, which can include a QoS activity map, which, for example, maps QoS classes based on application, service usage, flow type, destination, time of day, network capacity, and/or other criteria/measures, as similarly described herein). In some embodiments, the QoS rules are implemented in the form of a verified QoS activity map in accordance with various embodiments described herein. At 826, the device monitors device activity, such as service/application usage activities. In some embodiments, the device detects the relevant activities based on various service usage monitoring techniques described herein. At 828, a QoS request is determined, for example, using various techniques described herein. At 830, a QoS level is determined based on the application and/or various device monitored service usage/application activities associated with the QoS request using various techniques described herein. For example, the QoS level can be determined using the QoS activity map, which provides a QoS policy defined by a table associating various QoS levels with a variety of activities that include various device monitored service usage/application activities. In some embodiments, the QoS activity map includes QoS level mappings based on one or more of the following: application, destination/source, traffic type, connection type, content type, time of day/day of week, network capacity, activity usage, service plan selection, current standing, user class, device class, home/roaming, network capabilities, and/or other criteria/measures as similarly described herein. In some embodiments, at 832, if the QoS level cannot be determined and/or in order to confirm a QoS level or selection among multiple potential appropriate/approved QoS levels, the UI presents options for a user to select the QoS level. At 834, the QoS request is initiated for the determined QoS level (e.g., QoS class and/or priorities). At 836, the process is completed.

[00188] FIG. 8C illustrates another flow diagram for quality of service (QoS) for device assisted services (DAS) in accordance with some embodiments. In some embodiments, QoS for DAS includes determining whether the network should grant the QoS request for a given device activity. At 842, the process begins. At 844, QoS request is determined. At 846, the communications device's standing for QoS is determined using various techniques described herein (e.g., a service processor in combination with a service controller or based on a

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

network capacity, workload balancing, QoS priority rules, and/or other criteria/measures/rules). At 860, the process is completed.

[00189] FIG. 9 illustrates another flow diagram for quality of service (QoS) for device assisted services (DAS) in accordance with some embodiments. In some embodiments, QoS for DAS includes QoS session provision for a service activity. At 902, the process begins. At 904, a new QoS session is granted and/or confirmed. At 906, a device service processor (e.g., policy decision point (PDP) agent, also referred to herein as a policy control agent) maps the QoS session grant to a QoS monitoring policy (e.g., based on a service controller provided QoS related policy, based on a service plan associated with the device, user, device/user group, and/or other criteria/measures, as similarly described herein). At 908, the QoS monitoring policy provides commands/instructions to a policy enforcement point (PEP) (e.g., PEP agent, also referred to herein as a policy implementation agent) for managing/enforcing the new QoS priorities/sessions. At 910, the PEP determines whether to allow, block, throttle, and/or queue priority (e.g., and/or otherwise control using various traffic control related techniques) a session based on the QoS monitoring policy. At 912, the process is completed.

[00190] FIG. 10 illustrates another flow diagram for quality of service (QoS) for device assisted services (DAS) in accordance with some embodiments. In some embodiments, Radio Access Bearer (RAB) support is available, and the following process is performed in accordance with some embodiments. At 1002, the process begins. At 1004, the device service processor detects a QoS request or QoS need (e.g., a QoS API request, a QoS request or need/benefit of QoS session based on service usage monitoring, such as by application and/or another service usage measure/activity). At 1006, the service processor and/or the service processor in communication with the service controller determines if the service plan allows/supports the requested QoS. If not, then at 1008, a UI event is generated (e.g., notifying the device user that such QoS/QoS level/class is not available, and potentially offering a QoS/service plan upgrade/purchase for that QoS/QoS level/class). At 1010, the service processor communicates the QoS request to the service controller (e.g., using a secure service control link or secure communication channel, as similarly described herein) to request the QoS level/class. At 1012, the service controller determines whether network resources are available using various techniques as described herein. In some embodiments, network capacity is determined using various techniques, such as local device measurements; dedicated local device measurement

reports; BTS reports; other network element reports; by assessing, for example, a combination of one or more of available bandwidth, traffic delay or latency, available QoS level, variability in available bandwidth, variability in latency, and/or variability in available QoS level; and/or other techniques as described herein. At 1014, the service controller responds to the QoS request (e.g., grants or denies the QoS request). In some embodiments, another UI event is generated if the QoS request is denied as similarly described herein. At 1016 (assuming the QoS request is granted), the device requests a QoS channel from the BTS. In some embodiments, the request includes a QoS request authorization code received from the service controller. In some embodiments, the service controller provides a notification of the QoS request approval for the communications device to the BTS, so that the BTS can verify the approval of the QoS request. In some embodiments, the BTS confirms the device QoS channel request directly with the service controller. For example, various other techniques for verifying the QoS channel request can also be used as similarly described herein and as would be apparent to one of ordinary skill in the art. In some embodiments, the device service processor and/or service controller provides QoS related reports informing the BTS of how many QoS channels (e.g., RABs) to provision and how many best effort resources to provision based on device demand projections. At 1018 (assuming the QoS channel request is verified), the QoS session is initiated based on an allocated RAB or multi-RAB reservation received from the BTS (e.g., and/or other network elements as similarly described herein). At 1020, the process is completed.

[00191] FIG. 11 illustrates another flow diagram for quality of service (QoS) for device assisted services (DAS) in accordance with some embodiments. In some embodiments, RAB support is not available, and the following process is performed in accordance with some embodiments. At 1102, the process begins. At 1104, the device service processor detects a QoS request or QoS need (e.g., a QoS API request, a QoS request or need/benefit of QoS session based on service usage monitoring, such as by application, or other service usage measure/activity). At 1106, the service processor and/or the service processor in communication with the service controller determines if the service plan allows/supports the requested QoS. If not, then at 1108, a UI event is generated (e.g., notifying the device user that such QoS/QoS level/class is not available, and potentially offering a QoS/service plan upgrade/purchase for that QoS/QoS level/class). At 1110, the service processor communicates the QoS request to the service controller (e.g., using a secure service control link or secure communication channel, as

similarly described herein) to request the QoS level/class. At 1112, the service controller determines whether network resources are available using various techniques as described herein. In some embodiments, network capacity is determined using various techniques, such as local device measurements, BTS reports, other network element reports, and/or other techniques as described herein. In some embodiments, the service controller throttles other devices on the link so that the requested QoS level can be achieved (e.g., as RAB support is not available). In some embodiments, the service controller time slots traffic from the device end in synchronization with a BTS clock or absolute clock to facilitate the requested QoS level and to achieve necessary network capacity to support/facilitate the requested QoS level (e.g., minimizing jitter/inter-packet delay variation) based on current/forecasted network capacity on the link. At 1114, the service controller responds to the QoS request (e.g., grants or denies the QoS request). In some embodiments, another UI event is generated if the QoS request is denied as similarly described herein. At 1116 (assuming the QoS request is granted), the device initiates the QoS session. At 1118, the device service processor and/or the device service processor in secure communication with the service controller monitors and verifies the QoS session using various monitoring and verification techniques described herein (e.g., checks CDRs to determine if the QoS channel is properly implemented by the device). In some embodiments, a UI event is generated to notify the device user if there are potential problems with the QoS session implementation, to periodically inform the user of QoS charging, and/or other events/information related to QoS activities. At 1120, the process is completed.

[00192] FIG. 12 illustrates a device stack for providing various service usage measurement techniques in accordance with some embodiments. FIG. 12 illustrates a device stack providing various service usage measurement from various points in the networking stack for a service monitor agent (e.g., for monitoring QoS related activities and/or for monitoring network capacity controlled services as described herein), a billing agent, and an access control integrity agent to assist in verifying the service usage measures, QoS related activities and functions, and billing reports in accordance with some embodiments. As shown in FIG. 12, several service agents take part in data path operations to achieve various data path improvements, and, for example, several other service agents can manage the policy settings for the data path service, implement billing for the data path service, manage one or more modem selection and settings for access network connection, interface with the user and/or provide

service policy implementation verification. Additionally, in some embodiments, several agents perform functions to assist in verifying that the service control or monitoring policies intended to be in place are properly implemented, the service control or monitoring policies are being properly adhered to, that the service processor or one or more service agents are operating properly, to prevent unintended errors in policy implementation or control, and/or to prevent/detect tampering with the service policies or control. As shown, the service measurement points labeled I through VI represent various service measurement points for service monitor agent 1696 and/or other agents to perform various service monitoring activities. Each of these measurement points can have a useful purpose in various embodiments described herein. For example, each of the traffic measurement points that is employed in a given design can be used by a monitoring agent to track application layer traffic through the communication stack to assist policy implementation functions, such as the policy implementation driver/agent 1690 (e.g., policy enforcement point driver/agent), or in some embodiments the modem firewall agent 1655 or the application interface agent, in making a determination regarding the traffic parameters or type once the traffic is farther down in the communication stack where it is sometimes difficult or impossible to make a complete determination of traffic parameters. The particular locations for the measurement points provided in these figures are intended as instructional examples, and other measurement points can be used for different embodiments, as will be apparent to one of ordinary skill in the art in view of the embodiments described herein. Generally, in some embodiments, one or more measurement points within the device can be used to assist in service control verification and/or device or service troubleshooting.

[00193] In some embodiments, the service monitor agent and/or other agents implement virtual traffic tagging by tracking or tracing packet flows through the various communication stack formatting, processing and encryption steps, and providing the virtual tag information to the various agents that monitor, control, shape, throttle or otherwise observe, manipulate or modify the traffic. This tagging approach is referred to herein as virtual tagging, because there is not a literal data flow, traffic flow or packet tag that is attached to flows or packets, and the book-keeping to tag the packet is done through tracking or tracing the flow or packet through the stack instead. In some embodiments, the application interface and/or other agents identify a traffic flow, associate it with a service usage activity and cause a literal tag to be attached to the traffic or packets associated with the activity. This tagging approach is referred to herein as

literal tagging. There are various advantages with both the virtual tagging and the literal tagging approaches. For example, it can be preferable in some embodiments to reduce the inter-agent communication required to track or trace a packet through the stack processing by assigning a literal tag so that each flow or packet has its own activity association embedded in the data. As another example, it can be preferable in some embodiments to re-use portions of standard communication stack software or components, enhancing the verifiable traffic control or service control capabilities of the standard stack by inserting additional processing steps associated with the various service agents and monitoring points rather than re-writing the entire stack to correctly process literal tagging information, and in such cases, a virtual tagging scheme may be desired. As yet another example, some standard communication stacks provide for unused, unspecified or otherwise available bit fields in a packet frame or flow, and these unused, unspecified or otherwise available bit fields can be used to literally tag traffic without the need to re-write all of the standard communication stack software, with only the portions of the stack that are added to enhance the verifiable traffic control or service control capabilities of the standard stack needing to decode and use the literal tagging information encapsulated in the available bit fields. In the case of literal tagging, in some embodiments, the tags are removed prior to passing the packets or flows to the network or to the applications utilizing the stack. In some embodiments, the manner in which the virtual or literal tagging is implemented can be developed into a communication standard specification so that various device or service product developers can independently develop the communication stack and/or service processor hardware and/or software in a manner that is compatible with the service controller specifications and the products of other device or service product developers.

[00194] It will be appreciated that although the implementation/use of any or all of the measurement points illustrated in FIG. 12 is not required to have an effective implementation, such as was similarly shown with respect to various embodiments described herein, various embodiments can benefit from these and/or similar measurement points. It will also be appreciated that the exact measurement points can be moved to different locations in the traffic processing stack, just as the various embodiments described herein can have the agents affecting policy implementation moved to different points in the traffic processing stack while still maintaining effective operation. In some embodiments, one or more measurement points are provided deeper in the modem stack where, for example, it is more difficult to circumvent and

can be more difficult to access for tampering purposes if the modem is designed with the proper software and/or hardware security to protect the integrity of the modem stack and measurement point(s).

[00195] Referring to FIG. 12, describing the device communications stack from the bottom to the top of the stack as shown, the device communications stack provides a communication layer for each of the modems of the device at the bottom of the device communications stack. Example measurement point VI resides within or just above the modem driver layer. For example, the modem driver performs modem bus communications, data protocol translations, modem control and configuration to interface the networking stack traffic to the modem. As shown, measurement point VI is common to all modem drivers and modems, and it is advantageous for certain embodiments to differentiate the traffic or service activity taking place through one modem from that of one or more of the other modems. In some embodiments, measurement point VI, or another measurement point, is located over, within or below one or more of the individual modem drivers. The respective modem buses for each modem reside between example measurement points V and VI. In the next higher layer, a modem selection & control layer for multimode device based communication is provided. In some embodiments, this layer is controlled by a network decision policy that selects the most desirable network modem for some or all of the data traffic, and when the most desirable network is not available the policy reverts to the next most desirable network until a connection is established provided that one of the networks is available. In some embodiments, certain network traffic, such as verification, control, redundant or secure traffic, is routed to one of the networks even when some or all of the data traffic is routed to another network. This dual routing capability provides for a variety of enhanced security, enhanced reliability or enhanced manageability devices, services or applications. In the next higher layer, a modem firewall is provided. For example, the modem firewall provides for traditional firewall functions, but unlike traditional firewalls, in order to rely on the firewall for verifiable service usage control, such as access control and security protection from unwanted networking traffic or applications, the various service verification techniques and agents described herein are added to the firewall function to verify compliance with service policy and prevent/detect tampering of the service controls. In some embodiments, the modem firewall is implemented farther up the stack, possibly in combination with other layers as indicated in other figures and described herein. In

some embodiments, a dedicated firewall function or layer is provided that is independent of the other processing layers, such as the policy implementation layer, the packet forwarding layer and/or the application layer. In some embodiments, the modem firewall is implemented farther down the stack, such as within the modem drivers, below the modem drivers, or in the modem itself. Example measurement point IV resides between the modem firewall layer and an IP queuing and routing layer (e.g., QoS IP queuing and routing layer and/or a network capacity controlled services queuing and routing layer). As shown, an IP queuing and routing layer is separate from the policy implementation layer where the policy implementation agent implements a portion of the traffic control and/or service usage control policies. As described herein, in some embodiments, these functions are separated so that a standard network stack function can be used for QoS IP queuing and routing and/or for network capacity controlled services queuing and routing, and the modifications necessary to implement the policy implementation agent functions can be provided in a new layer inserted into the standard stack. In some embodiments, the IP queuing and routing layer is combined with the traffic or service usage control layer. For example, a combined routing and policy implementation layer embodiment can also be used with the other embodiments, such as shown in FIG. 12. Measurement point III resides between the IP queuing and routing layer and a policy implementation agent layer. Measurement point II resides between the policy implementation agent layer and the transport layer, including TCP, UDP, and other IP as shown. The session layer resides above the transport layer, which is shown as a socket assignment and session management (e.g., basic TCP setup, TLS/SSL) layer. The network services API (e.g., HTTP, HTTPS, FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), POP3, DNS) resides above the session layer. Measurement point I resides between the network services API layer and an application layer, shown as application service interface agent in the device communications stack of FIG. 12.

[00196] As shown in FIG. 12, the application service interface layer (e.g., QoS application service interface layer and/or network capacity controlled services interface layer) is above the standard networking stack API and, in some embodiments, its function is to monitor and in some cases intercept and process the traffic between the applications and the standard networking stack API. In some embodiments, the application service interface layer identifies application traffic flows before the application traffic flows are more difficult or practically impossible to

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

[00197] As shown in FIG. 12, a service monitor agent, which is also in communication with the agent communication bus 1630, communicates with various layers of the device communications stack. For example, the service monitor agent, performs monitoring at each of measurement points I through VI, receiving information including application information, service usage and other service related information, and assignment information. An access control integrity agent is in communication with the service monitor agent via the agent communications bus 1630, as also shown.

[00198] FIG. 13 illustrates another device stack for providing various service usage measurement techniques in accordance with some embodiments. FIG. 13 illustrates an embodiment similar to FIG. 12 in which some of the service processor is implemented on the modem and some of the service processor is implemented on the device application processor in

accordance with some embodiments. In some embodiments, a portion of the service processor is implemented on the modem (e.g., on modem module hardware or modem chipset) and a portion of the service processor is implemented on the device application processor subsystem. It will be apparent to one of ordinary skill in the art that variations of the embodiment depicted in FIG. 13 are possible where more or less of the service processor functionality is moved onto the modem subsystem or onto the device application processor subsystem. For example, such embodiments similar to that depicted in FIG. 13 can be motivated by the advantages of including some or all of the service processor network communication stack processing and/or some or all of the other service agent functions on the modem subsystem (e.g., and such an approach can be applied to one or more modems). For example, the service processor can be distributed as a standard feature set contained in a modem chipset hardware or software package or modem module hardware or software package, and such a configuration can provide for easier adoption or development by device OEMs, a higher level of differentiation for the chipset or modem module manufacturer, higher levels of performance or service usage control implementation integrity or security, specification or interoperability standardization, and/or other benefits.

[00199] Referring to FIG. 13, describing the device communications stack from the bottom to the top of the stack as shown, the device communications stack provides a communication layer for modem MAC/PHY layer at the bottom of the device communications stack. Measurement point IV resides above the modem MAC/PHY layer. The modem firewall layer resides between measurement points IV and III. In the next higher layer, the policy implementation agent is provided, in which the policy implementation agent is implemented on the modem (e.g., on modem hardware). Measurement point II resides between the policy implementation agent and the modem driver layer, which is then shown below a modem bus layer. The next higher layer is shown as the IP queuing and routing layer, followed by the transport layer, including TCP, UDP, and other IP as shown. The session layer resides above the transport layer, which is shown as a socket assignment and session management (e.g., basic TCP setup, TLS/SSL) layer. The network services API (e.g., HTTP, HTTPS, FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), POP3, DNS) resides above the session layer. Measurement point I resides between the network services API layer and an application layer, shown as application service interface agent in the device communications stack of FIG. 13.

[00200] Additional Embodiments of DAS for Protecting Network Capacity

[00201] In some embodiments, DAS for protecting network capacity includes classifying a service activity as a network capacity controlled service and implementing a network capacity controlled services policy. In some embodiments, DAS for protecting network capacity includes device assisted/based techniques for classifying a service activity as a network capacity controlled service and/or implementing a network capacity controlled services policy. In some embodiments, DAS for protecting network capacity includes network assisted/based techniques (e.g., implemented on a network element/function, such as a service controller, a DPI gateway, a BTS/BTSC, etc., or a combination of network elements) for classifying a service activity as a network capacity controlled service and/or implementing a network capacity controlled services policy. In some embodiments, DAS for protecting network capacity includes providing a network access API or an emulated or virtual network access API (e.g., such an API can provide network busy state information and/or other criteria/measures and/or provide a mechanism for allowing, denying, delaying, and/or otherwise controlling network access). In some embodiments, DAS for protecting network capacity includes implementing a service plan that includes a network capacity controlled services policy (e.g., for differential network access control and/or differential charging for network capacity controlled services, which can also be based on a network busy state and/or other criteria/measures).

[00202] In some embodiments, DAS for protecting network capacity techniques also provide improved user privacy and facilitate network neutrality requirements. In contrast, network based techniques (e.g., DPI based techniques) can give rise to user privacy and network neutrality concerns and problems as discussed above. In some embodiments, DAS for protecting network capacity techniques include allowing a user to specify (e.g., permit or not permit) whether the network is aware of the user's Internet behavior (e.g., using UI input). In some embodiments, DAS for protecting network capacity techniques include allowing a user to select how they want their traffic usage and service plan costs to be managed.

[00203] FIG. 14 illustrates a flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments. At 1402, the process begins. At 1404, monitoring a network service usage activity of a device in network communication (e.g., wireless network communication) is performed. At 1406, whether the monitored network service usage activity is a network capacity controlled service is determined. At 1408 (the monitored network service usage activity was determined not to be a network

capacity controlled service), the network service usage activity is not classified for differential network access control. At 1410, (the monitored network service usage activity was determined to be a network capacity controlled service), the network service usage activity is classified (e.g., into one or more network capacity controlled services) for differential network access control for protecting network capacity. In some embodiments, classifying the network service usage activity includes classifying the network service usage activity into one or more of a plurality of classification categories for differential network access control for protecting network capacity (e.g., one or more network capacity controlled service classifications and/or a priority state classification, such as a background services classification and/or a background priority state classification). At 1412, associating the network service usage activity with a network capacity controlled services control policy based on a classification of the network service usage activity to facilitate differential network access control for protecting network capacity is performed. At 1414, implementing differential network access control for protecting network capacity by implementing different traffic controls for all or some of the network service usage activities (e.g., based on a network busy state or another criteria/measure) is performed. At 1416, the process is completed.

[00204] FIG. 15 illustrates another flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments. At 1502, the process begins. At 1504, monitoring network service usage activities of a device in network communication is performed. At 1506, monitored network service usage activity of the device is reported (e.g., to a network element/function). At 1508, a statistical analysis of a reported network service usage activities across a plurality of devices is performed (e.g., by a network element/function). At 1510, the device receives a network service usage activity classification list (e.g., a network capacity controlled services list, which can be generated, for example, based on the monitored network service usage activities and the statistical analysis as well as other criteria/measures, including, for example, a service plan and/or a network busy state) from the network element. At 1512, implementing differential network access control based on the network service usage activity classification list for protecting network capacity is performed. At 1514, the process is completed. In some embodiments, DAS for protecting network capacity further includes associating the network service usage activity with a network service usage control policy (e.g., a network capacity controlled services policy) based on a classification of

the network service usage activity to facilitate differential network access control for protecting network capacity. In some embodiments, DAS for protecting network capacity further includes differentially controlling the network service usage activity (e.g., network capacity controlled service) based on the service usage activity classification list.

[00205] FIG. 16 illustrates another flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments. At 1622, the process begins. At 1624, a first report of network service usage activity of a first device is received (e.g., at a network element/function) from the first device. At 1626, a second report of network service usage activity of a second device (e.g., at a network element/function) from the second device is received. At 1628, a statistical analysis of a plurality of reported service usage activities across a plurality of devices, including the first device and the second device, is performed (e.g., by a network element/function). At 1630, a network service usage activity classification list (e.g., a network capacity controlled services classification list) is sent to the first device (e.g., from a network element/function) for classifying network service usage activities (e.g., network capacity controlled services) based on the network service usage activity classification list for differential network access control for protecting network capacity. At 1632, a network service usage activity classification list is sent to the second device (e.g., from a network element/function) for classifying network service usage activities based on the network service usage activity classification list for differential network access control for protecting network capacity. At 1634, the process is completed. In some embodiments, DAS for protecting network capacity further includes associating the network service usage activity with a service usage control policy (e.g., a network capacity controlled services policy) based on a classification of the network service usage activity to facilitate differential network access control for protecting network capacity. In some embodiments, DAS for protecting network capacity further includes differentially controlling the network service usage activity (e.g., network capacity controlled service) based on the service usage activity classification list (e.g., network capacity controlled services classification list). In some embodiments, classifying network service usage activities is based on which network to which the device is connected. In some embodiments, the network service usage control policy is based on which network to which the device is connected.

[00206] FIG. 17 illustrates another flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments. At 1702, the process

begins. At 1704, monitoring a network service usage activity of a plurality of devices in network communication using network based techniques is performed. At 1706, a statistical analysis of monitored network service usage activities across the plurality of devices is performed. At 1708, a network service usage activity classification list (e.g., a network capacity controlled services classification list) is sent to each of the plurality of devices for classifying network service usage activities (e.g., network capacity controlled services) based on the service usage activity classification list for differential network access control for protecting network capacity. At 1710, the process is completed.

[00207] FIG. 18 illustrates another flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments. At 1802, the process begins. At 1804, monitoring network service usage activities of a device in network communication is performed. At 1806, associating a network service usage activity (e.g., a network capacity controlled service) with a service usage control policy (e.g., a network capacity controlled services policy) based on a classification of the network service usage activity (e.g., a network capacity controlled services classification list) for differential network access control for protecting network capacity is performed. At 1808, a user notification based on the service usage control policy is generated. At 1810, the process is completed.

[00208] In some embodiments, the service usage control policy includes a service usage notification policy. In some embodiments, the user notification includes one or more of the following: a notification that the application to be downloaded and/or launched is a network capacity controlled service; a list of one or more service activities (e.g., applications, OS/other software functions/utilities, and/or other functions/utilities as described herein) that have a network capacity controlled services classification; type of service policy in effect for one or more network capacity controlled services; notification that a service activity belongs to a network capacity controlled services class; notification that a service activity that is classified as network capacity controlled service can have the service class changed; notification that if the service class is changed for a service activity the service charges will change; notification that one or more networks are available (e.g., one or more alternative networks and/or network busy state information and/or charging information and/or incentives associated with such networks), a service plan upgrade/downgrade offer/option; and an offer for a service plan that rewards a user that responds to the notification a service plan is lower cost/discounted for responding to

notification to use or not to use service activity based on usage level warning notification. In some embodiments, the user notification includes a user preference selection, including one or more of the following: a provision to associate an access policy control with the application (e.g., allow/block, notify of usage, notify of usage at a given threshold, traffic control settings, allow during certain times, allow when network not busy, and/or other policy controls as described herein), an over-ride option for selecting the service usage control policy; a modify option to select the service usage control policy; a select option to select a new service plan (e.g., an option to review and select alternative/new service plan upgrade/downgrade options), and an acknowledgement request (e.g., to confirm/acknowledge receipt of the notification, in which the acknowledgement can be transmitted to a network element/function and/or stored locally for later reference/transmission).

[00209] In some embodiments, before a given device application, process, function, OS service or other service activity is allowed to start, the intention to start is intercepted by a launch manager, the background service policy set or the network protection service policy set for the service activity is retrieved, and any necessary user notification or service launch control policies are implemented prior to allowing the service activity to launch. In such embodiments, a launch intercept manager may be used to implement this functionality. In some embodiments, this launch intercept manager is provided with a list identifying the service activities (e.g., application identifiers, OS function identifiers, aggregate service activity identifiers, and/or component service activity identifiers) that have a launch control policy in effect. In some embodiments, the list of launch control policies includes blocking or delaying launch of the one or more service activities. In some embodiments, the launch control policy includes a user notification before, during or after the service activity is launched. In some embodiments, the user is informed that a service activity that has a background service control policy in effect or a network protection service control policy in effect is attempting to launch, is about to launch or has launched. In a further set of embodiments, the launch is held up until the user is notified and is allowed to decide if they would like to launch the service activity. In some embodiments, the user notification includes a message that the service activity attempting to launch consumes a large amount of service usage and asks the user if they would like to continue (e.g., “This application consumes a large amount of data, would you like to continue?”, “This application consumes data even when you are not using it, would you like to continue?” “This application

consumes data while you are roaming which adds cost to your usage bill, would you like to continue?”, etc). In some embodiments, the decision on whether or not to launch a service activity is pre-programmed into the list identifying the service activities (e.g., application identifiers, OS function identifiers, aggregate service activity identifiers, and/or component service activity identifiers) that have a launch control policy in effect. In some embodiments a portion of the list is pre-programmed by the user in accordance with user preference for controlling usage of service activities. In some embodiments, a portion of the list is pre-programmed by a network element (e.g., a service controller) in accordance with network background service or network protection service policies specified by a service policy design management system operated by a service provider as described herein. In some embodiments, the policy implementation defined by the list identifying the service activities (e.g., application identifiers, OS function identifiers, aggregate service activity identifiers, and/or component service activity identifiers) that have a launch control policy in effect is verified to ensure that the user or malicious software has not defeated the policy enforcement specified in the list. In some embodiments the list identifying the service activities that have a launch control policy in effect includes launch policies that are a function of one or more of: background service state, network busy state (or performance state or QoS state), type of network the device is connected to, home or roaming connection, time of day or day of week.

[00210] In some embodiments, the various design techniques described herein that allow for intercepting a service activity intention to launch, and applying a background service policy set or a network protection service policy set can be designed into the OS itself. For example, the intercept and policy implementation functions can be designed into the activity manager, broadcast intent manger, media service manager, service manager, or other application or service activity management function in the Android OS. One of ordinary skill in the art will recognize that similarly, the various design techniques described herein that allow for intercepting a service activity intention to launch, and applying a background service policy set or a network protection service policy set can be designed into application launch management functions in the iPhone OS, windows mobile OS, windows PC OS, Blackberry OS, Palm OS, and other OS designs.

[00211] In some embodiments, the pre-launch user notification information indicates one or more of: typical service usage or cost, or projected service usage or cost for the service activity attempting to launch. In some embodiments, the user sets limitations on access for one

or more service activities and once this limit is hit then when the service activities with exceeded limits attempt to launch the user is notified. In some embodiments, the user chooses from a set of service restrictions rather than simply blocking or allowing service activity launch, with example service restrictions including but not limited to: a pre-configured set of restriction policies to chose from (e.g., full access, limited access, highly restricted access or block access), block, throttle, delay, aggregate and hold, limit amount of usage per unit time, cap usage, set limit for additional notification, specify type of network, specify busy state (performance, QoS) or background state, or choose from pre-configured settings options.

[00212] In some embodiments, the user notification occurs after the user attempts to download or load an application onto the device (e.g., an application downloaded from the web or an online application store for a smart phone or other wireless/network computing device, such as an Apple iPhone or iPad, or Google Android/Chrome based device). In some embodiments, the user notification occurs after the user attempts to run the service activity or to initiate usage of a cloud based service/application (e.g., Google or Microsoft cloud service based apps). In some embodiments, the user notification occurs after one or more of the following: the service usage activity hits a usage threshold event, the service usage activity attempts a network service usage that satisfies a pre-condition, an update to a network capacity protection service activity classification list or policy set, and a network message is sent to the device triggering the notification. In some embodiments, the user notification provides information on the service usage activity that is possible, typical, or likely for the service usage activity. In some embodiments, the user notification includes a user option for obtaining more information about the service usage of the service activity (e.g., a message that the service usage activity may result in a high service usage and/or that the service usage activity may or will result in a high service usage as compared in some way to a limit of the current service plan) to make informed user preference settings.

[00213] In some embodiments, a user notification includes displaying (e.g., and as applicable, allowing users to provide UI input) one or more of the following: current and/or past/historical/logged network service usage activity list, current and/or past/historical/logged network capacity controlled service usage activities, current activity policy settings, current or available networks, service plan options (e.g., for how to treat one or more network capacity controlled service traffic types), selection option(s) to assign a network capacity controlled

service activity into a different priority traffic control and/or charging buckets, network service usage by activity (e.g., network capacity controlled services and other services), network busy state (e.g., and with resulting policies in force), service activity policy setting vs. busy state and time/day/week, network service activity priority, network service activity usage statistics (e.g., vs. network busy state and/or network service usage control policy state).

[00214] In some embodiments, a UI notification is displayed when user attempts a network capacity controlled service activity during a network busy state (e.g., that modifies a network capacity controlled services policy). In some embodiments, the UI notification includes information on service plan choice and a network capacity controlled services policy over-ride option (e.g., one time, time window, usage amount, permanent by activity, and/or all), charging information based on a user selection, and/or service plan upgrade information and options.

[00215] In some embodiments, a UI notification is displayed for user input for preferences/configurations for multiple networks (e.g., WiFi, 4G, 3G, and/or other wired or wireless access networks) including charging policy. In some embodiments, a UI notification is displayed when a specified network traffic service usage activity (e.g., based on network capacity controlled services classification, QoS classification, priority classification, time based criteria, network capacity, service plan, charging criteria, and/or other criteria/measures) is being attempted or is occurring and providing options (e.g., allow, block, delay, throttle, and/or other options).

[00216] In some embodiments, a UI fuel gauge is displayed (e.g., to depict current and/or historical network service usage, for example, relative to a service plan for the device, by network, relative to network busy state, time based criteria, and/or other criteria/measures). In some embodiments, a user notification includes a communication sent to the user (e.g., an email, SMS or other text message, voice message/call, and/or other electronic form of communication). In some embodiments, the communication sent to the user includes network service usage information, network capacity controlled service usage related information, and/or an instruction to log into a web page or send a communication for more information (e.g., regarding an information update and/or alert or warning message, such as related to network service usage and/or charging for network service usage).

[00217] In some embodiments, a notification (e.g., a user or network service cloud notification) is generated based on an aggregate service activity reports usage (e.g., allows network provider to generate user notifications and/or to notify application provider/service activity provider). In some embodiments, a notification (e.g., a user or network service cloud notification) is generated based on a publishing of an updated/new network capacity controlled services list based on an aggregate monitored activity (e.g., based on a service plan, velocity, sockets opening frequency/rate (e.g., messaging layer behavior), total data usage, peak busy time usage to formulate or update black list for monitoring, notifying, and/or controlling, which can be applied to one, multiple, group, or all devices). In some embodiments, a notification (e.g., a user or network service cloud notification) is generated based on data usage trends for particular device relative to an associated service plan and/or other comparable devices or data usage thresholds/statistical based data usage measures.

[00218] In some embodiments an application is actually composed of several component applications, processes or functions. Examples of this include but are not limited to: the components of a Java application JAR file; applications that use OS functions; applications that use a proxy service function; applications, functions or processes that coordinate with one another to implement a composite process, function or application; and OS process functions that support an application or overall OS function. In such embodiments it is important to be able to categorize all applications, functions and processes on a device that contribute to the service usage of a service activity so that the service activity can be monitored for service usage, have the service usage accounted for, implement the appropriate user notification when one or more service activity components attempts to start or use the network, implement the appropriate user notification when one or more service activity components reaches a pre-determined service usage level that requires user notification, and implement the appropriate background service or network protection service usage controls as specified herein ((including but not limited to for example: block network access, restrict network access, throttle network access, delay network access, aggregate and hold network access, select for time of day network access restrictions, select network type restrictions, select roaming network access restrictions, select service usage restrictions such as a usage limit, select service cost restrictions such as a cost limit or otherwise place on another form of background service status or network usage restriction as described herein). In the case of service activity components that belong exclusively to one aggregate

service activity (e.g., an application, application JAR file or OS function), this may be accomplished by including each of the component service activities on a list that identifies the service activity components that belong to the aggregate service activity, and then monitoring, possibly controlling and providing user notifications based on the aggregate or component behavior of each service activity in accordance with the policies specified for the aggregate service activity. For example, it is necessary to group all application launch behavior and/or network access behavior under the monitoring, launch, notification, accounting and background service controls or network protection service controls (or other background or network protection service policies as specified herein) in accordance with the background service or network protection service policies for the aggregate application that the JAR file supports. As another example, if an OS network synch or update function utilizes various software components or processes to implement the network synch or update function, then each of the software components or process must be monitored and aggregated under the background service policies or network protection service policies for the aggregate OS synch or update function.

[00219] In some embodiments, this ability to group usage for a related set of service activity components dedicated to an aggregate service activity as described herein is used to improve usage reporting of service activities to a service controller for the purpose of statistically identifying service activities that are candidates for background service policy controls or network protections service policy controls.

[00220] In some cases, multiple applications, processes, functions, OS services or other service activities can utilize a common set of component software applications, processes, functions or OS services. In such cases, in order to implement background service policies and/or network protection service policies for service activity monitoring and accounting, service activity launch control, user notification, or network access control as described herein, it is necessary to associate the specific network access data or information flows to and from the common component software applications, processes or functions that belong to the specific initiating application, process, function or other service activity that is to be managed according to a background service or network protection service policy set. In what follows, a specific set of examples is provided on how to map common component service activity for a set of common OS functions referred to as proxy service functions to a specific application, process, function, OS service or other service activity for the purpose of implementing a background service policy

set or a network protection service policy set as described herein. Once these examples are reviewed, it will be obvious to one of ordinary skill in the art how to apply similar mapping of service activity for a common set of components to a service activity that is to be managed in accordance with a background service policy set or a network protection service policy set as described herein.

[00221] In some embodiments, this ability to group usage for a common set of service activity components as described herein is used to improve usage reporting of service activities to a service controller for the purpose of statistically identifying service activities that are candidates for background service policy controls or network protections service policy controls.

[00222] In some embodiments, a proxy network service manager refers to an intermediary data flow function in a device operating system that sits on a data path between a device application and a device networking stack interface to provide a level of network service abstraction from the network stack interface, a higher level service function above the network stack interface, enhanced or special traffic processing functions, media service transfer management, file download service, HTTP proxy service functions, QoS differentiation, or other similar or related higher level traffic processing. Example Proxy Service Managers include the following: media service manager (e.g., android media service library function), email service manager, DNS function, software download service manager, media download manager (e.g., audio player, streaming media player, movie downloader, media service OS function, etc.), data download service manager, Android “media” library function, Android.net library function, Jave.net library function, Apache library function, other similar software/library functions or services in other device operating systems, SMTP/IMAP/POP proxy, HTTP proxy, IM proxy, VPN service manager, SSL proxy, etc. Herein these alternative network access data flows that are initiated by an application are termed application proxy service flows. In such embodiments an app can sometimes simply request a network access service activity from an OS component such as a proxy service component rather than directly accessing the network. In such embodiments, in order to implement background service controls or user notification of application service usage, it is necessary to monitor the application proxy service flows, classify them as being initiated by or belonging to a particular application or service activity, and implement the proper background service classifications, user notifications, application process launch intercept, background service accounting, and background service usage restrictions as

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

[00223] In some embodiments, this ability to track service usage for an service activity through a proxy service as described herein is used to improve usage reporting of service activities to a service controller for the purpose of statistically identifying service activities that are candidates for background service policy controls or network protections service policy controls.

[00224] In some embodiments, the various design techniques described herein that allow for monitoring, accounting for and/or implementing service policy for component service activities that belong to an aggregate service activity can be designed into the OS itself. For example, in certain current mobile OS implementations (e.g., Android, iPhone, Blackberry, etc) there are some applications available in the market that allow a user to get an estimate for how much data a certain subset of applications are consuming on a wireless service provider network, but it is not possible for the user or application to get an indication of the service usage for certain OS functions, whereas the embodiments disclosed herein will allow for this. As another

example, in certain current mobile OS implementations it is not possible to associate proxy service usage (e.g., media download and media streaming proxy library software functions) with the specific applications that use the proxy service, so while the user can be informed of generic common OS functions or proxy services (e.g., in the case of Android: “media service,” “media,” “gallery,” “Google service framework” and other generic common OS software library functions or proxy services), there is no way for the user to determine what applications widgets or other service activities are actually generating this common service function usage, whereas the invention described herein permits the user full visibility on such usage monitoring examples. Furthermore, if the OS is retrofitted with the intercept and policy implementation functions can be designed into the activity manager, broadcast intent manger, media service manager, service manager, or other application or service activity management function in the Android OS. One or ordinary skill in the art will recognize that similarly, the various design techniques described herein that allow for intercepting a service activity intention to launch, and applying a background service policy set or a network protection service policy set can be designed into application launch management functions in the iPhone OS, Windows mobile OS, Windows PC OS, Blackberry OS, Palm OS, and other OS designs.

[00225] FIG. 19 illustrates another flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments. At 1902, the process begins. At 1904, determining a network busy state of one or more networks is performed. In some embodiments, the one or more networks are selected from an access network, a wired network, and a wireless network. At 1906, classifying a network service usage activity (e.g., a network capacity controlled service) of a device based on the network busy state determination is performed to facilitate differential network access control for protecting network capacity of the one or more networks. In some embodiments, the network busy state is based on one or more of the following: network performance, network congestion, network availability, network resource availability, network capacity, or any other network service usage measure, and one or more time windows (e.g., time based criteria). In some embodiments, protecting network capacity of the one or more networks includes protecting network capacity of a last edge segment of a wireless network (e.g., RAN, BTS, BTSC, and/or other network elements). In some embodiments, the determining and classifying are performed using device assisted/based techniques. In some embodiments, the determining and classifying are performed using network

assisted/based techniques (e.g., implemented on a network element/function, such as a service controller, a DPI gateway, a BTS/BTSC, etc., or a combination of network elements). In some embodiments, the determining and classifying are performed using a combination of device assisted/based techniques and network assisted/based techniques. At 1908, implementing differential traffic controls is performed based on the service usage activity classification for protecting network capacity. At 1910, the process is completed. In some embodiments, a network busy state is determined based on one or more of the following: a time of day, a network reported busy state, and/or a device (e.g., near-end and/or far-end) determined/reported network busy state. In some embodiments, a network busy state is determined using one or more of the following: a network probe, a device query, a network probe report (e.g., including a BTS and/or BTSC), a network probe analysis, a device analysis based on performance of native traffic without probe such as TCP timeout, UDP retransmissions, a multiple network test, a device monitored network congestion based on network service usage activity (e.g., application based network access performance data) performed for a network to which the device is connected and/or one or more alternative networks. In some embodiments, a network congestion state is associated with a network busy state (e.g., a network busy state setting/level). For example, a network congestion level of 40% of network usage can be associated with a network busy state setting of 4, a network congestion level of 80% of network usage can be associated with a network busy state setting of 8, and so forth.

[00226] FIG. 20 illustrates another flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments. At 2002, the process begins. At 2004, monitoring a network service usage activity of a device in network communication is performed. At 2006, classifying the network service usage activity (e.g., based on a classification of the network service usage activity for protecting network capacity, for example, as a network capacity controlled service) for protecting network capacity is performed. At 2008, accounting for network capacity controlled services (e.g., accounting for the network service usage activity based on a classification of the network service usage activity for protecting network capacity) is performed. At 2010, charging for network capacity controlled services is performed. At 2012, the process is completed. In some embodiments, DAS for protecting network capacity further includes classifying the network service usage activity as a network capacity controlled service. In some embodiments, DAS for protecting

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

[00227] FIG. 21 illustrates another flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments. In some embodiments, DAS for protecting network capacity includes providing a device service access API that provides an interface for applications, OS functions, and/or other service usage activities to a

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

[00228] In some embodiments, the API is served or located on the device, on a network element (e.g., using a secure communication between the device and the network element for the API communication, such as HTTPS, TLS, SSL, an encrypted data connection or SS7 control channel, and/or other well known secure communication techniques), and/or both/partly in both. In some embodiments, a network based API is an API that facilitates an API or other interface

communication (e.g., secure communication as discussed above) between an application executing on the device and a network element and/or service cloud for protecting network capacity. For example, a network API can provide an interface for an application to communicate with a service cloud (e.g., network server) for obtaining network access control information (e.g., network busy state, multiple network information based on available networks and/or network busy state information of available networks, network capacity controlled service priorities and availability, scheduled time/time slots for network access based on network busy state, service plan, network capacity controlled service, and/or other criteria/measures). As another example, a network API can facilitate an application provider, central network/service provider, and/or a third party with access to communicate with the application to provide and/or request information (e.g., physical location of the application, network location of the application, network service usage information for the application, network busy state information provided to the application, and/or other criteria/measures). As yet another example, a network API can facilitate a broadcast to one or more applications, OS functions, and/or devices (e.g., partitioned based on geography, network, application, OS function, and/or any other criteria/measure) with network capacity related information (e.g., network busy state, availability based on network capacity controlled service classification and/or priority level, scheduled time/time slots for certain network capacity controlled service classification and/or priority level, emergency/high priority software/antimalware/vulnerability update and scheduled time/time slots for such software updates, and/or other criteria/measures). In some embodiments, the network access API for protecting network capacity is an open API or standard/required API (e.g., required or standardized for applications for a certain network service provider, such as to be provided via the Verizon application store or the Apple AppStore) published for application and OS developers so that the applications and OS functions are designed to understand and implement the network access API for protecting network capacity. For example, a certification program can be established to provide application and OS developers with test specifications, working implementations, and/or criteria to make sure the network access API is properly implemented and is functioning in accordance with the specified requirements. In some embodiments, the network access API is an interface for communication with a service controller (e.g., service controller 122) or another network element/function (e.g., a service usage API for communication with a service usage server or billing interface/server or

another network element/function that facilitates a secure communication for sending/receiving or otherwise communicating network access related information for protecting network capacity). In some embodiments, the network API provides for sponsored billing (e.g., reverse billing) of all, classified, and/or a subset of network service usage charges to a sponsored partner associated with the network service usage activity (e.g., application) that accesses the network API. In some embodiments, the network API provides for a sponsored service in which the network service usage activity (e.g., application) that accesses the network API provides a sponsored service partner credential to the network API, the credential is used as a billing mechanism to charge the sponsored partner, the user account is mediated to remove the sponsored partner charge, and the network API provides access service and/or information service (e.g., location information, local information, content information, network information, and/or any other information).

[00229] FIG. 22 illustrates another flow diagram for device assisted services (DAS) for protecting network capacity in accordance with some embodiments. At 2202, the process begins. At 2204, network service usage activities of a device are monitored (e.g., using a verified/verifiable service processor). At 2206, a network busy state (e.g., a measure of network capacity, availability, and/or performance) is determined based on the monitored network service usage activities (e.g., using various techniques as described herein). In some embodiments, a service processor on the device is used to determine (e.g., measure and/or characterize) a network busy state experienced by the device (e.g., which can be used to determine the network access control policy for one or more network capacity controlled services). At 2208, a network busy state report is sent to a network element/function (e.g., a service controller and/or another network element/function as described herein). At 2210, the process is completed. In some embodiments, the service processor is verified using various techniques described herein. In some embodiments, the network busy state report includes one or more of the following: data rate, latency, jitter, bit error rate, packet error rate, number of access attempts, number of access successes, number of access failures, QoS level availability, QoS level performance, and variability in any of the preceding parameters. In some embodiments, the network busy state report includes one or more of the following: base station ID, cell sector ID, CDMA ID, FDMA channel ID, TDMA channel ID, GPS location, and/or physical location to identify the edge network element that is associated with the network busy state report to a network element. In

some embodiments, the monitoring of network service usage activities includes measuring the network performance for traffic the device is transmitting/receiving and/or generating network performance testing traffic. In some embodiments, the network busy state is collected (e.g., and/or used to assist, supplement, and/or verify device based network busy state measures) by one or more network elements that can measure and/or report network busy state (e.g., BTS, BTSC, base station monitor, and/or airwave monitor). For example, airwave monitors and/or base station monitors can be provided to facilitate a reliable characterization of network busy state in a coverage area of one or more base stations and/or base station sectors, such as affixed mobile terminals (e.g., trusted terminals that can include additional network busy state monitoring and/or reporting functionality) installed (e.g., temporarily or permanently) in the coverage area of one or more base stations and/or base station sectors (e.g., in which a sector is the combination of a directional antenna and a frequency channel) so that the affixed mobile terminals perform network busy state monitoring and reporting to the service controller, the local base station, and/or other network element(s)/function(s) as similarly described herein. In some embodiments, the permanently affixed mobile terminals provide network monitors for reporting, for example, network busy state, to a central network element, such as the service controller, which can, for example, aggregate such network busy state information to determine network busy state for one or more network coverage areas. In some embodiments, the permanently affixed mobile terminals are always present in these locations where installed and always on (e.g., performing network monitoring), and can be trusted (e.g., the permanently affixed mobile terminals can be loaded with various hardware and/or software credentials). For example, using the permanently affixed mobile terminals, a reliable characterization of network busy state can be provided, which can then be reported to a central network element and aggregated for performing various network busy state related techniques as described herein with respect to various embodiments. In some embodiments, the network element/function uses the network busy state report (e.g., and other network busy state reports from other devices connected to the same network edge element) to determine the network busy state for a network edge element connected to the device. In some embodiments, network element/function sends a busy state report for the network edge element to the device (e.g., and to other devices connected to the same network edge element), which the device can then use to implement differential network access control policies (e.g., for network capacity controlled services) based on the network busy

state. In some embodiments, a network busy state is provided by a network element (e.g., service controller or service cloud) and broadcast to the device (e.g., securely communicated to the service processor).

[00230] FIG. 23 illustrates a network capacity controlled services priority level chart for device assisted services (DAS) for protecting network capacity in accordance with some embodiments. In some embodiments, various applications, OS functions, and/or other utilities/tools installed/loaded onto and/or launched/executing/active on a communications device (e.g., device 100) are classified as network capacity controlled services for protecting network capacity. In some embodiments, one or more of the network capacity controlled services are assigned or classified with network capacity controlled service levels or priority levels for protecting network capacity. In some embodiments, one or more of the network capacity controlled services are dynamically assigned or classified with network capacity controlled service levels or priority levels based on one or more criteria/measures (e.g., dynamic criteria/measures), such as network busy state, current access network, time based criteria, an associated service plan, and/or other criteria/measures. In some embodiments, a higher priority level means that the application or utility/function is granted higher relative priority for network access (e.g., a priority level 10 can provide for guaranteed network access and a priority level 0 can provide a blocked network access, while priority levels between 1 through 9 can provide relatively increasing prioritized network access potentially relative to allocated network access and other services requesting network access).

[00231] As shown in FIG. 23, the network capacity controlled services are dynamically assigned or classified with network capacity controlled service levels or priority levels based on the network busy state of the current access network. For example, an email application, Microsoft Outlook, is assigned different priority levels for protecting network capacity based on the network busy state, as shown: a priority level 6 for a network busy state (NBS) level of 10% (e.g., up to about 10% of the network capacity is being utilized based on current or recently/last measured/detected/determined network capacity/resources usage using various techniques as described herein), a priority level 5 for a network busy state (NBS) level of 25%, a priority level 4 for a network busy state (NBS) level of 50%, a priority level 3 for a network busy state (NBS) level of 75%, and a priority level 2 for a network busy state (NBS) level of 90%. As also shown, an antivirus (AV) software update application/utility/function is assigned different priority levels

for protecting network capacity based on the network busy state: a priority level 9 for a network busy state (NBS) level of 10%, a priority level 7 for a network busy state (NBS) level of 25%, a priority level 5 for a network busy state (NBS) level of 50%, a priority level 3 for a network busy state (NBS) level of 75%, and a priority level 1 for a network busy state (NBS) level of 90%.

Various other applications and utilities/functions are shown with various priority level assignments/classifications based on the network busy state levels shown in the network capacity controlled services priority level chart of FIG. 23. As will be apparent to one of ordinary skill in the art, various assignments and/or techniques for dynamically assigning priority levels for network access based on network busy state levels can be applied for protecting network capacity (e.g., based on user preferences, service plans, access networks, a power state of device, a device usage state, time based criteria, and various other factors such as higher priority for urgent software and/or security updates, such as a high priority security or vulnerability software patch or update, and/or urgent or high priority emails or other communications, such as a 911 VOIP call).

[00232] Referring again to FIGS. 1 through 3, DAS for protecting network capacity is implemented using a service processor (e.g., a service processor 115) of the device (e.g., a device 100) using various DAS techniques as described herein to facilitate differential network service access control (e.g., for network capacity controlled services) to assist in protecting network capacity in accordance with some embodiments. In some embodiments, the service processor and/or one or more agents of the service processor is/are verified using one or more of the following verification techniques (e.g., and/or to specifically verify monitoring the network service usage activity, classifying one or more service activities into one or more network capacity controlled service classes, associating the one or more network capacity controlled service classes with one or more differential service activity policies, and/or determining a network busy state): compare a network based service usage measure with a service policy and/or service plan associated with the device, compare a device assisted service usage measure with the service policy and/or service plan associated with the device, compare the network based service usage measure to the device assisted service usage measure, compare a first device assisted service usage measure to a second device assisted service usage measure, verify presence of the service processor and/or one or more agents of the service processor, verify configuration of the service processor, verify service usage activities are reported properly (e.g.,

using test service usages to generate service usage events/reports for analysis and confirmation), verify billing events are reported properly, compare the network based service usage measure with reported device billing data, verify reporting of a test billing event, verify reporting of the communications device reports billing events from a transaction server, verify presence of an activation tracking system, verify device configuration or operation, verify device standing or service plan standing, verify proper operation of the service processor, verify service processor heartbeat response reports, verify monitoring of a test service event, download a new service processor (e.g., and/or one or more agents or new configuration settings of the service processor) and perform integrity checks, verify a service processor code configuration with agent self-diagnosis checks, verify that the communications device uses the first service only after being authorized, verify user standing, verify a network busy state (e.g., compare and/or statistically process network busy state measures from more than one device in which the network busy state monitoring apparatus, for example, is located in a secure execution environment on the device), verify various differential network access control implementations (e.g., network capacity controlled services are properly monitored/determined/detected, controlled, accounted for, and/or charged for), verify various QoS implementations (e.g., as discussed above), and verify an agent communications log. Various other verification techniques are described herein and similar and other verification techniques for providing DAS for protecting network capacity using device based implementations (e.g., service processors and/or other device based agents or software/hardware techniques) will now be apparent to one of ordinary skill in the art in view of the various embodiments described herein.

[00233] In some embodiments, the service processor is secured using various hardware and software techniques described herein, including, for example, implementing all and/or portions of the service processor in a secure virtual machine, protected execution environment, secure storage (e.g., secure memory), secure modem, and/or other secure implementation techniques as described herein and/or other or similar techniques as will now be apparent to one of ordinary skill in the art in view of the various embodiments described herein. For example, the service processor can be implemented in software and executed in a protected area of an OS executed on the device and/or executed in protected execution partitions (e.g., in CPU, APU, SIM chipset, modem, modem secure execution partition, SIM, other hardware function on the device, and/or any combination of the above).

[00234] In some embodiments, a network service usage counter is embedded into a secure execution environment (e.g., a program store in secure non-volatile memory located on a modem card and/or a modem chip not accessible by device applications, secure CPU environment for executing program and/or secure program operation for data path monitoring and/or control that cannot be bypassed by device applications to get to the modem connection to the network) in a device modem (e.g., using measurement points V, VI, and/or other measurement points of FIG. 12). In some embodiments, the service usage counter counts data traffic (e.g., bytes and/or any other measure of service usage, such as file transactions, message transactions, connection time, time of connection or duration of connection, and/or traffic passed or transactions passed for a given QoS or network capacity controlled service priority level), traffic as a function of time, traffic according to a network service activity classification (e.g., by application, destination/source, port, traffic type, content type, time of day, network busy state, and/or any other criteria/measure). In some embodiments, the service usage counter counts data traffic (e.g., as discussed above) while coordinating with a VPN layer established, for example, for both layer-III (e.g., IPSEC) and layer-II (e.g., L2TP tunnel) so that precise over the air service usage measure is counted for billing mediation and/or network service usage charging (e.g., customer billing, sponsored service bill by service and/or any other charging or billing). In some embodiments, the service usage counter counts data traffic (e.g., as discussed above) while coordinating with accelerator software (e.g., a compression/decompression engine) which transforms frames for more efficient over the air transmission. As similarly discussed above, service processor coordination with the accelerator layer facilitates a precise over the air service usage measure for billing mediation and/or network service usage charging. In some embodiments, the service usage counter counts data traffic (e.g., as discussed above) while coordinating with both the VPN layer and accelerator software layer to facilitate a precise over the air service usage measure for billing mediation and/or network service usage charging.

[00235] In some embodiments, the service usage counter reports the service usage to a network element (e.g., a service controller, charging gateway, PCRF, AAA, HA, billing system, mediation system, traffic accounting database, base station or base station controller, and/or another network element/function or central network element/function). In some embodiments, the information reported to the network element is encrypted or signed with a corresponding key known by the network element. In some embodiments, the communication link to the network

element to pass the service usage count is conducted over a wireless network specific channel such as SMS, MMS, SS-7, or another specialized control channel. In some embodiments, the communications link to the network element to pass the service usage count is conducted over a network channel (e.g., via IP, TCP, UDP, HTTP, HTTPS, TLS, SSL, point to point signed variants of TLS or SSL, or another data network channel via the network control channel connection to the device). In some embodiments, the data network control channel traffic is injected into the PPP stream at the modem. In some embodiments, the data network control channel traffic is passed up to the device networking stack for connection to the network. In some embodiments, a signed or encrypted service usage count from the modem subsystem is coordinated to provide a service usage count for a time period that also corresponds to a similar time period for a service processor heartbeat report that includes a service usage measure or count. For example, this provides the service controller or another network element with a secondary set of information that can be used to verify and/or secure the service usage measures reported by the service processor. Various techniques can be used to synchronize the time period for the modem service usage count and the service processor service usage count. For example, the service processor can request a latest count message from the modem, in which the modem counts all service usage since the previous request for latest count until the present request for latest count, encrypts the latest count message so that the service processor or other application software or OS software on the device cannot decode and/or tamper with the message, and the modem service usage counter then passes the encrypted message to the service processor. The service processor can then pass the encrypted service usage count message from the modem to the service controller along with the service processor service usage accounting message(s) for the same or similar time period. The service controller can then decode both service count messages from the secure modem subsystem and the service processor and correlate the two measures to verify the service usage reporting by, for example, looking for discrepancies that would indicate service usage control or charging errors or device service processor tampering. In some embodiments, the secure modem subsystem records byte counts for streams (e.g., and/or flows, socket connections, or combinations of IP destination/source/ports), potentially along with time of day, network busy state, QoS level, and/or other criteria/measures, and reports these counts for each stream that had traffic activity during the current reporting interval. For example, the service controller can then correlate the stream service usage information with the

service usage information provided by the service processor heartbeat service usage report to verify that the service processor service usage report is consistent with the independent measure made in the modem subsystem. In some embodiments, service usage reports (e.g., certified service usage reports) are correlated on the device and/or in the network (e.g., using one or more network elements/functions, such as the service controller).

[00236] In some embodiments, a deeper analysis of traffic can be conducted in the modem subsystem service usage count. For example, a layer 7 analysis of the service usage can be conducted for HTTP or HTTPS traffic flowing through the modem in which the modem subsystem service usage counter performs an HTTP level analysis of the traffic to associate web traffic gets and other transfers with a given higher level service classification (e.g., ad server, content server, proxy server, and/or traffic that is referred by the local host serving up a web page). In some embodiments, the modem subsystem service usage count can be augmented for HTTPS, SSL or TLS traffic by including a trusted proxy server embedded in the modem system. For example, the proxy server can be trusted by the device stack so that the encryption keys for HTTPS, TLS or SSL are known by the proxy server allowing the modem based proxy server, located, for example, in a secure execution environment, to perform layer 7 analysis of encrypted traffic in a manner similar to that described above. In some embodiments, the embedded proxy server generates server SSL certificates for each connection to a specific remote host in real time based on a root certificate trusted by the device (e.g., and/or by network service usage activity, such as by application) and also trusted by the embedded proxy server, and the proxy server then becomes a middle man emulating a remote SSL host on one side and emulating the device (e.g., and/or network service usage activity, such as application) on the other side, decrypting the traffic, analyzing it and re-encrypting before forwarding to and from the remote host. Similarly, as in the case of layer 3 and 4 traffic analysis performed by the modem service usage counting subsystem, the layer 7 service usage count messages can be encrypted and passed to the service controller via various channels. In some embodiments, the layer 7 modem subsystem service usage counting system records service usage counts for a reporting time period that is similar to the reporting time period used by the service processor so that the service controller can correlate the service processor accounting messages against the modem accounting messages with layer 7 information.

[00237] In some embodiments, the secure service usage reporting system elements are located in a secure execution environment that includes the modem driver. In some embodiments, all traffic that gets to the modem for the network traffic being controlled or accounted for is required to go through the secure modem driver so that an independent count can be generated and reported to the service controller as described above without the need to embed the secure service usage counting and reporting elements in the modem.

[00238] In some embodiments, the secure service usage reporting system elements are located in a secure execution environment that includes the modem driver and modem hardware interface controller driver (e.g., USB controller for 2/3/4G and SDIO controller for WiFi). In some embodiments, all traffic that gets to the modem for the network traffic being controlled or accounted for is required to go through the secure modem driver and modem hardware interface controller driver (e.g., USB controller for 2/3/4G and SDIO controller for WiFi) so that precise count can be generated by either the modem driver and/or modem hardware interface controller driver (e.g., USB controller for 2/3/4G and SDIO controller for WiFi) and passed to the secure service usage reporting element to send it to the service controller for customer charging/billing. This scheme provides flexibility (e.g., most of the device software and operation system and its services/applications need not be located/executed in the secure execution environment) while ensuring usage counting to occur securely as it pertains to the customer accounting and billing.

[00239] In some embodiments, the layer 7 proxy server traffic accounting and reporting techniques used for processing HTTPS, TLS, and SSL traffic, as discussed above, are also used in the service processor itself to allow a detailed accounting of encrypted layer 7 traffic by the device. In some embodiments, the information thus obtained is filtered so that private user information is not transmitted to the network (e.g., service controller, PCRF, and/or any other network element/function) but only service usage information sufficient to allow for accounting of service plan usage, to verify service control policy implementation, or to verify service charging policy implementation is transmitted to the network (e.g., service controller, PCRF, and/or any other network element/function). In some embodiments, the layer 7 proxy server for processing secure or in the clear device service usage accounting messages is located in secure hardware execution environments in the device application processor or within secure software partitions in the operating system.

[00240] Various techniques can be used to verify and/or secure service usage controls or service usage charging reports. For example, if the secondary service usage reports indicate that service usage is outside of the service usage policy limits that are intended to be in effect (e.g., based on a service plan and/or service policy associated with the device), then the service controller can indicate an error flag for further analysis and action (e.g., implementing various verification and responsive actions as described herein, such as blocking the activity, throttling the activity, quarantining the device, updating/replacing the service processor, and/or monitoring the device using various additional DAS and/or network assisted monitoring techniques). As another example, if the service usage reports from the service processor do not match up with the secondary service usage reports, then the service controller can indicate an error flag for further analysis and action. For example, the correlation can be based on bulk measures of service usage (e.g., total bytes over a given period of time), or using finer grain measures of service usage (e.g., verifying the accounting between one group of service usage activities, such as application, destination/source, port, content type, time of day, network busy state, QoS level, and/or other criteria/measures) charged to one service plan charging record versus the accounting for another group of service usage activities charged to another service plan charging record. In some embodiments, the correlation process between the two service usage accounting reports is performed continuously on all device traffic in real time or near real time as the usage accounting reports are received. In some embodiments, the usage accounting reports are stored and analyzed or correlated later (e.g., periodically, based on a request or audit, and/or based on certain events, such as threshold network service usage events and/or any other events based on various criteria/measures). In some embodiments, only an audit of a portion of time is used to correlate the two usage accounting reports, which, for example, can reduce network traffic and/or network processing load in the service controller.

[00241] In some embodiments, correlation techniques are applied by the service controller to compare two different service usage measures as described above based on one or more of the following: total amount of data (e.g., bytes for file transfers, sessions, and/or other measures), amount of data per unit time, total number of accesses, number of accesses per unit time or frequency of accesses, accesses during a time interval (e.g., peak time), accesses during a network busy state, access requests, and individual versus group transmissions at a point in time (e.g., each for a given set of destinations or destinations and traffic types).

[00242] In some embodiments, service usage monitoring includes characterizing service usage activities by streams, flows, destination/port, packet inspection, and/or other criteria/measures using the various techniques as described herein and/or other or similar techniques as would be apparent to one of ordinary skill in the art. In some embodiments, service usage monitoring includes characterizing service usage activities by streams, flows, destination/port, packet inspection, and/or other criteria/measures and then correlating to find network service usage behavior patterns that identify likely association of behavior with one or more service activities being managed.

[00243] In some embodiments, DAS for network capacity control includes classifying traffic to determine which network service usage activity(ies) are causing traffic (e.g., increasing network capacity/resources usage beyond a threshold), and then determining if access network service usage activity(ies) are violating any rules (e.g., service usage policies or service plan settings associated with the device/user). In some embodiments, DAS for network capacity control includes generating a list for network capacity controlled services that specifies behavioral characteristics for one or more network service usage activities with expected access limits based on access control policy for each managed network service usage activity (e.g., based on service usage policies or service plan settings associated with the device/user). In some embodiments, DAS for network capacity control includes monitoring and/or controlling network service usage activities based on limits, which, for example, can be based on one or more of the following: total access traffic counters, counters for different types of access traffic, destinations, ports, frequency of accesses, access behavior during a given time, access behavior during a given busy state, access behavior for groups of activities (e.g., verify clumping), and/or other criteria/measures.

[00244] Accordingly, in some embodiments, a second secure and trusted service usage measure is provided that the service controller (e.g., or another network element/function) can use to verify or secure the service control or service charging reports for the service processor. In some embodiments, the secure and trusted service usage measure also provides for enhanced verification and service security in cases, in which, for example, network based service usage measures are available for additional correlation with the service processor service usage reports. In cases in which network based service usage measures are either not available or are only available at widely spaced time intervals (e.g., roaming networks or other networks with no

timely network based service usage measure), these techniques facilitate real time or near real time verification or security for the device assisted service controls and charging.

[00245] In some embodiments, a SIM card performs a portion or all of the secure environment processing described above, with the device modem traffic, or a copy of the device modem traffic, being directed to the SIM secure subsystem for traffic accounting and reporting. In some embodiments, a SIM card is used to store QoS classifications and/or network capacity controlled services classifications for various service usage activities so that the user behavior in using certain network service usage activities and/or the user preferences in controlling certain network service usage activities do not need to be relearned or redownloaded as the user swaps the SIM between different devices. In some embodiments, the SIM keeps a local record of service usage activity for multiple devices that belong to the user or the user family plan, so that the service usage notification and policies can be immediately updated on a given device as the user swaps the SIM from device to device. In some embodiments, the manner in which this service usage history is stored on the SIM is secure so that it cannot be tampered with. In some embodiments, the SIM card is used to implement various application management and/or traffic control techniques described herein. In some embodiments, the SIM card is used to inspect traffic, classify traffic, create reports (e.g., certified service activity usage reports), encrypt the report, send the report to a network element/function, and the network element/function correlates the reports (e.g., using network assisted measures for comparisons and/or using various other techniques as described herein). In some embodiments, a SIM card performs a portion or all of the secure environment processing described above using one or more modem measurement points. For example, the traffic that is to be classified can be routed through the SIM and correlated with what is measured by the modem. In some embodiments, network assisted/based network service usage activity classifications are compared SIM based/assisted classifications for service usage monitoring/reporting verification (e.g., detected inconsistencies in monitored/reported network service usage activities can be identified, such as based on total traffic, streams/flows/sockets activities, and/or other criteria/measures). In some embodiments, the reports include a verified sequence so that reports cannot be spoofed and/or missing reports can be determined.

[00246] In some embodiments, a portion or all of the secure environment processing described above are applied to implement and/or verify QoS for DAS techniques and/or DAS for network capacity controlled services techniques as described herein.

[00247] In some embodiments, the reports include one or more of the following: a number of times the device is cycled from or to a power cycle state in the modem, a number of times during a time window or network busy state, a power cycle versus number of streams initiated during the cycle, and a power cycle versus the streams that are transmitted during that cycle, In some embodiments, device power cycle events trigger generating of a report.

[00248] In some embodiments, monitoring, reporting, control, accounting, charging, and/or policy implementation for network capacity controlled services is verified (e.g., using various verification techniques described herein). If any of the verification techniques determine or assist in determining that the network capacity controlled services monitoring, reporting, control, accounting, and/or charging, and/or policy implementation has been tampered with, disabled, and/or is not properly implemented or functioning, then responsive actions can be performed, for example, the device (e.g., and/or suspect services) can be suspended, quarantined, killed/terminated, and/or flagged for further analysis/scrutiny to determine whether the device is malfunctioning, needs updating, has been tampered with or compromised, is infected with malware, and/or if any other problem exists.

[00249] In some embodiments, the service processor monitors a network service usage activity of a device. In some embodiments, monitoring of the service usage activity includes monitoring for multiple networks (e.g., to determine which networks are available and/or a network busy state of the available networks). In some embodiments monitoring a network service usage activity is performed by and/or assisted by a service cloud (e.g., one or more network elements that provide such a service). In some embodiments, monitoring the network service usage activity includes identifying the network service usage activity, measuring the network service usage of the network service usage activity, and/or characterizing the network service usage of the network service usage activity (e.g., using device assisted/based techniques, network assisted/based techniques, testing/offline monitoring/analysis techniques, and/or a combination thereof).

[00250] In some embodiments, the service processor implements differential network access service control (e.g., for network capacity controlled services), network service usage accounting, network service usage charging, and/or network service usage notification on the device to facilitate DAS for protecting network capacity.

[00251] In some embodiments, the service processor (e.g., a service processor 115) is updated, communicated with, set, and/or controlled by a network element (e.g., a service controller 122). In some embodiments, the service processor receives service policy information from a network function selected from a base station (e.g., a base station 125), a RAN gateway, a core gateway, a DPI gateway, a home agent (HA), a AAA server (e.g., AAA server 121), a service controller, and/or another network function or combinations of network functions as described herein and/or as will now be apparent to one of ordinary skill in the art in view of the various embodiments described herein. In some embodiments, the service processor is updated through over the air or over the network OS software updates or application software updates or device firmware updates. In some embodiments, the service processor uses an IP connection, SMS connection, and/or MMS connection, for a control channel with a service controller. In some embodiments, the service processor queries a service controller to determine the association of a monitored network service usage activity with a network service usage control policy. In some embodiments, the device (e.g., service processor) maintains a network capacity controlled services list and/or network capacity controlled services policy for one or more of the active services (e.g., actively executing and/or previously installed/downloaded to the device) that have been classified as a network capacity controlled service (e.g., as the number of applications continues to grow, as hundreds of thousands of applications are already available on certain platforms, maintaining a list specific and/or a set of policies unique or specific to each application is not efficient). In this embodiment, when a new application is active/launched and/or downloaded to the device, the device can request an updated network capacity controlled services list and/or an updated network capacity controlled services policy accordingly (e.g., and/or periodically refresh such lists/policies).

[00252] In some embodiments, differential network access control for protecting network capacity includes controlling network services traffic generated by the device (e.g., network capacity controlled services based on a network service usage control policy (e.g., a network capacity controlled services policy)). In some embodiments, differential network access control

for protecting network capacity includes providing assistance in control of the distribution of bandwidth among devices, network capacity controlled services (e.g., applications, OS operations/functions, and various other network services usage activities classified as network capacity controlled services), a differentiated QoS service offering, a fair sharing of capacity, a high user load network performance, and/or preventing one or more devices from consuming so much network capacity that other devices cannot receive adequate performance or performance in accordance with various threshold and/or guaranteed service levels. In some embodiments, differential network access control for protecting network capacity includes applying policies to determine which network the service activity should be connected to (e.g., 2G, 3G, 4G, home or roaming, WiFi, cable, DSL, fiber, wired WAN, and/or another wired or wireless or access network), and applying differential network access control rules (e.g., traffic control rules) depending on which network to which the service activity is connected. In some embodiments, differential network access control for protecting network capacity includes differentially controlling network service usage activities based on the service usage control policy and a user input (e.g., a user selection or user preference). In some embodiments, differential network access control for protecting network capacity includes differentially controlling network service usage activities based on the service usage control policy and the network the device or network service activity is gaining access from.

[00253] In some embodiments, the network service usage control policy is dynamic based on one or more of the following: a network busy state, a time of day, which network the service activity is connected to, which base station or communication channel the service activity is connected to, a user input, a user preference selection, an associated service plan, a service plan change, an application behavior, a messaging layer behavior, random back off, a power state of device, a device usage state, a time based criteria (e.g., time/day/week/month, hold/delay/defer for future time slot, hold/delay/defer for scheduled time slot, and/or hold/delay/defer until a busy state/availability state/QoS state is achieved), monitoring of user interaction with the service activity, monitoring of user interaction with the device, the state of UI priority for the service activity, monitoring the power consumption behavior of the service activity, modem power cycling or power control state changes, modem communication session set up or tear down, and/or a policy update/modification/change from the network. In some embodiments, the network service usage control policy is based on updated service usage behavior analysis of the

network service usage activity. In some embodiments, the network service usage control policy is based on updated activity behavior response to a network capacity controlled service classification. In some embodiments, the network service usage control policy is based on updated user input/preferences (e.g., related to policies/controls for network capacity controlled services). In some embodiments, the network service usage control policy is based on updates to service plan status. In some embodiments, the network service usage control policy is based on updates to service plan policies. In some embodiments, the network service usage control policy is based on availability of alternative networks. In some embodiments, the network service usage control policy is based on policy rules for selecting alternative networks. In some embodiments, the network service usage control policy is based on network busy state or availability state for alternative networks. In some embodiments, the network service usage control policy is based on specific network selection or preference policies for a given network service activity or set of network service activities.

[00254] In some embodiments, associating the network service usage activity with a network service usage control policy or a network service usage notification policy, includes dynamically associating based on one or more of the following: a network busy state, a time of day, a user input/preference, an associated service plan (e.g., 25 MB data plan, 5G data plan, or an unlimited data plan or other data/service usage plan), an application behavior, a messaging layer behavior, a power state of device, a device usage state, a time based criteria, availability of alternative networks, and a set of policy rules for selecting and/or controlling traffic on one or more of the alternative networks.

[00255] In some embodiments, a network service usage control policy (e.g., a network capacity controlled services policy) includes defining the network service usage control policy for one or more service plans, defining network access policy rules for one or more devices or groups of devices in a single or multi-user scenarios such as family and enterprise plans, defining network access policy rules for one or more users or groups of users, allowing or disallowing network access events or attempts, modulating the number of network access events or attempts, aggregating network access events or attempts into a group of access events or attempts, time windowing network access events or attempts, time windowing network access events or attempts based on the application or function being served by the network access events or attempts, time windowing network access events or attempts to pre-determined time windows,

time windowing network access events or attempts to time windows where a measure of network busy state is within a range, assigning the allowable types of access events or attempts, assigning the allowable functions or applications that are allowed network access events or attempts, assigning the priority of one or more network access events or attempts, defining the allowable duration of network access events or attempts, defining the allowable speed of network access events or attempts, defining the allowable network destinations for network access events or attempts, defining the allowable applications for network access events or attempts, defining the QoS rules for one or more network access events or attempts, defining or setting access policy rules for one or more applications, defining or setting access policy rules for one or more network destinations, defining or setting access policy rules for one or more devices, defining or setting access policy rules for one or more network services, defining or setting access policy rules for one or more traffic types, defining or setting access policy rules for one or more QoS classes, and defining or setting access policy rules based on any combination of device, application, network destination, network service, traffic type, QoS class, and/or other criteria/measures.

[00256] In some embodiments, a network service usage control policy (e.g., a network capacity controlled services policy) includes a traffic control policy. In some embodiments, the traffic control policy includes a traffic control setting. In some embodiments, the traffic control policy includes a traffic control/tier, and the traffic control/tier includes the traffic control setting. In some embodiments, the traffic control policy includes one or more of the following: block/allow settings, throttle settings, adaptive throttle settings, QoS class settings including packet error rate, jitter and delay settings, queue settings, and tag settings (e.g., for packet tagging certain traffic flows). In some embodiments, QoS class settings include one or more of the following: throttle level, priority queuing relative to other device traffic, time window parameters, and hold or delay while accumulating or aggregating traffic into a larger stream/burst/packet/group of packets. In some embodiments, the traffic control policy includes filters implemented as indexes into different lists of policy settings (e.g., using cascade filtering techniques), in which the policy filters include one or more of the following: a network, a service plan, an application, a time of day, and a network busy state. For example, a two dimensional traffic control implementation scheme can be provided using a network busy state and/or a time of day as an index into a traffic control setting (e.g., a certain application's priority

level can be increased or decreased based on a network busy state and/or time of day). In some embodiments, the traffic control policy is used for selecting the network from a list of available networks, blocking or reducing access until a connection is made to an alternative network, and/or modifying or replacing a network stack interface of the device to provide for intercept or discontinuance of network socket interface messages to applications or OS functions.

[00257] In some embodiments, a traffic control setting is selected based on the network service usage control policy. In some embodiments, the traffic control setting is implemented on the device based on the network service usage control policy. In some embodiments, the implemented traffic control setting controls traffic/traffic flows of a network capacity controlled service. In some embodiments, the traffic control setting is selected based on one or more of the following: a time of day, a day of week, a special time/date (e.g., a holiday or a network maintenance time/date), a network busy state, a priority level associated with the network service usage activity, a QoS class associated with the network service usage activity (e.g., emergency traffic), which network the network service activity is gaining access from, which networks are available, which network the network service activity is connected to, which base station or communication channel the network service activity is connected to, and a network dependent set of traffic control policies that can vary depending on which network the service activity is gaining access from (e.g., and/or various other criteria/measures as described herein). In some embodiments, the traffic control setting includes one or more of the following: allow/block, delay, throttle, QoS class implementation, queue, tag, generate a user notification, random back off, clear to send received from a network element, hold for scheduled transmission time slot, selecting the network from the available networks, and blocking or reducing access until a connection is made to an alternative network. In some embodiments, the traffic control setting is selected based on a network capacity controlled services priority state of the network service usage activity and a network busy state. In some embodiments, the traffic control setting is selected based on a network capacity controlled services priority state of the network service usage activity and a network busy state and is global (e.g., the same) for all network capacity controlled services activities or varies based on a network service usage activity priority, user preferences or option selection, an application, a time based criteria, a service plan, a network the device or service activity is gaining access from, a redetermination of a network congestion state

after adapting to a previously determined network busy state, and/or other criteria/measures as described herein.

[00258] In some embodiments, network capacity controlled services traffic (e.g., traffic flows) is differentially controlled for protecting network capacity. For example, various software updates for an OS and one or more applications on the device can be differentially controlled using the various techniques described herein. As another example, security/antimalware software (e.g., antivirus, firewall, content protection, intrusion detection/prevention, and/or other security/antimalware software) can be differentially controlled using the various techniques described herein. As yet another example, network backups/imaging, content downloads (e.g., exceeding a threshold individually and/or in aggregate, such as for image, music, video, eBook content, email attachments, content/media subscriptions, RSS/news feeds, text/image/video chat, software updates, and/or other content downloads) can be differentially controlled using the various techniques described herein.

[00259] For example, using the DAS for protecting network capacity techniques described herein an adaptive policy control for protecting network capacity can be provided. A network capacity controlled services list can be generated, updated, reported, and/or received by the device and stored on the device (e.g., the list can be based on adapted to the service plan associated with the device). If a monitored network service usage activity is not on the list, then the device can report the monitored network service usage activity to a network element (e.g., for a monitored network service usage activity that also exceeds a certain threshold, based on a network busy state, based on a time based criteria, and/or other criteria/measure). As an example, monitored network service usage activity can be reported if/when the monitored network service usage activity exceeds a data usage threshold (e.g., 50 MB total data usage per day, a socket opening frequency/rate, velocity of data usage at an instant in time, or more complicated thresholds over time, over peak periods, by content and time, by various other parameters/thresholds). As another example, the monitored network service usage activity can be reported based on testing of the network service usage behavior and/or application developer characterization input. The report can include information that identifies the network service usage activity and various network service usage parameters.

[00260] In some embodiments, a notification setting is selected based on a service usage notification policy. In some embodiments, a notification setting includes a user notification setting (e.g., various user notifications settings as described above with respect to FIG. 18).

[00261] In some embodiments, classifying the network service usage activity further includes classifying the network service usage activity (e.g., using a usage threshold filter and/or cascading filter techniques) into one or more of a plurality of classification categories for differential network access control for protecting network capacity. In some embodiments, classifying the network service usage activity further includes classifying the network service usage activity into one or more network capacity controlled services in which the network capacity controlled services include one or more of the following: applications requiring data network access, application software updates, applications requiring network information, applications requiring GPS or physical location, operating system software updates, security software updates, network based backups, email downloads, and a set of activities configured as network capacity controlled service activities based on a service profile and/or user input (e.g., and/or various other types of network service usage activities as described herein and as will now be apparent to one of ordinary skill in the art). For example, network capacity controlled services can include software updates for OS and applications, OS background network accesses, cloud synchronization services, RSS feeds and other background information feeds, browser/application/device behavior reporting, background email downloads, content subscription service updates and downloads (e.g., music/video downloads, news feeds), text/voice/video chat clients, security updates (e.g., antimalware updates), peer to peer networking application updates, inefficient network access sequences during frequent power cycling or power save state cycling, large downloads or other high bandwidth accesses, and greedy application programs that constantly/repeatedly access the network with small transmissions or requests for information. In some embodiments, a network capacity controlled services list is static, adaptive, generated using a service processor, received from a network element (e.g., service controller or service cloud), received from a network element (e.g., service controller or service cloud) and based at least in part on device activity reports received from the service processor, based on criteria set by pre-testing, report of behavior characterization performed by the application developer, and/or based at least in part on user input. In some

embodiments, the network capacity controlled services list includes one or more network service activity background (QoS) classes.

[00262] In some embodiments, classifying the network service usage activity further includes classifying the network service usage activity based on one or more of the following: application or widget (e.g., Outlook, Skype, iTunes, Android email, weather channel weather widget, iCal, Firefox Browser, etc), application type (e.g., user application, system application/utility/function/process, OS application/utility/function/process, email, browser, widget, malware (such as a virus or suspicious process), RSS feed, device synchronization service, download application, network backup/imaging application, voice/video chat, peer to peer content application or other peer to peer application, streaming media feed or broadcast reception/transmission application, network meeting application, chat application or session, and/or any other application or process identification and categorization), OS/system function (e.g., any system application/utility/function/process and/or OS application/utility/function/process, such as a OS update and/or OS error reporting), modem function, network communication function (e.g., network discovery or signaling, EtherType messages, connection flow/stream/session set up or tear down, network authentication or authorization sequences, IP address acquisition, and DNS services), URL and/or domain, destination/source IP address, protocol, traffic type, socket (e.g., IP address, protocol, and/or port), socket address/label/identifier (e.g., port address/port number), content type (e.g., email downloads, email text, video, music, eBooks, widget update streams, and download streams), port (e.g., port number), QoS classification level, time of day, on peak or off peak, network time, network busy state, access network selected, service plan selected, user preferences, device credentials, user credentials, and/or status, modem power cycling or power state changes, modem authentication processes, modem link set up or tear down, modem management communications, modem software or firmware updates, modem power management information, device power state, and modem power state. In some embodiments, classifying the network service usage activity further includes associating the classified network service usage activity with an ID (e.g., an application ID, which can be, for example, a unique number, name, and/or signature). In some embodiments, classifying the network service usage activity further includes classifying the network service usage activity using a plurality of classification parameters, including one or more of the following: application ID, remote IP (e.g., URL, domain, and/or IP address), remote

port, protocol, content type, a filter action class (e.g., network busy state class, QoS class, time of day, network busy state, and/or other criteria/measures), and access network selected. In some embodiments, classifying the network service usage activity further includes using a combination of parameters as discussed above to determine the classification of the network service usage activity.

[00263] In some embodiments, classifying the network service usage activity further includes classifying the network service usage activity as a network capacity controlled service, a non-network capacity controlled service, a blocked or disallowed service, and/or a not yet classified/identified service (e.g., unknown/yet to be determined classification or pending classification). In some embodiments, an application connection, OS connection, and/or other service activity is classified as a network capacity controlled service activity when the device has been inactive (e.g., or in a power save state) for a period of time (e.g., when the user has not interacted with it for a period of time, when it has not displayed user notification policy, and/or a user input has not been received for a period of time, and/or when a power save state is entered). In some embodiments, an application connection, OS connection, and/or other service activity is classified as a network capacity controlled service activity when the monitored network service usage activity exceeds a data usage threshold for more than one application connection, OS connection, and/or other service activity (e.g., aggregated data usage exceeds the data usage threshold); or for a specific application connection. In some embodiments, an application connection, OS connection, and/or other service activity is classified as a network capacity controlled service activity when the monitored network service usage activity exceeds a data usage threshold based on a predetermined list of one or more data usage limits, based on a list received from a network element, usage time limit (e.g., based on a period of time exceeding a usage limit), and/or based on some other usage related criteria/measures. In some embodiments, classifying the network service usage activity further includes classifying the network service usage activity as a network capacity controlled service based on a network peak time, a network busy state, or a network connection to the device falls below a certain performance level (e.g., higher/lower priorities assigned based on various such criteria/other input/factors).

[00264] In some embodiments, one or more of the network capacity controlled services are associated with a different network access policy set for one or more networks and/or one or

more alternative networks. In some embodiments, one or more of the network capacity controlled services are associated with a different notification policy set for one or more networks and/or one or more alternative networks. In some embodiments, the network capacity controlled services list is stored on the device. In some embodiments, the network capacity controlled services list is received/periodically updated from a network element and stored on the device. In some embodiments, the network capacity controlled services list includes network capacity controlled services, non-network capacity controlled services (e.g., foreground services or services based on various possibly dynamic criteria are not classified as network capacity controlled services), and an unclassified set of services (e.g., grey list including one or more network service activities pending classification based on further analysis and/or input, such as from a network element, service provider, and/or user). In some embodiments, the network capacity controlled services list is based on one or more of the following: predefined/predesignated (e.g., network, service plan, pre-test and/or characterized by an application developer) criteria; device assisted/based monitoring (e.g., using a service processor); network based monitoring (e.g., using a DPI gateway); network assisted analysis (e.g., based on device reports of DAS activity analysis). For example, the device can report device monitored network service usage activities (e.g., all monitored network service usage activities or a subset based on configuration, threshold, service plan, network, and/or user input) to the network element. As another example, the network element can update the network capacity controlled services list and send the updated list to the device. As yet another example, the network element can perform a statistical analysis of network service activities across a plurality of devices based on the device based and/or network based network service usage activity monitoring/reporting. In some embodiments, a network service usage activity is determined to be an active application or process (e.g., based on a user interaction with the device and/or network service usage activity, such as a pop-up and/or other criteria/measures).

[00265] In some embodiments, implementing traffic control for network capacity controlled services is provided using various techniques. In some embodiments, the device includes a service processor agent or function to intercept, block, modify, remove or replace UI messages, notifications or other UI communications generated by a network service activity that whose network service usage is being controlled or managed (e.g., using various measurement points as shown in and described with respect to FIGS. 12 and 13). For example, this technique

can be used to provide for an improved user experience (e.g., to prevent an application that is being controlled for protecting network capacity from generating repeated and/or confusing messages/alerts to the user). In some embodiments, a network stack interface of the device is replaced or modified to provide for intercept or discontinuance of network socket interface messages to applications or OS functions or other functions/software.

[00266] In some embodiments, implementing traffic control for network capacity controlled services using DAS techniques is provided using various techniques in which the network service usage activity is unaware of network capacity control (e.g., does not support an API or other interface for implementing network capacity control). For example, network service application messaging interface based techniques can be used to implement traffic control. Example network service application messaging interfaces include the following: network stack API, network communication stream/flow interface, network stack API messages, EtherType messages, ARP messages, and/or other messaging or other or similar techniques as will now be apparent to one of ordinary skill in the art in view of the various embodiments described herein. In some embodiments, network service usage activity control policies or network service activity messages are selected based on the set of traffic control policies or service activity messages that result in reduced or modified user notification by the service activity due to network capacity controlled service policies applied to the network service activity. In some embodiments, network service usage activity control policies or network service activity messages are selected based on the set of traffic control policies or service activity messages that result in reduced disruption of device operation due to network capacity controlled service activity policies applied to the network service activity. In some embodiments, network service usage activity control policies or network service activity messages are selected based on the set of traffic control policies or service activity messages that result in reduced disruption of network service activity operation due to network capacity controlled service activity policies applied to the network service activity. In some embodiments, implementing traffic control for network capacity controlled services is provided by intercepting opens/connects/writes. In some embodiments, implementing traffic control for network capacity controlled services is provided by intercepting stack API level or application messaging layer requests (e.g., socket open/send requests). For example, an intercepted request can be copied (e.g., to memory) and queued (e.g., delayed or throttled) or dropped (e.g.,

blocked). As another example, an intercepted request can be copied into memory and then a portion of the transmission can be retrieved from memory and reinjected (e.g., throttled). As yet another example, intercepting messaging transmissions can be parsed inline and allowed to transmit (e.g., allowed), and the transmission or a portion of the transmission can be copied to memory for classifying the traffic flow. In some embodiments, implementing traffic control for network capacity controlled services is provided by intercepting or controlling or modulating UI notifications. In some embodiments, implementing traffic control for network capacity controlled services is provided by killing or suspending the network service activity. In some embodiments, implementing traffic control for network capacity controlled services is provided by deprioritizing the process(es) associated with the service activity (e.g., CPU scheduling deprioritization).

[00267] In some embodiments, implementing traffic control for network capacity controlled services using DAS techniques for network service usage activities that are unaware of network capacity control is provided by emulating network API messaging (e.g., effectively providing a spoofed or emulated network API). For example, an emulated network API can intercept, modify, block, remove, and/or replace network socket application interface messages and/or EtherType messages (e.g., EWOULDBLOCK, ENETDOWN, ENETUNREACH, EHOSTDOWN, EHOSTUNREACH, EALREADY, EINPROGRESS, ECONNREFUSED, EINPROGRESS, ETIMEDOUT, and/or other such messages). As another example, an emulated network API can modify, swap, and/or inject network socket application interface messages (socket(), connect(), read(), write(), close(), and other such messages) that provide for control or management of network service activity service usage behavior. As yet another example, before a connection is allowed to be opened (e.g., before a socket is opened), transmission, or a flow/stream is initiated, it is blocked and a message is sent back to the application (e.g., a reset message in response to a sync request or another message that the application will understand and can interpret to indicate that the network access attempt was not allowed/blocked, that the network is not available, and/or to try again later for the requested network access). As yet another example, the socket can be allowed to open but after some point in time (e.g., based on network service usage, network busy state, time based criteria, and/or some other criteria/measure), the stream is blocked or the socket is terminated. As yet another example, time window based traffic control techniques can be implemented (e.g., during non-peak, not

network busy state times), such as by allowing network access for a period of time, blocking for a period of time, and then repeating to thereby effectively spread the network access out either randomly or deterministically. Using these techniques, an application that is unaware of network capacity control based traffic control can send and receive standard messaging, and the device can implement traffic controls based on the network capacity control policy using messaging that the network service usage activity (e.g., application or OS or software function) can understand and will respond to in a typically predictable manner as would now be apparent to one of ordinary skill in the art.

[00268] In some embodiments, implementing traffic control for network capacity controlled services using DAS techniques is provided using various techniques in which the network service usage activity is aware of network capacity control (e.g., the network service usage activity supports an API or other interface for implementing network capacity control). For example, a network access API as described herein can be used to implement traffic control for network capacity controlled services. In some embodiments, the API facilitates communication of one or more of the following: network access conditions, network busy state or network availability state of one or more networks or alternative networks, one or more network capacity controlled service policies (e.g., the network service can be of a current network access setting, such as allow/block, throttle, queue, scheduled time/time slot, and/or defer, which can be based on, for example, a current network, a current network busy state, a time based criteria, a service plan, a network service classification, and/or other criteria/measures), a network access request from a network service activity, a query/poll request to a network service activity, a network access grant to a network service activity (e.g., including a priority setting and/or network capacity controlled service classification, a scheduled time/time slot, an alternative network, and/or other criteria/measures), a network busy state or a network availability state or a network QoS state.

[00269] In some embodiments, implementing traffic control for network capacity controlled services using network assisted/based techniques is provided using various techniques in which the network service usage activity is unaware of network capacity control (e.g., does not support an API or other interface for implementing network capacity control). In some embodiments, DPI based techniques are used to control network capacity controlled services (e.g., to block or throttle network capacity controlled services at a DPI gateway).

[00270] In some embodiments, implementing traffic control for network capacity controlled services using network assisted/based techniques is provided using various techniques in which the network service usage activity is aware of network capacity control (e.g., does support an API or other interface for implementing network capacity control). In some embodiments, the application/messaging layer (e.g., a network API as described herein) is used to communicate with a network service activity to provide associated network capacity controlled service classifications and/or priorities, network busy state information or network availability of one or more networks or alternative networks, a network access request and response, and/or other criteria/measures as similarly described herein.

[00271] In some embodiments, DAS for protecting network capacity includes implementing a service plan for differential charging based on network service usage activities (e.g., including network capacity controlled services). In some embodiments, the service plan includes differential charging for network capacity controlled services. In some embodiments, the service plan includes a cap network service usage for network capacity controlled services. In some embodiments, the service plan includes a notification when the cap is exceeded. In some embodiments, the service plan includes overage charges when the cap is exceeded. In some embodiments, the service plan includes modifying charging based on user input (e.g., user override selection as described herein, in which for example, overage charges are different for network capacity controlled services and/or based on priority levels and/or based on the current access network). In some embodiments, the service plan includes time based criteria restrictions for network capacity controlled services (e.g., time of day restrictions with or without override options). In some embodiments, the service plan includes network busy state based criteria restrictions for network capacity controlled services (e.g., with or without override options). In some embodiments, the service plan provides for network service activity controls to be overridden (e.g., one time, time window, usage amount, or permanent) (e.g., differentially charge for override, differentially cap for override, override with action based UI notification option, and/or override with UI setting). In some embodiments, the service plan includes family plan or multi-user plan (e.g., different network capacity controlled service settings for different users). In some embodiments, the service plan includes multi-device plan (e.g., different network capacity controlled service settings for different devices, such as smart phone v. laptop v. net book v. eBook). In some embodiments, the service plan includes free network capacity

controlled service usage for certain times of day, network busy state(s), and/or other criteria/measures. In some embodiments, the service plan includes network dependent charging for network capacity controlled services. In some embodiments, the service plan includes network preference/prioritization for network capacity controlled services. In some embodiments, the service plan includes arbitration billing to bill a carrier partner or sponsored service partner for the access provided to a destination, application, or other network capacity controlled service. In some embodiments, the service plan includes arbitration billing to bill an application developer for the access provided to a destination, application or other network capacity controlled service.

[00272] In some application scenarios, excess network capacity demand can be caused by modem power state changes on the device. For example, when an application or OS function attempts to connect to the network for any reason when the modem is in a power save state wherein the modem is not connected to the network, it can cause the modem to change power save state, reconnect to the network, and then initiate the application network connection. In some cases, this can also cause the network to re-initiate a modem connection session (e.g., PPP session) which in addition to the network capacity consumed by the basic modem connection also consumes network resources for establishing the PPP session. Accordingly, in some embodiments, network service usage activity control policies are implemented that limit or control the ability of applications, OS functions, and/or other network service usage activities (e.g., network capacity controlled services) from changing the modem power control state or network connection state. In some embodiments, a service usage activity is prevented or limited from awakening the modem, changing the power state of the modem, or causing the modem to connect to the network until a given time window is reached. In some embodiments, the frequency a service usage activity is allowed to awakening the modem, changing the power state of the modem, or causing the modem is limited. In some embodiments, a network service usage activity is prevented from awakening the modem, changing the power state of the modem, or causing the modem until a time delay has passed. In some embodiments, a network service usage activity is prevented from awakening the modem, changing the power state of the modem, or causing the modem until multiple network service usage activities require such changes in modem state, or until network service usage activity is aggregated to increase network capacity and/or network resource utilization efficiency. In some embodiments, limiting the ability of a

network service usage activity to change the power state of a modem includes not allowing the activity to power the modem off, place the modem in sleep mode, or disconnect the modem from the network. In some embodiments, these limitations on network service usage activity to awaken the modem, change the power state of the modem, or cause the modem to connect to a network are set by a central network function (e.g., a service controller or other network element/function) policy communication to the modem. In some embodiments, these power control state policies are updated by the central network function.

[00273] FIG. 24 depicts a diagram of a network capacity protection system 2400 utilizing device-assisted services (DAS). The system 2400 includes wireless devices 2402-1 to 2402-N (referred to collectively as the wireless devices 2402), wireless networks 2404-1 to 2404-N (referred to collectively as the wireless networks 2404), a network traffic analysis engine 2406, a network service usage classification engine 2408, and a differential network access control engine 2410.

[00274] The wireless devices 2402 will at a minimum include a processor, memory (though the memory could be implemented in the processor), a radio, and a radio interface (though the radio interface could be implemented as “part of” the radio). In order to make the wireless devices 2402 useful, they will typically have at least one input device and at least one output device, including input and output interfaces, if applicable.

[00275] The wireless devices 2402 can be implemented as stations. A station, as used herein, may be referred to as a device with a media access control (MAC) address and a physical layer (PHY) interface to the wireless medium that comply with, e.g., the IEEE 802.11 standard. A station can be described as “IEEE 802.11-compliant” when compliance with the IEEE 802.11 standard is intended to be explicit. (I.e, a device acts as described in at least a portion of the IEEE 802.11 standard.) One of ordinary skill in the relevant art would understand what the IEEE 802.11 standard comprises today and that the IEEE 802.11 standard can change over time, and would be expected to apply techniques described in this paper in compliance with future versions of the IEEE 802.11 standard if an applicable change is made. IEEE Std 802.11™-2007 (Revision of IEEE Std 802.11-1999) is incorporated by reference. IEEE 802.11k-2008, IEEE 802.11n-2009, IEEE 802.11p-2010, IEEE 802.11r-2008, IEEE 802.11w-2009, and IEEE 802.11y-2008 are also incorporated by reference.

[00276] In alternative embodiments, one or more of the wireless devices 2402 may comply with some other standard or no standard at all, and may have different interfaces to a wireless or other medium. It should be noted that not all standards refer to wireless devices as “stations,” but where the term is used in this paper, it should be understood that an analogous unit will be present on all applicable wireless networks. Thus, use of the term “station” should not be construed as limiting the scope of an embodiment that describes wireless devices as stations to a standard that explicitly uses the term, unless such a limitation is appropriate in the context of the discussion.

[00277] The wireless networks 2404 will typically include an internetworking unit (IWU) that interconnects wireless devices on the relevant one of the wireless networks 2404 with another network, such as a wired LAN. The IWU is sometimes referred to as a wireless access point (WAP). In the IEEE 802.11 standard, a WAP is also defined as a station. Thus, a station can be a non-WAP station or a WAP station. In a cellular network, the WAP is often referred to as a base station.

[00278] The wireless networks 2404 can be implemented using any applicable technology, which can differ by network type or in other ways. The wireless networks 2404 can be of any appropriate size (e.g., metropolitan area network (MAN), personal area network (PAN), etc.). Broadband wireless MANs may or may not be compliant with IEEE 802.16, which is incorporated by reference. Wireless PANs may or may not be compliant with IEEE 802.15, which is incorporated by reference. The wireless networks 2404 can be identifiable by network type (e.g., 2G, 3G, WiFi), service provider, WAP/base station identifier (e.g., WiFi SSID, base station and sector ID), geographic location, or other identification criteria.

[00279] The wireless networks 2404 may or may not be coupled together via an intermediate network. The intermediate network can include practically any type of communications network, such as, by way of example but not limitation, the Internet, a public switched telephone network (PSTN), or an infrastructure network (e.g., private LAN). The term “Internet” as used herein refers to a network of networks which uses certain protocols, such as the TCP/IP protocol, and possibly other protocols such as the hypertext transfer protocol (HTTP) for hypertext markup language (HTML) documents that make up the World Wide Web (the web).

[00280] In the example of FIG. 24, the network traffic analysis engine 2406 is coupled to the wireless device 2402-1. In a specific implementation, the network traffic analysis engine 2406 is implemented on a server and is coupled to the wireless device 2402-1 through the Internet. However, at least a portion of the network traffic analysis engine 2406 can alternatively be implemented on the wireless device 2402-1, with or without a connection to a server that includes another portion (e.g., a server portion) of the network traffic analysis engine 2406.

[00281] As used in this paper, an engine includes a dedicated or shared processor and, typically, firmware or software modules that are executed by the processor. Depending upon implementation-specific or other considerations, an engine can be centralized or its functionality distributed. An engine can include special purpose hardware, firmware, or software embodied in a computer-readable medium for execution by the processor. As used in this paper, a computer-readable medium is intended to include all mediums that are statutory (e.g., in the United States, under 35 U.S.C. 101), and to specifically exclude all mediums that are non-statutory in nature to the extent that the exclusion is necessary for a claim that includes the computer-readable medium to be valid. Known statutory computer-readable mediums include hardware (e.g., registers, random access memory (RAM), non-volatile (NV) storage, to name a few), but may or may not be limited to hardware.

[00282] The network traffic analysis engine 2406 analyzes a subset of traffic between the wireless device 2402-1 and a source or destination. The analyzed traffic may or may not be limited to a network segment, such as between a cellular phone and a base station. The network traffic analysis engine 2406 can analyze traffic for a subset of devices in the wireless network 2404-1 service area. The analyzed traffic may or may not be limited to subscribers.

[00283] In the example of FIG. 24, the network service usage classification engine 2408 is coupled to the network traffic analysis engine 2406. In a specific implementation, the network service usage classification engine 2408 is implemented on a server, which may or may not be the same server on which the network traffic analysis engine 2406 is implemented. However, at least a portion of the network service usage classification engine 2408 can alternatively be implemented on the wireless device 2402-1, with or without a connection to a server that includes another portion (e.g., a server portion) of the network service usage classification engine 2408.

[00284] The network service usage classification engine 2408 can categorize traffic based upon the service class (e.g., conversational, streaming, interactive, background, or some other service class) requested or needed for a service. The categorization facilitates identification of a snapshot of service class use at a given time, and, in some implementations, predictions of future service class use based upon the snapshot (e.g., making an assumption that future service class use is at least somewhat related to service class use of the snapshot), historical data analysis (e.g., service class usage at certain times of day/days of the week), identification of trends, or the use of some other predictive technology.

[00285] In the example of FIG. 24, the differential network access control engine 2410 is coupled to the network service usage classification engine 2408. In a specific implementation, the network access control engine 2410 is implemented on a server, which may or may not be the same server on which the network traffic analysis engine 2406 and/or the network service usage classification engine 2408 are implemented. However, at least a portion of the network access control engine 2410 can alternatively be implemented on the wireless device 2402-1, with or without a connection to a server that includes another portion (e.g., a server portion) of the network access control engine 2410.

[00286] The differential network access control engine 2410 uses the predicted service class use from the network service usage classification engine 2408 to dynamically adjust resources allocated to service classes. For example, the differential network access control engine 2410 can perform a service class availability assessment to determine whether service class capacity for service classes on a channel is sufficient for predicted service usage, and either add resources if service class availability is insufficient for predicted service usage or reduce resources if service class availability is more than sufficient for predicted service usage.

[00287] Alternatively, the differential network access control engine 2410 can instead or in addition control applications on devices such that the applications change service usage levels or delay consumption of wireless resources (e.g., by delaying software updates until more resources become available). In an embodiment, a service usage control policy is implemented on the wireless device 2402-1. This may be necessary in some cases to ensure the wireless device 2402-1 can adjust application settings that are normally fixed, optimize network service usage activation based on network state (e.g., if the network is busy), control over-the-air

software updates, throttle resource-hungry applications, manage network service usage requests from repeated power down modes, keep PPP sessions active, or otherwise facilitate dynamic service class adjustments or other device behavior.

[00288] In a specific implementation, subscribers can be incented to change service classes by, for example, charging more for higher service classes. The differential network access control engine 2410 can send a notification of differential charges for service classes. Alternatively, the charges could be implemented via subscriber account settings or preferences.

[00289] In the example of FIG. 24, in operation, the network traffic analysis engine 2406 analyzes traffic from one or more devices, including the wireless device 2402-1. The network service usage classification engine 2408 predicts the amount of resources needed for service classes, and the differential network access control engine 2410 dynamically allocates resources on an as-needed basis to adjust the service classes that are available to the one or more devices and/or adjusts device behavior for a subset of the one or more devices or instructs a subset of the one or more devices to adjust device behavior such that the device consumes service class-specific resources in accordance with an access control policy appropriate for the resources allocated to the applicable service classes.

[00290] FIG. 25 depicts a diagram an example of a differential access control notification system 2500. In the example of FIG. 25, the system 2500 includes a network service usage analysis engine 2502, a network service usage classification engine 2504, a differential network access control engine 2506, a network service usage control policy datastore 2508, a network service usage notification engine 2510, a user interface 2512, and a service plan update engine 2514.

[00291] In the example of FIG. 25, the network service usage analysis engine 2502 analyzes network service usage activity. The analysis can include an analysis of traffic sent to or from a device, an application running on a device, a request for services, or other analysis that is informative of past, current, or future network service usage. For example, the network service usage activity can include an attempt to download or load an application onto the communications device, an attempt to execute the network service activity or the network service usage activity attempts to access the network, meeting or exceeding a network service usage threshold, satisfying a network service usage pre-condition, an update to a network capacity

controlled service activity classification list, an update to a network capacity controlled services policy, and a network message is sent to the device triggering the notification, to name several by way of example. The analysis can occur on a non-WAP station, a WAP or base station, a server, or partly on one of these devices or some other device.

[00292] In the example of FIG. 25, the network service usage classification engine 2504 is coupled to the network service usage analysis engine 2502. The network service usage classification engine 2504 classifies the analyzed network service usage into one or more service classes. The classification can occur on a non-WAP station, a WAP or base station, a server, or partly on one of these devices or some other device.

[00293] In the example of FIG. 25, the differential network access control engine 2506 is coupled to the network service usage classification engine 2504. The differential network access control engine 2506 determines network access parameters using the service classes associated with the network service usage activity and network service usage control policies stored in the network service usage control policy datastore 2508. The determination can occur on a non-WAP station, a WAP or base station, a server, or partly on one of these devices or some other device. The network service usage control policy datastore 2508 can be implemented on a wireless device, but it is also possible to maintain the datastore remotely relative to the device (e.g., on a server). In a specific implementation, even if the network service usage control policy datastore 2508 is maintained remotely relative to the wireless device, the wireless device will still have a network service usage control policy implemented.

[00294] A datastore can be implemented, for example, as software embodied in a physical computer-readable medium on a general- or specific-purpose machine, in firmware, in hardware, in a combination thereof, or in an applicable known or convenient device or system. Datastores in this paper are intended to include any organization of data, including tables, comma-separated values (CSV) files, traditional databases (e.g., SQL), or other applicable known or convenient organizational formats. Datastore-associated components, such as database interfaces, can be considered “part of” a datastore, part of some other system component, or a combination thereof, though the physical location and other characteristics of datastore-associated components is not critical for an understanding of the techniques described in this paper.

[00295] Datastores can include data structures. As used in this paper, a data structure is associated with a particular way of storing and organizing data in a computer so that it can be used efficiently within a given context. Data structures are generally based on the ability of a computer to fetch and store data at any place in its memory, specified by an address, a bit string that can be itself stored in memory and manipulated by the program. Thus some data structures are based on computing the addresses of data items with arithmetic operations; while other data structures are based on storing addresses of data items within the structure itself. Many data structures use both principles, sometimes combined in non-trivial ways. The implementation of a data structure usually entails writing a set of procedures that create and manipulate instances of that structure.

[00296] In the example of FIG. 25, the network service usage notification engine 2510 is coupled to the differential network access control engine 2506 and the network service usage control policy datastore 2508. The network service usage notification engine 2510 is configured to generate a notification sufficient to indicate relevant access control information. For example, the notification could indicate what network service usage activities are network capacity controlled services, the type of network service policy in effect for one or more network capacity controlled services, that a network service activity belongs to a network capacity controlled services classification, that a service activity that is classified as network capacity controlled services classification can have the classification changed, that if the service class is changed for the network service activity that the associated network service usage charges will change, a service plan upgrade/downgrade offer, and an offer for a service plan that provides discounts and/or incentives for responding to one or more user notifications for protecting network capacity, to name several by way of example.

[00297] The notification may or may not also include a user preference selection. For example, the notification could include a provision to associate a network service usage control policy with the network service usage activity, an over-ride option for selecting the network service usage control policy, a modify option to select the service usage control policy, and a select option to select a new service plan, to name several by way of example. Other examples include network service usage activity information for one or more network capacity controlled services, predicted network service usage activity information for one or more network capacity controlled services, an option for obtaining more information about the network service usage of

the network service usage activity, a message that the network service usage activity may result in network service usage that exceeds a threshold for a service plan associated with the device, an option to review or select an alternative service plan, an acknowledgement request, and an option to submit the acknowledgement request, to name several more by way of example.

[00298] In the example of FIG. 25, the user interface 2512 is coupled to the network service usage notification engine 2510. It may be noted that notifications can be disposed of by consulting user preferences (e.g., when a user indicates that maximum performance or minimum cost should be automatically selected). However, unless subscriber preferences are set as a default, a user is likely to have notifications displayed in the UI 2512. The notification can be in an applicable known or convenient form, such as SMS, email, a popup window, or the like. To the extent a response is permitted, a user can input a response to the notification using an input device (not shown).

[00299] In the example of FIG. 25, the service plan update engine 2514 is coupled to the UI 2512. As was previously mentioned, the UI can be bypassed because of, e.g., user preferences that are determinative of a selection provided in the notification. Regardless of how the selection associated with the notification is made, the service plan update engine 2514 can update a service plan, network service usage control policy, user preferences, or other parameters in accordance with the selection. The service plan update engine 2514 can also update accounting if costs accrue.

[00300] FIG. 26 depicts an example of a computer system 2600 on which techniques described in this paper can be implemented. The computer system 2600 may be a conventional computer system that can be used as a client computer system, such as a wireless client or a workstation, or a server computer system. The computer system 2600 includes a computer 2602, I/O devices 2604, and a display device 2606. The computer 2602 includes a processor 2608, a communications interface 2610, memory 2612, display controller 2614, non-volatile storage 2616, and I/O controller 2618. The computer 2602 may be coupled to or include the I/O devices 2604 and display device 2606.

[00301] The computer 2602 interfaces to external systems through the communications interface 2610, which may include a modem or network interface. It will be appreciated that the communications interface 2610 can be considered to be part of the computer system 2600 or a

part of the computer 2602. The communications interface 2610 can be an analog modem, ISDN modem, cable modem, token ring interface, satellite transmission interface (e.g., “direct PC”), or other interfaces for coupling a computer system to other computer systems.

[00302] The processor 2608 may be, for example, a conventional microprocessor such as an Intel Pentium microprocessor or Motorola power PC microprocessor. The memory 2612 is coupled to the processor 2608 by a bus 2670. The memory 2612 can be Dynamic Random Access Memory (DRAM) and can also include Static RAM (SRAM). The bus 2670 couples the processor 2608 to the memory 2612, also to the non-volatile storage 2616, to the display controller 2614, and to the I/O controller 2618.

[00303] The I/O devices 2604 can include a keyboard, disk drives, printers, a scanner, and other input and output devices, including a mouse or other pointing device. The display controller 2614 may control in the conventional manner a display on the display device 2606, which can be, for example, a cathode ray tube (CRT) or liquid crystal display (LCD). The display controller 2614 and the I/O controller 2618 can be implemented with conventional well known technology.

[00304] The non-volatile storage 2616 is often a magnetic hard disk, an optical disk, or another form of storage for large amounts of data. Some of this data is often written, by a direct memory access process, into memory 2612 during execution of software in the computer 2602. One of skill in the art will immediately recognize that the terms “machine-readable medium” or “computer-readable medium” includes any type of storage device that is accessible by the processor 2608 and also encompasses a carrier wave that encodes a data signal.

[00305] The computer system 2600 is one example of many possible computer systems which have different architectures. For example, personal computers based on an Intel microprocessor often have multiple buses, one of which can be an I/O bus for the peripherals and one that directly connects the processor 2608 and the memory 2612 (often referred to as a memory bus). The buses are connected together through bridge components that perform any necessary translation due to differing bus protocols.

[00306] Network computers are another type of computer system that can be used in conjunction with the teachings provided herein. Network computers do not usually include a hard disk or other mass storage, and the executable programs are loaded from a network

connection into the memory 2612 for execution by the processor 2608. A Web TV system, which is known in the art, is also considered to be a computer system, but it may lack some of the features shown in FIG. 26, such as certain input or output devices. A typical computer system will usually include at least a processor, memory, and a bus coupling the memory to the processor.

[00307] In addition, the computer system 2600 is controlled by operating system software which includes a file management system, such as a disk operating system, which is part of the operating system software. One example of operating system software with its associated file management system software is the family of operating systems known as Windows® from Microsoft Corporation of Redmond, Washington, and their associated file management systems. Another example of operating system software with its associated file management system software is the Linux operating system and its associated file management system. The file management system is typically stored in the non-volatile storage 2616 and causes the processor 2608 to execute the various acts required by the operating system to input and output data and to store data in memory, including storing files on the non-volatile storage 2616.

[00308] FIG. 27 depicts a diagram of an example of a system 2700 for application-specific differential network access control. In the example of FIG. 27, the system 2700 includes a network service consuming application 2702, a network service usage analysis engine 2704, an application behavior datastore 2706, a network service usage classification engine 2708, an application traffic prioritization engine 2710, a network service usage control policy datastore 2712, a differential network access control engine 2714, an application traffic cache 2716, an application traffic override engine 2718, and a network interface 2720. The system 2700 is intended to represent a specific implementation of techniques described previously in this paper for illustrative purposes. The techniques may be applicable to an applicable known or convenient (wired or wireless) device for which there is a motivation to control network service usage.

[00309] In the example of FIG. 27, the network service consuming application 2702 is a application that is implemented on a device. In an expected use, the application is a software application stored at least in part in memory on a wireless device, though kernel-level instructions could be implemented as firmware or even hardware. The application can be

referred to as “running” on the device or as being “executed” by the device in accordance with known uses of those terms. Wireless media are known to have more bandwidth constraints, which is why a wireless device is an expected use, though the technique may be applicable to wired devices in certain situations.

[00310] In the example of FIG. 27, the network service usage analysis engine 2704 is coupled to the network service consuming application 2702. The network service usage analysis engine 2704 analyzes traffic from the network service consuming application 2702 and stores relevant data in the application behavior datastore 2706. The data can include all traffic that is sent by the application, or a subset of the traffic (e.g., that which has a certain QoS classification or priority, that which has high resource consumption due to frequent transmission from the application, that which is sent to a particular destination, etc.) The data can also include traffic that is received for the application. The application behavior datastore 2706 can alternatively or in addition be implemented as a traffic source/destination datastore, which can be valuable if differential access control is based upon the source and/or destination of traffic. The application behavior datastore 2706 includes data structures (e.g., records) representative of data that is organized with implementation-specific granularity. For example, the data structures could be representative of frames (L2), packets (L3), or messages. (It may be noted that the term “packets” is often used to mean collections of data that are not limited to L3.) The desired granularity may depend upon where the network service usage analysis engine 2704 is located. Whether the data structures are changed over time (e.g., to change data associated with a record), replaced as records age, or maintained as historical data is also implementation-specific.

[00311] In the example of FIG. 27, the network service usage classification engine 2708 is coupled to the network service usage analysis engine 2704 and the application behavior datastore 2706. The network service usage classification engine 2708 can categorize the traffic stored in the application behavior datastore 2706 based on, e.g., network type, time of day, connection cost, whether home or roaming, network busy state, QoS, and whether the particular service usage activity is in foreground of user interaction or in the background of user interaction, or other characteristics that are obtained from network service usage analysis or through other means. Classification rules can include, for example, examining if one or more of the following has taken place within a specified period of time: user has interacted with the device, user has interacted with the service usage activity, user has picked up the device, service usage activity UI

content is in the foreground of the device UI, audio or video information is being played by the service usage activity, a certain amount of data has been communicated by the service usage activity, service usage activity is or is not on a foreground or background service list. Rules that define which service usage activities to classify as, e.g., background service usage activities can be user-selected, set by a service provider, or through some other applicable means.

[00312] Advantageously, the network service usage analysis engine 2704 can examine a particular service usage activity and the network service usage classification engine 2708 can determine if the particular service usage activity fits a set of one or more classification rules that define the particular service usage activity as, e.g., a background service usage activity.

[00313] In the example of FIG. 27, the application traffic prioritization engine 2710 uses a policy stored in the network service usage control policy datastore 2712 to determine an appropriate prioritization for traffic to and/or from the network service consuming application 2702. Prioritization can enable the system 2700 to fine-tune the amount of network resources consumed by the network service consuming application 2702, or the rate of network resource consumption. The control policy can require applications to throttle network resource consumption, prohibit the use of network resources by certain applications, etc.

[00314] Advantageously, the application traffic prioritization engine 2710 can determine a particular service usage activity has a particular characteristic, such as being a background service usage activity. This can involve checking whether a condition is satisfied.

[00315] In the example of FIG. 27, the differential network access control engine 2714 is coupled to the application traffic prioritization engine 2710 and the network service usage control policy datastore 2712. The differential network access control engine 2714 causes the network service consuming application 2702 traffic to be queued in the application traffic cache 2716. (If no throttling is required to follow the control policy, of course, the traffic need not be cached anywhere other than is typical, such as in an output buffer.) The application traffic cache 2716 is intended to represent a cache that is implemented on top of an output buffer or other standard caching device, and is used by the differential network access control engine 2714 to facilitate control over “rogue” applications, applications having anomalous behavior, or applications that must otherwise be controlled to conform with the control policy.

[00316] Advantageously, the differential network access control engine can restrict network access of a particular service usage activity when a condition is satisfied, such as when the service usage activity is a background activity.

[00317] In the example of FIG. 27, the application traffic override engine 2718 is coupled to the differential network access control engine 2714 and the application traffic cache 2716. The application traffic override engine 2718 enables a user or device to deviate from the control policy. Such deviation can be prompted by, for example, an incentive offer or a notification of cost.

[00318] In an illustrative example, the device 2700 blocks chatter for an application running in the background that is attempting to report device or user behavior. The application traffic prioritization engine 2710 determines that the chatter has zero priority, such that the network service consuming application 2702 is prevented from consuming any resources. The user can be sent a notification by the application traffic override engine 2718 that their control policy prohibits the application from consuming network resources, but that the user can opt to deviate from the control policy if they are willing to pay for the consumed resources. If the user is willing to pay for the resources, traffic can be sent at a certain rate from the application traffic cache 2716 through the network interface 2720, or perhaps sent without using the application traffic cache 2716.

[00319] As another illustrative example, the device 2700 could identify application traffic as a software update. The differential network access control engine 2714 may determine that software updates can be received at a throttled rate (perhaps even slower than the lowest QoS categorization). The application traffic override engine 2718 can receive an indication from the user, from user preferences, service provider settings, or the like that the updates can ignore the control policy for a particular application (or for all applications).

[00320] Advantageously, the control policy can set up a priority to communicate cached elements, set minimum update frequencies, provide control policy overrides (typically for payment), or the like to fine-tune differential network access control policies. This can enable the system 2700 to encourage certain behavior, such as sending low QoS traffic when it is cheaper (e.g., when the network does not have a busy state, at historically low-use times of day, when on a certain type of network, such as Wi-Fi, as opposed to another, such as cellular, etc.).

[00321] Some portions of the detailed description are presented in terms of algorithms and symbolic representations of operations on data bits within a computer memory. These algorithmic descriptions and representations are the means used by those skilled in the data processing arts to most effectively convey the substance of their work to others skilled in the art. An algorithm is here, and generally, conceived to be a self-consistent sequence of operations leading to a desired result. The operations are those requiring physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical or magnetic signals capable of being stored, transferred, combined, compared, and otherwise manipulated. It has proven convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers, or the like.

[00322] It should be borne in mind, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities. Unless specifically stated otherwise as apparent from the following discussion, it is appreciated that throughout the description, discussions utilizing terms such as “processing” or “computing” or “calculating” or “determining” or “displaying” or the like, refer to the action and processes of a computer system, or similar electronic computing device, that manipulates and transforms data represented as physical (electronic) quantities within the computer system's registers and memories into other data similarly represented as physical quantities within the computer system memories or registers or other such information storage, transmission or display devices.

[00323] The present invention, in some embodiments, also relates to apparatus for performing the operations herein. This apparatus may be specially constructed for the required purposes, or it may comprise a general purpose computer selectively activated or reconfigured by a computer program stored in the computer. Such a computer program may be stored in a computer readable storage medium, such as, but is not limited to, read-only memories (ROMs), random access memories (RAMs), EPROMs, EEPROMs, magnetic or optical cards, any type of disk including floppy disks, optical disks, CD-ROMs, and magnetic-optical disks, or any type of media suitable for storing electronic instructions, and each coupled to a computer system bus.

[00324] The algorithms and displays presented herein are not inherently related to any particular computer or other apparatus. Various general purpose systems may be used with

programs in accordance with the teachings herein, or it may prove convenient to construct more specialized apparatus to perform the required method steps. The required structure for a variety of these systems will appear from the description below. In addition, the present invention is not described with reference to any particular programming language, and various embodiments may thus be implemented using a variety of programming languages.

[00325] 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.

INCORPORATION BY REFERENCE

[00326] This application incorporates by reference the following U.S. Patent Applications for all purposes: U.S. serial No. 14/082,040, filed November 15, 2013, entitled “Device-Assisted Services for Protecting Network Capacity,” U.S. serial No. 13/134,028, filed May 25, 2011, entitled “Device-Assisted Services for Protecting Network Capacity,” U.S. serial No. 12/380,759 filed March 2, 2009, entitled “Verifiable Device Assisted Service Policy Implementation,” U.S. serial No. 12/380,779 filed March 2, 2009, entitled “Device Assisted Service Profile Management with User Preference, Adaptive Policy, Network Neutrality, and User Privacy,” U.S. serial No. 12/380,758 filed March 2, 2009, entitled “Verifiable Device Assisted Service Usage Monitoring with Reporting, Synchronization, and Notification,” U.S. serial No. 12/380,778 filed March 2, 2009, entitled “Verifiable Device Assisted Service Usage Billing with Integrated Accounting, Mediation Accounting, and Multi-Account,” U.S. serial No. 12/380,768 filed March 2, 2009, entitled “Network Based Service Policy Implementation with Network Neutrality and User Privacy,” U.S. serial No. 12/380,767 filed March 2, 2009, entitled “Network Based Service Profile Management with User Preference, Adaptive Policy, Network Neutrality and User Privacy,” U.S. serial No. 12/380,780 filed March 2, 2009, entitled “Automated Device Provisioning and Activation,” U.S. serial No. 12/380,755 filed March 2, 2009, entitled “Device Assisted Ambient Services,” U.S. serial No. 12/380,756 filed March 2, 2009, entitled “Network Based Ambient Services,” U.S. serial No. 12/380,770 filed March 2, 2009, entitled “Network Tools for Analysis, Design, Testing, and Production of Services,” U.S. serial No. 12/380,772 filed March 2, 2009, entitled “Roaming Services Network and Overlay Networks,” U.S. serial No. 12/380,782 filed March 2, 2009, entitled “Open Development System for Access Service Providers,” U.S. serial No. 12/380,783 filed March 2, 2009, entitled “Virtual Service Provider Systems,” U.S. serial No. 12/380,757 filed March 2, 2009, entitled “Service Activation Tracking System,” U.S. serial No. 12/380,781 filed March 2, 2009, entitled “Open Transaction Central Billing System,” U.S. serial No. 12/380,774 filed March 2, 2009, entitled “Verifiable and Accurate Service Usage Monitoring for Intermediate Networking Devices,” U.S. serial No. 12/380,771 filed March 2, 2009, entitled “Verifiable Service Billing for Intermediate Networking Devices,” U.S. serial No. 12/380,773 filed March 2, 2009, entitled “Verifiable Service Policy Implementation for Intermediate Networking Devices,” U.S. serial No. 12/380,769 filed March 2, 2009, entitled “Service Profile Management with User Preference, Adaptive Policy, Network

Neutrality and User Privacy for Intermediate Networking Devices;" U.S. serial No. 12/380,777 filed March 2, 2009, entitled "Simplified Service Network Architecture;" U.S. serial No. 12/695,019 filed January 27, 2010, entitled "Device Assisted CDR Creation, Aggregation, Mediation and Billing;" U.S. serial No. 12/695,020 filed January 27, 2010, entitled "Adaptive Ambient Services;" U.S. serial No. 12/694,445 filed January 27, 2010, entitled "Security Techniques for Device Assisted Services;" U.S. serial No. 12/694,451 filed January 27, 2010, entitled "Device Group Partitions and Settlement Platform;" U.S. serial No. 12/694,455 filed January 27, 2010, entitled "Device Assisted Services Install;" U.S. serial No. 12/695,021 filed January 27, 2010, entitled "Quality of Service for Device Assisted Services;" U.S. serial No. 12/695,980 filed January 28, 2010, entitled "Enhanced Roaming Services and Converged Carrier Networks with Device Assisted Services and a Proxy;" and U.S. application serial No. 13/134,005, filed May 25, 2011, entitled "System and Method for Wireless Network Offloading,"

[00327] This application also incorporates by reference the following U.S. provisional applications: U.S. provisional application serial No. 61/206,354, filed January 28, 2009, entitled "Services Policy Communication System and Method;" U.S. provisional application serial No. 61/206,944, filed February 4, 2009, entitled "Services Policy Communication System and Method;" U.S. provisional application serial No. 61/207,393, filed February 10, 2009, entitled "Services Policy Communication System and Method;" U.S. provisional application serial No. 61/207,739, filed February 13, 2009, entitled "Services Policy Communication System and Method;" U.S. provisional application serial No. 61/270,353, filed July 6, 2009, entitled "Device Assisted CDR Creation, Aggregation, Mediation and Billing;" U.S. provisional application serial No. 61/275,208, filed August 25, 2009, entitled "Adaptive Ambient Services;" U.S. provisional application serial No. 61/237,753, filed August 28, 2009, entitled "Adaptive Ambient Services;" U.S. provisional application serial No. 61/252,151, filed October 15, 2009, entitled "Security Techniques for Device Assisted Services;" U.S. provisional application serial No. 61/252,153, filed October 15, 2009, entitled "Device Group Partitions and Settlement Platform;" U.S. provisional application serial No. 61/264,120, filed November 24, 2009, entitled "Device Assisted Services Install," and U.S. provisional application serial No. 61/264,126, filed November 24, 2009, entitled "Device Assisted Services Activity Map;" U.S. provisional application serial No. 61/348,022, filed May 25, 2010, entitled "Device Assisted Services for

Protecting Network Capacity;" U.S. provisional application serial No. 61/381,159, filed September 9, 2010, entitled "Device Assisted Services for Protecting Network Capacity;" U.S. provisional application serial No. 61/381,162, filed September 9, 2010, entitled "Service Controller Interfaces and Workflows;" U.S. provisional application serial No. 61/384,456, filed September 20, 2010, entitled "Securing Service Processor with Sponsored SIMs;" U.S. provisional application serial No. 61/389,547, filed October 4, 2010, entitled "User Notifications for Device Assisted Services;" U.S. provisional application serial No. 61/385,020, filed September 21, 2010, entitled "Service Usage Reconciliation System Overview;" U.S. provisional application serial No. 61/387,243, filed September 28, 2010, entitled "Enterprise and Consumer Billing Allocation for Wireless Communication Device Service Usage Activities;" U.S. provisional application serial No. 61/387,247, filed September 28, 2010, entitled "Secured Device Data Records;" U.S. provisional application serial No. 61/407,358, filed October 27, 2010, entitled "Service Controller and Service Processor Architecture;" U.S. provisional application serial No. 61/418,507, filed December 1, 2010, entitled "Application Service Provider Interface System;" U.S. provisional application serial No. 61/418,509, filed December 1, 2010, entitled "Service Usage Reporting Reconciliation and Fraud Detection for Device Assisted Services;" U.S. provisional application serial No. 61/420,727, filed December 7, 2010, entitled "Secure Device Data Records;" U.S. provisional application serial No. 61/422,565, filed December 13, 2010, entitled "Service Design Center for Device Assisted Services;" U.S. provisional application serial No. 61/422,572, filed December 13, 2010, entitled "System Interfaces and Workflows for Device Assisted Services;" U.S. provisional application serial No. 61/422,574, filed December 13, 2010, entitled "Security and Fraud Detection for Device Assisted Services;" U.S. provisional application serial No. 61/435,564, filed January 24, 2011, entitled "Framework for Device Assisted Services;" and U.S. provisional application serial No. 61/472,606, filed April 6, 2011, entitled "Managing Service User Discovery and Service Launch Object Placement on a Device."

CLAIMS

We claim:

1. A system, comprising:

a processor of a communications device configured to:

monitor a network service usage activity of the communications device in network communication;

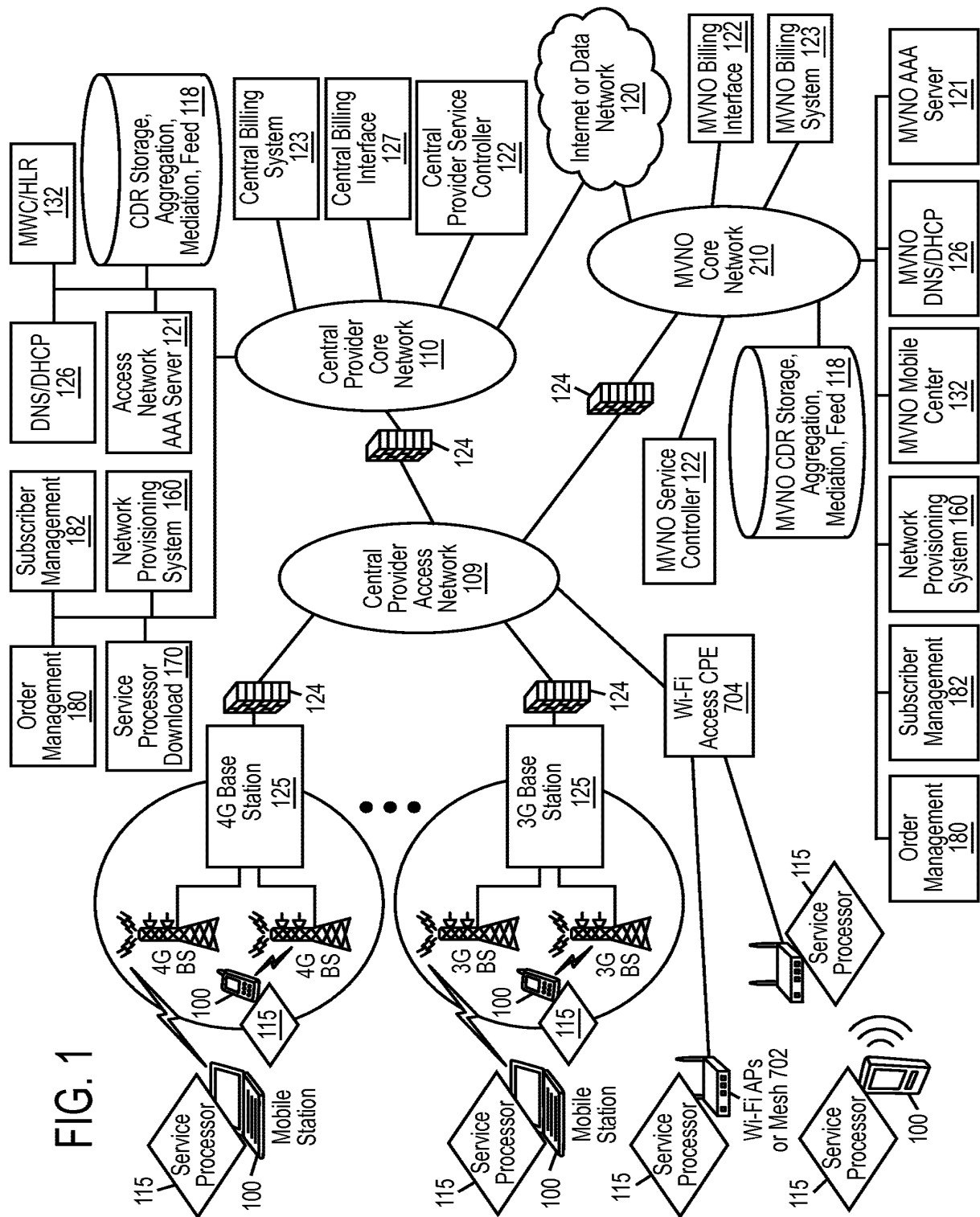
classify the network service usage activity for differential network access control for protecting network capacity; and

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

a memory coupled to the processor and configured to provide the processor with instructions.

ABSTRACT

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



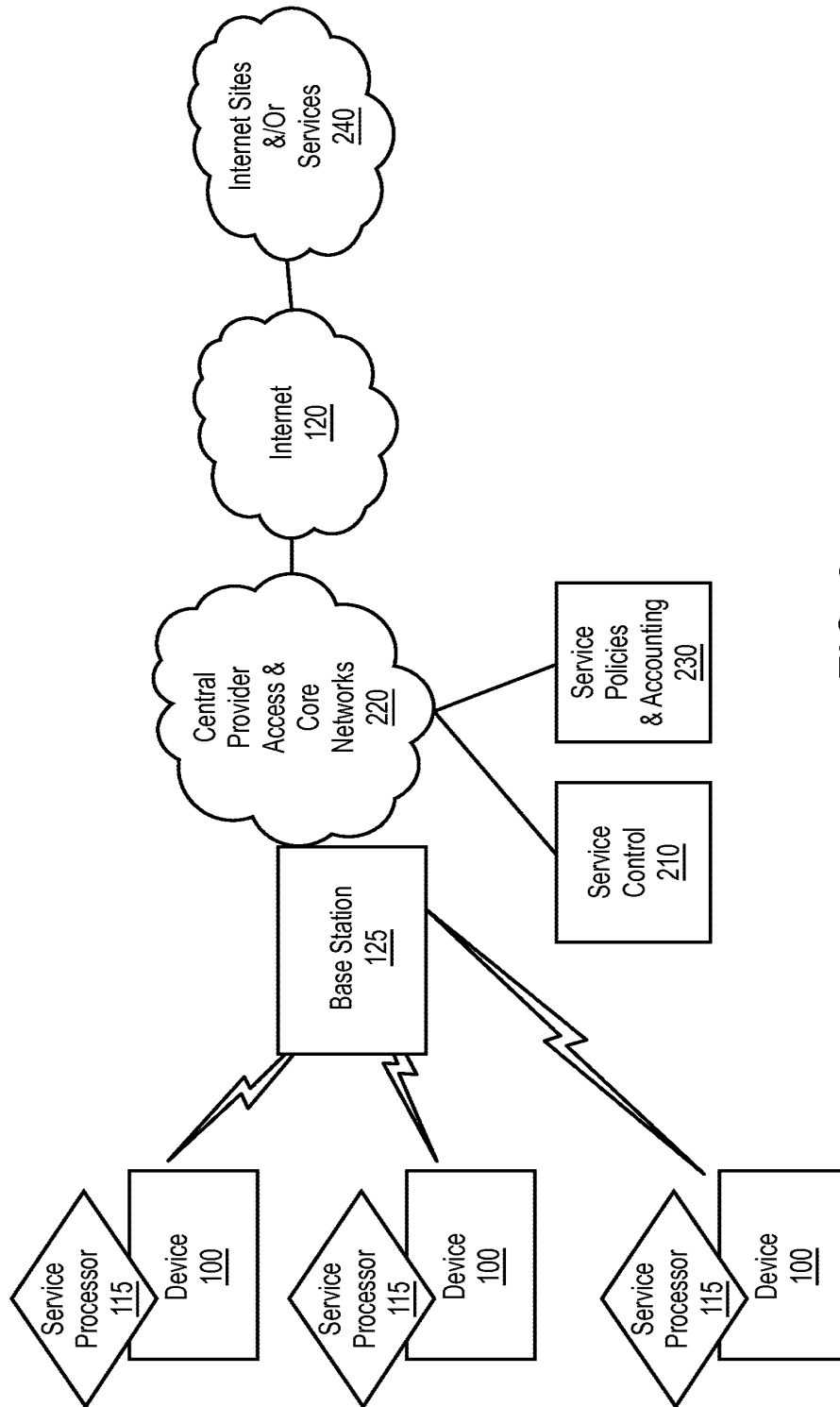
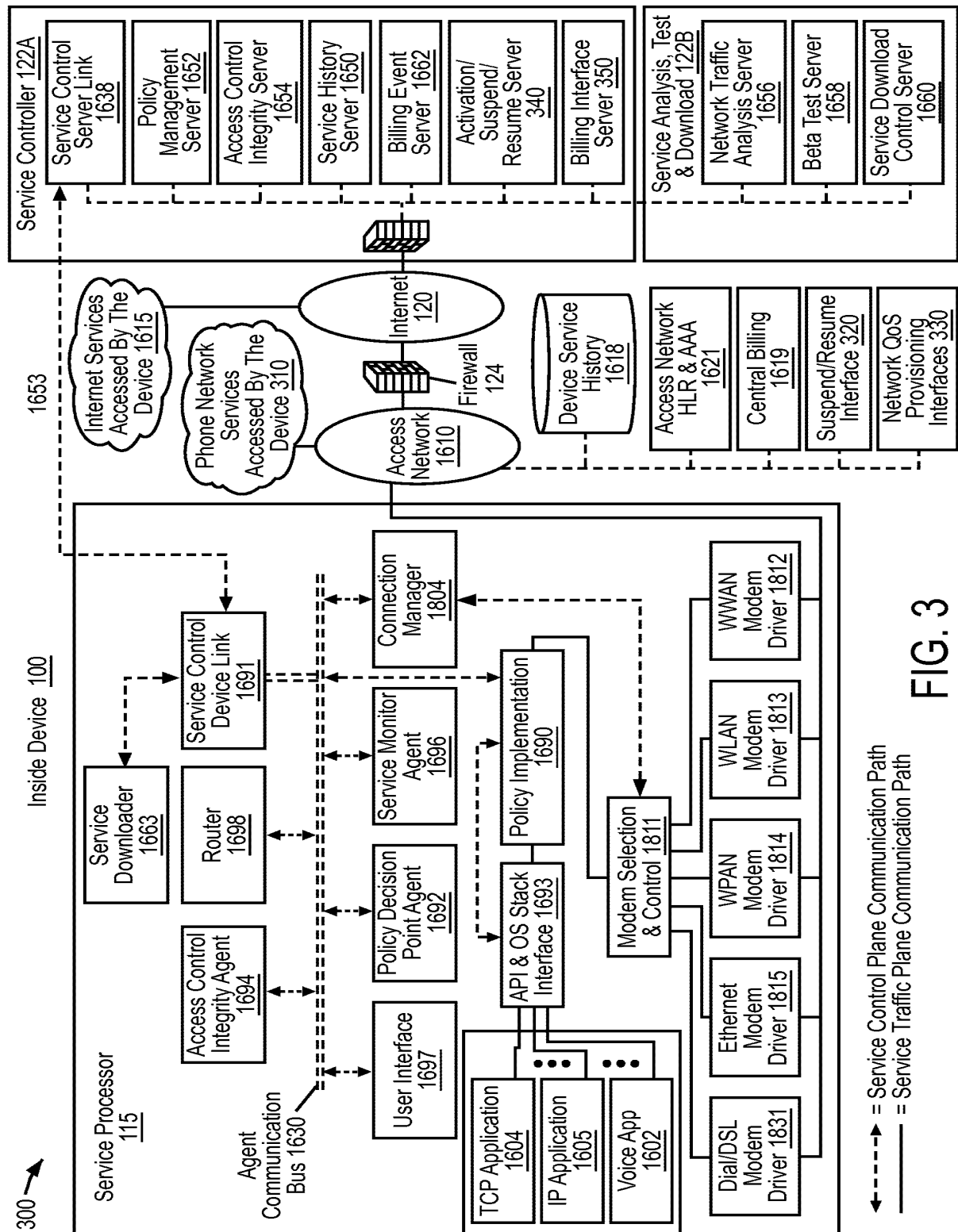


FIG. 2



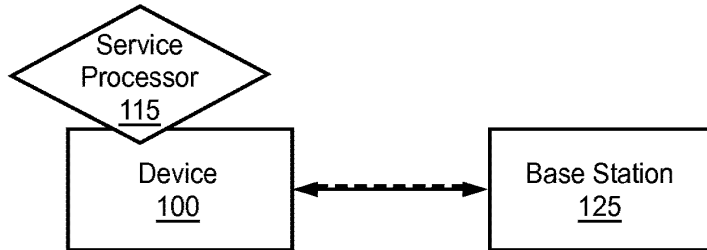


FIG. 4A

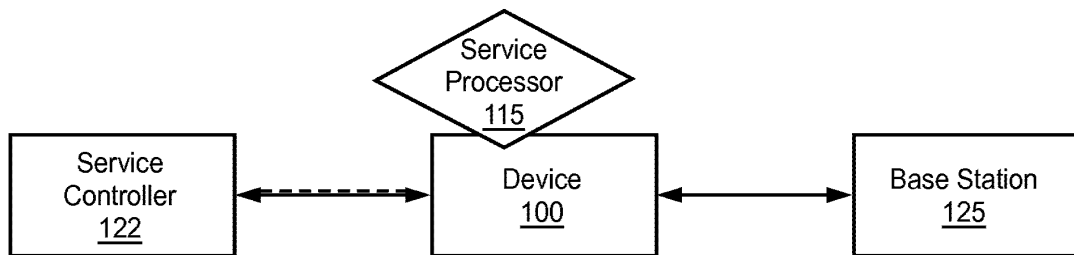


FIG. 4B

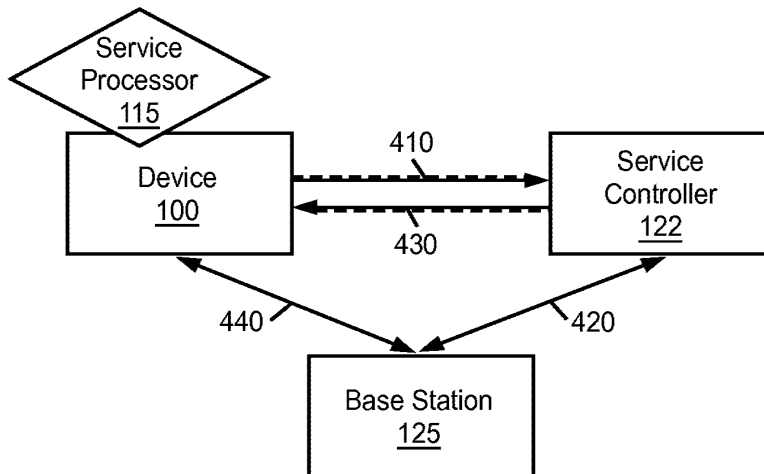


FIG. 4C

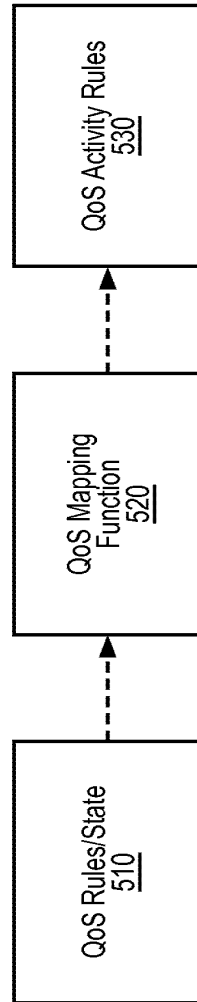


FIG. 5



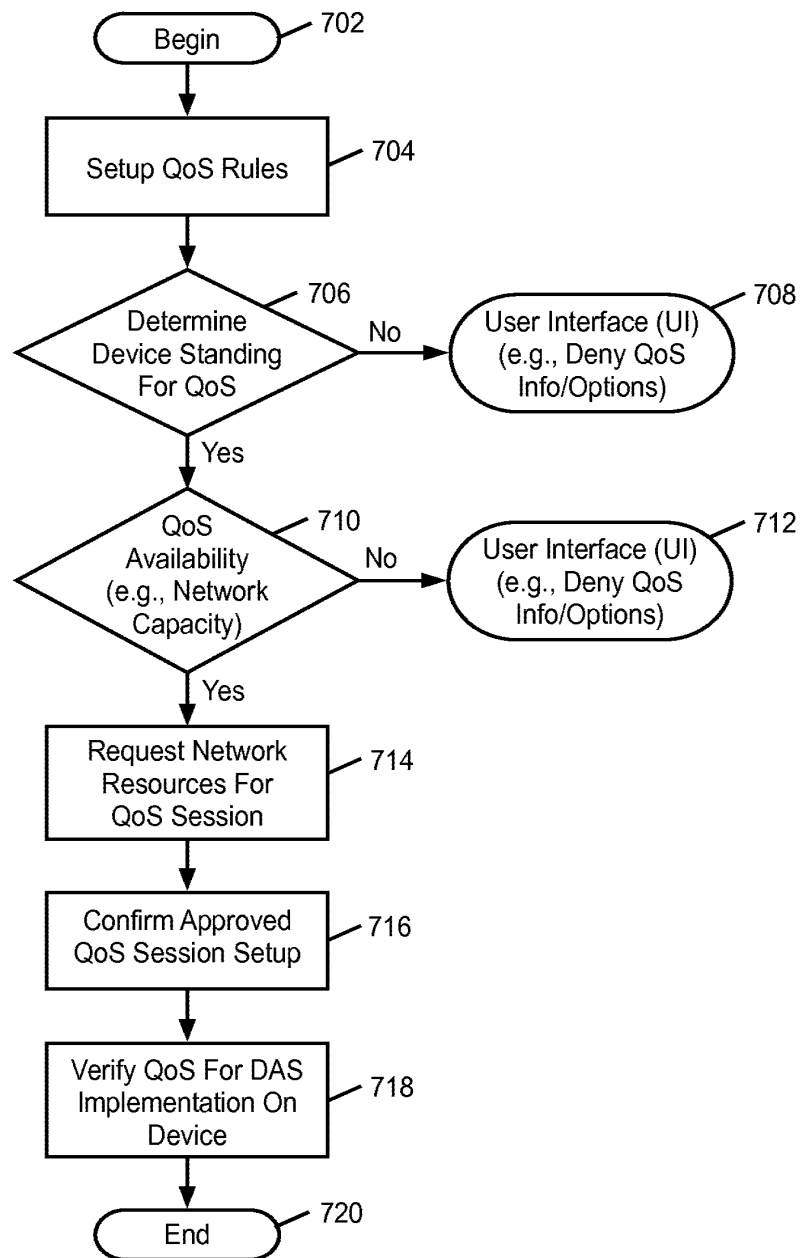


FIG. 7

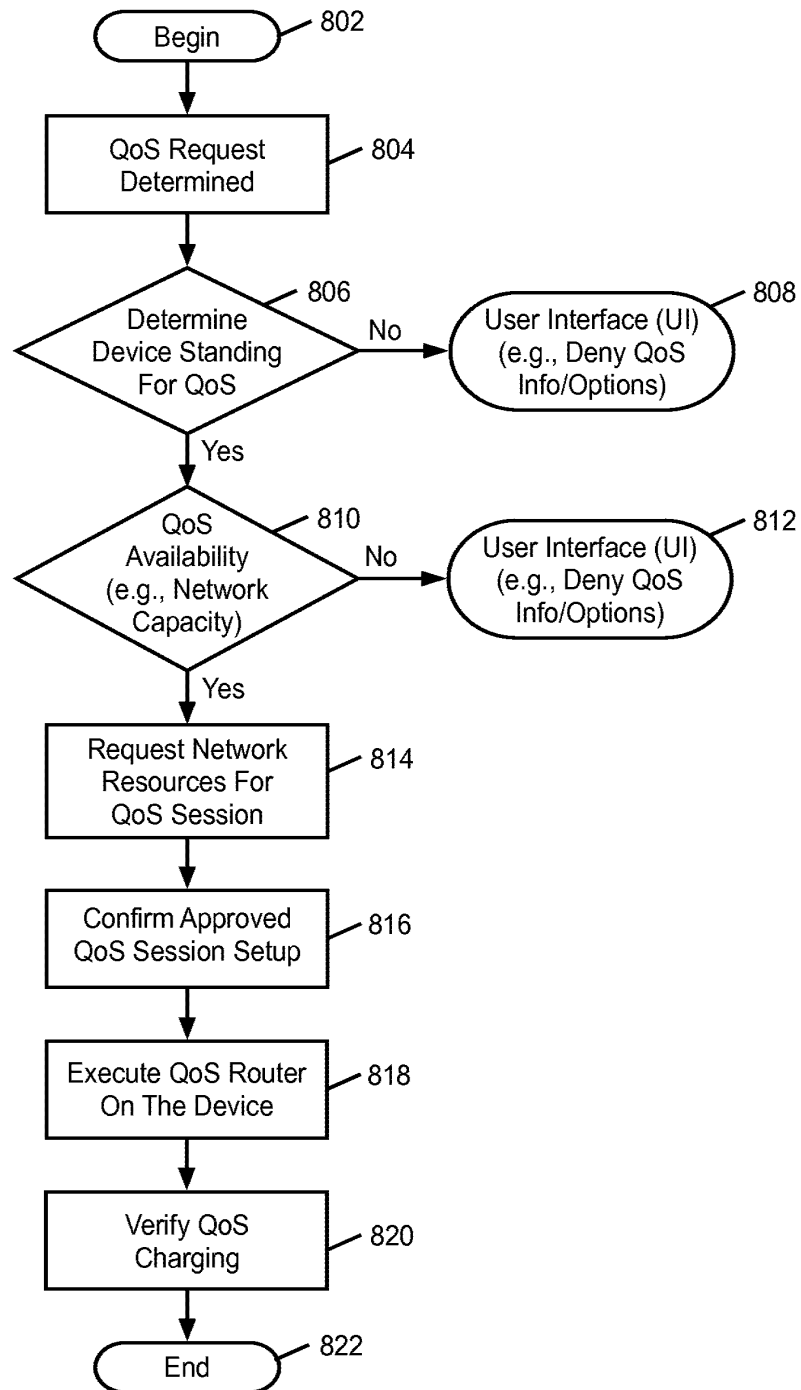


FIG. 8A

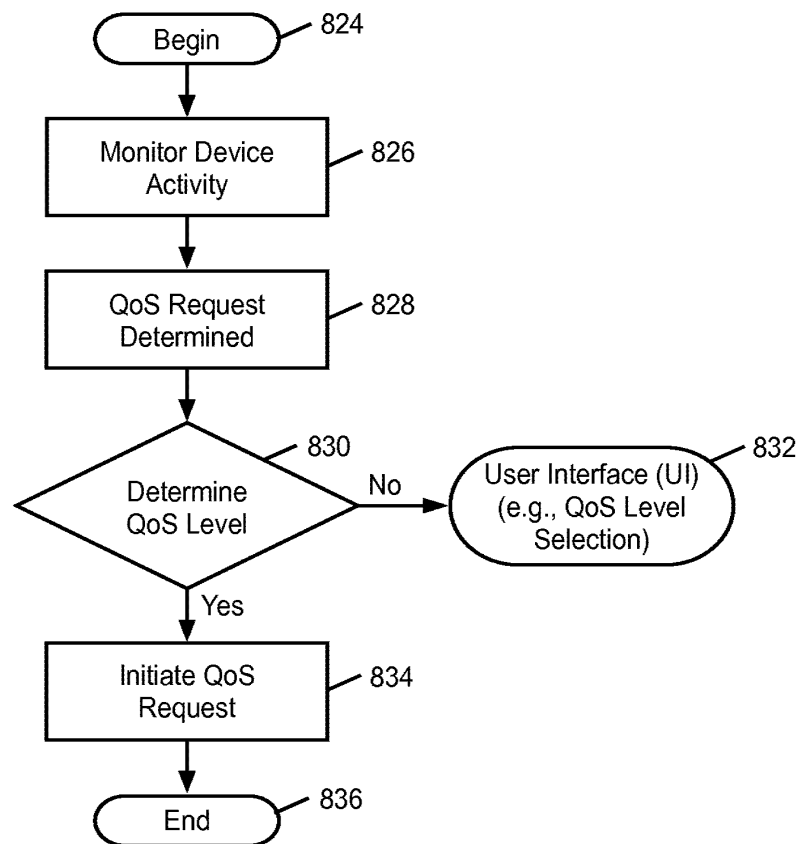


FIG. 8B

10/29

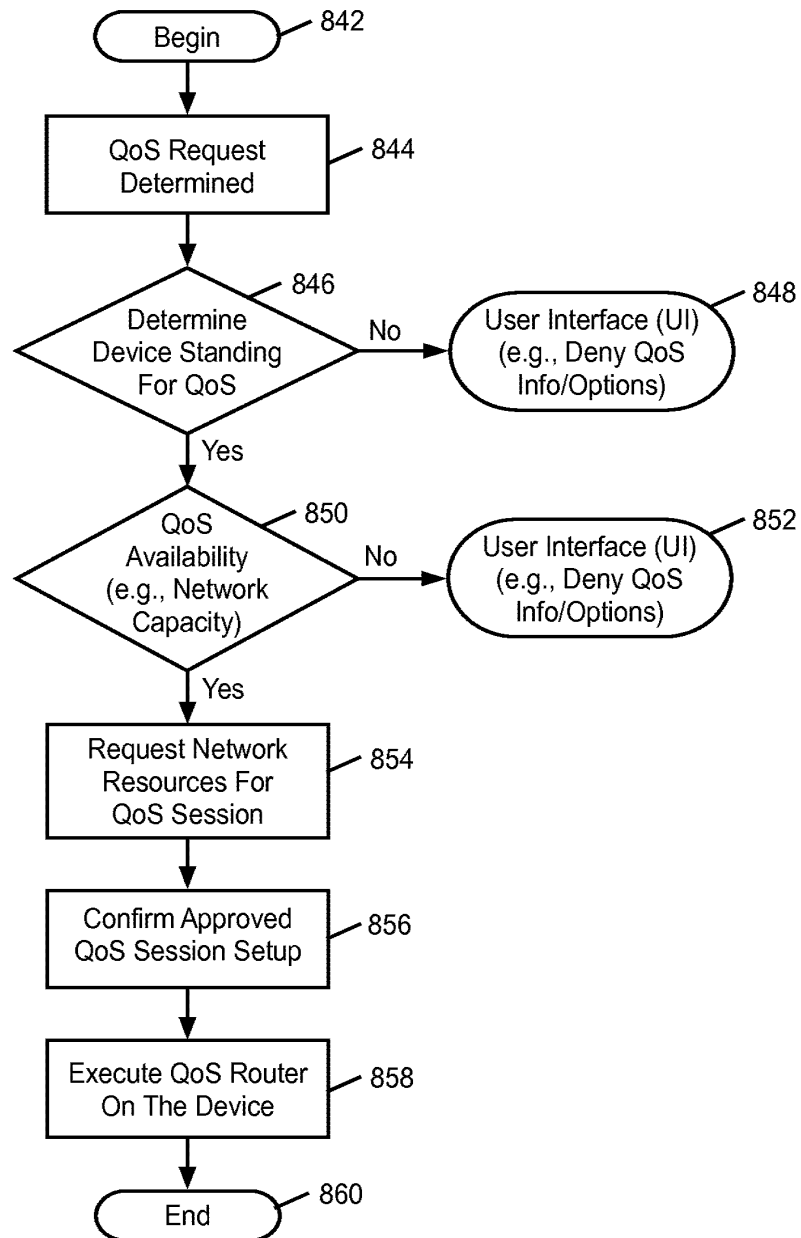


FIG. 8C

11/29

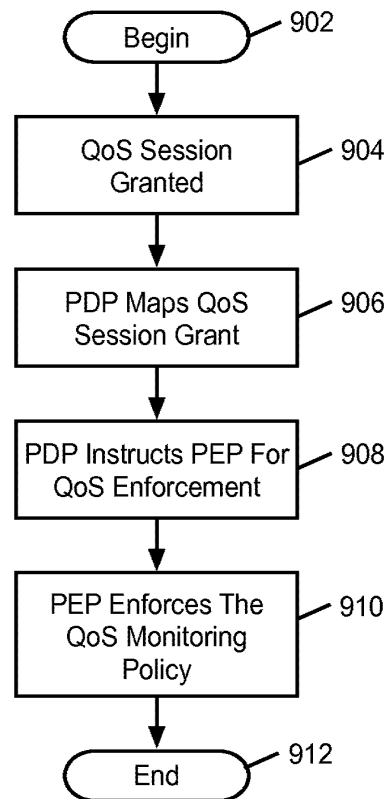


FIG. 9

12/29

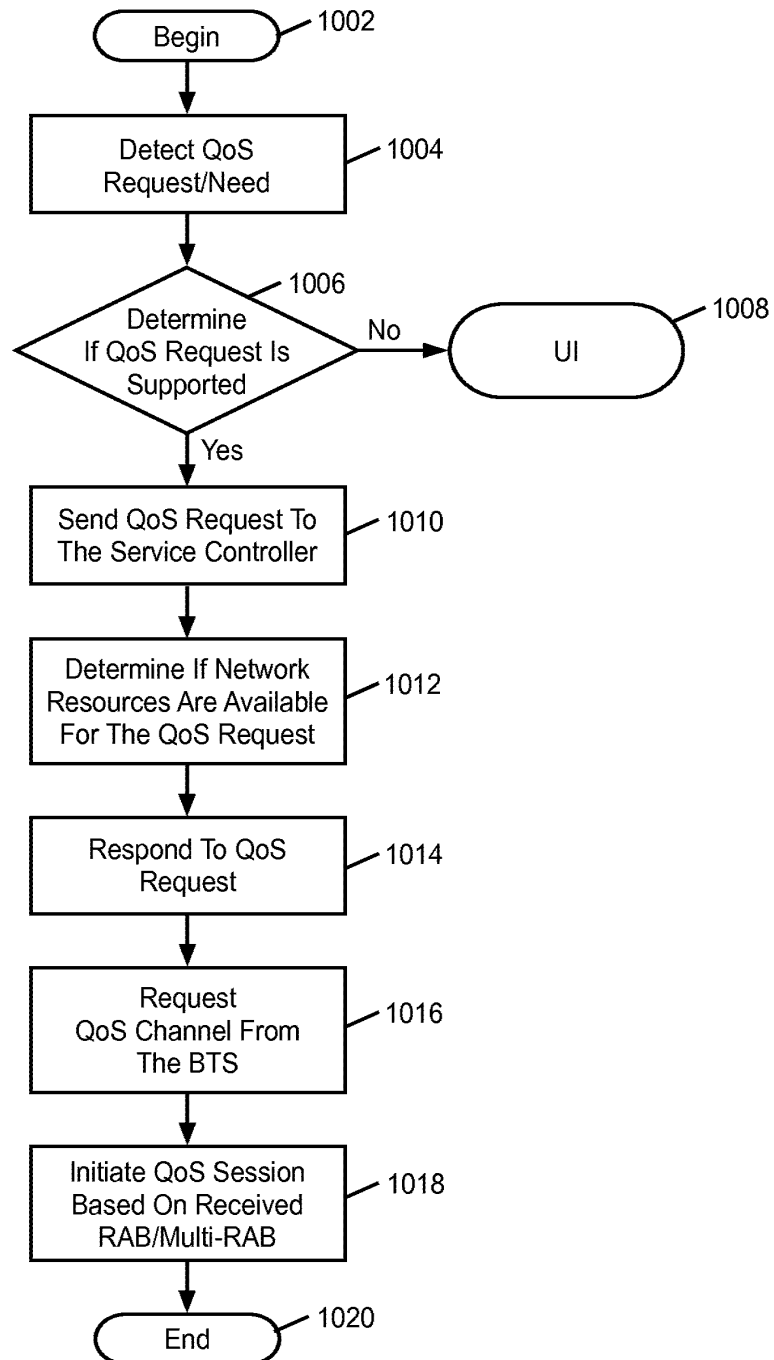


FIG. 10

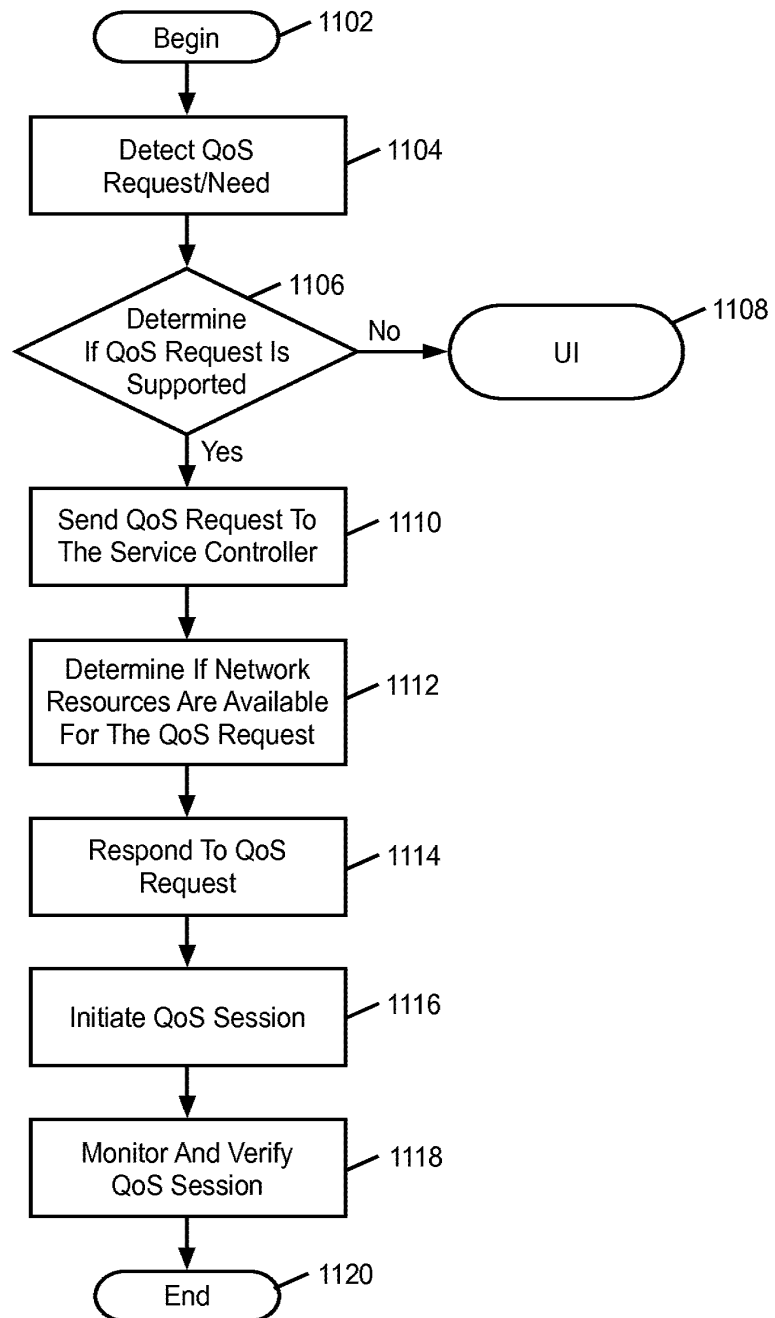
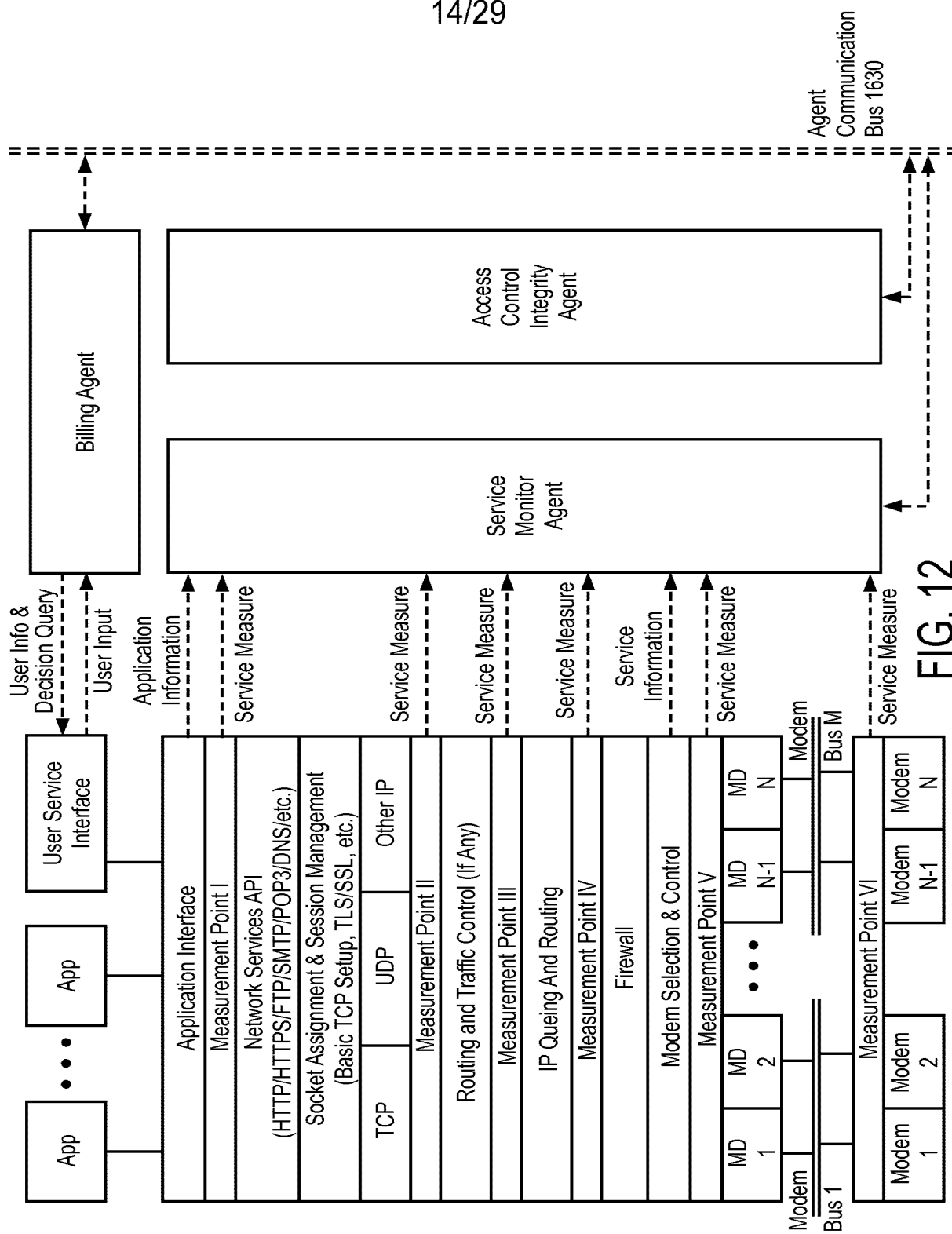


FIG. 11



15/29

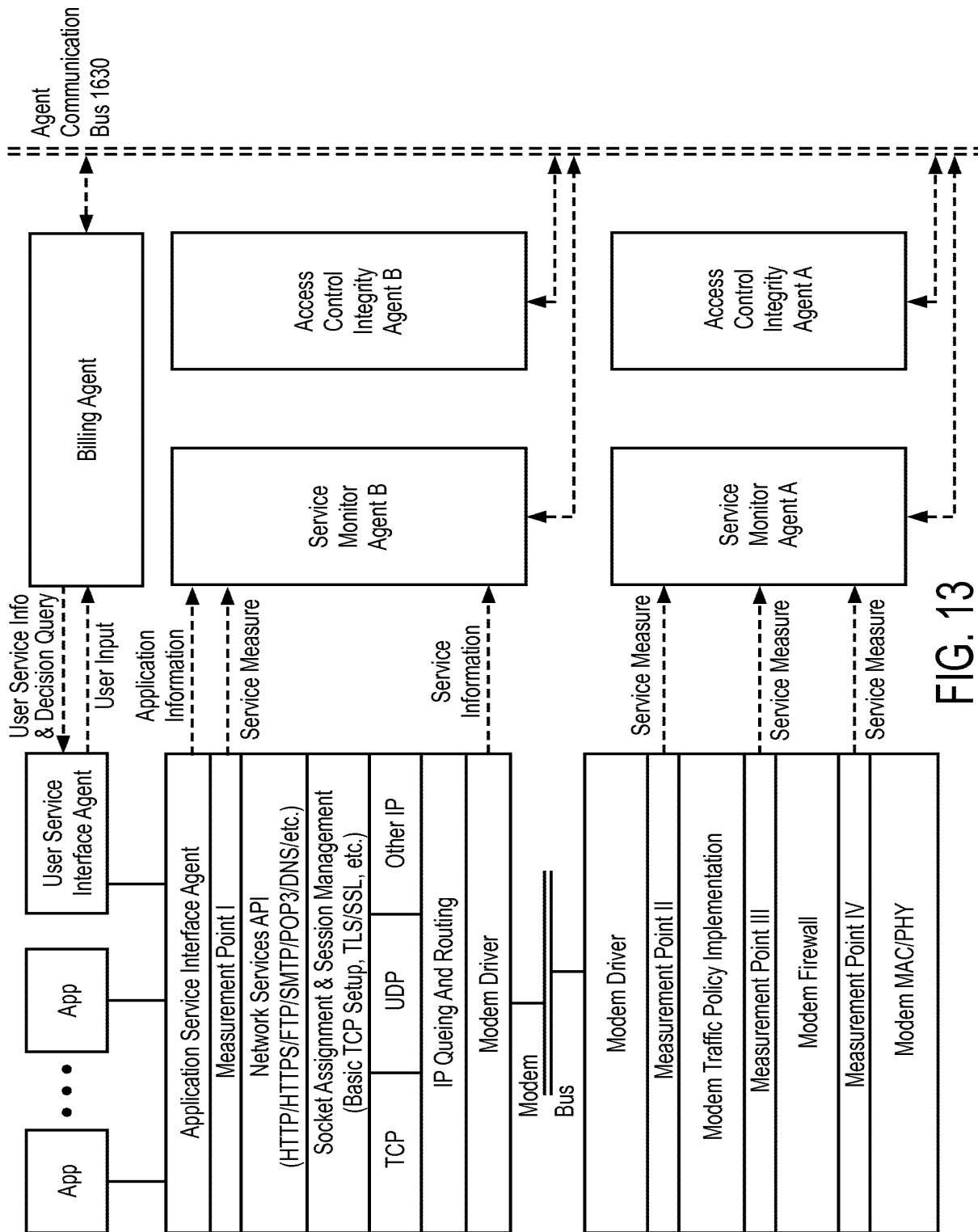


FIG. 13

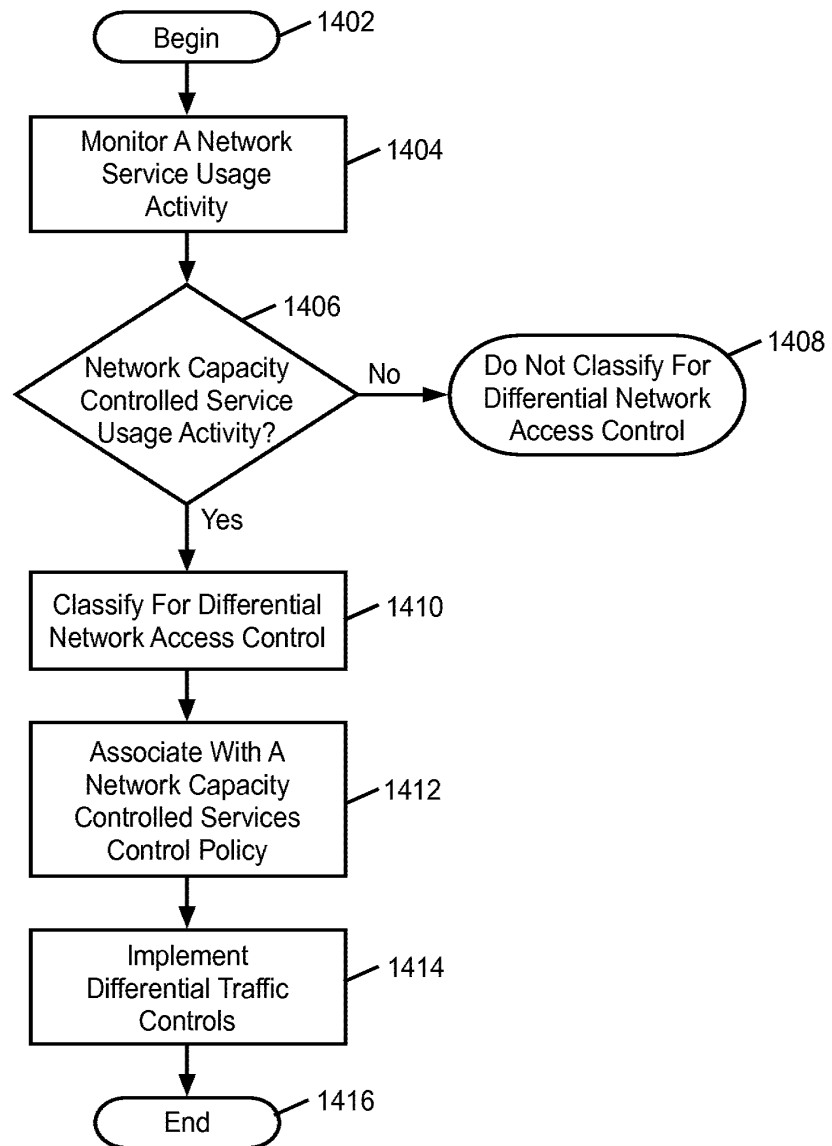


FIG. 14

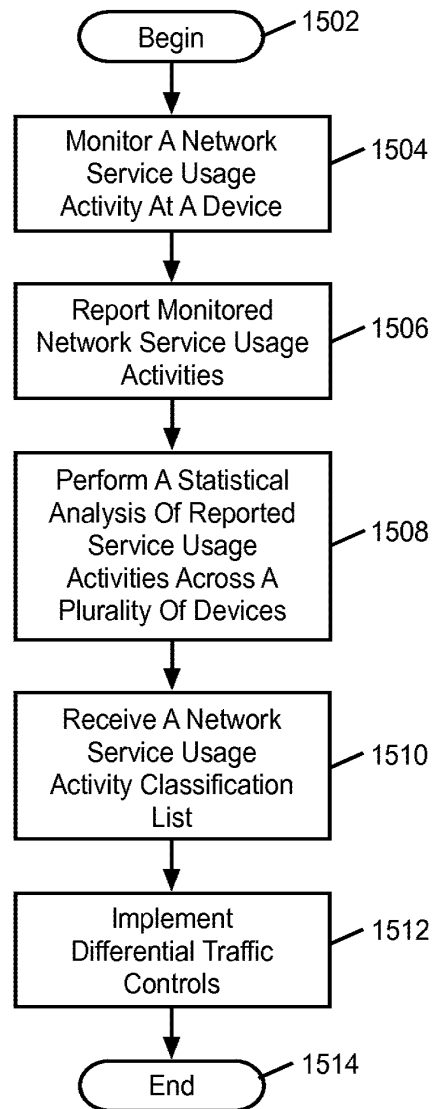


FIG. 15

18/29

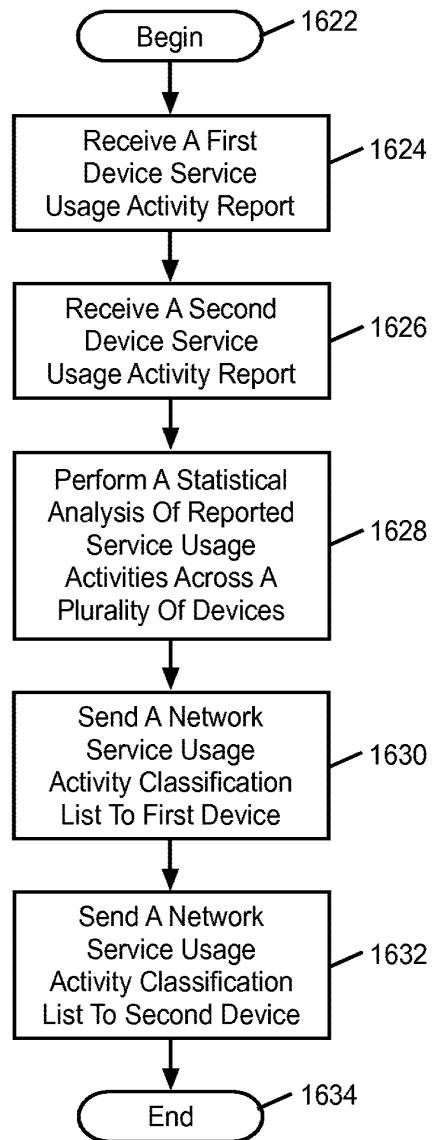


FIG. 16

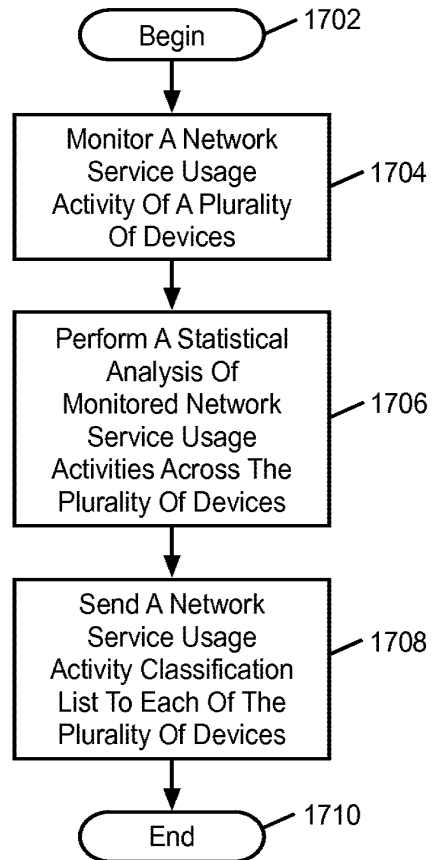


FIG. 17

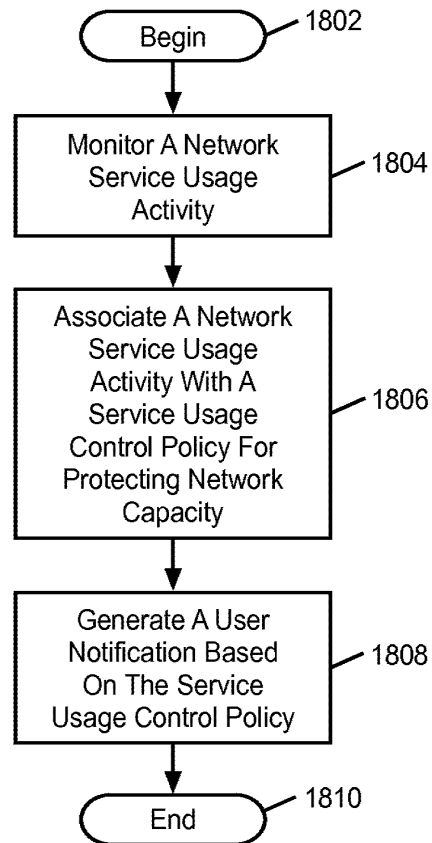


FIG. 18

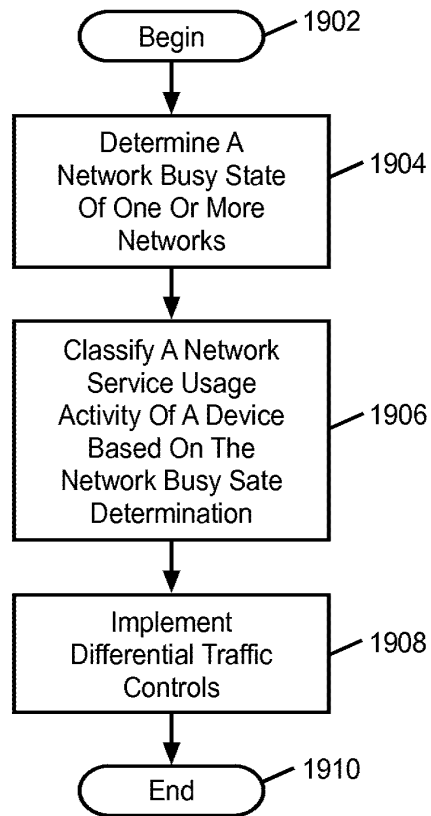


FIG. 19

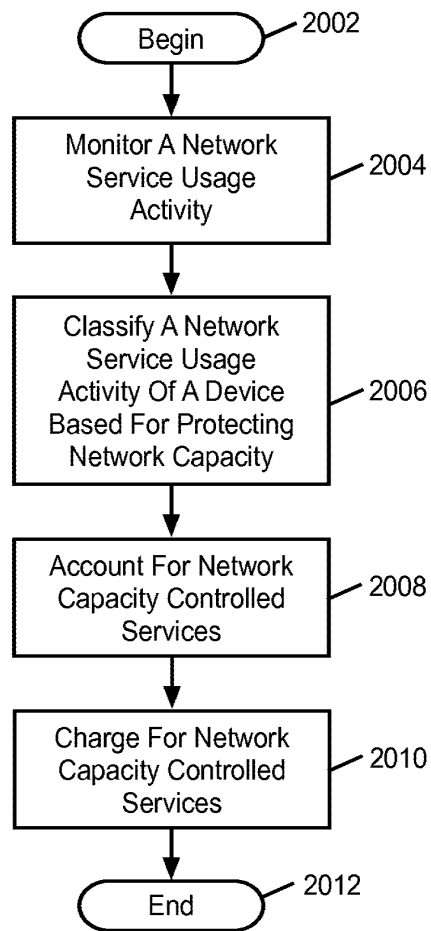


FIG. 20

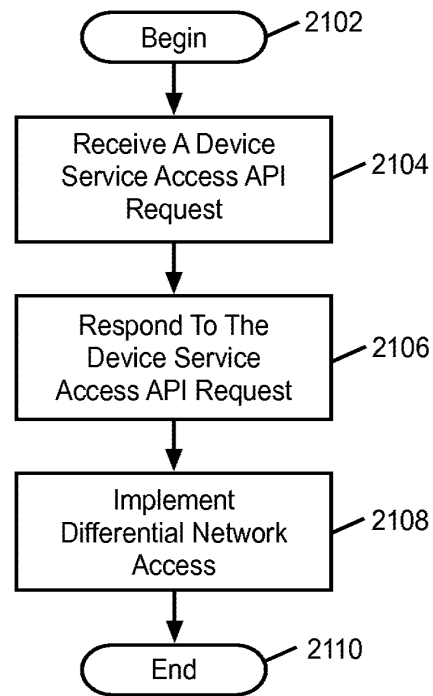


FIG. 21

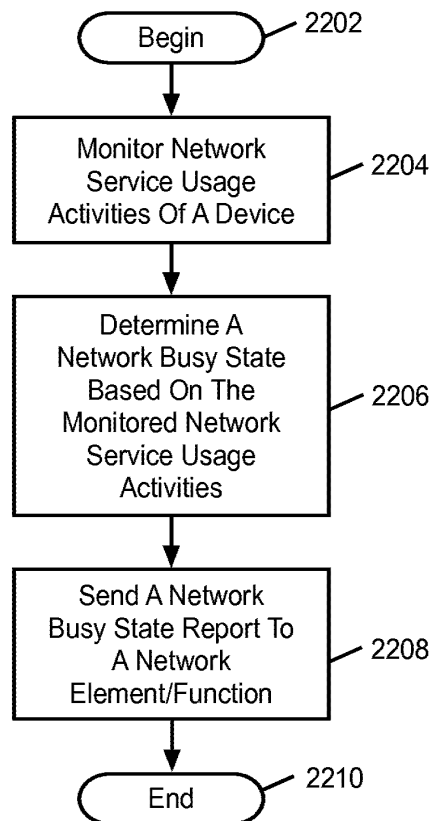
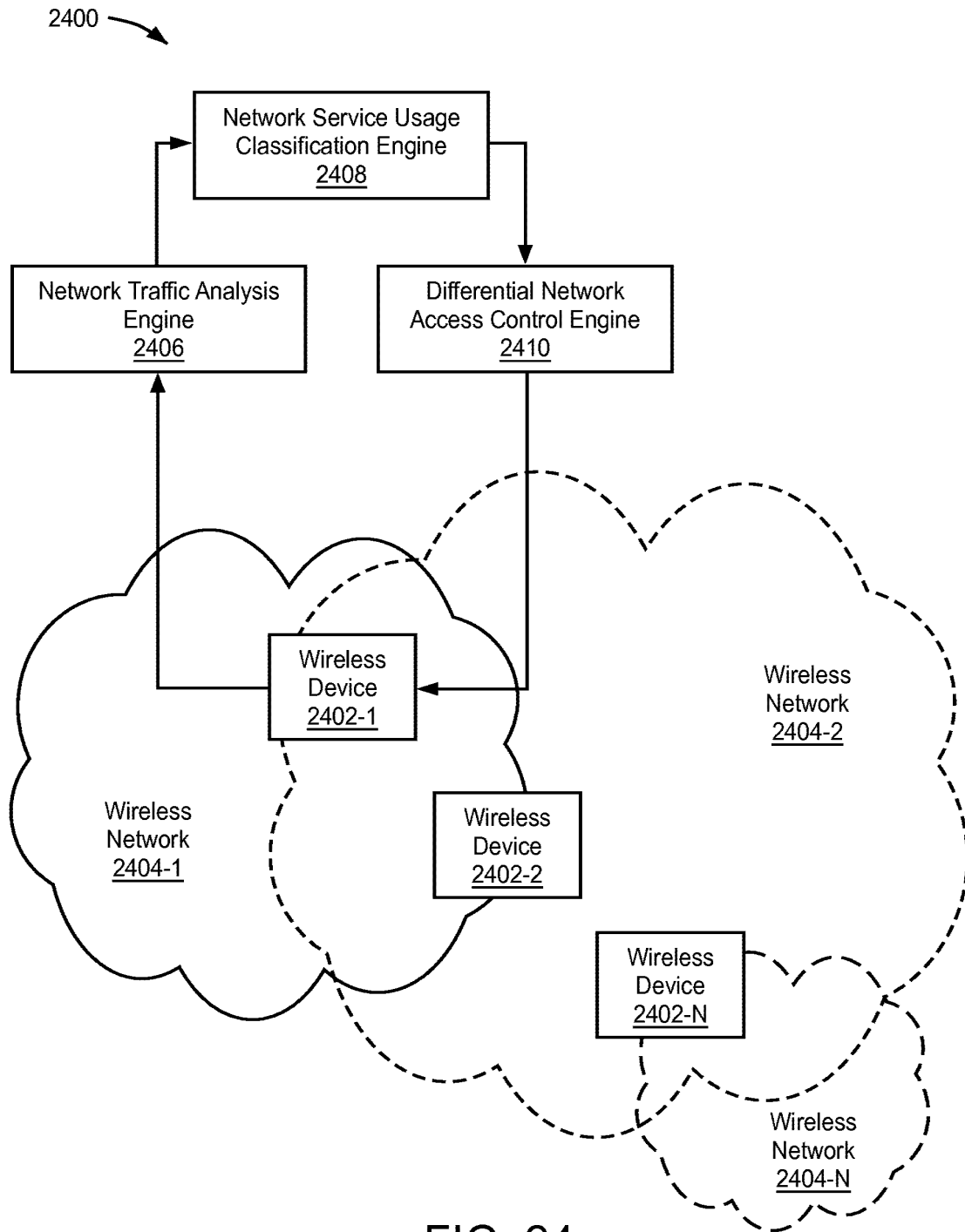


FIG. 22

	NBS 10%	NBS 25%	NBS 50%	NBS 75%	NBS 90%
Outlook	6	5	4	3	2
Skype	7	6	2	1	0
Safari	5	4	3	2	1
Pandora	5	4	3	2	1
FaceBook	4	3	2	1	0
iTunes	7	6	3	1	0
QuickTime	8	6	4	1	0
AV Software	9	7	5	3	1
Online Backup	3	2	1	1	0
OS Update	2	1	0	0	0

FIG. 23



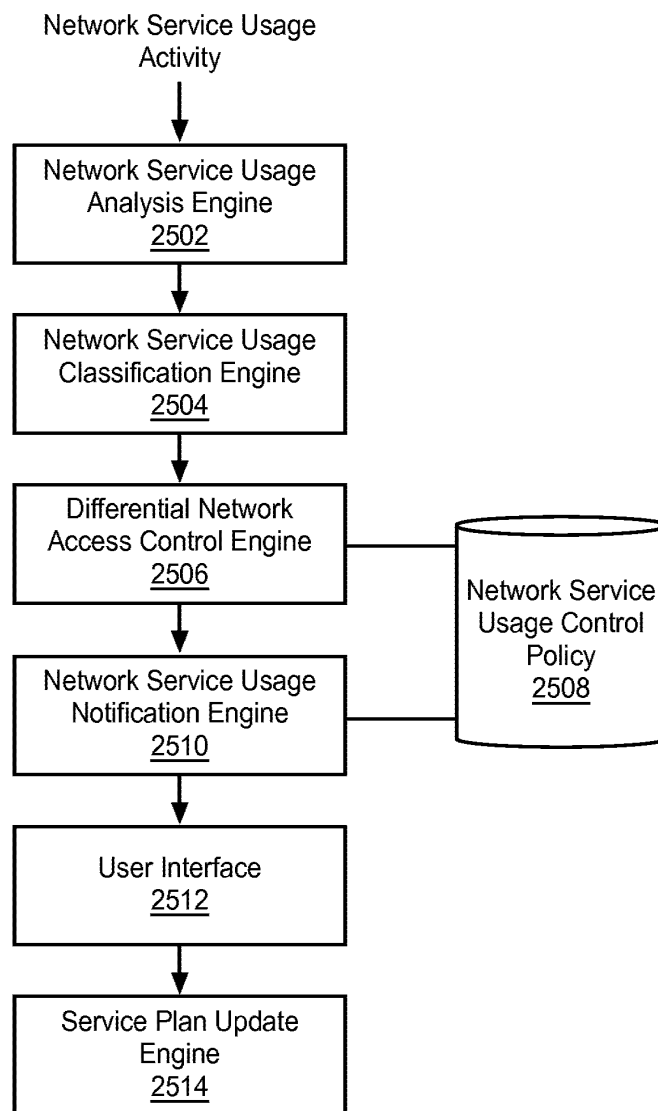
2500 

FIG. 25

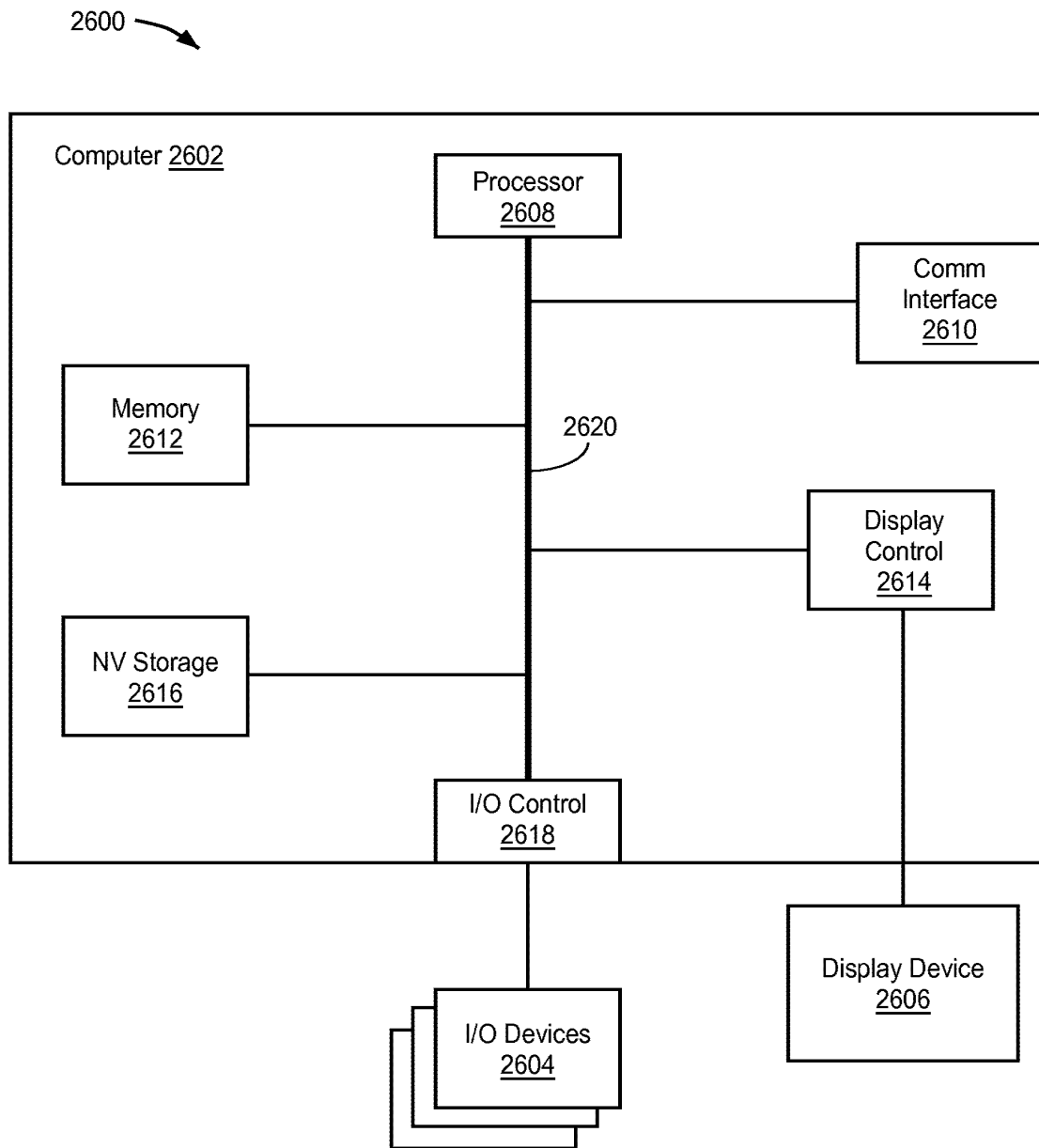


FIG. 26

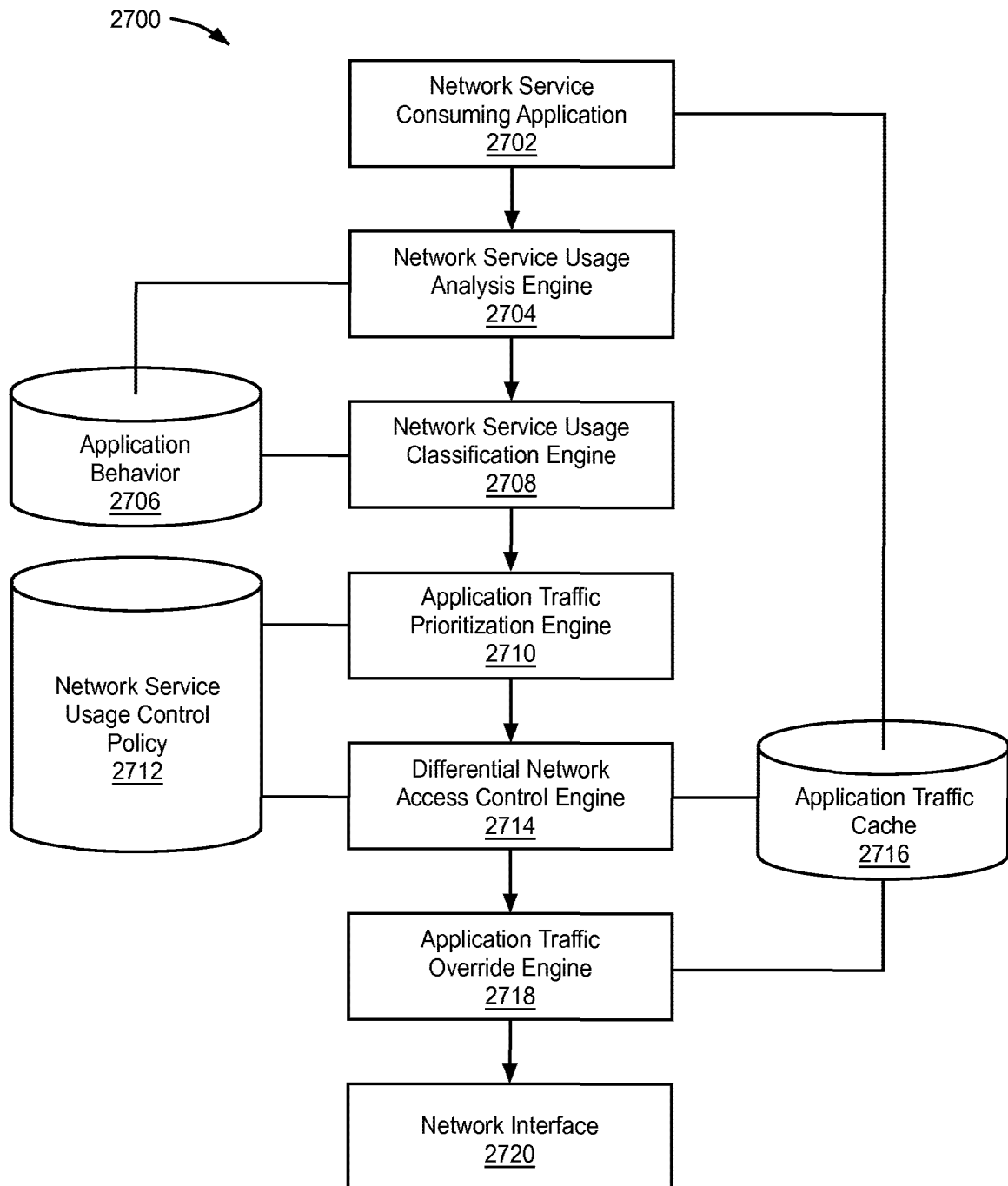


FIG. 27

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

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

Title of Invention	Device-Assisted Services for Protecting Network Capacity (RALEP032C1)
-------------------------------	---

As the below named inventor, I hereby declare that:

This declaration is directed to: ☒ The attached application, or
☐ United States application or PCT international application number _____
filed on _____

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

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

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

WARNING:

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

LEGAL NAME OF INVENTOR

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

Signature: 

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

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

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

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

Title of Invention	Device-Assisted Services for Protecting Network Capacity (RALEP032C1)
<p>As the below named inventor, I hereby declare that:</p> <p>This declaration is directed to: ☒ The attached application, or ☐ United States application or PCT international application number _____ filed on _____.</p> <p>The above-identified application was made or authorized to be made by me.</p> <p>I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.</p> <p>I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.</p> <p style="text-align: center;">WARNING:</p> <p>Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.</p>	
<p>LEGAL NAME OF INVENTOR</p> <p>Inventor: <u>James Lavine</u> Date (Optional): <u>11/11/13</u></p> <p>Signature: <u>[Signature]</u></p>	
<p><small>Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.</small></p>	

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

If you need assistance in completing the form, call 1-800-PTO-8199 and select option 2.

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

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

Title of Invention	Device-Assisted Services for Protecting Network Capacity (RALEP032C1)
-------------------------------	---

As the below named inventor, I hereby declare that:

This declaration is directed to: ☒ The attached application, or
☐ United States application or PCT international application number _____
filed on _____

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

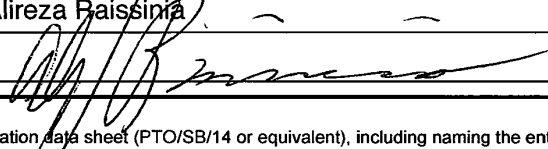
I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

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

WARNING:

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

LEGAL NAME OF INVENTOR

Inventor: Alireza Baissinia Date (Optional): 11/13/2013
Signature: 

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

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

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

Electronic Patent Application Fee Transmittal				
Application Number:				
Filing Date:				
Title of Invention:		Device-Assisted Services for Protecting Network Capacity		
First Named Inventor/Applicant Name:		Gregory G. Raleigh		
Filer:		James E. Harris/Ann Taylor		
Attorney Docket Number:		RALEP032C1C2		
Filed as Small Entity				
Filing Fees for Track I Prioritized Examination - Nonprovisional Application under 35 USC 111(a)				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Utility filing Fee (Electronic filing)	4011	1	70	70
Utility Search Fee	2111	1	300	300
Utility Examination Fee	2311	1	360	360
Request for Prioritized Examination	2817	1	2000	2000
Pages:				
Utility Appl Size fee per 50 sheets >100	2081	1	200	200
Claims:				
Miscellaneous-Filing:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Publ. Fee- Early, Voluntary, or Normal	1504	1	0	0
PROCESSING FEE, EXCEPT PROV. APPLS.	2830	1	70	70
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				3000

Electronic Acknowledgement Receipt	
EFS ID:	21921395
Application Number:	14673625
International Application Number:	
Confirmation Number:	9085
Title of Invention:	Device-Assisted Services for Protecting Network Capacity
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	James E. Harris/Ann Taylor
Filer Authorized By:	James E. Harris
Attorney Docket Number:	RALEP032C1C2
Receipt Date:	30-MAR-2015
Filing Date:	
Time Stamp:	19:34:34
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$ 3000
RAM confirmation Number	6532
Deposit Account	505876
Authorized User	
<p>The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:</p> <p>Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)</p> <p>Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)</p>	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)					
Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)					
Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)					
File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	TrackOne Request	P032C1C2_TrackOneRequest.pdf	139535 2f4773d9c30053fe72c5efa65436a67c70fb2b36	no	2
Warnings:					
Information:					
2	Application Data Sheet	P032C1C2_ADS.pdf	1563020 fa72727fbfe3c20924a6893ccd0cc5cfd71649ae	no	11
Warnings:					
Information:					
3		P032C1C2_Spec.pdf	712416 2fb0d19f5dc1d5c3001f3e4a0e4f967045081f3	yes	154
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Specification		1	152	
	Claims		153	153	
	Abstract		154	154	
Warnings:					
Information:					
4	Drawings-only black and white line drawings	P032C1C2_Drawings.PDF	150761 ac7246ee5ca09e393b3f612f53effe5b049e98b2	no	29
Warnings:					
Information:					
5	Oath or Declaration filed	P032C1C2_RaleighDecl.pdf	63907 c6a50cad9c7a434f4f78f93ab5a1e92a8474542f	no	1
Warnings:					
Information:					
6	Oath or Declaration filed	P032C1C2_LavineDecl.pdf	276545 36ee0f95bf0cdc129378ac847054b11d3d11d866	no	2

Warnings:					
Information:					
7	Oath or Declaration filed	P032C1C2_RaissiniaDecl.pdf	65020 52dd45edafeb4a71acd6368bc129cf6e798b60ea	no	1
Warnings:					
Information:					
8	Fee Worksheet (SB06)	fee-info.pdf	41971 454ac21ca79b6901a0ae361ea1e81d840abb505a2	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			3013175		
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>					